Albert-Ludwigs-Universität Freiburg
Wirtschafts- und Verhaltenswissenschaftliche Fakultät

Transparency through Decentralized Consensus: The Bitcoin Blockchain and Beyond

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der Wirtschafts- und Verhaltenswissenschaftlichen Fakultät

an der Albert-Ludwigs-Universität Freiburg i. Br.

Vorgelegt von

Christian Brenig

Geboren in Bonn-Duisdorf

WS 2016/17

Albert-Ludwigs-Universität Freiburg im Breisgau

Wirtschafts- und Verhaltenswissenschaftliche Fakultät

Kollegiengebäude II

Platz der Alten Synagoge

Dekan:	Prof. Dr. Alexander Renkl
Erstgutachter:	Prof. Dr. Dr. h.c. Günter Müller
Zweitgutachter:	Prof. Dr. Dieter K. Tscheulin

Datum der Einreichung:	28.11.2016
Datum des Promotionsbeschlusses:	16.01.2017

Acknowledgements

In the course of developing this doctoral thesis and during my doctorate, I have enjoyed the continuous support of a great number of people I would like to express my sincere gratitude.

First and foremost, I want to express my deep gratitude to my doctoral supervisior Prof. Dr. Dr. h.c. Günter Müller for his mentorship and support over the past couple of years. I am very thankful for his open-minded attitude towards me, which led to many interesting and insightful discussions even beyond purely professional interests. I do not want to miss his advices and recommendations, which were extremely valuable to my professional as well as personal development and of great help in writing this dissertation. Overall, I could not have picked a better environment for this important stage of my life, because I always felt to be trusted and was granted the academic freedom to pursue the objectives I was interested in. I would further like to thank the people at SBA Research, for offering me the opportunity to participate on the BITCRIME project and for funding parts of my research. I would like to explicitly point out Dr. Thomas Neubauer and Dr. Stefan Fenz in this respect. I would further like to express my gratitude towards Prof. Dr. Dieter K. Tscheulin for accepting the task of the second reviewer for the dissertation at hand and as examiner in my Rigorosum. Additionally, I would like to thank Prof. Dr. Günter Knieps for his role as examiner in the Rigorosum.

I would also like to mention my colleagues and friends at the Institute of Computer Science and Social Studies in Freiburg. Primarily, I want to thank Prof. Dr. Jens Strüker and Dr. Thomas Koslowski, who have introduced me to the field of academic research and gave me the opportunity to work on my first research contributions. Furthermore, I express my sincere appreciation to Dr. Rafael Accorsi for his encouragement and the fruitful discussions especially in the early stage of my doctorate. A special thanks goes to Dr. Christian Zimmermann for his continuous support in work-related topics and the many memorable experiences we have had outside the office. I further thank Anja Jülch for the time she spent in helping me with administrative issues. I want to thank my fellow colleagues Adrian, Arnt, Claus, Julius, Markus, Nadine and Thomas for their efforts to support me during the time I worked at the Institute. In particular, I would like to express my sincere gratitude to Richard, who often challenged and inspired me with his perspective on different issues. I am glad that I got the opportunity to get to know such a good friend on the job. Finally, I would like to point out Jonas for his ongoing support in every conceivable professional and private aspect of my life during the past years in

Freiburg. I really appreciate his commitment to my research and the countless times we spent together on our common interests. Overall, I could not have had better colleagues to work with.

Last but not least, I want to express my deepest gratitude towards my family. All this would not have been possible without the unconditional support of my parents throughout my whole life. I would like to especially thank them for all the possibilities they offered me and their encouragement in writing this thesis.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AML	Anti-Money Laundering
ASIC	Application-Specific Integrated Circuit
ATM	Automated Teller Machine
BTC	Bitcoins (The Token)
DAO	Decentralized Autonomous Organizations
DCS	Distributed Consensus System
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
ECB	European Central Bank
EPS	Electronic Payment System
FATI	Financial Asset Trading Infrastructure
FINCEN	Financial Crime Enforcement Network
GORE	Goal-Based Requirements Engineering
IOT	Internet of Things
IOU	I Owe You
IS	Information Systems
IT	Information Technology
LR	Liberty Reserve Virtual Currency

ML	Money Laundering
MSP	Multi-Sided Platform
P2P	Peer-to-Peer
POS	Proof-of-Stake
POW	Proof-of-Work
RAM	Random-Access Memory
RE	Requirements Engineering
RQ	Research Question

1 Hype and Promises of Decentralized Consensus Systems

The technology behind distributed ledgers, which are shared and continuously updated registers replicated across multiple nodes on the Internet or private networks, has been receiving a lot of attention recently. In particular, it is discussed as an enabler for systems facilitating a decentralized consensus between different entities on a set of acceptable transactions. This deliberately general formulation reflects the wide range of applications, where so-called Decentralized Consensus Systems (DCSs) are envisaged to potentially reshape digital interactions. Their design is inspired by and can be based on a blockchain like it was originally introduced with the decentralized payment system Bitcoin in 2009. Soon the idea arose to utilize the technology as infrastructure for different kinds of scenarios besides payments. Meanwhile DCSs are increasingly discussed for applications involving the invention, registration and transfer of all kinds of digital assets (Franco, 2015; Vigna and Casey, 2015). Examples could be of intangible nature such as shares, bonds or emission rights, but also physical objects like cars or houses (European Banking Authority, 2015; Al Kawasmi *et al.*, 2015). The reason for this attention is that DCSs enable cryptographically secured transactions according to rules concretely specified in their respective protocols and programmable applications. They are organized in a decentralized fashion and ensure that solely transactions in conformance with these rules are processed. Additionally, transparency is established by an accessible distributed ledger storing valid transactions. As a consequence, DCSs may become a disruptive technology and imply a fundamental shift in how societies are organized.

Bob Greifeld, the NASDAQ CEO, sees systems driven by distributed ledgers as “the biggest opportunity set we can think of over the next decade” (Shin, 2015). A survey conducted by the World Economic Forum expects 10 percent of the global gross domestic product to be stored on distributed ledgers in the near future (World Economic Forum, 2015). In a recent report providing an in-depth analysis of case studies across nine sectors of financial services, the same foundation acknowledges distributed ledgers as “one of many technologies that will form the foundation of next generation financial services infrastructure” (World Economic Forum, 2016,

p. 18). The bank Santander gets even more concrete and assumes that financial institutions using the technology will be able to reduce their infrastructure costs by up to 20 billion US-Dollar per year. (Santander, 2015).

But there are also rather skeptical voices who question the economic and societal impact of DCSs and consider them as excessively hyped up. The distributed ledger concept and the associated technologies are exposed “to become one of those almost generic chromewash terms, like, 'big data' or 'cloud'” as David Birch, director of Consult Hyperion, predicts (Finextra, 2016). Consistent with this statement, the American bank BNY Mellon just had to discontinue a distributed ledger project, as it was not able to enthuse enough participants (the Economist 2016). Adi Shamir, one of the inventors of the RSA algorithm, published the statement that he was “yet to see a use-case […] that can't be solved with an existing simpler technology” (GluuFederation, 2016). This interpretation clarifies that the decision of implementing a new technological development always involves a trade-off between benefits and costs. While a system based on a distributed ledger may be a technically feasible solution, it is not necessarily the most practicable approach to implement a DCS for every conceivable use case.

The statements above reflect the wide range of different opinions and expectations regarding the potentials of DCSs, ranging from enthusiasm in view of the opportunities promised by systems providing complete transparency of transactions, to more sceptic views concerning the novelty and feasibility of the suggested concepts. In face of this diverging perceptions and uncertain future prospects, a number of issues can be derived that need to be discussed. It is apparent that use cases where such systems could provide utility and improve on existing or enable novel business models are still a topic of controversy. Therefore, any analysis dealing with DCSs has to account for the lack of clearly formulated problems, for which these systems may offer a practical solution. In connection with this observation, challenges arise in identifying the corresponding functionalities and mechanisms required by DCSs to support applications in various industries and scenarios. Furthermore, the concrete technical realization of these systems is still subject to debates, since actual implementations corresponding to the formulated visions have not been deployed on a larger scale yet. Tackling the issues described above, the present dissertation intends to shed light on what DCSs are able to achieve as novel means for digital interaction and what they are not. In particular, it concerns itself with the economic benefits that can be realized by utilizing DCSs. Therefore, the concept of decentralized consensus is introduced and its potential effects on the digital transformation of societies are sketched out as a first step.

1.1 Digital Transformation Facilitated by Decentralized Consensus

The development and diffusion of digital technologies already transforms the processes of entire industries and provides the foundation for completely new business models based on the digitization of information (Brynjolfsson and McAfee, 2014). The societal implications of this development are subsumed under the term digital transformation and result in an environment that is increasingly dependent on socially embedded IT systems affecting our everyday lives (Stolterman and Fors, 2004). In the electricity industry, for instance, the ongoing deployment of advanced metering infrastructures enables demand response applications to intelligently control consumers' electricity demand (Borenstein *et al.*, 2002). Digital ecosystems emerge around platforms such as Facebook, Google, Amazon or Alibaba as catalysts for business models in technology-enabled and interconnected environments (El Sawy and Pereira, 2013). Simultaneously, the omnipresence of mobile devices like smartphones, tablets or smartwatches allows for ubiquitous access to services offered by means of digital ecosystems. The corresponding network economy is characterized by distributed service environments exhibiting network effects, where data collection, processing and analysis constitutes a core component of business activities (Shapiro and Varian, 1999). As the Internet is firmly embedded and strongly interlinked with the real world and the boundaries between the traditional and information society have become increasingly blurry. For this reason, not only business models and value chains are more and more reliant on the rules governing digital infrastructures, but generally all kinds of interactions involving the creation, use and distribution of information (Castells, 2000).

Prevailing online services, however, rely on centralized service providers mediating any form of digital interaction. These intermediaries on the one hand reduce uncertainties in digital environments and ensure that online transactions are even taking place, but on the other hand need to be trusted to act in the interest of their users (Kim *et al.*, 2004). Thereby, transaction costs occur due to expenditures for delegation, inducing new inefficiencies in the transaction process (Sumanjeet, 2009). It is important to note that every interaction in digital environments involving the exchange of information can be understood as transaction between at least two entities on its most atomic level (e.g. IBM, 2015; Pranata *et al.*, 2012). DCSs promise a paradigm shift, removing conventional intermediaries in online transactions with a distributed ledger maintained through a decentralized consensus (e.g. Böhme *et al.*, 2015; Brenig *et al.*, 2016). Consensus is established by a peer-to-peer (P2P) network, whose participants are jointly responsible for maintaining the distributed ledger in order to avoid any centralized control. The term consensus in this respect refers to a collective decision-process, where the individual participants each compute their own version of the ledger, provide it to the rest of the network and finally agree on a commonly accepted state. This state includes all transactions validated by the network. The actual procedure of agreeing on the commonly accepted state is called consensus process, which is enabled by DCSs through a technical consensus mechanism. Such a system stands in stark contrast to centralized solutions employed in today's online services, where analogously a central intermediary determines the set of correct transactions. In the social network Facebook, for instance, it is the eponymous provider that determines the rules for interaction between its users and controls the respective user data. Utilizing DCSs consequently may substitute for the trust required in currently employed solutions and significantly reduce transaction costs of business models in digital environments. However, the implementation of such a decentralized paradigm, challenging established business models and operations, does not only provide opportunities, but is also associated with risks.

1.2 Cryptocurrencies: Opportunities & Money Laundering Risk

The Bitcoin system serves as an exemplary use case to illustrate the disruptive potential and risks associated with DCSs in the payments industry. As the first implementation of a DCS, it has already been running for several years and constitutes the role model for all subsequent realizations (Nakamoto, 2008). Therefore, it is particularly suited to study the effects of DCSs on an industry, where services are traditionally characterized by proprietary, complex solutions based on financial networks comprised of various intermediaries. Bitcoin implements its own exchange medium, bitcoin, which circulates independently of any central issued fiat currency like Euro or US-Dollar (Yermack, 2013). For that reason, the Bitcoin system is often referred to as virtual currency or cryptocurrency. In the Bitcoin system, the consensus is established regarding which transfers of bitcoin are valid and hence included in the distributed ledger called blockchain (Glaser and Bezzenberg, 2015). It is thereby possible to avoid any financial intermediaries. Since the introduction of Bitcoin, a plethora of similar currencies based on design principles (e.g. Litecoin, Ripple) appeared. This is because these cryptocurrencies can offer many benefits for honest individuals. They, for example, provide low transaction costs, may ensure privacy in online transactions or even act as a substitute for bank accounts in countries with immature financial systems.

In contrast, features such as decentralization and perceived transaction anonymity attracted the interest of criminal structures in adopting cryptocurrencies as financial instrument to conduct illegal activities including Money Laundering (ML). Profits resulting from illegal activities committed by criminal networks such as drug or human trafficking, smuggling and illicit gambling pose a serious threat to economic systems as well as public safety. ML describes the process by which the illegal sources of profits are disguised to obscure the link between the funds and the original criminal activity (International Monetary Fund, 2014). The emergence of complex financial instruments and global networking through technical developments and increased use of the Internet offers hitherto unknown pathways to conduct ML (European Central Bank, 2012). As a result, there is a tendency of criminals to abuse information and communication technology and virtual environments, which has become problematic for law enforcement in this context (McCusker, 2007; Stokes, 2012). The FBI recognizes the increasing attractiveness for criminals who avoid traditional financial systems to conduct global monetary transfers and motivates it with "difficulties detecting suspicious activity, identifying users, and obtaining transaction records" (FBI, 2012, p. 1). Prominent incidents like the case of a group of Dutch, who got arrested for laundering around 20 million Euros acquired from drug deals using Bitcoin, emphasize the severity of the ML risk related to cryptocurrencies (Reuters, 2016).

The above-described threat of DCSs to be misused for ML has distortive effects on the economy. Laundered money is normally untaxed, which means that the whole society ultimately has to bear the consequences of the loss in tax revenue. Legitimate businesses are also negatively affected, because they have competitors whose main objective is not the generation of profits. Instead the purpose of this competing businesses is laundering funds, which is why they even might sell a good or service below costs. Especially developing countries are exposed to be exploited for ML, resulting in economic distortions and political instability (Aluko and Bagheri, 2012; McDowell and Novis, 2001). Therefore, it is necessary to elaborate on the suitability of DCSs for criminal activities in the course of investigating their use for payments. Even though their wider dissemination in the context of payment services may be prevented by the emerging risks, DCSs could reshape other information-based industries where the invention, registration and transfer of assets constitutes the core of business activities far beyond payment systems. Consequently, the practicability of the concept of DCSs in systems beyond Bitcoin and similar cryptocurrencies need to be addressed.

1.3 Distributed Consensus Systems Beyond Cryptocurrencies

The industry, especially in the financial sector, is actively engaged in examining the potentials of systems based on distributed ledgers for use cases such as supporting decentralized securities trading (DTCC, 2016) or the feasibility of self-executing and self-enforcing contractual clauses (McKinsey, 2015a). A global consortium is working on the applicability in financial markets, representing over 50 of the biggest financial institutions (e.g. J.P. Morgan, Deutsche Bank or HSBC) (Kelly, 2015). As the first stock exchange worldwide, NASDAQ recently implemented a platform called Linq enabling asset trading in their private equity market based on ledgers (NASDAQ, 2015). The IT industry also shows considerable interest in DCSs. Microsoft offers corresponding solutions as a service through their scalable cloud platform Azure, providing customers with the infrastructure to come up with their own products (Marley, 2015). Under the umbrella of the Linux Foundation, technology companies such as IBM, Intel or Fujitsu are developing an open source distributed ledger framework to “focus on building robust, industry-specific applications, platforms and hardware systems to support business transactions” (Linux Foundation, 2015). Beside these already established companies, a wide range of new competitors is entering the market. The venture-backed startup Ripple Labs. operates a global settlement network for instant, low-cost international payments denominated in a variety of currencies (Ripple Labs., 2016). In addition, Ethereum is worth mentioning as platform providing security and reducing costs associated with contractual agreements (Ethereum, 2015).

The majority of projects, however, is still at an early stage of development and has not overcome the status of conceptual studies and prototypes yet. Although Bitcoin proves the practical functioning of the concept, major technological and non-technological challenges have to be overcome. In particular, DCSs are exposed to serious concerns regarding the scalability to support the timely processing of a large number of transactions (Cobben *et al.*, 2015). There also is a need for approaches that are feasible to ensure the correctness of shared ledgers, while at the same facilitating integration with established businesses and governance (European Banking Authority, 2015). Moreover, it is necessary to clarify how these systems can be implemented to comply with applicable law (International Monetary Fund, 2016). Consequently, it is necessary to elaborate on the general architecture of DCSs and provide means to evaluate their economic potentials in different use cases.

As the notion of DCSs characterizes still an emerging field of technologies, so are the terms used to describe different concepts and specific features subject to continuous changes. It is consequently not surprising that terms like Bitcoin, blockchain or distributed ledger are often understood as interchangeable and allocated with a varying scope in the current literature. Even though the terminology is still evolving and formal definitions are not existing so far, it is important to distinguish elements to arrive at a common understanding. Figure 1 presents the key terms in a hierarchical order, whereby their meaning gets broader from bottom to the top. This means, every term includes the terms positioned beneath it. For instance, Bitcoin in fact is a cryptocurrency, but the converse does not necessarily hold true, since there are other cryptocurrencies aside from Bitcoin.

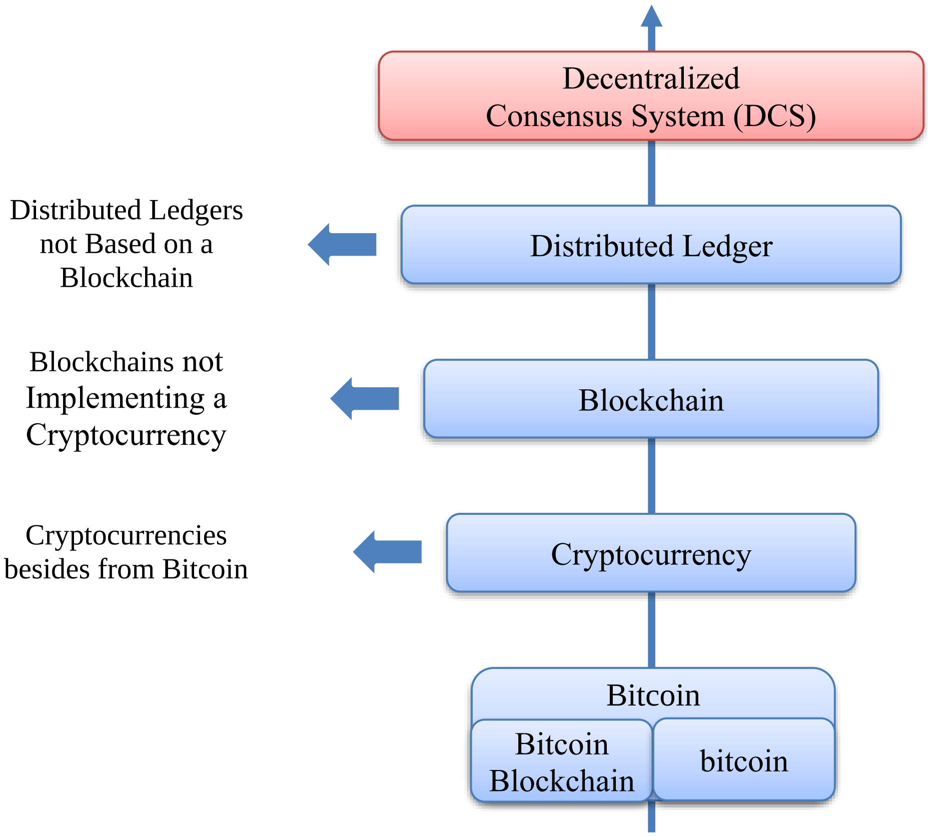

Decentralized Consensus System (DCS)
Distributed Ledgers not Based on a Blockchain
Distributed Ledger
Blockchains not Implementing a Cryptocurrency
Blockchain
Cryptocurrencies besides from Bitcoin
Cryptocurrency
Bitcoin
Bitcoin Blockchain
bitcoin

Figure 1: Terminology of the Central Concepts

Bitcoin is a payment-system with which two parties can exchange value over the internet. Therefore, it possesses its own integrated token called **bitcoin** or BTC that serves as exchange medium and is used as a unit of account. The respective value of bitcoins is determined by supply and demand and trust in the system Bitcoin is not operated by a central administrator, instead a decentralized P2P network is responsible for maintaining the **Bitcoin blockchain**. The bitcoin blockchain is a data structure distributed across the network which can be visualized as a ledger. It contains a record about all ever-conducted transactions and is continuously updated (Nakamoto, 2008).

Cryptocurrency specifies a new form of a virtual currency. The term is derived from the cryptographic methods underpinning the supply and tracking of the respective exchange medium implemented in each system. This token may be regarded as a kind of money, depending on the extent to which it fulfills the monetary functions of a medium of exchange, store of value and unit of account (Government Office for Science, 2016). Bitcoin is undisputedly the most famous cryptocurrency, but there are currently over 700 other representatives actively traded on markets (CoinMarketCap, 2016).

Blockchain is used to when referring to a data structure inspired by the bitcoin blockchain. The term includes all types of ledgers that link blocks sequentially in a chronological order. Blockchains can be built directly upon the open source code of Bitcoin, or be based on different approaches to realize similar functionalities. For instance, alternate algorithms can be used to modify the consensus mechanism (Evans-Greenwood *et al.*, 2016). Blockchains can be utilized as technical basis for the functioning of a cryptocurrency, but also to realize alternative applications that may benefit from the transparency provided by a blockchain.

Distributed ledger is a generic term to describe a data structure that serves as store for transactions and is replicated on multiple nodes on the Internet or private networks. Integrity of the ledger is ensured by a consensus process, in which course the participating nodes verify the correctness of transactions to a set of given rules. The underlying consensus mechanism defines procedures to determine the right ledger in case of conflicting versions (Government Office for Science, 2016). Although it is frequently the case, a distributed ledger does not necessarily have to use a blockchain for storing transactions. For this reason, it is accounted for other data structures potentially appropriate to achieve a consensus and provide security (Fielder and Light, 2015).

Decentralized Consensus System (DCS) describes systems “based on P2P principles rather than central authority and rely on cryptography for network-wide verification (by consensus) of a systems state" (Glaser and Bezzenberg, 2015; p. 2). The notion of DCS is used when considering the system in its entirety, including the organization perspective, whereas the technical basis of every system is a distributed ledger (Brenig *et al.*, 2016).

1.4 Research Questions & Objectives

As described above, the concept of systems based on distributed ledgers that enable a decentralized consensus on acceptable transactions is controversy discussed lately. Especially the concept of a publicly accessible ledger, which provides transparency regarding a set of transactions different entities agree upon without relying on any centralized entities, sounds promising for nearly all potential use cases involving digital interactions. If it is feasible to provide such systems in practice, this could dramatically reduce the costs associated with intermediation through third parties and enable digital business models formerly not possible due to trust issues. It is, however, far from clear whether this vision will actually become reality and if DCSs really are the disruptive technology they are sometimes envisaged as. People concerned with DCSs are divided into at least three groups. On the one side of the spectrum there are the optimists who expect these systems to completely revolutionize the way how organizations are going to operate and digital interactions will be facilitated in the near future. The pessimists on the other side of the spectrum assume the complete concept to be buzzword describing something that can already be achieved much cheaper with existing solutions or is not practically feasible. The third group reflects realists trying to figure out advantageous application fields in different industries. What is missing right now are works thoroughly investigating the phenomenon by conceptualizing DCSs and providing means for their design and evaluation.

Any examination of DCSs necessarily needs to be concerned with the Bitcoin system, since it established the concept of distributed ledgers and is one of the actual realizations that provides practical evidence for a cryptocurrency as the narrowest and most widespread application of DCSs. The success of Bitcoin and its open source nature further inspired the development of several hundred alternative cryptocurrencies, which are also traded on exchanges as well as for goods and services and thus interact with the real economy. What is even more important, however, all systems either already running or in development implement some of the characteristics of Bitcoin to a greater or lesser extent or get deliberately separated from it. Therefore, it it must be clear what the specific characteristics of Bitcoin in terms of, for example, authentication methods, degree of transparency or the verification of transactions, are and what they imply. Only then it is possible to draw conclusions about the potentials as well as inherent risks of the system and to offer suggestions regarding the design of future DCSs. In accordance with this, the first research question for this dissertation is formulated as follows:

RQ1: *What are the specific characteristics of the Bitcoin system?*

Bitcoin and other cryptocurrencies directly derived from it are grounded on the same specific characteristics and, therefore, implications resulting from the design of Bitcoin apply to all of these systems. This is why the general notion of cryptocurrencies is used to reason about them. There is a rich body of literature emphasizing on the effects of cryptocurrencies for the payment industry (e.g. Hagiu and Beach, 2014) and their monetary aspects (e.g. Yermack, 2013) available, therefore they are not covered in this thesis. Instead their abuse for criminal purposes, in particular in the context of ML, will be explored. As already mentioned, ML has severe consequences on the economic performance of entire societies as well as negative effects on single individuals. Thus, the suitability of cryptocurrencies for ML has to be discussed when examining their impact on society and to prevent this risk from arising in future developments of DCSs.

The topic of ML with cryptocurrencies is eagerly discussed in related disciplines such as computer science (e.g. Meiklejohn *et al.*, 2013), legal studies (e.g. Stokes, 2012) and economics (e.g. Dostov and Shust, 2014) lately. Although these works provide insights into e.g. regulatory aspects, their embeddedness in the financial system and methods to derive implications from publicly available transaction data, the majority of studies focus on the challenges cryptocurrencies pose on Anti-Money Laundering (AML) efforts (Brezo and Bringas, 2012). However, existing literature lacks in-depth analysis of the particular factors originating from their unique characteristcs, which provide the economic incentives for money launderers. Instead, it implicitly assumes that cryptocurrencies are attractive for money launderers, because of their technical design features and the few publicly known ML incidents. But only if cryptocurrencies are perceived economically beneficial from a criminal’s point of view, they may be qualified as a promising instrument to support the process of ML and consequently pose a real threat to AML efforts. Consequently, factors that have an effect on the execution of the ML process, and thereby influence the economic incentives of criminals, need to be identified and analyzed. This challenge leads to the second research question:

RQ2: *Does the system design of cryptocurrencies, especially Bitcoin, lead to risks in the context of money laundering? More precisely, what are the factors that shape the incentives for criminal individuals to utilize them for money laundering?*

In order to abstract from systems designed like Bitcoin and to consider a broad range of applications and use cases besides cryptocurrencies, the general architecture of DCSs needs to be conceptualized. The commonality of all DCSs is a distributed ledger that provides transparency regarding transactions that are included in accordance with rules formalized in the system. However, they do not necessarily need to possess the same specific characteristics like Bitcoin. Having analyzed risks arising from the design of Bitcoin, concretely in the context of ML, it is apparent that modifications are required to prevent such risks from occurring and to facilitate certain applications.

A systematic approach for elaborating on the high-level purpose of such systems, which is to enable an agreement between several entities on a commonly accepted state of a distributed ledger, is missing right now. However, this is essential to determine which form of consensus is facilitated by DCSs. Generally, two different approaches for the design of DCSs have become apparent and are discussed in the literature: permissionless systems and permissioned systems (e.g. Government Office for Science, 2016; International Monetary Fund, 2016). These approaches differ with regard to their openness and the toleration of centralized entities with exclusive rights. Bitcoin is the most famous representative of a permissionless system, since its specific characteristics determine that there are no restrictions on the participation in the system. Additionally, these DCSs in theory avoid any kind of central entities at the governance level. Permissioned systems, in contrast, provide means to restrict the access to the system and tolerate a certain degree of centralization. The type of system implemented depends on the specific needs of users in each particular application. To this end, concrete properties have to be identified in order to precisely distinguish the design approaches from each other. Consequently, research question *RQ3a* needs to be addressed in order to investigate architecture of DCSs in general.

Moreover, there is a lack of research on the fundamental functional requirements DCSs must meet to achieve their high-level purpose and provide economic value. Requirements describe both desires and objectives of users as well as conditions and characteristics of DCSs resulting from organizational and legal obligations (IEEE, 1990). Identifying and analyzing requirements is an important step in the process of designing and building a DCS, because it ensures that its functionalities are in line with stakeholders' objectives (Beckers *et al.*, 2013). Stakeholders in this respect are individuals as well as organizations and institutions intending to use a DCS. Accordingly, the research objective of *RQ3b* is the identification of fundamental functional requirements DCSs need to fulfill on the most fundamental level in order to support the development of actual systems.

RQ3a: *Based on the analysis of Bitcoin and similar cryptocurrencies, which implications result for the architecture of Decentralized Consensus Systems in general?*
RQ3b: *What are the functional requirements for Decentralized Consensus Systems?*

Currently there is a lack of methods and frameworks to elaborate on the economic potentials of DCSs in general and for the evaluation of specific systems. Especially in consideration of the growing propagation of DCSs enabling various types of applications ranging from cryptocurrencies up to smart property, the value they provide for the different stakeholders needs to be assessed. This is exacerbated owing to short development cycles and a flexible environment, where novel systems, applications and services emerge regularly. Therefore, an approach is required that is general enough to take these dynamics into account, but at the same time sufficiently specific to capture the particular technology-related features.

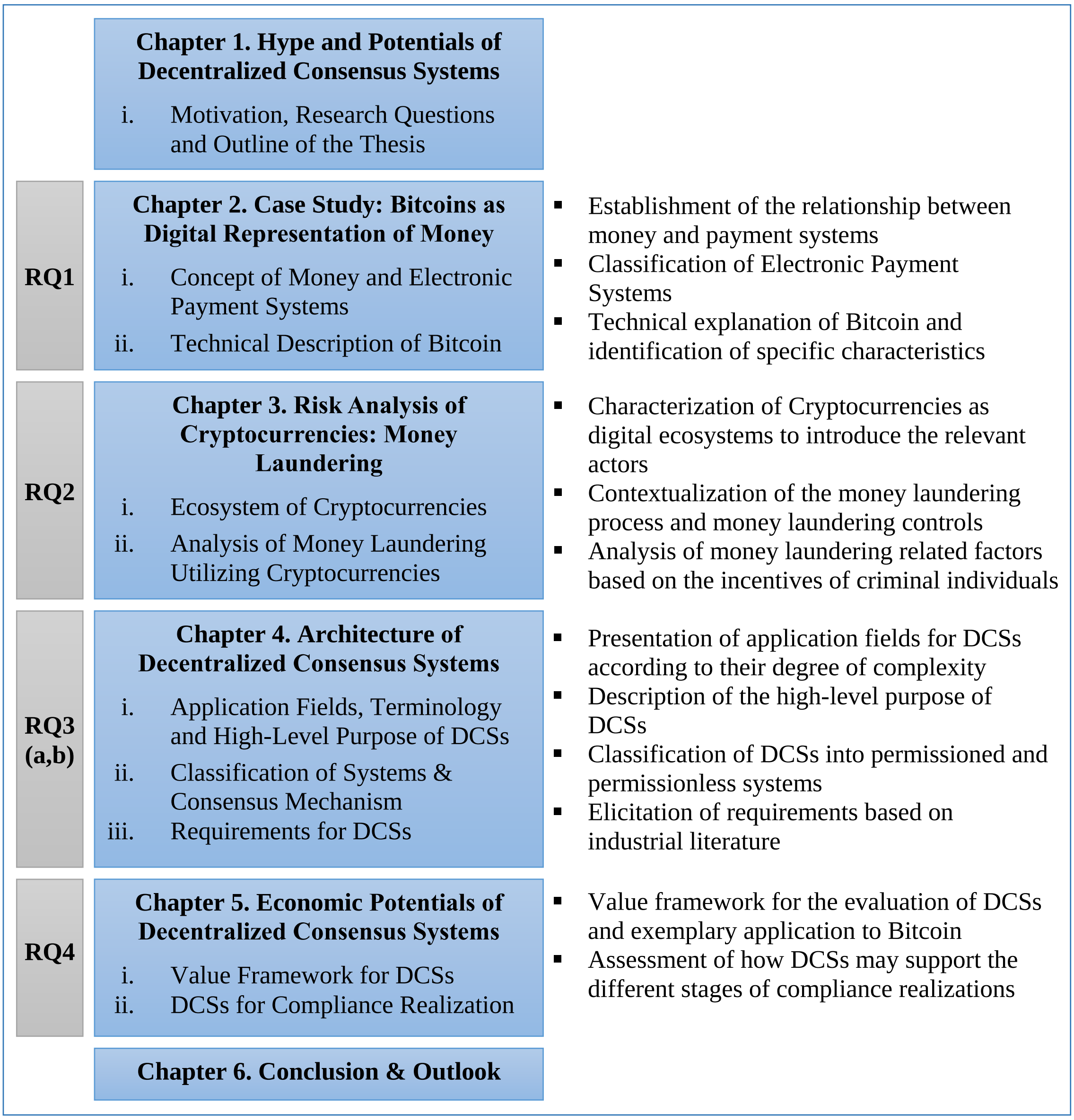
Previous contributions addressing the value dimension of DCSs include a taxonomy concerning the concept of DCSs (Glaser and Bezzenberg, 2015) or examine digital business models for Bitcoin companies (Kazan *et al.*, 2015). However, it is crucial to complement existing works by developing frameworks and concepts that can be used for the rigorous assessment of concrete business models. This will allow to evaluate the economic potentials and value that DCSs provide for their stakeholders in different applications fields as reflected in *RQ4*:

RQ4: *How can the economic potentials of Decentralized Consensus Systems be evaluated?*

1.5 Outline & Contributions

The issues formulated by the research questions described above are addressed in the subsequent chapters of the present thesis and focus on different aspects of DCSs at the intersection of economics, computer science and Information Systems (IS). The field of IS is characterized by two major research streams: researchers following a design science approach focused on the creation and evaluation of Information Technology (IT) artifacts and those who address behavioral issues to predict organizational and human reactions regarding the implementation of IS (e.g. Hevner *et al.*, 2004; Müller, 2009). This dissertation adopts a pluralistic methodological approach in order to investigate the behavioral dimension associated with the disruptive potential of DCSs as well as to support the design of these systems by presenting conceptual artifacts (Frank, 2006). According to Hevner *et al.* (2004) the behavioral science paradigm describes works that "develop and justify theories (i.e., principles and laws) that explain or predict organizational and human phenomena surrounding the analysis, design, implementation, management, and use of information systems" (Hevner *et al.*, p. 76). The thesis at hand provides explanations regarding the use of DCSs in the context of money and Electronic Payment Systems (EPSs), analyses their influence on the behaviour of criminal individuals and elaborates on the functionalities they offer in an organizational context. The design science approach is a problem-solving paradigm "to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of IS can be effectively and efficiently accomplished." (Hevner and Chatterjee, 2010, p. 11). A set of requirements is derived to support the design of DCSs in line with the stakeholders' objectives. Further, a framework to assess the value of such systems in different application fields and scenarios is developed. The requirements and the evaluation framework constitute conceptual artefacts which can be attributed to the design science approach.

Figure 2 depicts the outline of the document and indicates which research question is tackled in the particular chapter. Furthermore, it provides a brief summary of the content included in the different chapters. The dissertation is structured according to the research questions *RQ1* to *RQ4*, with each of the chapters is specifically targeted at one of these questions except for the concluding chapter 6.



	Chapter 1. Hype and Potentials of Decentralized Consensus Systems i. Motivation, Research Questions and Outline of the Thesis	
RQ1	**Chapter 2. Case Study: Bitcoins as Digital Representation of Money** i. Concept of Money and Electronic Payment Systems ii. Technical Description of Bitcoin	▪ Establishment of the relationship between money and payment systems ▪ Classification of Electronic Payment Systems ▪ Technical explanation of Bitcoin and identification of specific characteristics
RQ2	**Chapter 3. Risk Analysis of Cryptocurrencies: Money Laundering** i. Ecosystem of Cryptocurrencies ii. Analysis of Money Laundering Utilizing Cryptocurrencies	▪ Characterization of Cryptocurrencies as digital ecosystems to introduce the relevant actors ▪ Contextualization of the money laundering process and money laundering controls ▪ Analysis of money laundering related factors based on the incentives of criminal individuals
RQ3 (a,b)	**Chapter 4. Architecture of Decentralized Consensus Systems** i. Application Fields, Terminology and High-Level Purpose of DCSs ii. Classification of Systems & Consensus Mechanism iii. Requirements for DCSs	▪ Presentation of application fields for DCSs according to their degree of complexity ▪ Description of the high-level purpose of DCSs ▪ Classification of DCSs into permissioned and permissionless systems ▪ Elicitation of requirements based on industrial literature
RQ4	**Chapter 5. Economic Potentials of Decentralized Consensus Systems** i. Value Framework for DCSs ii. DCSs for Compliance Realization	▪ Value framework for the evaluation of DCSs and exemplary application to Bitcoin ▪ Assessment of how DCSs may support the different stages of compliance realizations
	Chapter 6. Conclusion & Outlook	

Figure 2: Outline of this Dissertation

Chapter 2 investigates research question *RQ1* by providing an examination of Bitcoin as the first representative of a DCS. Since Bitcoin is intended as a payment system and implements a virtual currency called bitcoins, it is natural to begin by exploring the historical development of money and classifying different kinds of EPSs. The classification categorizes these systems according to the type of money they facilitate to transfer. Thereby, the concept of virtual currencies is explained and some examples are briefly discussed. The chapter then introduces the technical design principles of Bitcoin and elaborates on its important characteristics, because Bitcoin acts as role model for all subsequent realizations. These characteristics provide the foundation for the analysis of ML risks and classification of DCSs covered in the further course of this dissertation. Subsequently, an alternative cryptocurrency is compared to Bitcoin in order to illustrate by which features such systems can be differentiated from each other.

Chapter 3 analyzes how cryptocurrencies following the Bitcoin design may be utilized for ML, in that addressing research question *RQ2*. It characterizes cryptocurrencies as digital ecosystems, in order to introduce the central actors emerging around these systems in a structured form. This is a necessary step to provide an understanding about the possibilities cryptocurrencies offer for executing transactions, as the actors provide complementary services and ensure the correct functioning of such systems. Two common transaction patterns involving cryptocurrencies are investigated to demonstrate the interplay between the different actors. To lay the theoretical foundation for the analysis of cryptocurrency backed ML, an economic perspective of ML is provided. Therefore, the existing literature regarding the economics of crime is presented and applied to the criminal act of ML. Consequently, the context of ML is conceptualized and the two central elements, namely the ML process and available AML controls, are outlined. This knowledge is used for a conceptualization of how economic incentives for using an instrument (e.g. a payment system or other kinds of value transfer mechanisms) for ML are provided. The conceptualization serves as basis for the subsequent assessment of factors that potentially set incentives for utilizing cryptocurrencies for ML. The identified factors are afterwards applied to a set of practical scenarios to evaluate their relevance in the respective context. The chapter concludes with an overview of actual technological developments and regulatory approaches as risk mitigation measures, which may influence the incentives of criminal individuals to use cryptocurrencies for ML. Chapter 3 is based upon and extends a paper that has been presented at the *23th European Conference on Information Systems* and is published in the respective proceedings (Brenig *et al.*, 2015).

Chapter 4 addressing research questions *RQ3(a,b),* introduces the architecture of DCSs based on the findings of the preceding analysis of Bitcoin and similar cryptocurrencies. Additionally, it elaborates on the functional requirements for these systems. DCSs in general are inspired by the design principles of Bitcoin and may be beneficial for a wide range of applications besides cryptocurrencies. Thus, chapter 4 firstly illustrates the changing relevance of involved concepts and presents possible application fields for DCSs categorized according to their degree of complexity. A model is invented that conceptualizes the high-level purpose of DCSs, which is an agreement on a common state between several entities based on a consensus process. Consequently, a classification of design approaches and consensus mechanisms used for the consensus process is provided. The classification accounts for the risks resulting from the specific characteristics of Bitcoin in the context of ML. Therefore, it contrasts permissionless systems like Bitcoin with permissioned types of systems that are based on different characteristics. Subsequently, requirements for DCSs are derived from a literature review including publications from actual and potential stakeholders. The requirements introduced are intended to provide a common understanding about the core requirements for a system to be regarded as a DCS. Only recently first attempts for their characterization have been conducted, however, they are limited to a specific industry and cannot be generally applied. Consequently, this chapter combines and extends previous findings and presents a set of requirements for permissionless as well as permissioned types of systems. Chapter 4 includes a paper that is currently in review for the *25th European Conference on Information Systems* (Brenig *et al.*, in review[a]). It contains a part of a paper that has been published in the *Proceedings of the 24th European Conference on Information Systems* (Brenig *et al.*, 2016). Furthermore, it includes a part of a paper that is currently in review for the *25th European Conference on Information Systems* (Brenig *et al.*, in review[b]).

Chapter 5 analyzes the economic potentials of DCSs and thereby tackles research question *RQ4*. To begin with, the economic foundations justifying the use of DCSs for supporting digital interactions are examined and a characterization of a business model is given. It presents a framework for the evaluation of the value proposition of DCSs building upon the prior architectural investigations and analyses the economic potentials of DCSs. The evaluation framework is developed to account for the wide variety of applications where DCSs are discussed as disruptive innovation, which are ranging from currencies to the decentralization of business operations. It serves as a basis for the assessment of concrete business models and is exemplarily applied to the Bitcoin system. The remainder of this chapter provides an interpretation of DCSs as instrument for compliance realization. It elaborates on the compliance process and shows how it can be ensured by DCSs before, during and after a transaction takes place. Afterwards, the core elements of DCSs regarding the realization of compliance are discussed in detail and illustrated based on the assessment of a practical use case. Chapter 5 includes a paper that has been published in the *Proceedings of the 24th European Conference on Information Systems* (Brenig *et al.*, 2016). Additionally, it includes parts of a paper that is currently in review for the *25th European Conference on Information Systems* (Brenig *et al.*, in review[b]).

Chapter 6 concludes this dissertation by providing a summary of the results. It further discusses the resulting implications and provides possible directions for future work.

1.6 Related and Unrelated Publications

Parts of this dissertation build upon research papers having been published in different proceedings and presented at international conferences. It further includes parts of research papers that are currently being reviewed for presentation at an international conference (a complete list of related and unrelated publications is depicted in Table 1).

Publications (double-blind peer-reviewed)
Brenig, C., Schwarz, J. and Nolte, C.-G. (in review [a]), “Requirements for Decentralized Consensus Systems”. *Submitted to ECIS2017 and currently in the review process.*
Brenig, C., Rückeshäuser, N. and Schwarz, J. (in review [b]), “Assessing the Potentials of Decentralized Consensus Systems: A Compliance Perspective”. *Submitted to ECIS2017 and currently in the review process.*
Zahoransky, R., Holderer, J., Lange, A. and Brenig, C. (2016), “Process Analysis as First Step Towards Automated Business Security”. In*: 24th European Conference on Information Systems (ECIS 2016)*, Istanbul, Turkey, June 12-15, 2016.
Brenig, C., Schwarz, J. and Rückeshäuser, N. (2016), “Value of Decentralized Consensus Systems – Evaluation Framework”. In: *24th European Conference on Information Systems (ECIS 2016)*, Istanbul, Turkey, June 12-15, 2016, Best Paper Award Nominee.
Zahoransky, R., Brenig, C. and Koslowski, T. (2015), “Towards a Process-centered Resilience Framework”. In: *ARES 2015 - 10th International Conference on Availability, Reliability and Security - Workshop FARES.*
Brenig, C., Accorsi, R. and Müller, G. (2015), “Economic Analysis of Cryptocurrency Backed Money Laundering”. In: *23rd European Conference on Information Systems (ECIS 2015)*. Münster: Germany.
Koslowski, T., Strüker, J. and Brenig, C. (2013), “Mastering the Energiewende – A Cross-disciplinary Teaching Approach”. In *21st European Conference on Information Systems (ECIS 2013)*, Utrecht, Netherlands, 6-8 Jun.
Brenig, C., Reichert, S. and Strüker, J. (2013), “Inter-Organizational Demand Response Applications: How to Address Moral Hazard in Smart Grids”. In *19th Americas Conference on Information Systems, AMCIS 2013*, Chicago, Illinois, USA, August 15-17, 2013.

Table 1: Related and Unrelated Publications

2 Case Study: Bitcoins as Digital Representation of Money

Bitcoin was envisioned in the corresponding whitepaper as a solution to the “inherent weaknesses of the trust based model” in internet-based commerce (Nakamoto, 2008, p. 1). These weaknesses are argued to emerge from the dependence on financial intermediaries, which are required for mediating conflicts and increase the transaction costs involved (Nakamoto, 2008). The resulting system to solve this issue is comprised of the actual Bitcoin protocol that facilitates exchanges as well as an implemented token called bitcoin (spelled with a lower b in line with the commonly used terminology) acting as transfer medium representing value. It is of interest for economists partly due to its potential to disrupt established payment systems, but also from a monetary perspective, since the value of bitcoins fluctuates independent of any government backed fiat currency. Therefore, these uses need to be examined firstly, in order to derive the specific characteristics of the Bitcoin system afterwards.

Accordingly, this chapter starts by describing the chronological development of money on basis of the monetary functions and the accompanied continuous reductions in transaction costs. Subsequently, different approaches for the digital representation and transfer of money are presented and classified. Bitcoin and other cryptocurrencies are in this manner delimited from existing solutions. Then the technical principles of Bitcoin are explained in order to derive the specific characteristics of DCSs based on its design as formulated in *RQ1*. Eventually, an alternative cryptocurrency is compared with Bitcoin to illustrate by which features concrete realizations can be differentiated from each other.

2.1 The Concept of Money

The term money is commonly used without further thinking about its precise meaning, when individuals are talking about currency (Mishkin, 2013). However, currency generally only covers banknotes and coins issued by the central bank responsible for a respective judicial area and which are required to be accepted as means of payment by law. This understanding is built upon the concept of monetary sovereignty, which determines the power of a state (e.g. the Federal Reserve responsible for the US-Dollar in the United States (Federal Reserve System, 2005)) or a supranational body (e.g. the European Central Bank (ECB) responsible for the Euro in the European Union (European Union, 2012)) to exercise legal control over its currency. Nevertheless, there is an ongoing controversy if currency is inevitable a governmental responsibility. A long literature advocating the feasibility of a private provision of currency exists (e.g. Klein, 1974; Monnet, 2002; Berentsen, 2006). The Austrian economist Friedrich August von Hayek is unquestionable the most prominent contributor who argues for the existence of equilibria with positive values, when several currencies are issued in a competitive environment. Such an equilibrium is therefore likely to dominate a monopoly under control of governmental authorities (Hayek, 1990). Irrespective of the concrete authority responsible for the supply and liable to ensure the value of a currency, it is today's omnipresent form of money. At the same time, it does not cover the whole spectrum of goods historically and presently accepted in exchange for other goods, services or to repay debts (for the sake of simplicity, the notion of goods is used in the following as umbrella to describe everything that is of economic value and can be transferred).

2.1.1 Economic Foundations

From an economist point of view, money is loosely speaking a set of assets used by individuals to purchase a good or service from other individuals (Schumpeter, 2009; Keynes, 2008; Goodhart, 1989). Modern societies characterized by specialization through division of labor would have been impossible without money as widely accepted payment instrument (Kiyotaki and Wirght, 1993). In order to investigate this argument and examine the economic implications of introducing money, a scenario involving the direct exchange of goods as the earliest form of commerce is assumed. The output of an individual may be specialized, but the desired consumption is diverse and enabled by trade. It is therefore the surplus of production, which is the result from his or her labor as input factor that is exchanged for other goods (Ostroy and Starr, 1990). Consequently, individuals providing goods in a non-monetized economy have to search for transaction partners offering something that they desire in exchange. Additionally, it requires effort to negotiate on the concrete value of the commodities involved in this barter (Menger, 1892). The situation where a transaction will be successfully carried out is called double coincidence of wants, which fulfillment imposes severe transaction costs and limitations on affected economies. The phrase was introduced by Jevons (1893) to describe the difficulties for the supplier of a good called A to find a demander for the good called B and vice versa. If exchange is difficult, it imposes high costs to implement specialization in equilibrium, which is why division of labor is dependent on means and mechanisms to enable efficient trading (Smith, 1775).

Money irrespective of its concrete form implies a fundamental shift in the process of exchanging a good for another good compared to a barter economy (Menger, 1892; Hicks, 1935). As already mentioned by Aristotle over 2000 years ago in his famous work Politics: “when the inhabitants of one country became more dependent on those of another, and they imported what they needed, and exported what they had too much of, money necessarily came into use” (Aristoteles and Rackham, 1944). In the event of two potential traders A and B, where A offers good 1 and B offers good 2, two cases can be distinguished. In the first case, A demands good 2 and B in turn demands good 1. It is characterized by a double coincidence of wants and A and B can negotiate to complete the transaction as already explained. In the much more probable second case, B demands good 1 offered by A, but A does not demand good 2 offered by B. Money was introduced to facilitate a for both potential traders’ beneficial transaction in situations like this, where a double coincidence of wants is not present (Ostroy and Starr, 1990). Even though A is not willing to take good 2, he or she may accept money if it can later be traded for another desired good 3 offered by trader C.

This statement already involves several important characteristics and functionalities of money required in order to support the transaction process illustrated in Figure 3. Instead of a single transaction, where a good in possession is directly exchanged for a desired good, the transaction process involving money consists of two transactions. Accordingly, it is the exchange value provided by money that provides access to the full range of goods available in the economy. Although the introduction of money goes along with a doubling of the number of transactions necessary to exchange the surplus of one good for a demanded good, it lowers transaction costs by eliminating time for searching transaction partners and negotiating values (Mishkin, 2013; Davies, 2002). Transaction costs in that context are “the costs in time and other resources that parties incur in the process of agreeing to and carrying out an exchange of goods and services” (Hubbard *et al.*, 2014, p. 505). It is an intertemporal asset allowing to reallocate purchasing power over time (i.e. money that is acquired at time t can be spent for another good at any time t+1 in the future). This role has been extensively formalized in intertemporal models, where equilibria are developed based on a sequence of budget constraints in several time periods (e.g. Hahn, 1973; Heller and Starr, 1976). Thus, money performs the role of a universally accepted IOU ("I owe you") – a promise to repay somebody at a later time – to account for the fact that heterogeneous people have varying needs at different times (McLeay *et al.*, 2014).

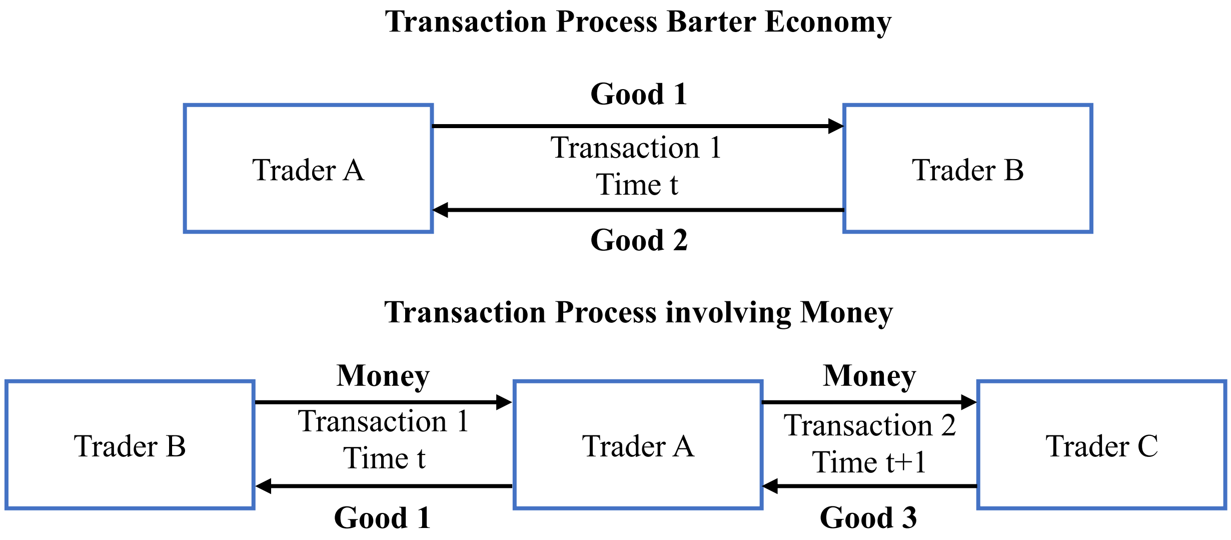


Figure 3: Transaction Process in a Barter Economy and Involving Money

Now that the superiority of an economy with an established monetary system has been outlined compared to a barter economy, it appears obvious to describe what qualifies an asset as money. Irrespective of its concrete form, whether something can be regarded as money depends on the extent to which it fulfills the three primary functions associated with money: **medium of exchange, unit of account** and **store of value** (Mishkin, 2013; Mankiw, 2016; Krugman, 1984). Historically, a fourth function entitled **standard of deferred payment** was considered as a distinguished function, which is often subsumed under the other functions in more recent works (Jevons, 1893).

A **medium of exchange** is generally defined as an asset that a buyer hands over to a seller in order to pay for goods. By fulfilling this function, money permits that the value of goods can be assessed in terms a common measure intermediating the exchange (Abel *et al.*, 2013). The Austrian School regards money as the most universal and therefore also most liquid medium of exchange (Mises and Batson, 2009). One can be confident that a retailer is willing to trade goods in exchange for money, since it is expected to be widely accepted. It is furthermore distinguished between the importance of the different functions of money. The functions of unit of account and store of value are assumed to be derived from the defining function of money as a medium of exchange (Menger, 1892). It is argumented that an asset that is increasingly accepted as medium of exchange also fulfills the other functions. According to Mishkin (2013), an asset must meet several criteria in order to function as medium of exchange:

1) Easily Standardized to determine its value
2) Widely accepted
3) Divisible to trade shares and allow for change
4) Can be carried without great effort
5) Not deteriorate quickly

A **unit of account** is used as a numerical measurement to state prices of goods and specify liabilities. Money is used to account and compare the different values of goods, providing an efficient mean to determine whether a good is worth exchanging it (Mankiw, 2016). A common unit of account increases the efficiency of trade, because it does away with the need to state the relative price of one good in terms of another good. The benefits can be best explained assuming a barter economy with a diverging number of different goods. With three goods one only needs to know three different prices (every good in terms of the others), which is manageable quite simple. However, the different prices required to know, and thereby also relations, increase exponentially with the number of goods in the economy. As a result, the utility provided by this function of money increases with the complexity of the economy (Mishkin, 2013).

A **store of value** is something that allows to shift purchasing power into the future. It forms the basis for the characteristic of money to act as an intertemporal asset. Critical requirement for money to be regarded as a store of value is, that it remains relatively stable over time and is not exposed to large fluctuations (Keynes, 2008). Therefore, individuals must quantify their expectations about its future value (Laidler, 1969). Fluctuations in the value of money, and therefore the suitability as a store of value, concretely depends on the price level of goods in the economy (Blanchard and Johnson, 2013). An increase in the price level during inflation implies that money loses its value (i.e. the same amount of money provides less purchasing power on the date t+1 than on the date t). Logically, a decrease in the price level during deflation implies that the value of money increases. The function of store of value is not exclusively attributable to money. Also (in-) tangible assets – like bonds, shares, real estate or art – can fulfill the function of a store of value (Abel *et al.*, 2013; Mankiw, 2016).

The aforementioned functions money should fulfill provide an indication of assets which are potentially qualified to be regarded as money due to their specific characteristics. Nobody would for example consider a living animal to fulfill the functions of money. It is not easily exchangeable, let alone divisible and simultaneously not a good unit of account or a store of value when it ultimately dies. However, many different assets have been accepted as money over centuries and what is regarded as money at a given point largely depends on the beliefs of individuals. To this end, decision makers in different monetary regimes define monetary aggregates, which are in line with international practice commonly called M1, M2 and M3. Assets are classified according to their liquidity, whereby M1 encompasses high liquid assets directly used as medium of exchange, M2 additionally includes intermediate assets and M3 characterizes money in the broad sense. The determination of this aggregates is an ongoing process of accounting for disruptive financial innovations that might have to be included. Table 2 exemplarily lists the money aggregates of the euro area as defined by the ECB.

Assets	**M1**	**M2**	**M3**
Currency in circulation	X	X	X
Overnight deposits	X	X	X
Deposits with an agreed maturity up to 2 years		X	X
Deposits redeemable at a period of notice up to 3 months		X	X
Repurchase agreements			X
Money market fund (MMF) shares/units			X
Debt securities up to 2 years			X

Table 2: Definition of Euro Monetary Aggregates[1]

2.1.2 Chronological Development of Payment Systems

The continuous expansion and increasing openness of societies up to today's globalised markets historically led to a steadily altered set of challenges imposed on payment systems (Davies, 2002; Goodhart, 1989). Additionally, the ongoing technological progress provides further

[1] Table 2 is based on European Central Bank (2016b)

contributions to enhance the functionality of payment systems (Ruiz-Martínez *et al.*, 2012; Dwyer, 2015). Money and payment systems are directly linked to each other. An asset is only able to fulfill the monetary function of a medium of exchange, if it features a payment system as a secure means of transfer (e.g. Robleh *et al.*, 2014; Hubbard and O'Brien, 2014; Mishkin, 2013). A payment system as defined by the Bank of International Settlement "consists of a set of instruments, banking procedures and, typically, interbank funds transfer systems that ensure the circulation of money" (Bank for International Settlements, 2003). Although the emphasis of this definition is on the aspects of payment systems specific to banking, it ultimately boils down to the issue of an efficient and safe transfer of money. Systems that are suitable for this purpose facilitate the physical, respectively, digital transfer of currency and/or update the balances of user-accounts in so-called ledgers. In order to illustrate the development of payment systems, from valuable commodities acting as money to innovative means of electronic payments including Bitcoin, this section provides a chronological overview of the different stages of development and forms money has taken. Each of the stages is characterized by an increased efficiency, as novel kind of systems have reduced the costs for settling transactions (Hubbard and O'Brien, 2014).

Assets are feasible to function as money if they are acceptable by everyone. In other words, individuals must voluntarily take them in exchange for other goods. Objects that have intrinsic value in themselves clearly fit into this category (Mankiw, 2016). They become **commodity money** when their overall value does not only consist of the mentioned intrinsic value, but also from the value in their use as money (O'Sullivan and Sheffrin, 2003). Conversely, this means that the commodities are also valuable without being used as money. Commodities are a suitable payment instrument when they are relatively easy to carry and transfer. Obvious candidates for commodity money are precious metals like gold or silver, because they are used as input for fabrication purposes and therefore likely to provide utility for individuals. Another recent example are cigarettes, which temporarily became popular as money in Europe after the Second World War (e.g. Radford (1945) describes how the economy in a prisoner-of-war camps evolved around cigarettes fulfilling the monetary functions). Challenging is the assurance of purity, which is important due to the fact that it determines the value of commodity money. The possibility for fraud hampers the extent to which commodity money is able to fulfill the functions of unit of account and store of value. As a countermeasure trusted third-parties are appointed that certificate its weight and purity (Hubbard and O'Brien, 2014).

In the next stage of development, it is abstracted from the need of money to exhibit intrinsic value. This money is usually currency in the form of paper or coins, where the material value does not correspond to the nominal value assigned to it. Initially, the value of such currency was ensured by a guarantee that it was convertible into a precious metal (Hubbard and O'Brien, 2014). The gold standard abandoned by most nations in the 20th century is an example, where currency was backed with gold administered by the national central banks. In the meantime, this type of currency evolved into **fiat money** declared to be of value by governments and which is not redeemable into precious metal (Mankiw, 2016). Therefore, it has no intrinsic value attached to it. Fiat money offers great advantages in terms of transaction costs compared to commodity money in the sense that it is usually much lighter and, therefore, more cost-effective to transport and store. Additionally, it avoids the high costs associated with using a commodity which could otherwise be used for other purposes (McLeay *et al.*, 2014). It is accepted as universally accepted means of payment under the prerequisite that the trust in the governmental authorities issuing and printing the currency is sufficiently high and the fiat money is forgery-proof (Mishkin, 2013; Mankiw, 2016).

Another important step in the evolution of payment systems was the introduction of **checks**, which has been closely linked with the establishment of modern banking systems. A check is payment order in a legally prescribed form to transfer a specified amount of money from an individual’s bank account to the account of the individual on which name the check was issued. They enable transactions in high denominations without requiring individuals to carry large amounts of currency with them. Additionally, payments are more efficient regarding to regular transactions between business partners in opposite directions. Instead of moving large amounts of currency, transactions can be settled by simply cancelling the respective checks (Mishkin, 2013). In most countries around the world checks are still an offered payment method, but their actual use is continuously decreasing. In Germany, for instance, the number of transactions dropped from 48,3 Million to 29,7 Million from 2010 to 2014 (Deutsche Bundesbank, 2015, p. 7) The decrease is partly due to the meanwhile widespread dissemination of online payment solutions. Moreover, checks consist of paper which can be easily tampered with, possibly leading to fraudulent transactions resulting from identity theft. Another downfall is the duration of a few business days it takes to clear a transaction (Centre for Retail Research, 2007).

The most recent innovation in payment solutions are **electronic payments systems**, which utilize the Internet as infrastructure to digitally transfer financial assets (e.g. Panurach, 1996;

Goos *et al.*, 2003; Giaglis and Kypriotaki, 2014). In the subsequent section, different categories of such systems get classified, their respective characteristics are explained and some examples will be introduced in detail. It serves the purpose to differentiate Bitcoin and other DCSs intended as cryptocurrencies from conventional centralized solutions and to explain the implications resulting from a decentralized design implementing a distributed ledger.

2.2 Different Types of Electronic Payment Systems

As already mentioned before, any asset intended to serve as a medium of exchange requires a secure transferring method. While EPSs were used for decades in applications ranging from withdrawing money from Automated Teller Machines (ATMs), to buying goods and services with credit or debit cards via point of sales terminals installed in stores, however, corresponding information were processed over secure networks and communication channels. On the contrary, the Internet posed novel challenges in terms of establishing a secure information exchange over an inherently insecure network (Putland *et al.*, 1997). But it also opened up new opportunities for instant and cost-effective worldwide communications, allowing individuals to collaborate without any spatial and temporal restrictions. The associated significant reductions in transaction costs enabled by IT are both, a driver for and requirement in modern economies characterized by a high degree of interconnectedness in a globalized environment (Dahlman, 2007). It is therefore no surprise that early proposals for systems enabling the digital transfer of money over the internet gained momentum with advances in technology and the associated widespread networking amongst individuals and organizations (e.g. Panurach, 1996; Wright, 2002). Consequently, this dissertation only considers systems utilizing the Internet and excludes proprietary infrastructures for the transfer of monetary value, when referring to the term EPS in the following.

Every transaction involving the trade of products and services in digital environments is conditional on an instrument to settle the necessary payment. At the end of the last millennium, however, it was extensively discussed whether Electronic Commerce even requires specifically designed payment systems (e.g. Böhle and Riehm, 1998). Instead, it is also possible to simply use conventional payment instruments like cash, check or bank transfer. Irrespective of any payment instrument, the growing importance of online trade is particularly well illustrated by the steadily increasing number of online transactions. They are expected to be 38,5 billion in 2015 and thereby nearly twice as many as in 2011 (Capgemini and Royal Bank of Scotland, 2014, p. 12). Simultaneously, payments are increasingly performed utilizing EPSs, suggesting that there is indeed demand for payment systems tailored to the needs of online buyers (IfH Köln, 2015; ibi research, 2014). Moreover, a tendency towards mobile payment solutions connecting digital with real environments can be observed. They can be used in a variety of payment scenarios: purchases of digital content like music or applications, payments for physical goods and services at vending or ticketing machines and at manned point-of-sale terminals (Dahlberg *et al.*, 2008). Amongst the most prominent and recent examples is Apple Pay, which was announced at the end of 2014 as payment system to buy in stores and apps utilizing Apple devices (Apple, 2016a).

To get a better understanding about how Bitcoin as a system fits into the context of contemporary and past approaches towards EPSs, a classification is presented in the following. It is intended to provide a common vocabulary regarding important terms like virtual- or digital currencies and electronic money, often used interchangeable and with varying meanings. There are actually many different criteria to classify EPSs (e.g. the timing when the payer is charged (Asokan *et al.*, 1997) or whether payments require an online verification from a central authority to prevent fraud or not (Sadeghi and Schneider, 2003)), whereby this thesis develops a categorization according to the type of money transferred by the system. This seems appropriate because Bitcoin is not solely an EPS, but also implements its own unit of account.

2.2.1 Classification Scheme According to Type of Money Supported

Since the advent of EPSs various approaches for their classification have been proposed. This is due to the reason that there are considerable differences in the design of such systems, which also has implications for their suitability in practical payment scenarios. These approaches distinguish EPSs by reference to a set of characteristics they exhibit. Besides the previously described timing when a payer is debited (i.e. prepaid, pay now, pay later) and the role of central authorities (i.e. offline payments are feasible or the system works only online), other differentiating features are, for instance, whether a system is software-based or a hardware-based and if it rests upon user-accounts or tokens (Reichenbach, 2001). The classification scheme depicted in Table 3 categorizes different types of EPSs according to the type of money they facilitate to transfer and implements some of the other characteristics mentioned in the literature for a further differentiation. This procedure accounts for the recent rise of EPSs inspired by Bitcoin, which implement their own unit of accounts exchangeable for conventional currency as well as goods and services in the real world. The top of the scheme maps the respective EPS, which acts as technology performing the function of a medium of exchange and is at the center of considerations. EPSs are generally used for the transfer of digital currencies. The notion of digital currencies is an umbrella term covering all digital representations of value. In this regard, it does not matter whether the value represented is issued by an authorized central bank or private entities (International Monetary Fund, 2016; Financial Action Task Force, 2014). The use of the term currency indicates that digital represented value should fulfill the function of banknotes and coins in online environments. However, this understanding is not completely in accordance with the narrow definition of currency in section 2.1, since some digital representations of value are in fact just bank deposits as it will be shown subsequently. It is distinguished between three different types of digital currencies exchanged via EPSs:

- Notational money
- Electronic money
- Virtual currency

<table>
<tr><th colspan="4">Technology
Electronic Payment System (EPS)</th></tr>
<tr><th colspan="4">Digital Currencies</th></tr>
<tr><th>Notational Money</th><th>Electronic Money</th><th colspan="2">Virtual Currency</th></tr>
<tr><td rowspan="7">▪ (In-)directly tied to deposits under control of financial institutions
▪ Account-based systems
Instruments
– Credit cards
– Direct debits
Payment Systems
– PayPal
– Apple Pay</td><td rowspan="7">▪ Issued & controlled by financial institutions
▪ No money creation
➢ Derived from notational money
▪ Token-based systems
Hardware-based
– Geldkarte
– Mondex
– Visa Cash
Software-based
– eCash
– Millicent</td><td colspan="2">▪ Issued & (controlled) by operator
▪ Money creation possible
▪ Account & token-based systems</td></tr>
<tr><td>**Centralized**</td><td>**Conver-tible**</td></tr>
<tr><td>– WoW Gold</td><td>✗</td></tr>
<tr><td>– Facebook Credits</td><td>✓</td></tr>
<tr><td>– Liberty Reserve</td><td>✓</td></tr>
<tr><td>**Decentralized**</td><td></td></tr>
<tr><td>– Cryptocurrencies (e.g. Bitcoin)</td><td>✓</td></tr>
</table>

Table 3: Classification Scheme of Electronic Payment Systems

Notational money is defined as value “stored as notations in a ledger or computer” (Camp *et al.*, 1995). In EPSs transferring notational money, every transaction is (in-) directly tied to value that exists as entries in such record books maintained by central authorities. In order for a clear delineation from virtual currencies, this category only encompasses EPSs supporting notational money nominated in governmental issued fiat currency. These record books are adjusted to complete a transaction, whereby the balance associated with the payer is reduced for the same amount as the balance of the payee is increased (Reichenbach, 2001). Central authorities responsible for updating the record books are typically the financial institutions where the users of an EPS possess deposit accounts. Therefore, EPSs that support notational money are account-based systems.

Online credit card payments belong to this type of payment instruments and extend the functionalities of existing credit cards for their online use. The payment processing remains the same as in the scenario with physical presence of the payer, however, the authorization of payments differs. Instead of authorizing a transaction by presenting the physical credit card and signing a bill or entering a personal identification number, payers are required to submit their credit card information via online channels. In order to ensure the integrity and confidentiality of this data transmission, security protocols like 3-D Secure, including technical specifications and requirements for issuers, acquirers and merchants, are implemented (Verified by Visa, 2011). Credit card payments are indirectly tied to deposits, because the payee’s bank account is credited before the payer’s account is debited. By this procedure, the card issuing company takes the default risk of the payer in the period between the payment and the debiting of its customer’s account. The online processing of debit card payments is equivalent to the processing of credit cards, but with one major difference, funds are withdrawn from the account of the payer directly (Asokan *et al.*, 1997).

PayPal and ApplePay are payment systems enabling the transfer of notational money by supporting the associated payment instruments. PayPal is relevant owing to its sheer size in terms of network participants, with 184 million active accounts that were used within the last 12 months as of 31.03.2016 (PayPal, 2016, p. 18). Users can open a PayPal account and fund it with various available payment instruments such as credit and debit cards. PayPal facilitates the instant transfer of these funds to other accounts, without disclosing payment instrument related data to anyone except for PayPal. This is one of the reasons for its worldwide success.

It does no longer take several days until a payment via, for instance, bank transfer is processed, instead the transaction can be terminated immediately.

ApplePay is worth mentioning since it is forecasted as system that potentially achieves a breakthrough of mobile payment solutions for the wider public (e.g. Williams, 2016). It is essentially a digital wallet, which supports major credit as well as debit cards and allows for contactless payments in stores using Near Field Communication. Further, it facilitates purchases in mobile applications. Advanced security measures to protect sensible information are provided by refraining from saving any card and payer related information on the device. Instead, a unique identification number is created and transmitted to the payee. This so-called Device Account Number is used for the authentication of a transaction, by assigning the number to the card data through the payment network. In this way, no entity except for the respective payment network has access to any personal data. As additional security measure, the fingerprint sensor of Apple devices is used for the verification of a transaction (Apple, 2016b).

Electronic Money (sometimes called e-cash, e-coins or digital cash) is reengineered physical currency in a digital form and intended to preserve the advantages of coins and notes while concurrently improving on its shortcomings. Low transaction costs, rapidity of transaction, anonymity at least regarding individuals not directly involved in the trade and high acceptance are just some of the benefits from using cash. Disadvantages comprise the high costs for its production and distribution, a limited divisibility and its unsuitability for a digital exchange (e.g. Clemons *et al.*, 1996; Párhonyi *et al.*, 2005). The European Parliament and the Council define it in Article 2(2) of its Directive 2009/110/EC as “electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […], and which is accepted by a natural or legal person other than the electronic money issuer” (European Union, 2009).

In Electronic money systems, there is no creation of money, since it is typically issued by converting notational money and consequently denominated in fiat currency (Financial Action Task Force, 2014). For this reason, electronic money is separated from notational money with a dashed line in Table 3. It is classified into hardware-based and software-based systems (Takao *et al.*, 2012). Both solutions have in common that they enable value to change hands without connecting it to account movements. Such types of systems make use of tokens for the transmission of value (Reichenbach, 2001). Hardware-based systems implement a physical device – i.e. a smart card - to store the value on and distribute the tokens. Software-based systems employ an application that functions on internet-ready devices like computers or smartphones (European Central Bank, 2016a). However, electronic money systems did not reach widespread acceptance by now, thus, proposals were discontinued after trials or remained on a theoretical level. They are nevertheless important, because Bitcoin and other cryptocurrencies are built upon their design primitives.

Mondex was a hardware-based electronic money system implemented as a smart card where monetary value was stored on and distributed with. Every smart card was equipped with P2P functionalities, which is why value could be directly exchanged between cards, without the need for intermediation through financial institutions. To this end a card-reading device was used as wallet which could be loaded with value. If the card of one user was used to transfer value onto the wallet, another user could put his or her card into it afterwards and withdraw the value. These transfers were final without requiring a third party and in addition also anonymous. Beside users transacting with Mondex smart cards, the system required a number of other actors responsible for fulfilling various functions. The originator issued Mondex value and sold the electronic money to banks responsible for its distribution. Merchants could deposit the electronic money back to the bank (Stalder, 2002).

eCash was the earliest proposal of software-based electronic money. The concept dates back to a publication of the year 1983 (Chaum, 1983) and was refined over time (Chaum *et al.*, 1990). The implementation was realized through the company Digicash, with the German Deutsche Bank as one of its best-known supporters from the financial industry (Strassel, 1996). The eCash software allowed users to locally store tokens cryptographically signed by issuing financial institutions. For this, blind signatures were used to render transactions untraceable by the issuer, while concurrently enabling this centralized party to verify their correctness. Transactions could thus be checked to involve no tokens that have already been spent and the respective transaction partners remained anonymous. After using them for a single transaction, tokens needed to be redeemed with the issuer and lost their value (Chaum, 1983).

Virtual Currency can be defined according the ECB as "a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money" (European Central Bank, 2015, p. 25). This understanding is consistent with a discussion note of the International Monetary Fund (2016), which complements the definition by the characteristic of virtual currencies to be denominated in their own unit of account. However, it differs from previous definitions of the ECB (European

Central Bank, 2012) and other authorities (e.g. Financial Action Task Force, 2014; European Banking Authority, 2014), emphasizing their fulfillment of the monetary functions as a medium of exchange, unit of account and store of value as essential classification criterion. Reflecting the evolving nature of virtual currencies, definitions will likely continue to be further adapted and refined.

The entity responsible for issuing and controlling a virtual currency is called operator. The term operator is deliberately chosen to delimit it from financial institution in the conventional sense, like central banks, credit institutions or e-money institutions. While it is controversially discussed to which extent virtual currencies meet economic and legal definitions of money, it is possible for the operator to determine the creation of this kind of money. Furthermore, there are both account- and token-based examples of EPSs transferring virtual currency. Given the diversity of different forms of virtual currencies, the following section is dedicated to a more detailed distinction according to a set of distinguishing features.

2.2.2 Virtual Currencies in Detail

Although the term is coined by Bitcoin in recent years, it was not the first actual realization of a virtual currency. Examples of virtual currencies existing before Bitcoin are prevalent in loyalty programs (e.g. frequent flyer miles, Payback Points), video games (e.g. World of Warcraft Gold, Linden Dollar), on online platforms (e.g. Facebook Credits) and other centralized schemes intended as instrument for the purchase of goods and services (e.g. E-Gold or Liberty Reserve). However, considerable differences are present in their level of convertibility and their model of operation. The section therefore categorizes virtual currencies by means of these dimensions as presented in Table 4.

2.2.2.1 Level of Convertibility

The level of convertibility of a virtual currency can have the attributes of **non-convertible** or **convertible** (European Central Bank, 2012). **Non-convertible** virtual currencies (or closed systems) operate exclusively in and are of value only within the boundaries of a virtual environment (International Monetary Fund, 2016). In EPSs transferring virtual currency, the exchange with other digital currencies (irrespective of whether they are notational money, electronic money or virtual currencies), fiat currencies and goods or services outside of the self-contained domain is not intended under the rules governing such systems. However, there is often a possibility for the existence of illegal markets used to facilitate these exchange, which violates the rules backing the EPS and does not constitute a convertibility of the respective virtual currency (Financial Action Task Force, 2014). Non-convertible virtual currencies are frequently encountered in online video games like World of Warcraft, where they are utilized as money in purposely closed economic systems.

Convertible virtual currencies (or open systems) are not restricted to a specific virtual environment and are of value in the real world too (International Monetary Fund, 2016). In EPSs transferring virtual currency, the exchange with other digital currencies, fiat currencies and goods or services in the real world is a desired feature of such systems. An example for a convertible virtual currency was Liberty Reserve, which is subsequently explained in more detail. The ECB further subdivides convertible virtual currencies into systems with a unidirectional flow and those with a bidirectional flow (European Central Bank, 2012). In unidirectional systems, the virtual currency is only convertible in one direction, which usually means there is a price in fiat currency for purchasing the virtual currency. Consequently, in bidirectional systems the virtual currency has to exchange rates to buy and sell it for fiat currency.

2.2.2.2 Model of Operation

The model of operation of virtual currencies can have the attributes of **centralized** or **decentralized** and also **hybrid models** are conceivable (International Monetary Fund, 2016). **Centralized** virtual currencies are characterized by the existence of a trusted third party responsible for issuing the virtual currency and determining the rules for using the EPS. This central operator accordingly exercises control over the money in circulation (Financial Action Task Force, 2014). The already mentioned virtual currencies used in online video games as well as Liberty Reserve are examples of centralized EPSs. In contrast, **decentralized** virtual currencies are not operated by a trusted third party, they are rather managed in a decentralized manner through the participants. Bitcoin and its successors, which are subsumed under the notion of cryptocurrencies, are decentralized systems. **Hybrid models** are employed by EPSs where some functions like the setting of general rules for the issuance of the virtual currency and the processing of transactions are determined by a central authority, while others such as the actual settlement is performed by the network of participants. An example for such a type of system is the global settlement network Ripple (International Monetary Fund, 2016).

		Model of Operation	
		Centralized	**Decentralized**
		↔ **Hybrid**	
Level of Convertibility	**Convertible** Unidirectional/ Bidirectional Flow	▪ Issued & controlled by Operator ▪ Exchangeable for other digital currencies ▪ e.g. Liberty Reserve, Facebook Credits	▪ Issued & controlled through participants ▪ Exchangeable for other digital currencies ▪ e.g. Bitcoin
	Non-Convertible	▪ Issued & controlled by operator ▪ Not exchangeable for other digital currencies ▪ e.g. World of Warcraft Gold	Not Existent

Table 4: Classification of Virtual Currencies[2]

2.2.3 Centralized Realizations of Virtual Currencies

In light of the increasing usage of the Internet for social interactions between individuals and business partners, an extensive dissemination of virtual communities can be observed. The ECB defines virtual communities as “a place within cyberspace where individuals interact and follow mutual goals” (European Central Bank, 2012, p. 11). Some of these virtual communities have, due to potential reductions in transaction costs or for practicability reasons, established their own virtual currencies. Social networks such as Facebook, Instagram or Twitter are widespread and constitute demonstrative examples for virtual communities. Besides social networks, there are virtual communities that represent complete virtual worlds like Second Life or World of Warcraft and whose virtual currencies are implemented for facilitating the exchange of virtual assets. What these virtual communities have in common is their centralized design, with an operator responsible for the virtual currency. This section introduces the former Facebook Credits as realization of a virtual currency in the eponymous social network and presents samples for convertible as well as non-convertible ingame currencies. Additionally, Liberty Reserve is described as virtual currency that got famous since it was misused for ML on a large scale. These centralized virtual currencies are elaborated on to provide a foundation for the better delimitation of decentralized representatives like Bitcoin, which is introduced in detail afterwards.

[2] Table 4 is adapted from Financial Action Task Force (2014)

2.2.3.1 Facebook Credits (Centralized / Convertible)

The virtual currency Facebook Credits existed from 2011 to 2013 and served as payment instrument for the purchase of paid content in Applications offered via the Facebook platform. The fundamental concept was to introduce a currency for digital products with global validity. A special feature of Facebook Credits was that they were worth the same in every country of the world. Therefore, they could be exchanged for 15 different conventional fiat currencies such as US-Dollar or Euro and were stored onto a central account (Facebook, 2011). For users of the social network this procedure was advantageous, since they no longer had to administrate individual accounts for every single application. In order to push the adoption of Facebook Credits, developers were obliged to integrate them into their applications.

30 percent of the turnovers generated through the use of the virtual currency were retained by Facebook, while the remaining 70 percent were debited to the developers of the applications that generated the revenues. The fraction of turnover retained by Facebook constituted de facto transaction costs, which let the virtual currency act as additional revenue source for Facebook. In this way, the introduction of Facebook Credits was intended to serve as second pillar for Facebook beside the trade of personal user data with advertisers. To illustrate the potential of this revenue stream, the turnover with social games on Facebook increased from 1,3 billion US-Dollar in 2010 to predicted 3,1 billion US-Dollar in 2014 (Statista, 2011).

The system was discontinued for the reason that most applications on Facebook already had their own virtual currencies integrated. Therefore, Facebook Credits became obsolete and the operator decided to launch a Local Currency Pricing, where digital content is displayed in the user’s local currencies (Facebook, 2012). This concept increases the flexibility regarding the price-setting, because it is possible to differentiate between different regions depending on their currency. The process running in the background has been preserved, since users still have to convert other types of digital currencies or fiat currencies into their Facebook equivalent.

The use case of Facebook Credits provides an example for a centralized, convertible virtual currency. Even though it could not be successfully applied in practice, the rationale behind the integration of virtual currencies by the operators of platforms like Facebook is illustrated. Amazon Coins, a recent example of a virtual currency operated by Amazon and useable for the purchase of applications and special items for applications on the Amazon Kindle, Android devices and the Amazon website, can be seen as evidence for the attractiveness of virtual currencies for online platform providers (Amazon, 2016).

2.2.3.2 InGame Currency (Centralized / Partial Convertible)

InGame currencies are present in virtual worlds within which individuals create their own avatars and where added value is generated on the basis of the personal performance in the particular world. Here, it is distinguished between two types of virtual currencies: implementations with convertibility into other digital currencies, fiat money or products and services and those that are not intended to be converted into value outside of the virtual community.

A convertible virtual currency is integrated into the online virtual world Second Life, where the developer Linden Lab implements a business model based on interactions of the virtual with the real world. Second Life is operated since 2003 and pursues the objective of providing a parallel universe, which allows users to interact, create valuable items and trade with each other. A comprehensive overview of all possibilities is accessible at the official website (Linden Lab, 2016). Beside individuals that participate for purely private reasons, companies, non-profit organizations and educational institutions are also encouraged to use Second Life as platform for self-presentation (Williams *et al.*, 2011). The virtual currency Linden Dollar was established to facilitate the trade in Second Life. Linden Dollars connect the virtual world with the normal economic cycle by being convertible into fiat currencies. There is one official exchange platform operated by Linden Lab, which is complemented by additional services offered through third party providers. It is theoretically possible to join Second Life without balances in the form of Linden Dollars, but only with restricted access to certain game elements like trading or the possession of specially created regions.

World of Warcraft from the developer Blizzard Entertainment is probably the most well-known representative of an online role playing game with a non-convertible virtual currency (Blizzard Entertainment, 2016). Users are required to pay a monthly fee in order to get access to World of Warcraft and earn so-called gold with their actions in the game world (e.g. by completing certain tasks or trade with other users). This gold, however, cannot be transferred into assets that are valuable in the real world in a legitimate way and Blizzard Entertainment takes measures against the operators of illegal exchanges (Blizzard Entertainment, 2015). The business model of World of Warcraft provides that the monthly fees are the sole revenue source and that the virtual currency acts as medium of exchange inside the virtual world only.

2.2.3.3 Liberty Reserve (Centralized / Convertible)

Liberty Reserve was a company based in Costa Rica and operated an EPS facilitating the transfer of virtual currency with the same name. The system has moved into the focus of a wider public with its forced closure in 2013 through governmental authorities. In concrete terms, Liberty Reserve was accused of having been misused as ML instrument for a sum of up to 6 billion Euro (Emiliy Flitter, 2013). The system behind Liberty Reserve functioned as follows:

The purchase of Liberty Reserve currency was settled by third party exchanges. Consequently, the operator did never receive any payments directly from its users. Instead exchanges acted as intermediaries who bought large contingents of the currency and sold them to the users afterwards. Liberty Reserve refrained from requiring any proof of identity from its users and allowed them to transfer the virtual currency effectively unlimited with transaction costs in the number of one percent. Furthermore, the system offered additional privacy protection by keeping the account data of the sender secretly for a small fee on top of the transaction costs (Liberty Reserve, 2016).

2.3 Technical Principles of Bitcoin

The subsequent section presents the components of Bitcoin, because it acts as role model for all subsequent realizations of DCSs, whose conceptual differences are regularly compared to and delimited from Bitcoin. Additionally, it constitutes the reference implementation for cryptocurrencies. The technical description of the components is used to derive the specific characteristics of Bitcoin, targeted to facilitate its application as EPS with an independent monetary unit. These characteristics provide the basis for the analysis of ML risks and to derive the general architecture of DCSs in the further course of this dissertation.

2.3.1 Design Philosophy

Bitcoin is an internet-based payment system with which two parties can carry out transactions over the internet. In addition, it is not tied to any fiat currency designated and issued by a central authority. Instead it possesses its own unit of account called bitcoin, while the respective value is determined by supply and demand and trust in the system. In general, for ascribing any value to money it needs to be scare (Böhme *et al.*, 2015; Becker *et al.*, 2013). In modern monetary systems, this scarcity is preserved by legal rules limiting the monetary supply controlled by central banks and commercial banks, creating a large portion of the actual money during the granting of new credits (Gischer *et al.*, 2012). The Bitcoin system takes a completely different approach by implementing an absolute limit on the money supply. Bitcoins are generated on a predetermined and thereby predictable growth path decreasing over time, leading to fixed number of total bitcoins that will ever be created. Therefore, the system is potentially qualified for being used as substitute for currency (e.g. Descôteaux, 2014; Velde, 2013; Yermack, 2013).

While there are virtual currencies around for some time (e.g. e-Gold, Liberty Reserve), the distinctive feature of Bitcoin is its decentralized nature, without a centralized repository and no single administration (Financial Action Task Force, 2014). The concept of Bitcoin is based on the use of advanced encryption techniques alias cryptography. An intuitive way to understand the underlying mechanisms is to think of a publicly accessible digital ledger book. The ledger records information about every accounts’ balance at a certain time and if somebody desires to transfer funds, it has to be broadcasted to and accepted by all participants of the system (Peck, 2012). Ultimately, all transactions ever conducted are stored in a replicated data structure providing read access for everyone who intends to view transaction-related data. The parties responsible for maintaining the correct functioning of the system – i.e. those who verify the validity of transactions according to certain rules - are incentivized by (voluntary) transaction fees and newly created bitcoins.

Figure 4 presents a schematic representation of the important elements of the Bitcoin system. The next subsections are organized according to these elements, to provide answers to the following questions and to derive the specific characteristics of Bitcoin:

1) How do users (individuals or organizations) authenticate themselves at the system and what qualifies a valid transaction?

   ➔ Execution of the Transaction Process

2) What are the constructs used to store transactions?

   ➔ Structure of the Blockchain

3) How is the validity of transactions verified?

   ➔ Maintaining the Blockchain

4) Who is responsible to verify the validity of transactions?

   ➔ Implementation of a Decentralized Network

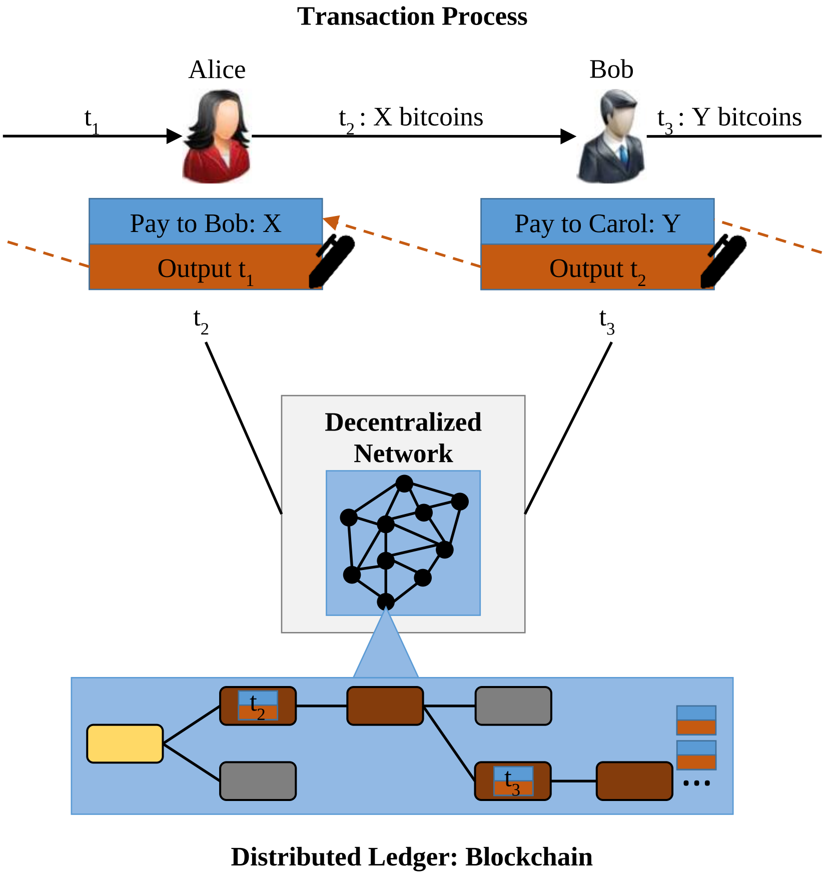


Figure 4: Schematic Representation of Important Elements of the Bitcoin System

2.3.2 Execution of the Transaction Process

To prevent an attacker from spending bitcoins by using the account number of a potential victim, the system relies on digital signatures to prove that the sender is the real owner of an account. Digital signatures can be interpreted as the digital equivalent of a handwritten signature or stamped seal. They are based on asymmetric encryption methods, which allow them to be issued by one party in order to facilitate the authentication of users (Müller *et al.*, 2003).

To this end, the digital signature must fulfill the property of being verifiable by the recipient of the message it is attached to and only the person who is identified by the respective signature is able to generate it. This also provides the characteristic of non-repudiation, which prevents the signer of a message from successfully denying he or she did so. Additionally, a valid signature should ensure that the integrity of the message sent is preserved and it is not altered in transmission (Katz and Lindell, 2015; Schneier, 1996).

Digital signatures employ asymmetric cryptography (which is also termed public-key cryptography) that uses pairs of keys: public keys *pk* which may be widely distributed and private keys *sk* which are kept secretly by the owner. The concept goes back to Diffie and Hellman (1976), who proposed an at that time new type of cryptographic systems distinguishing between encryption and decryption keys and extended previous works by Ralph Merke. Generally, a private key is used to digitally sign a message and everyone in possession of the associated public key can verify that the sender had access to the private key and is likely to be the legitimate owner. Besides digital signatures, the second major application field for asymmetric cryptography is public key encryption, where a message is encrypted with a public key in order to only qualify the owner of the corresponding private key to decrypt and, consequently, read the message. Compared to symmetric cryptography, where only one key is used to encrypt and decrypt data, the main advantage of asymmetric encryption is that it removes the need for secure channels to share a common secret key between eligible parties. Furthermore, only asymmetric encryption schemes can provide digital signatures that fulfill the property of non-repudiation (Müller *et al.*, 2003).

The security of asymmetric cryptography depends on the incomputability of the private key from the public key. Therefore, the derivation of the private key from the public key in a cryptosystem has be computationally infeasible. The encryption or decryption of messages must, however, be computationally easy when in possession the appropriate key. Additionally, the determination of the private key from a chosen plaintext attack must be computationally infeasible (Bishop, 2005, p. 113). The notion computationally infeasible relates to the idea of computational security, which is a weaker requirement than information-theoretic security. While the latter implies that it must be theoretically impossible to break a cryptographic scheme, the former allows cryptographic schemes to be breakable given enough time and effort in terms of computational resources. The amount of computing power and time necessary to break these encryption schemes needs to be sufficiently high, in order for these schemes to be useful for practical purposes (Katz and Lindell, 2015). Most systems actually used rely on cryptographic algorithms utilizing mathematical problems for which no efficient solutions exist right now (i.e. integer factorizations, discrete logarithms and elliptic curve relations). RSA is one of the first and most widespread ciphers and based on the difficulty of factoring the product of two large prime numbers (Rivest *et al.*, 1978). Other examples include various elliptic curve techniques (e.g. Malhotra *et al.*, 2007) or the Digital Signature Standard (DSS) incorporating the Digital Signature Algorithm (DSA) (*Digital Signature Standard (DSS)*, 2013).

A **Digital Signature Scheme** can be defined as a tuple of three probabilistic polynomial-time algorithms (generateKeys, Sign, Vrfy):

(pk, sk):= generateKeys(keysize) The key-generation algorithm **generateKeys** takes as input a keysize (also noted security parameter) and outputs a pair of keys (pk, sk). The public key *pk* is publicly distributed and used for verifying digital signatures. The private key *sk* remains secretly and is used to sign messages.

sig:= sign(sk, message) The signing algorithm takes a *message* and a private key *sk* as input. It outputs a signature *sig* for the *message* used as input with the private key *sk*.

isValid:= vrfy(pk, message, sig) The deterministic verification algorithm takes as input a public key *pk*, a *message* and a *signature*. It outputs a Boolean value, *isValid*, that will be **true** if *sig* a valid signature for the *message* used as input with the public key *pk*. If this is not the case it returns a **false**.

It is required that for every (pk, sk) every output by generateKeys(keysize) and every message in the appropriate underlying plaintext, two properties hold:

Vrfy(pk, message, sign(sk, message)) = = **true**

If a message is signed with a private key *sk* and the signature is later validated with the corresponding public key *pk* it must validate correctly.

Signatures are **existentially unforgeable**

Unforgeability requires that it is impossible for an attacker to create a signature for a message that is verified as valid, even though the message was not signed by the legitimate signer in the past.

Definition adapted from (Narayanan *et al.*, 2016, p. 37) and (Katz and Lindell, 2015, p. 402)

The general process of digital signature creation by the sender of a message and the verification of its correctness through the receiver afterwards is depicted in Figure 5. One disadvantage of using asymmetric encryption algorithms is their computationally complex nature, wherefore the message intended to be transferred is typically hashed before it is signed (e.g. Müller *et al.*, 2003). A hash function is designed to map data of any length to a data of a fixed predetermined length (Katz and Lindell, 2015). They take a message as input and the resulting output is referred to as a hash. An important characteristic of any cryptographic hash function is collision resistance, describing that it is nearly impossible to find two inputs that lead to the same output. Completely avoiding that different inputs yield the same output is theoretically not possible, but the probability needs to be sufficiently low in order for a function to be regarded as suitable hash function (Menezes *et al.*, 1997).

A **hash function** can be defined as a function h that at least meets the properties of:

Compression: h maps an input x of an arbitrary finite bitlength to an output $h(x)$ of a fixed bitlenghth n.

Ease of Computation: given h and input x it is easy to compute $h(x)$.

Definition adapted from (Menezes *et al.*, 1997, p. 322)

The hashed message is subsequently encrypted by the sender using his or her private key *sk* and forms the signature which is attached to the original message. Then the signed message is transmitted to the receiver who can verify the validity of the digital signature. For this the following procedure is employed:

1) The signature is decrypted with the public key *pk* associated to the private key *sk* of the sender
2) The message received from the sender is hashed
3) It is compared whether the decrypted signature is equal to the hashed message

If they are the same, the document is authentic and signed by the sender (assuming that no attacker gained unauthorized access to the private key), otherwise the message cannot be trusted.

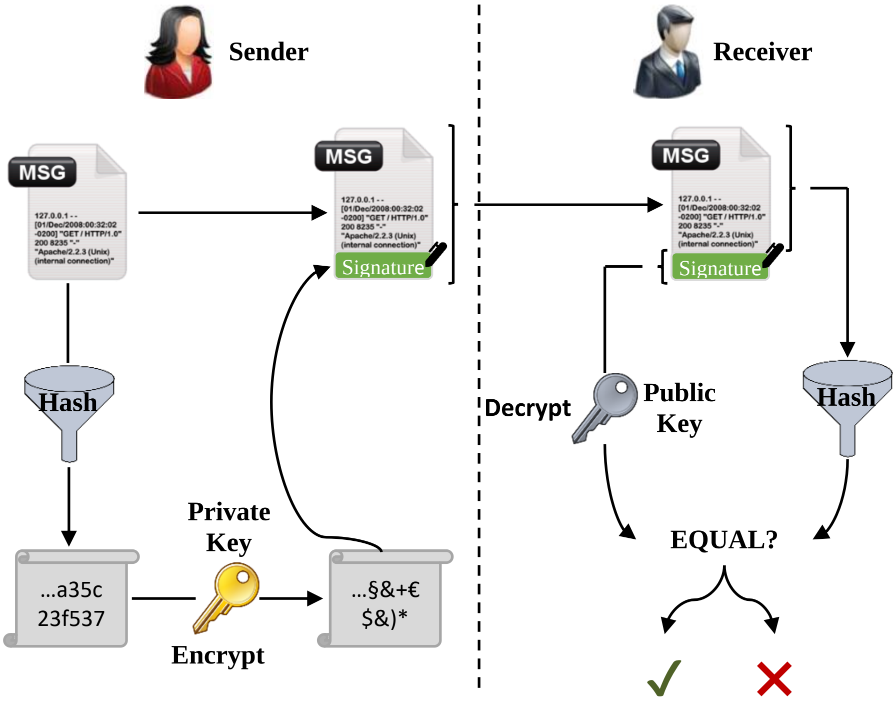


Figure 5: Process of Digital Signature Creation and Verification[3]

Having introduced the cryptographic primitives backing the Bitcoin system, it is now feasible to explain its transaction process. The Bitcoin whitepaper technically defines "electronic coins as chain of digital signatures" (Nakamoto, 2008, p. 2). The system concretely uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to sign transactions (e.g. Hankerson *et al.*, 2003;

[3] Figure 5 builds upon the findings in Schneier (1996)

Johnson *et al.*, 2001). It is a U.S. government standard and variant of the DSA using elliptic curves.

Accounts get tied to individuals via this asymmetric key encryption scheme. They are not really accounts in the traditional understanding, because funds "can be transferred and stored without using centralized storage or settlement institutions" (Dostov and Shust, 2014, p. 250). For the sake of simplicity, we call them accounts in the following, having in mind that they are in fact pairs of private and public keys. Account numbers are public keys *pk* and *ownership* is established by knowing the corresponding private key *sk*. Individuals can generate multiple of such key pairs, which allow them to handle more than one account simultaneously. To this end, individuals are not required to disclose personal information such as their names or addresses. Though each transaction is recorded in a public log, names of buyers and sellers are never revealed. The system works rather pseudonymous as long as the account number cannot be associated with the identity of the individual by making statements leaking personal identifying information (e.g. Möser *et al.*, 2013; Narayanan *et al.*, 2016).

Figure 6 provides a schematic representation of a transaction and depicts bitcoins as chain of digital signatures. As a result, an individual does not simply carry a bitcoin as the notion of coin suggests, instead one "participates in a publicly verifiable transaction" (Böhme *et al.*, 2015, p. 215). This transaction is showing how much bitcoins a receiver address received from a sender address. Consequently, one could follow the mental model of deriving the total number of bitcoins an individual can spend from the total number of bitcoins ever received from transactions, deducting the bitcoins transferred to other individuals in the past. However, this would require anyone verifying the validity of a transaction to check the whole history of transaction the individual was part of. In stark contrast to such an account-based model, transferring a bitcoin always includes a reference to the previous transaction of this coin. It is thus possible to validate the correctness of transactions, by simply verifying that the bitcoins used as input are an output of a previous transaction addressed to the sender (Narayanan *et al.*, 2016). The logic behind this can also be seen in the transaction process illustrated at the upper part of Figure 6. Each sender transfers funds to the receiver (transaction n) by signing a hash of the previous transaction (n-1) and the public key of the next owner with his or her private key. The hash algorithm actually used is SHA-256 and serves as globally unique transaction ID (Bonneau *et al.*, 2015). The digital signature confirms that the transaction was indeed initiated by the sender. The receiver verifies the validity of the signature with the sender's public key.

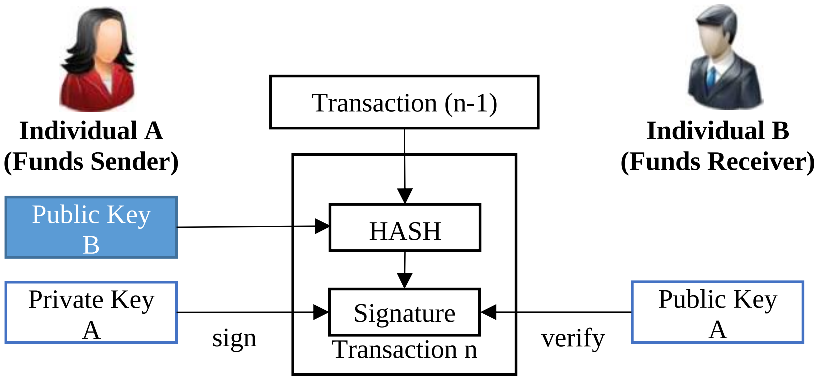


Figure 6: Schematic Representation of a Transaction[4]

In carrying out transactions in this way, a symbolic chain that is constantly extended by recent transactions emerges for all bitcoins in circulation (Nakamoto, 2008). This chain is intended to prevent *double-spending*, which is a common failure mode of digital cash schemes and describes the opportunity of spending one coin more than once. A solution to this problem in implementations prior to Bitcoin was the introduction of a trusted third party responsible for ensuring that a particular coin was not already spent before (e.g. Chaum, 1983; Clemons *et al.*, 1996). This trusted third party was the only instance that could issue new coins and check every transaction for its correctness. The intention behind Bitcoin is a payment system without requiring to trust any centralized authorities. Therefore, the Bitcoin system specifies that only the earliest transaction of a particular coin is the one that counts (Nakamoto, 2008). It nevertheless requires entities that verify the correctness of transactions and a data structure storing transactions. Before explaining these issues in more detail, Table 5 subsumes the implications of this section by presenting characteristics of the Bitcoin system inferred therefrom.

Property	Characteristic	Explanation
System Participation	Permissionless	Potential participants are granted public access to the system.
User Authentication	Pseudonymous	Participants are allowed to use pseudonymous authentication methods.

Table 5: Characteristics of Bitcoin Transactions

[4] Figure 6 is based on Nakamoto (2008)

2.3.3 Structure of the Blockchain

All Bitcoin transactions that ever took place are stored in a data structure that is widely replicated and commonly called blockchain (e.g. Duivestein *et al.*, 2015; EY, 2016). This solution has been chosen to facilitate the verification of correct transactions on the basis of transparency regarding past activities. From a very basic viewpoint, the Bitcoin blockchain can be understood as digital equivalent to a banking ledger containing unique identifiers for all accounts in the system and the corresponding balances denominated in bitcoins. Bitcoins are exchanged by modifications to this ledger, whereby the balance of the sending account drops in the same amount as the balance of the receiving account rises. However, even though a blockchain fulfills the same function like such an account-based ledger, technically it just keeps track of transactions instead of individual balances. It is a central element of the Bitcoin system, ensuring that all valid transactions ever conducted are securely stored.

A timestamp server is established with the purpose of listing transactions in chronological order, which serves as foundation to prevent *double-spending*. The general idea dates back to a proposal of Haber and Stornetta (Haber and Stornetta, 1991), who considered it for the digital timestamping of documents. The overarching objective of timestamping is to provide a proof when a particular piece of data was created and also to keep track of modifications prior to a specific point in time (Une, 2001). It is important in many other contexts beside digital money, like for companies who must prove that they were the first with an invention in order to receive a patent. Every timestamping mechanism needs to be secure in such a manner that it should be impossible – even for the creator – to change data once it has been timestamped (Narayanan *et al.*, 2016). Trusted timestamping processes are specified in the RFC 3161 (Adams *et al.*, 2001) and ANSI ASC X9.95 (ANSI, 2005) standard. These standards, however, describe procedures requiring a central authority issuing timestamps and validating their correctness. Bitcoin was the first system enabling the decentralized timestamping of data. Consequently, the blockchain serves as proof that a transaction existed (or did not exist) at a given time.

The Bitcoin blockchain continuously evolves by bundling previously unrecorded transactions into so-called blocks. The term is derived from the capability of the Bitcoin system to link every new block to its temporal predecessor as illustrated at the top of Figure 7. Note that there is a fork in the depicted blockchain, leading to temporarily competing versions of the truth. The occasional appearing of forks is an intended design feature, which will be discussed in detail later. The blocks entail, amongst other things, information regarding when a transaction between whom of which amount took place. Thus, a global and permanent transaction log develops, allowing the verification of transactions to depend on their correct specification and successful publishing in this log (Bonneau *et al.*, 2015). It constitutes the technical solution for the *double-spending* problem, by empowering the validators maintaining the system to comprehend the transaction history. Based on the temporal ordering of transactions in the blockchain, they decide which transaction occurred first in case of a conflict and is therefore valid according to the rules of the Bitcoin system (Nakamoto, 2008).

Hash pointers are used in order to link blocks with each other and realize the blockchain. They connect a block with its ancestor to tell where the value of that block was and take a hash of the data contained in the block. Therefore, they additionally enable to determine whether the data in a block was changed. So, it gets possible to add new blocks at the end of the blockchain and also detect modifications of earlier data. In this way, a blockchain achieves tamper-evidence as important property of the Bitcoin system. Tamper-evidence describes that the blockchain provides awareness if the integrity of data contained in previous blocks was compromised and effectively secures the system against attackers trying to alter transaction data. Imagine that an attacker modifies transaction data in any past block in a way, that he or she is the recipient of the involved bitcoins. This would change every hash pointer afterwards, which qualifies any entity validating the correctness of transactions to reject this version of the truth, by detecting the difference between the subsequent hash pointers of the modified blockchain and the respective hash pointers of the original blockchain (Narayanan *et al.*, 2016).

Beside the hash pointer to its predecessor, a block consists of a block header containing primarily data important for the actual process of maintaining the blockchain and a certain linkage of transaction data. Before elaborating on the actual process of maintaining the blockchain, the structure of transactions in the blockchain is explained. Aiming at compressing transactions to reduce the space required to store the whole blockchain, they are hashed in a data structure that draws on the concept of hash pointers and is called Merkle Tree. Generally, it is intended to facilitate the efficient verification of large amounts of data without compromising the security of the system (Merkle, 1988). As the name suggests and the lower part of Figure 7 illustrates, a Merkle Tree hashes the transactions of a block in form of a tree. To carry the analogy further, all branches contain the hash of their subsequent level and the leafs represent the transactions included in the particular block. The approach does away with the need to indefinitely store the whole set of transactions in every block by "stubbing of branches of the tree" (Nakamoto, 2008, p. 4). Only the root hash containing the hashes of all branches is mandated to prove the existence of a transaction in a specific block. If an attacker tries to modify an arbitrary transaction, this will change all hashes of the branch up to the root hash and reveal any fraud.

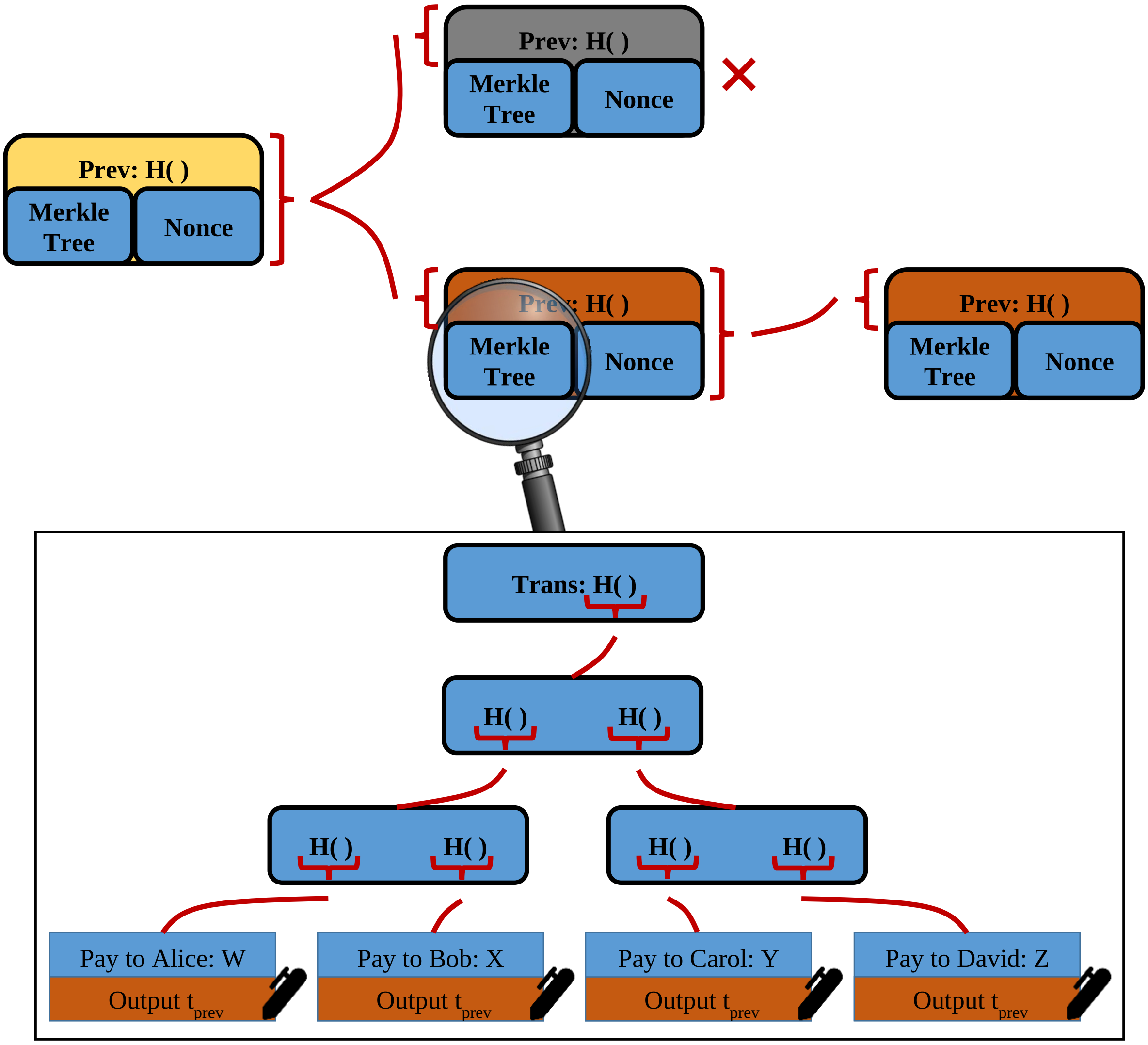


Figure 7: The Bitcoin Blockchain

The technical design of the blockchain facilitates a publicly accessible log including transactional data regarding all ever-conducted transactions. This transactional data provide information about the amount of bitcoins transferred when and between which addresses represented as public keys. Transparency is the foundation for validating transactions based on the history of the bitcoins involved. The record, however, is not restricted to participants of the decentralized network, instead everybody interested in the information can read the blockchain. This characteristic resulting from the structure of the blockchain is mentioned in Table 6.

Property	Characteristic	Explanation
Read Access	No Access Control	The blockchain provides transparency regarding all ever-conducted transactions for everybody who want to access this information.

Table 6: Characteristic of the Structure of the Blockchain

2.3.4 Maintaining the Blockchain

After having outlined the execution of the transaction process and the structure of the blockchain, the fundamentals components are present to describe how the system is actually maintained. The design of Bitcoin requires consensus between the entities using the system on the content of the blockchain. If any two parties transacting with each other have access to different versions of the blockchain, they are exposed to the risk of fraudulent behavior from the other party. A trusted third party is traditionally implemented in electronic cash schemes to solve this issue as already mentioned (e.g. Chircu *et al.*, 2000; Baddeley, 2004). Here, this party would collect all occurring transactions and publish them in signed blocks to guarantee their authenticity. One of the main inventions of the Bitcoin system is the abandonment of such a central authority, which need to be trusted not to prevent certain - from its perspective unwanted - transactions from being included into a block, not to go offline and not to intentionally spend bitcoins repeatedly (Bonneau *et al.*, 2015).

Instead, Bitcoin implements a consensus process for the decentralized and pseudonymous maintenance of the blockchain. It determines which block will be regarded as the next valid block that is periodically added to the chain. Therefore, the protocol is specified to ensure that a new block is published approximately every 10 minutes. The participants of the decentralized P2P network are the entities qualified to add new blocks and thereby operate the Bitcoin system. The process for consensus finding may be sketched out as follows: The challenge is to find a sequence of data that produces a certain pattern when a hash algorithm is applied to it. That process requires a lot computing power, and hence, the network participant (so-called miner) who finds a solution to this mathematical problem first is rewarded with transaction fees paid by the senders of funds and an amount of newly generated bitcoins, until a certain threshold specified in the protocol is reached. The term miner is adopted from the digging of precious metals, where resources are invested to gather scarce goods. The winning miner broadcasts a summary of all previously unrecorded transactions in a block to the other nodes in network, which validate and incorporate it into the blockchain and start working on the next block. In addition to preventing *double-spending* such a proof of work principle also establishes scarcity, an important property of every virtual currency (Becker *et al.*, 2013).

Mechanisms for decentralized consensus-building have long been studied in the area of distributed computing, with the objective that all parties eventually agree on a specific state or set of values of an IT system, even if some nodes of the network are compromised or fail (e.g. Chen *et al.*, 1992; Kim *et al.*, 2008). In a more technical terminology, nodes correspond to the entities participating on the consensus process for updating the blockchain. They intend to achieve a consensus on pending transactions getting grouped into blocks and subsequently added to the chain of prior blocks. Transactions are send to all P2P nodes of the Bitcoin system and they have to "agree on exactly which transactions were broadcast and the order in which these transactions happened" (Narayanan *et al.*, 2016, p. 52f.). At any given point in time, the nodes have stored the blockchain pooling transactions the P2P network has agreed upon and a set of transactions that still need to be validated.

The **Consensus Process of Bitcoin** must consider *n* nodes which all have transactions pending for validation. It is assumed that some of these nodes are potentially faulty or malicious. The associated **consensus protocol** has the following properties:

Agreement: It must terminate with all honest nodes in the network agreeing on the same block pooling the transactions

Generation: The block must have been generated by an honest node

Definition applied to Bitcoin from (Narayanan *et al.*, 2016, p. 53)

The process of how nodes agree on the following block is straightforward: The Bitcoin system uses a computational puzzle to determine the node that is empowered to publish the subsequent block of transactions. The Hashcash Proof-of-Work (POW) algorithm, which was already proposed in 1997 as denial-of-service countermeasure against the systematic abuse of applications such as e-mail, is used for the consensus mechanism of the Bitcoin system (Back, 2002). For this, nodes have to expend computing power to find a nonce value that, "when hashed with additional fields (i.e., the Merkle hash of all valid and received transactions, the hash of the previous block, and a timestamp), the result is below a given target value" (Karame *et al.*, 2012, p. 907). In general, the problem for which the POW provides a solution must be hard to solve but easy to verify (Kroll *et al.*, 2013). Recall Figure 7, which illustrates the merkle tree used to calculate the merkle hash and the block header Prev: H( ) containing the hash of the previous block and a timestamp. These values are all invariable and depend on the particular block. Therefore, a nonce "a number used only once" is included into the hash as an arbitrary number the node is free to choose. Specifically, the POW describes the required computing power nodes need to invest in trying different random nonces until a solution is found, where the SHA-256 hash is less than a target value specified by the Bitcoin system (Nakamoto, 2008). The puzzle is generally explained as searching for a hash beginning with a predetermined number of consecutive zero bits. Any node that comes up with a solution that meets this requirement is authorized to publish the next block.

This leads to a competition between the nodes in the P2P network on who finds a matching hash first. Consequently, the probability of success increases proportionally with the individual available computing power (Bonneau *et al.*, 2015). If the published block is considered as valid from the nodes, they start working on the next block. Additionally, the node that has published the correct block is awarded with a defined amount of newly created bitcoins and (voluntary) transaction fees paid by the senders of transactions included. An increase in the overall computing capacity of the network tends to reduce the average period of time for finding a new block (this also holds true in the opposite direction, where a decrease in the overall computing capacity of the network increases the average period of time for finding a new block). In order to ensure that a block is found on average all 10 minutes, the protocol automatically adjusts the difficulty of the POW by varying the target value. It is important to note, that this 10 minutes are an intentional design decision taken by the Bitcoin developers (Barber *et al.*, 2012). Figure 8 sumps up the function of the POW used in the Bitcoin system.

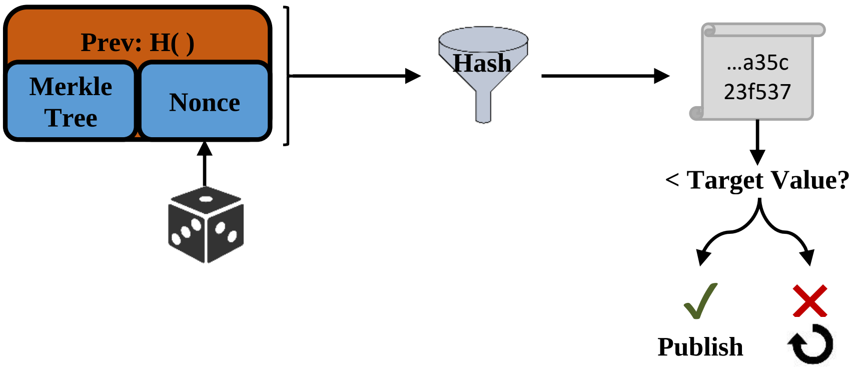


Figure 8: Functioning of the Proof-of-Work

As shortly mentioned previously in section 2.3.3, sometimes a temporal fork in the blockchain occurs and is also a desirable feature of Bitcoin. With knowledge of how the Bitcoin system is actually maintained, the reasons for this can be explained. The blockchain forks when two nodes solve the POW for a block roughly at the same time and concurrently publish a correct block. This blocks may differ in the transactions included, since not all transactions reach all nodes timely. Lags or disconnected nodes in the P2P architecture may prevent transactions from propagating across the whole network (Narayanan *et al.*, 2016). One of the blocks will eventually be discarded and is called an orphan block. It is therefore advised to wait for at least six consecutive blocks until considering a transaction as finalized (Böhme *et al.*, 2015). Otherwise a risk arises that the same bitcoins are double-spend to a different address in a transaction listed in another branch of the blockchain (Karame *et al.*, 2012). The process of discarding is achieved based on a simple rule: The correct blockchain all nodes finally follow is the longest one. It is determined by the combined computational difficulty of the blocks from which it is composed. This ensures that the blockchain dynamically resolves forks without any intervention of a single authority deciding about the branch to continue (Franco, 2015).

The structure of the consensus process ensures that all transactions according to the rules specified in the protocol are added to the Bitcoin blockchain and that it is computational infeasible to alter transactions after waiting for enough consecutive blocks. Consequently, it is not possible for a designated authority – for instance a stakeholder of the system or governmental bodies - to modify transactions or prevent transactions from being processed to impose a particular set of transactions to be included into the ledger. This property is called censorship resistance (e.g. Perng *et al.*, 2005). One of the core characteristics of Bitcoin is the use of pseudonyms, whereby no persistent identified identities are established. It conforms to the philosophy of a permissionless system offering public access for anyone who intends to carry out transactions with bitcoins. However, a system without an entity certifying identities of participants allows the creation of an unlimited number of nodes. Such systems face security threats from adversaries who present multiple identities. Several identities can correspond to a single attacker, which is represented by the nodes he or she creates to compromise a substantial fraction of the system. Implementing a consensus mechanism based on POW, as Bitcoin does, is an approach for avoiding these Sybil attacks (Douceur, 2002). It enables the relinquishment of access controls for the consensus participation, by binding the probability for publishing a block on the expenditure of economic resources. Therefore, the number of identities an attacker possesses is irrelevant for the chances to solve the computational puzzle. This secures the system, as long as no attacker controls a disproportionate share of the available network capacity. The characteristics of the consensus process are listed in Table 7.

Property	**Characteristic**	**Explanation**
Censorship Resistance	Fulfilled	The impossibility for third parties to impose a particular set of transactions to be included into the ledger.
Consensus Mechanism	Proof-of-Work	Computational puzzle based on the expenditure of resources, which makes the publisher of the next block unpredictable.
Consensus Participation	Unrestricted	Every entity is free to participate on the consensus process without restrictions.

Table 7: Characteristics of the Consensus Process

2.3.5 Implementation of a Decentralized Network

The decentralized P2P network is responsible for maintaining the blockchain in order to avoid any centralized control. Continuous updating of this transaction log keeps the Bitcoin system running and can be regarded as a public good (Böhme *et al.*, 2015). A public good is defined as non-excludable and non-rivalrous, which at least partly applies to Bitcoin in its present design (e.g. Mankiw, 2016). Due to its permissionless nature, it is not feasible to exclude individuals from using the system. Furthermore, there is no rivalry in consumption as long as the demand for transaction does not exceed the processing capabilities of the system. An ongoing debate about increasing the maximum block size – and by that allowing more transactions to be included and processed simultaneously – demonstrates the possibility for rivalry when Bitcoin's popularity keeps growing (e.g. Popper, 2016). If information provided by the blockchain are interpreted as valuable separately, their public visibility can also be understood as a public good (Möser and Böhme, 2015). To compensate for the computing power expended while participating on the consensus process, economic incentives are provided in the form of bitcoins granted to the successful publisher of a block and currently voluntary transaction fees. But not only the operation of the system depends on the provision of incentives, the security warranted by the POW is based on an economic rationale too. The compensation in form of valuable bitcoins secures the network through two channels. It firstly encourages consensus participants to contribute computing power raising the overall network capacity. Thus, the threshold value for controlling a sufficiently large fraction of the system to centralize the decision power increases (e.g. Paul *et al.*, 2014; Eyal and Sirer, 2014). It secondly ensures that honest behavior is the most advantageous alternative for every individual (e.g. Houy, 2014). Because the technical consensus mechanism only works as intended when it provides the right incentives for nodes in the consensus process, the economic aspects of how to implement a decentralized network preserving the rules specified by the protocol are explained in the rest of this section.

Both incentive mechanisms implemented in Bitcoin, the block reward as well as the transaction fees, make use of the native token which constitutes the virtual currency bitcoins. Having a token worth of value permanently integrated into the system is thus imperative for ensuring that honest behavior is incentive-compatible for all users. Currently, every node publishing a correct block that gets finally added to the blockchain is rewarded with a fixed amount of bitcoins. Each block therefore contains a so-called coinbase transaction with no inputs, which specifies an address belonging to the successful miner. This transaction occurs on average every 10 minutes when a new block is added and provides a channel through which bitcoins are initially distributed without relying on a centralized issuer. The number of bitcoins created through that process is not static, instead it is halved every 210.000 blocks, corresponding to roughly every four years. As a result, the number of total bitcoins that will ever be issued approaches towards a value of 21 million approximately reached in 2140 (bitcoinwiki, 2016). Or in more economic terms, the money creation is bound to a fixed path and preserves the inherently deflationary character of bitcoins. Transaction fees are intended to substitute for the constantly decreasing amount of newly created bitcoins and need to be sufficiently high in order to incentivize consensus participants in the future. They are completely voluntary right now and get determined by the difference between the value of transaction outputs and transaction inputs. The node who solves the POW is rewarded with all fees of the transactions contained in the respective block. Paying fees currently provides the advantage for a transaction to be privileged compared to those with lower or even no fees in terms of a higher chance of being included into a block immediately. How the practices and rules regarding transaction fees will evolve is not yet foreseeable, because it is amongst other things dependent on the future valuation of bitcoins (e.g. Houy, 2014; Möser and Böhme, 2015). What can be stated is it seems highly probable that transaction fees will be required in the future (e.g. Kaskaloglu, 2014; Kroll *et al.*, 2013).

The **Economics of the Consensus Process** focus on how financial incentives for rational individuals that already participate or intend to participate in the consensus building are provided.

A representative individual faces the decision whether he or she should invest computing power in order to act as a node in the decentralized network or not. The provision of additional computing power is beneficial as long the following statement is true:

block reward + transaction fees > hardware investments + operative costs

The **overall compensation** an individual obtains consists of the fixed block reward as well as the variable transaction fees. Since the consensus process is competitive, the overall reward is an expected value with a probability of publishing a block depending on the fraction of the computing power of the whole network in possession of the individual. The **overall costs** are the sum of the fixed costs in terms of hardware investments and the variable operative costs. The operative costs include expenditures such as for electricity, cooling or the opportunity costs for using computing power to solve the POW instead of utilizing it for other economically advantageous purposes. When the overall compensation is greater than the overall costs, additional computing power will be added up to a level where both sides of the equation match each other in an equilibrium. Comparing the compensation with the costs, however, is challenging as long as bitcoins are not widely accepted as a payment instrument and have to be converted into conventional currencies with fluctuating exchange rates. Presently, the costs are usually nominated in conventional currencies, while the compensation is in the form of bitcoins (Narayanan *et al.*, 2016).

After having joined the network as an active node, the representative individual has to decide whether he or she acts honest or tries to attack the system. Acting honest is defined as choosing a strategy in line with the rules of the Bitcoin system, while an attack implies special personal benefits or putting other individuals in a worse position than they normally would be. A rational individual chooses a strategy in line with the rules as long as:

costs attack > gains attack

or

gains intended use > gains attack

The economic rationale assumes that if a sufficiently high level of costs in terms of computing power is required to perform a successful attack, it induces rational individuals to behave honest. This may be a level of costs higher than the expected gains from an attack, or that the intended use of the system is the most profitable alternative. An individual is able to exercise control over the consensus mechanism, if he or she controls the majority of the computing power of the network and is capable of determining the longest chain of blocks. It is often referred to in the literature as the 51 percent attack (e.g. Kroll *et al.*, 2013). The **costs for this kind of attack** are the expenses for the required hardware and the associated operative costs. When these costs are higher than the gains resulting from an attack, a rational individual will hesitate from attacking the system.

To identify the possible **gains from an attack**, it needs to be examined what an attacker is capable of achieving at all. As a first remark, the attacker cannot steal bitcoins from an address he is not in possession of the private key, since they are cryptographically secured. Honest nodes in the network will simply not accept blocks including transactions involving the transfer of bitcoins from an address without knowledge of the associated private key as validate. This also affects all subsequent transactions involving such illicitly acquired bitcoins, which are therefore worthless for the attacker. The same holds true for increasing the block reward, which would not be in line with the rules specified in the protocol and lead to a rejection of the respective blocks (Narayanan *et al.*, 2016). What is feasible with a majority of computing power is double-spending, by including a transaction into a valid block and recomputing the block as well as all subsequent blocks afterwards. The rest of the network will finally accept the recomputed blockchain when it gets the longest chain. Having already received goods and services in exchange for the alleged payment, this results in a payoff for the attacker (Kroll *et al.*, 2013).

Even in a situation where the gains from an attack outweigh the costs, a rational attacker must take the gains from an intended use of the system into account. The **gains from an intended use** describe pecuniary advantages resulting from a behavior in conformance with the rules of Bitcoin. An individual that controls a large fraction of the network has a high probability of publishing a block and obtaining the overall compensation. This may incentivize honest behavior if the compensation is more beneficial than the gains from an attack. Furthermore, a potential attacker has to consider the medium- and long-term consequences of compromising the confidence in and reputation of Bitcoin. Other individuals would hesitate from using such

> an unreliable system, resulting in a reduced demand and, consequently, value of bitcoins. In the most extreme scenario, bitcoins would end up being completely worthless.

It can be seen from the statements above that the rules specified in the Bitcoin protocol are enforced by the participants of the decentralized network. Assuming the consensus process works correctly, only transactions according to these common criteria are processed and included into the blockchain. Major changes to the system, like increases in the allowed block size, adjustments of the block rewards or mandatory transaction fees, can only become effective if a large fraction of the network decides to incorporate them. This is technically realized by a fork, which will become the largest chain, if enough nodes decide to expend computing power to continue it instead of the branch operating according old specifications (Nakamoto, 2008). This has severe consequences for the governance structure of Bitcoin. It is, at least theoretically, a democratic process of proposing changes to the community, whose members vote is weighted according to their available computing power. The economics of the consensus process rely on bitcoins compensating for the computing power required to operate the blockchain and secure the system. Therefore, beside that the purpose of Bitcoin is the exchange of valuable tokens exchangeable for conventional currency or goods and services, the native token is also imperative for the correct functioning of the system. These findings are presented as specific characteristics in Table 8.

Property	Characteristic	Explanation
Governance	Community-Driven	The system is governed by a community enforcing the rules specified in the protocol. Rules can only be changed through a consensus decision of the majority of the network.
Native Token	Imperative	A native token firmly integrated into the system that is of value be exchanged for conventional currency or pay for goods and services.

Table 8: Characteristics Regarding the Decentralized Network

2.4 Comparing Bitcoin with an Alternative Cryptocurrency

The technical explanations regarding DCSs which utilize a distributed ledger as technical infrastructure for the exchange of virtual currency remained limited to Bitcoin so far. This section shortly introduces Litecoin as alternative to Bitcoin and illustrates how they can be differentiated from each other. The comparison is carried out by contrasting the respective systems on a technical level and deriving the relevant economic implications. Table 9 gives an overview regarding the Bitcoin distributed ledger examined in the preceding paragraph, which is used as reference for the following explanations.

Distributed Ledger	Blockchain as a public log that records entire activities in the Bitcoin network, including: • All blocks ever created (whole transaction history) • First block: genesis block (generated: 03. Jan. 2009) • Each block provides a hash pointer to its predecessor • Blocks contain transactions describing the state of the system • Total number of 21 million bitcoins (Bonneau *et al.*, 2015)
Block	A block is created approximately every 10 minutes Each block contains: ▪ Unique block ID in form of a hash ▪ Block ID of the preceding block in form of a hash ▪ Timestamp when the block was created ▪ Difficulty of the Proof-of-Work ▪ Hashcash Proof-of-Work: Finding a nonce so that the corresponding hash is below a target value ▪ Transactions in the data structure of a Merkle Tree (Antonopoulos, 2015)
Bitcoin Address	▪ Bitcoin address is the hash of a public key with 26-35 alphanumeric characters ▪ Identification of Bitcoin users (users are capable of creating indefinite addresses) ➢ Allows for pseudonymous transactions (Narayanan *et al.*, 2016)

Table 9: Overview of the Bitcoin Distributed Ledger

Litecoin was launched in 2011 and is one of the most successful cryptocurrencies apart from Bitcoin based on its market capitalization (CoinMarketCap, 2016). The market capitalization normally describes a method for estimating the value of a publicly traded company by multiplying the number of total shares with the associated price (Financial Times, 2016). In order to calculate the market capitalization for a cryptocurrency, the number of units of the currency in circulation is multiplied with its exchange value and the result is an estimate of the overall value. The differences of Litecoin compared to Bitcoin are listed in Table 10.

On the one hand, Litecoin establishes shorter time intervals by changing some of the parameters underlying the system. The difficulty for the block creation is therefore adjusted so that a new block arrives at about 2,5 minutes on average. The overall litecoins issued are simultaneously increased to a maximum of 84 million, which is four times as much as the maximum limit of bitcoins and is also reached in 2140. On the other hand, Litecoin introduces Scrypt as an alternative POW mining algorithm to hashcash implemented in Bitcoin (Percival and Josefsson, 2012). Scrypt is a memory-hard algorithm initially designed for protecting hashed passwords against brute force attacks. So, the process of maintaining the blockchain remains the same as in Bitcoin, with the difference that Scrypt replaces SHA-256. Memory-hard in this context means, it is way more efficient to compute values filling a buffer of Random Access Memory (RAM) than refraining from doing so. The reason for choosing Scrypt can be explained by the way the hardware requirements to successfully participate in Bitcoin mining evolved. SHA-256 is based on calculations whose computing speed can be tremendously accelerated with specialized hardware enabling their parallel processing. Due to this, the probability of publishing a block tended to approach zero without investments into Application-Specific Integrated Circuits (ASICs) specialized for the mining of bitcoins (Antonopoulos, 2015). The resulting increase in the difficulty of the block creation leads to a concentration of computing capacity to a few parties which are able to leverage economies of scale.

This ongoing development has fallen short of the original vision behind Bitcoin, because it fosters the centralization of power to those with the largest computing capacity under control (Gervais *et al.*, 2014). Implementing the Scrypt algorithm had the intention to break the resulting self-reinforcing cycle of mining remaining only profitable for increasingly large companies equipped with specialized hardware. When Litecoin was introduced no ASICs for memory-hard puzzles were available, which rendered it possible to participate on the consensus process with general-purpose hardware. However, ASICs for DCSs based on Scrypt have been deployed in the meantime, leading to a similar trajection like Bitcoin has already experienced.

Distributed Ledger	Blockchain as a public log that records entire activities in the Litecoin network, including: • First block: genesis block (generated: 13. Oct. 2011) • Total number of 84 million litecoins (Antonopoulos, 2015)
Block	A block is created approximately every 2,5 minutes ▪ Scrypt Proof-of-Work: memory-hard mining puzzle for finding a nonce (Percival and Josefsson, 2012) ▪ Difficulty for the block creation is adapted more quickly than in the Bitcoin system (Narayanan *et al.*, 2016)
Litecoin Address	▪ Litecoin address is the hash of a public key with 33 alphanumeric characters ▪ Always begins with the letter L

Table 10: Overview of the Litecoin Distributed Ledger

2.5 Concluding Remarks

The preceding chapter addressed this dissertation's research question *RQ1: What are the specific characteristics of the Bitcoin system?* For this purpose, the chapter firstly described its intended application as a decentralized EPS, preventing the need for financial intermediaries involved in the transaction process. As this scenario requires an asset which is issued and fluctuates independent of any centralized governmental control, monetary aspects also had to be considered. Thereby, a link between an asset serving as money and the respective payment system facilitating its exchange was established. The investigation in form of a classification delimited this kind of systems from conventional centralized EPSs according to their convertibility and the decentralized model of operation. Thereby, the basis was set for the subsequent identification of Bitcoin's specific characteristics, which enable a decentralized payment system based on a distributed ledger providing transparency regarding transactions processed.

The specific characteristics were derived from a technical description of the Bitcoin architecture. Therefore, the overall system was divided into its important elements: transaction process, decentralized network and the distributed ledger in form of a blockchain. The actual characteristics result from the design of these elements and specify the properties of Bitcoin and other cryptocurrencies based on its reference implementation. Overall, the set consists of 8 characteristics determining the system participation, user authentication, consensus participation, censorship resistance, read access, governance, consensus mechanism and native token. By means of these characteristics, it is possible to deduce the architecture of such DCSs, but also to identify economic opportunities and risks resulting from this design approach.

In the following chapter, a risk analysis of cryptocurrencies based on the Bitcoin design is conducted. As already been illustrated, cryptocurrencies are not fitting into existing classifications of EPSs. This is due to their decentralized model of operation together with convertibility into other currencies and real world goods or services. Therefore, their emergence leads to new challenges in the context of ML utilizing financial instruments. Since ML has severe consequences on the economic performance of the society as a whole, these risks have to be considered when developing DCSs. Consequently, factors will be identified that influence the economic incentives of criminal individuals to misuse cryptocurrencies for ML, based on a conceptualization of how these incentives are provided. However, the actual factors are resulting from the specific characteristics of the Bitcoin design approach. The following chapter further presents the important actors in the ecosystem of cryptocurrencies, because they are involved in ML schemes utilizing cryptocurrencies.

3 Risk Analysis of Cryptocurrencies: Money Laundering

The previous chapter introduced bitcoins as digital representation of money. To this end the concept of money was examined theoretically and it was elaborated on the intrinsical link between any asset used as money and the corresponding payment system enabling its exchange. Accordingly, different types of EPSs for the transfer of digital money were characterized based on the type of money supported. It was demonstrated that decentralized systems implementing an exchange medium convertible into conventional currencies and assets worth of value in the real world constitute a completely new category of payment systems. In order to derive the specific characteristics of these cryptocurrencies, Bitcoin was technically explained as their foremost representative. However, every system transferring valuable assets is potentially vulnerable for being misused as instrument for criminal purposes such as ML. This risks are even exacerbated when the system is decentralized and facilitates the international transferability of funds over the Internet, like it is the case with cryptocurrencies. Therefore, the present chapter of this dissertation conducts an economic analysis of cryptocurrency backed ML to analyze risks emerging from the specific characteristics of systems like Bitcoin. Addressing *RQ2*, this analysis provides insights for the architecture and possible applications for DCSs in general.

Starting point is the observation that the increasing popularity of cryptocurrencies attracts the attention of practitioners and scholars particularly because of raising AML concerns. Consequently, work has already been conducted in this area, mainly focusing on implications on AML efforts. However, it is argued that the potential benefits for criminal individuals are an important, yet neglected factor in the dissemination of cryptocurrencies as ML instrument. First of all, cryptocurrencies are represented as digital ecosystems in order to explain the relevant actors that emerged in the periphery of such systems. It is important to have an understanding about these entities, since they are either deliberately or unknowingly involved in the process of ML. Then, a conceptualization is developed via which channels economic incentives are provided to use a monetary instrument for ML[5]. In particular, it is focused on the ML process

[5] The following includes and extends Brenig *et al.* (2015)

and AML controls. In light of their growing spread, cryptocurrencies are examined as a concrete example. Therefore, an analysis considering both contextual and transactional factors influencing the incentives of criminals is shown. It addresses the question whether, and if so why, cryptocurrencies represent a risk of being misused for ML. The identified factors are then applied to set of practical scenarios in order to illustrate their relevance in the respective contexts. The chapter closes with an overview on actual technological developments and regulatory approaches that may potentially mitigate the risks by influencing the incentives provided by the factors.

3.1 Cryptocurrencies as Digital Ecosystems

By conceptualizing cryptocurrencies as digital ecosystems, the relevant actors emerging around them can be introduced in a structured form. These actors are integral part of interaction patterns involving the transfer of cryptocurrencies and, consequently, have to be taken into account when analyzing the suitability of cryptocurrencies for ML. Before presenting the individual actors, it must be clear how an ecosystem is constituted from an economist's perspective and why cryptocurrencies can be understood as such. The general idea of viewing companies as part of a business ecosystem for strategic planning dates back to a Harvard Business Review article from James F. Moore (Moore, 1993). He illustrates the concept, by using a number of ecological metaphors, to describe that companies in a business ecosystem "coevolve capabilities around a new innovation: they work cooperatively and competitively to support new products, satisfy customer needs, and eventually incorporate the next round of innovations" (Moore, 1993, p. 76). This definition emphasizes on the aspects of competition and cooperation between the actors within the ecosystems, with the overarching objective of value creation (Walley, 2007). It builds upon the assumption that a holistic view is more suitable to describe the behavior of a complex interconnected system, instead of independently examining its single elements. The term digital ecosystem is related to a subset of business ecosystems primarily relying on IT to generate value in a self-organizing, scalable and sustainable community (Dini *et al.*, 2005). Holdgaard (2014) already characterized cryptocurrencies as digital ecosystems using Bitcoin as an example.

Existing literature in the field of business and digital ecosystems suggests their classification into three different levels: micro-level, meso-level and macro-level (e.g. Frow *et al.*, 2014; Henningsson and Hedman, 2014). This is due to the reason that the extent of cooperation between the different actors is heterogeneous, which results in groupings within ecosystems. In the following, the three levels are explained and related to cryptocurrencies:

Micro-Level: On this level, the competition between individual entities is at the center of considerations. Every entity tries to gain advantages compared to the others by creating more value than them (Brandenburger and Stuart, 1996). It describes the companies offering applications and services as well as the end-users in possession of units of a specific cryptocurrency. There is competition between companies offering similar applications and services, where every single company intends to achieve a leading position through innovation.

Meso-Level: At the meso-level, the individual entities jointly create value through cooperation. In order to develop innovations in a digital environment, companies are reliant on external changes. The innovative capability of a company is, consequently, depending on the concurrent advancement of associated companies (Adner and Kapoor, 2010). This can lead to closer relationships between entities within the ecosystem. These networks are called clusters and compete with other clusters. The commonly used technologies constitute decisive criteria regarding which cluster obtains a competitive advantage. However, besides competition there is also system-wide cooperation involving all actors (and therefore also clusters), since they are interested in the continuance of the ecosystem as a whole (Henningsson and Hedman, 2014). The meso-level characterizes cooperation between companies offering complementary applications and services for a cryptocurrency.

Macro-Level: The macro-level considers all actors in their entirety and accordingly forms the overall ecosystem. Every ecosystem competes with other ecosystems on an institutional and industrial layer, whereby the competition results from the innovations provided by the underlying technology (Henningsson and Hedman, 2014). Moreover, the ecosystem consists of dynamic entities, with the ability to continuously adapt to an ever-changing environment. For all entities on the micro-, meso- and macro-level, this is an ongoing process, whereby changes of a significant entity lead to dynamic adaptions of all other entities (Selander *et al.*, 2010). Competing ecosystems for cryptocurrencies might be further cryptocurrencies, but also already established payment systems and potentially even other existing currencies.

3.1.1 Central Actors

Originating from the generic structure of digital ecosystems and after having classified cryptocurrencies into this model, central actors are briefly explained on the micro-level subsequently. The list presented below is not necessarily exhaustive, because the premature and dynamic nature of the technology leads ecosystems that are constantly evolving, with novel actors potentially emerging to satisfy changing needs of users. Figure 9 sketches the ecosystem of an arbitrary cryptocurrency, whereby the importance of different actors may differ and some of them may even not be present. Nonetheless, the general model can be applied to any existing cryptocurrency.

The macro-level consists of the underlying technology, which is a distributed ledger whose correctness is ensured by providing adequate economic incentives to a decentralized network responsible for verifying transactions, as well as the different actors and their interaction patterns. On this level, the respective system competes with other systems performing the same functions. For the purpose of clarity, Figure 9 abstains from presenting any clustering of actors and, hence, the meso-level is omitted. However, it is important to keep in mind that cooperation may lead to alliances between various actors.

External influences have an effect on the ecosystem by affecting its conditions and the strategic decisions of the actors within the system. The whole ecosystem needs to possess capabilities to adapt when challenged with external constraints set by, for instance, regulations in order to persist over time (Holland, 1995). Investors provide capital for the involved actors and promote growth and innovation in this way. They facilitate the invention of additional services and allows for completely new business models, which increases the overall attractiveness of the ecosystem. In order to preserve governmental interests, national as well as supranational institutions act as regulatory bodies. Every regulatory intervention ultimately has an effect on the transaction costs, which effects the economic decisions of the actors within the cryptocurrency ecosystem and potentially also leads to inefficiencies (e.g. Renda *et al.*, 2013; Whynes and Bowles, 1981). Regulation may include extensive customer identification procedures, ongoing monitoring of accounts and transactions or even the prohibition of a cryptocurrency in certain jurisdictions. Ecuador is one of the countries that banned Bitcoin and other virtual currencies in favor of a governmental-backed own implementation (Dennehy, 2015). Simultaneously, there is technological competition with other systems enabling the transfer of value. These include already established EPSs, but also future developments that conceivably substitute for cryptocurrencies have to be considered. The same holds true for alternative cryptocurrencies as direct competitors with actors potentially present in several ecosystems, which due to the similarity of the technology and the associated low level of switching costs (Shapiro and Varian, 1999). The conventional financial sector fulfills a special role, since its boundaries with the ecosystems of cryptocurrencies are becoming increasingly blurry. Some actors within cryptocurrency ecosystems interface with the financial sector by offering services to exchange cryptocurrencies for conventional financial products (Möser *et al.*, 2014). Furthermore, financial institutions are also more and engaged as actors in the respective ecosystems or develop own implementations. One of the latest example is the Utility Settlement Coin, which is a project from Deutsche Bank, UBS, Santander and BNY Mellon (Kannenberg, 2016). Another actor worth mentioning are attackers aiming at compromising the system by disrupting its correct functioning. Such attacks further decrease the reputation of a system, whereby a negative reputation discourages companies as well as end-users (potentially) taking part in the ecosystem (Olshavsky and Spreng, 1996; Apreda *et al.*, 2013).

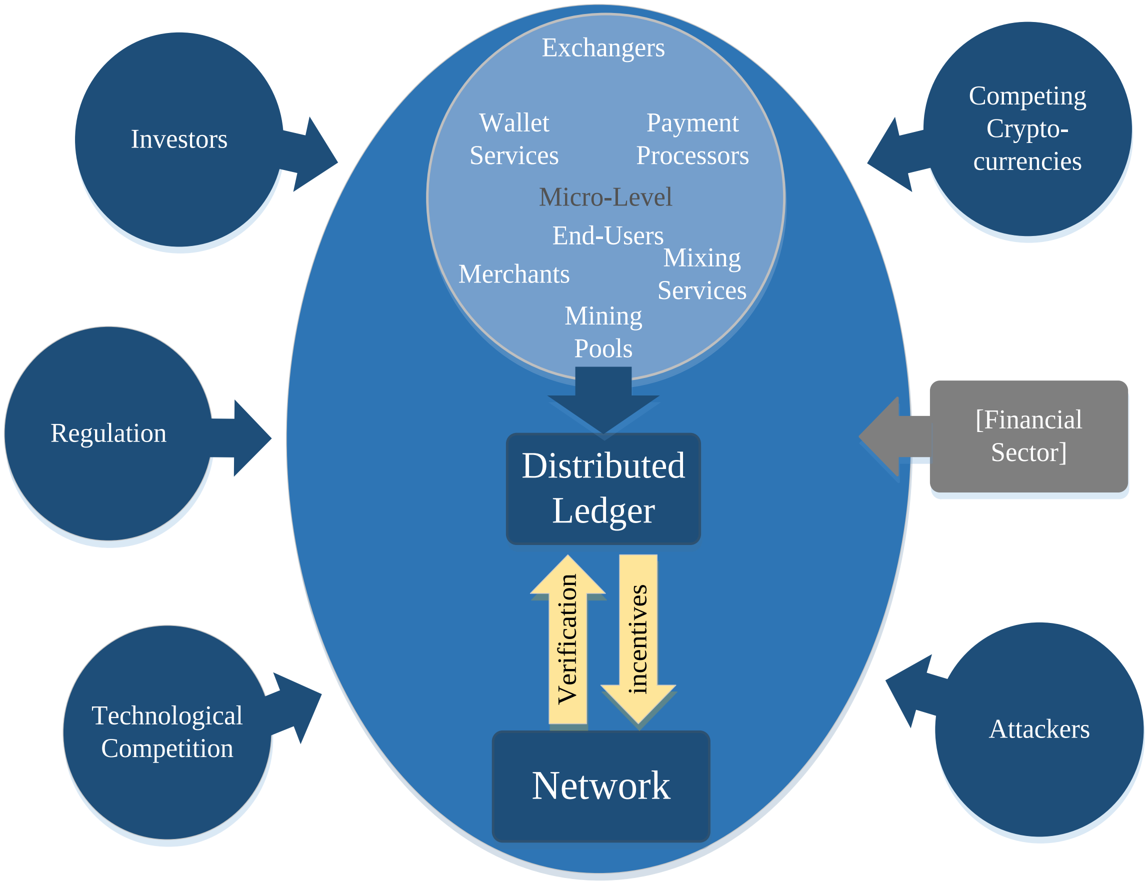


Figure 9: An Exemplary Cryptocurrency Ecosystem

3.1.1.1 Consensus Participants

The actor of the consensus participant was already detailed covered in section 2.3.5 about the implementation of a decentralized network for verifying transactions and updating the distributed ledger in the Bitcoin system. They are denoted as an individual “that participates in a decentralized virtual currency network by running special software to solve complex algorithms in a distributed POW or other distributed proof system used to validate transactions in the virtual currency system” (Financial Action Task Force, 2014, p. 7). In doing so, consensus participants ensure the security of the system given that the right economic incentives are provided.

3.1.1.2 End-Users

An end-user is a person or entity in possession of units of a cryptocurrency, which is used for the purchase of real or virtual goods and services, sends it to other users or keeps it as an investment for a period of time (Financial Action Task Force, 2014).

3.1.1.3 Exchangers

An agent that is denoted as an exchanger is “a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other form of virtual currency and also precious metals, and vice versa, for a fee” acting like a bourse or as an exchange desk (Financial Action Task Force, 2014, p. 7). Some of these trading platforms offer advanced trading options like limit or stop orders, but more sophisticated financial instruments remain rare. The majority of transactions transferring cryptocurrencies with the purpose of trading for goods and services currently involve conversions into or from conventional currency. This is owing to the fact that most retailers do not directly accept cryptocurrencies. Instead, prices quoted in conventional currency are converted into the corresponding amount of the respective cryptocurrency in real time and the received amount of cryptocurrency is immediately exchanged back into conventional currency (Böhme *et al.*, 2015). Exchangers are important for facilitating these services, since retailers predominately hesitate to bear the risk of fluctuations in value. Additionally, exchangers allow end-users not willing to earn units of a cryptocurrency as reward for participating in the consensus process to buy cryptocurrencies. Thereby a wide range of payment methods like credit cards, cash or other virtual currencies are accepted. Depending on the concrete cryptocurrency, exchangers can be affiliated as well as non-affiliated with the administrator of the system or be provided by a third party (Financial Action Task Force, 2014).

3.1.1.4 Merchants

The utility a cryptocurrency provides for end-users to a large extent depends on the number of merchants accepting it in exchange for goods and services. Consequently, the actor of merchant is highly relevant within the ecosystem of a cryptocurrency. The majority of merchants accepting cryptocurrencies to date offer it as alternative payment option beside already established ones. Integrating cryptocurrencies is a differentiator for acquiring new customers, as some merchants already expressed (Hagiu and Beach, 2014).

3.1.1.5 Mining Pools

As the probability for a single consensus participant to successfully publish a set of transactions in cryptocurrency systems with POW depends on the available computing power, he or she is endangered to waste economic resources, when the individual fraction of the overall computing power is too low. Therefore, consensus participants increasingly bundle their capacities in so-called mining pools, especially in representatives with a large network like Bitcoin. Units of cryptocurrency received as newly created coins or transaction fees are split between the participants and individual financial risks resulting from investments into hardware are diversified.

3.1.1.6 Mixing Services

The technical design of a majority of cryptocurrencies implies transactions between trading partners to be publicly visible for anyone who accesses the underlying public distributed ledger. Privacy guarantees are provided by allowing end-users to authorize transactions through the use of pseudonyms of which they can create an infinite number. In doing so, every transaction is solely associated with the particular public keys of the sender and receiver of units of the respective cryptocurrency. An important vulnerability of this approach in terms of privacy can be exploited, if it is possible to assign real world identities to the pseudonyms through information from outside the system. In this case the transparency of the system makes it possible to trace back any transaction ever conducted by an end-user. This has severe consequences for the privacy regarding the individual history of payments.

Mixing services are intended as a countermeasure to prevent this kind of linking or at least complicate it. Even though the concrete method of concealing payment flows differs depending on the individual service, mixing services are primarily third parties that receive transactions of a (in the ideal case) large number of senders and forward them to the respective recipients. In the process of mixing, payment flows of several senders are combined in a manner which hinders observers from drawing conclusions about their origin. The protocols of mixing services are mostly not public, why it is difficult to make statements about their effectivity (Böhme *et al.*, 2015). However, works examining this issue suggest that correlations in time may lead to the identification of end-users (e.g. Möser *et al.*, 2013).

3.1.1.7 Payment Processors

The primary task of a payment processor is reducing the effort accompanied by the acceptance of cryptocurrencies as payment option. Many merchants that decide to accept cryptocurrencies in exchange for goods and services, do not want to take the volatility risks associated with this type of exchange medium. Other challenges involve the implementation of the protocol to facilitate the transfer between end-users and merchants, converting the received funds into other currencies and integrating corresponding interfaces into online shopping systems (Hagiu and Beach, 2014). Payment processors act as intermediaries, which settle payments in cryptocurrencies and pay the merchants in conventional currencies. Thereby, the risks connected with accepting cryptocurrencies for payments are transferred from the merchant to the payment processor and merchants are not required to fully integrate cryptocurrencies into their processes and IS.

3.1.1.8 Wallet Services

The holding, storage and transfer of cryptocurrencies requires the use of wallets to keep the private keys that provide access to the units of cryptocurrency associated with an address. The term wallet is derived from the understanding of cryptocurrencies as digital form of paper currency and coins and considered as analogy to a physical purse. Software wallets are programs that manage the private keys of a user and provide interfaces to render the use of cryptocurrencies more convenient. They include functionalities for generating additional key pairs, display the overall amount of currency available and choose addresses to use for carrying out transactions (Narayanan *et al.*, 2016). Beside software wallets also other devices can be used for the storage of keys. One can simply print a key on a piece of paper or other physical item, memorize it, use another data storage medium or special hardware wallets with implemented security measures. The advantage of this cold storage methods is that keys are no longer stored on devices connected to the internet, which prevents remote attackers from stealing by getting access to the wallet (Hagiu and Beach, 2014).

Irrespective of the concrete wallet chosen the risk that private keys get lost or stolen, and with it the means to authenticate at the system to access the corresponding units of the cryptocurrency, always remains with the end-user. For this reason, wallet services emerged to take the risk and store the required files on shared servers. Additionally, wallet services often offer further features that make the use of their wallets more convenient than conventional wallets operated by end-users (Böhme *et al.*, 2015). Consequently, wallet services support the participation in the networks of cryptocurrencies, by providing end-users, exchangers and merchants with means for the simple processing of transactions (Financial Action Task Force, 2014). There are services where the storage of the private keys remains a responsibility of their customers, which protects the service provider against attacks from the outside, but transfers the risk of losing the private key to the customers. Other services manage the private keys for their customers, which further simplifies the procedures, however, it increases the risk of theft on the side of the service operator (Böhme *et al.*, 2015). Many wallet services providers intend to offer a large bandwidth of complementary services for cryptocurrencies, which is why some providers also include, for instance, exchange services into their portfolio (Financial Action Task Force, 2014).

3.1.2 Interaction Patterns Involving Cryptocurrencies

The actors presented above interact with each other within the ecosystems of cryptocurrencies. Despite the decentralized design of a majority of implementations, certain central actors are commonly involved in a large part of actual transactions. In order to provide a basis for the analysis of opportunities for criminal individuals to misuse cryptocurrencies for ML later on, two frequently encountered interaction patterns are described in the following.

3.1.2.1 Interaction Pattern End-User-Merchant

The scenario covered by the end-user merchant interaction pattern assumes, that the end-user wants to buy goods or services from a merchant offering a cryptocurrency as payment option and is depicted in Figure 10. Furthermore, the end-user das not participate in the consensus process, so there is no chance to get units of the cryptocurrency as reward, and the cryptocurrency is considered to be the most favorable available payment instrument. In this case the end-user will use an exchanger to convert value denominated in a fiat currency into the accepted cryptocurrency. The personal wallet is operated by a wallet service in order to minimize the risk of loss of the balances. Therefore, a risk transfer from the end-user to the operator of the wallet service takes place. Of course, it is also possible to relinquish from using an intermediating wallet service, if the end-user prefers to manage the wallet independently. In the next step, the balances in the form of units of the cryptocurrency required to settle the transaction are passed on to a payment processor. The payment processor is interposed by the merchant to offer the cryptocurrency as payment option, without taking the risk of exchange rate fluctuations and needing to invest capital for integrating it into the particular processes and systems. Currently all established merchants accepting cryptocurrencies use payment processors for the settlement of transactions (examples include Dell (Dell, 2016) and Mircrosoft (Microsoft, 2016)). The payment processor maintains accounts of the respective cryptocurrency and exchanges it back to fiat currencies. Alternatively, the payment processor may additionally act as exchanger itself. The merchant is paid by the payment processor in balances denominated in a fiat currency and the transaction is complete. As in the stage of using a wallet services, it is also conceivable to finalize the transaction without intermediation by a payment processor.

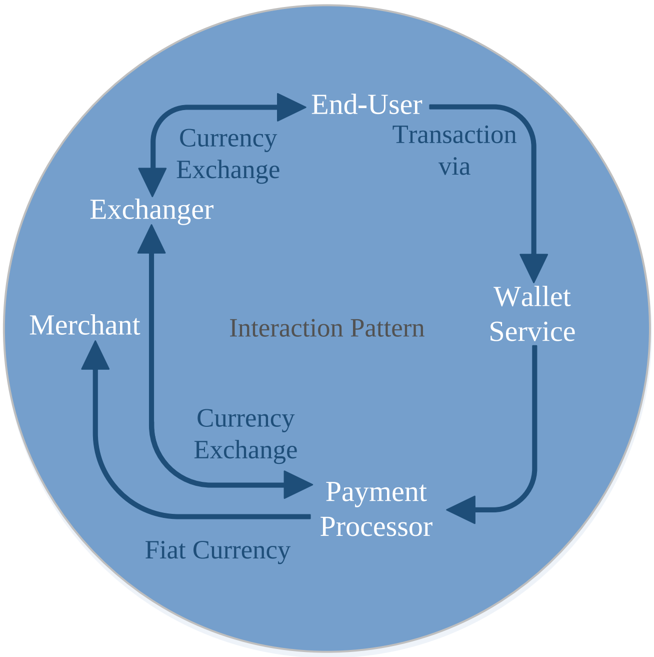


Figure 10: Interaction Pattern End-User-Merchant

3.1.2.2 Interaction Pattern Sender-Receiver

The second interaction pattern sender-receiver is related to the private transfer of a cryptocurrency between two end-users (entitled as sender and receiver afterwards) and presented in Figure 11. One of the specific features of cryptocurrencies is the possibility for the direct transfer of balances between private individuals. This is in contrast to other payment instruments like credit cards, which are deliberately designed to facilitate payments in business-to-consumer relationships. It is again assumed that the sender obtains the cryptocurrency in exchange for balances denominated in a fiat currency from an exchanger. The purchased units of the cryptocurrency are then transferred to one or more public keys where the sender is in possession of the respective private key. These private keys are either stored in a wallet administered by him or her or one which is operated by a wallet service. Subsequently, the actual transfer of balances takes place. Just as the sender, the receiver may interpose a wallet service. Finally, the receiver converts the received units of the cryptocurrency into fiat currency by using an exchanger.

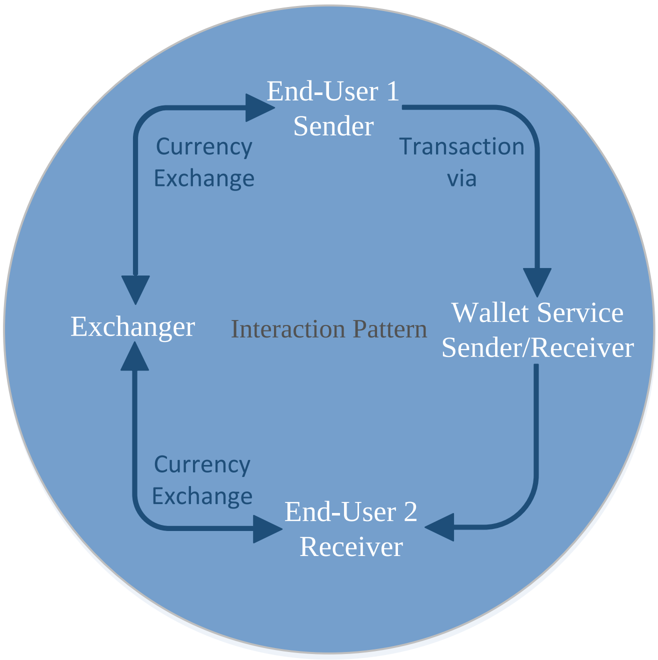


Figure 11: Interaction Pattern Sender-Receiver

3.2 From Illegal Profits to Apparently Legitimate Funds

Profits resulting from illegal activities committed by criminal networks such as drug or human trafficking, smuggling and illicit gambling pose a serious threat to economic systems as well as public safety. They provide e.g. the financial resources for criminals and terrorists to operate and expand their business, undermine the legitimate private sector and financial markets and diminish tax revenues (McDowell and Novis, 2001). ML describes the process by which the illegal sources of profits are disguised to obscure the link between the funds and the original criminal activity (International Monetary Fund, 2014). While the origin of the term lies in the US Mafia's activities to 'launder' illegal money via cash-intensive washing salons (Schneider and Windischbauer, 2008), nowadays it has to be understood in a much broader context. The emergence of complex financial instruments and global networking through technical developments and increased use of the Internet offers hitherto unknown pathways to conduct ML (European Central Bank, 2012). Therefore, it is not surprising that around USD 1.6 trillion funds from illicit sources were laundered in 2009, which amounts up to 2,6 percent of the global GDP (United Nations Office on Drugs and Crime, 2011). These numbers emphasize the severity of the problem, but should be treated cautiously due to the absence of precise statistics.

3.2.1 Related Work: Economics of Crime

The idea to adapt well-known economic theories to analyze the rationale of individuals faced with the decision whether they should pursue criminal activities or not can be traced back to the year 1843. A first simple explanation of the economic intuition behind the motives of criminals is attributed to Jeremy Bentham, who is considered as founder of the classical utilitarism (Bentham, 1843). According to Bentham, the incentives to conduct crimes emerge due to the profits and advantages resulting from these activities. The expected profits and benefits incentivize an individual to commit a crime and the costs and pain that correlate with a potential punishment serve as disincentives. Consequently, a criminal act only takes place if the utility it provides exceeds the expenses required for committing it.

The basic idea of viewing criminal acts as a result of rational decisions by economic agents was developed and employed by Becker in 1968 (Becker, 1968). Therefore, he incorporated the general rationale into a model intended to determine the economic optimal investments into countermeasures to prevent and detect criminal activities by considering the incentives of potential criminals. The model integrates a government, which role is to deteriorate crime through the setting of adequate punishments and the implementation of measures to increase the probability of detection. As a result, the costs of criminal activities need to exceed the benefits for criminal individuals.

Bentham and Becker were the first to approach the problem of crime through a pure microeconomic manner, addressing criminals as rational individuals and investigating the factors which incentivize or respectively discourage them. The microeconomic perspective allows to analyze how changes in the corresponding environmental variables, such as punishments, fees for the transfer of money or the punishment probability, influence the rational behavior of criminal agents. Their works laid the foundation for the scientific research stream of the economics of crime. The associated studies can be divided into different categories. Bouckaert and Geest (1992), Walker and Unger (2009), Unger (2009), Masciandaro and Barone (2008), Polinsky and Shavell (2000) and Garoupa (1999) tackle the general issue and provide a solid overview of literature on the topic. Addressing the concrete topic of ML, the publications by Masciandaro (1998) and Masciandaro and Barone (2008) arguably represent the most influential relevant works based on their frequency of citations. Their focus is on the interaction relationships between the illegal part of the economy and legal financial markets. This distinction is drawn, since illegally acquired profits only possess purchasing power in legal financial circuits, if they appear to be originated from legal sources. The process of disguising the illegal origin of these funds is consequently called ML (Schneider and Windischbauer, 2008). They present an economic model to illustrate the decision process of money launderers and to examine their optimal strategies based on the assumption of rational behavior. Further models with economic underpinnings are suggested in Argentiero *et al.* (2008), Bagella *et al.* (2009) and Schneider and Windischbauer (2008).

Actual literature addresses the suitability of cryptocurrencies for ML. Bryans (2014) discusses the effects of Bitcoin and analogous virtual currencies on the implementation and enforcement AML legislation. Gruber (2013) analyzes possible threats of ML and tax evasion using the Bitcoin system and highlights the use and potentially problematic implications of bitcoins. Möser *et al.* (2013) aim to give a systematic account of the available ML tools in the Bitcoin environment. Their modes of operation are compared in order to draw conclusions on the effectiveness of AML efforts with respect to Bitcoin. Considerable scientific attention is attributed to the consequences after prominent scandals about criminal cases connected with Bitcoin (e.g. the closure of the illegal market place Silk Road trough state authorities, which only accepted Bitcoin as payment option for anonymity reasons (Raymond, 2015)). The literature analyzes the consequences for the reputation and adoption of Bitcoin on the one hand, and the challenges for the AML and anti-crime mechanisms on the other hand (Brito and Castillo, 2013; Raeesi, 2015; Trautman, 2014; Christin, 2013).

3.2.2 Setting the Context: Money Laundering Process & Controls

The success of ML is crucial dependent on the existence of information asymmetries between money launderers and investigative authorities. ML activities share two key-characteristics: illegality and concealment (Masciandaro, 1999). In order to reuse illegally acquired funds for legal activities without causing suspicion, they need to appear generated from legitimate sources. Therefore, money launderers' aim is to obfuscate the stream of cash in a way that prevents any connection to the underlying criminal activity (United Nations Office on Drugs and Crime, 2005). In economic terms, the transfer of potential purchasing power into actual purchasing power, to minimize incrimination risks (Masciandaro, 1998). The process of establishing these information asymmetries is called ML Process and is carried out by utilizing a ML Instrument. Policies and procedures employed by investigative authorities to prevent, detect and investigate money are called AML controls. They aim at decreasing the information asymmetries between money launderers and investigative authorities. The more effective AML Controls are, the more difficult it is for criminals to successfully execute the ML Process and benefit from their offences due to an increasing risk of prosecution and conviction (Becker, 1968). The interrelations between the actors and important elements in the context of ML are summarized in Figure 12.

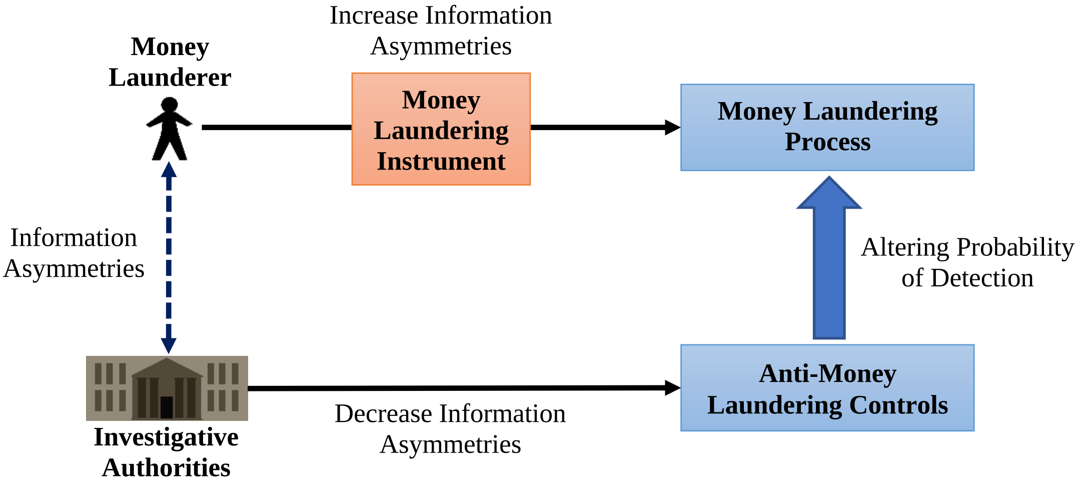

Increase Information Asymmetries
Money Launderer
Money Laundering Instrument
Money Laundering Process
Information Asymmetries
Altering Probability of Detection
Investigative Authorities
Decrease Information Asymmetries
Anti-Money Laundering Controls

Figure 12: The Context of Money Laundering

Consequently, the economic incentives of a money launderer to utilize a ML instrument are conditional on: How well it is suited to establish a high degree of information asymmetry between the money launderer and investigative authorities, at the lowest possible expense of financial resources. This depends on the effects it has on the execution of the ML process and the available AML Controls. For that reason, the general structure of the ML Process and prevailing AML Controls are introduced and their influence on the incentives is examined in the following. The results are used as input for the conceptualization of the subsequent analysis of cryptocurrency backed ML.

3.2.2.1 Money Laundering Process

There will always be a criminal agent or a criminal organization having committed a predicate offence (i.e. a transaction which generated and accumulated illicit funds) such as drug trafficking, kidnapping, arms smuggling, extortion or financial crime occurred before the process execution (United Nations Office on Drugs and Crime, 1988). In the majority of all illegal transactions cash is exchanged for the payment of illegal goods and services. This can be attributed to the properties of cash, which allow for anonymous and irrevocable transactions (with respect to third parties not involved in the transaction) without leaving eminent traces for investigative authorities (Schneider and Windischbauer, 2008; Villasenor *et al.*, 2011). As depicted in Figure 13, the process of ML itself consists of three stages: placement, layering and integration (Reuter and Truman, 2004).

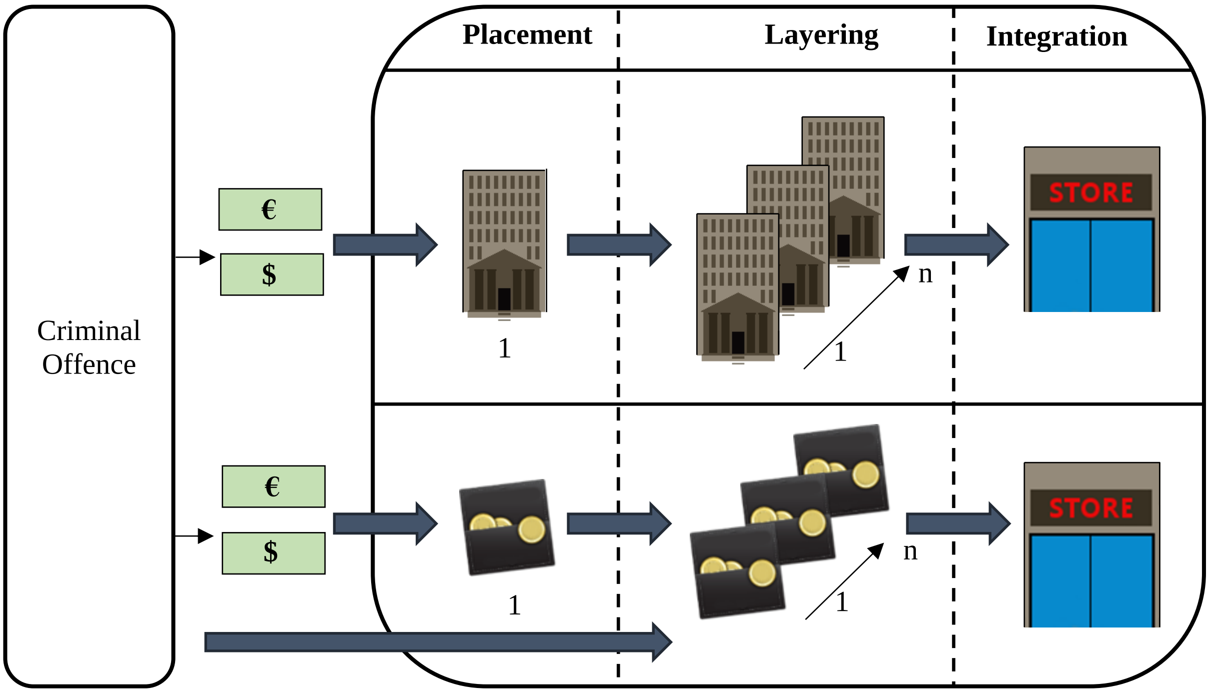


Figure 13: Money Laundering Process

In the initial **placement stage**, illicitly obtained funds are introduced into the financial system in a form or a place that is less suspicious to public authorities and convenient to make them more liquid. One method commonly used for placement is structuring, which describes the act of altering a financial transaction to avoid reporting requirements. The placement stage is highly risky due to strict compliance requirements for financial institutions (e.g. Survey Transaction Reports, Customer Due Diligence and Suspicious Activity Reports). The U.S. Bank Secrecy Act obligates financial institutions to report cash transactions in excess of US$ 10.000, which may be either one transaction or a combination of cash transactions traced to a certain individual or group of individuals (Federal Financial Institutions Examination Council, 2014). Similar considerations apply for the European Union, where the threshold is at EUR 15.000 (European Union, 2005).

One method commonly used for placement is structuring, which describes the act of altering a financial transaction to avoid reporting requirements. It involves breaking down cash transactions into amounts below the reporting threshold often realized by couriers, so-called 'smurfs', performing multiple financial transactions (Reuter and Truman, 2004). The placement utilizing cryptocurrencies involves exchanges converting cash into cryptocurrency, but this procedure also necessitates launderers to bypass control mechanisms of banks and additionally exchanges. To avoid these risks and thereby omit the placement of illegally acquired funds, criminals may directly accept cryptocurrencies as payment for illegal goods and services. This is possible due to their feature of sharing some common characteristics with cash. Individuals are capable of interacting without identification to each other or an intermediary and past payments are irreversible (Meiklejohn *et al.*, 2013; Brito and Castillo, 2013).

In the subsequent **layering stage**, the funds usually get passed through many institutions and jurisdictions using multiple complex financial transactions in order to obfuscate their illegal origin. They are channeled through the purchase and sale of investment instruments such as bonds, stocks and checks or they are simply transferred between a series of accounts at various banks, particularly to those jurisdictions with lax AML regimes (Bauer and Ullmann, 2001). The same mechanism holds true for cryptocurrencies, where funds are transferred through different accounts in different locations, which does not require much effort within the P2P network.

Finally, the **integration stage** integrates ill-gotten proceeds into the legal economy, where they appear to be legitimate, through financial or commercial operations. One may exchange the funds held in cryptocurrencies into fiat currency or use them to buy products and services.

From an economic perspective, the ML process consists of a series of transactions between individuals, third parties, accounts and jurisdictions. Positive incentives for criminals to utilize an instrument for ML are provided, when it is relatively advantageous compared to alternatives that allow for the transfer of funds (Mantel and McHugh, 2001).

3.2.2.2 Anti-Money Laundering Controls

The economic incentives of money launderers for utilizing a ML instrument are also conditional on the available measures and procedures to detect suspicious transactions and individuals. Depending on the effectiveness of the implemented controls, the probability of being detected while laundering money is altered. This risk imposes costs on criminals and therefore negatively influences their economic incentives for utilizing a ML instrument (Masciandaro, 1998; Geiger and Wuensch, 2007; Ferwerda, 2009). Rational criminals generally have three alternatives to mitigate the risk. They can implement more sophisticated laundering schemes (e.g. involving additional jurisdictions, transactions, parties), which generally imply higher costs while reducing risk. If available, money launderers also have the alternative to utilize a different, less risky instrument. The third option, which constitutes the ultimate objective of AML controls, is that criminals refrain from laundering money. That is the case when the costs for laundering money undetected are greater than its valuation (Masciandaro, 1999). The conclusion is that the effectiveness of the implemented control mechanisms is negatively correlated with the attractiveness of an instrument for money launderers. Consequently, if no controls are implemented or it is possible to circumvent them with little effort, positive economic incentives to utilize an instrument for ML are provided.

In order to enable the analysis of how the factors of cryptocurrencies influence the effectiveness of controls (and thus the economic incentives of money launderers), an overview of prevailing AML controls is given. The main driver behind AML investment decisions are regulatory requirements which oblige financial institutions and certain non-financial businesses to comply with AML legislation (KPMG, 2014). In order to be compliant, they have to implement preventive measures to identify and assess customers or transactions and report suspicious activities to law enforcement, which is considered “to be a crucial tool in the investigation and prosecution of money laundering offences” (Bauer and Ullmann, 2001, p. 21). The global standard are the recommendations published by the Financial Action Task Force on Money Laundering. As international standard-setting body, the Financial Action Task Force established AML measures that should be adopted by financial institutions and designated non-financial businesses (Financial Action Task Force, 2012). A central element of the overall framework is the shift from a rule-based towards a risk-based approach countering ML. Risk management becomes increasingly important because solely relying on rules (i.e. if characteristics of a transaction meet conditions specified in the rule, then a specified action is taken) produces insufficient reports. In the European Union financial institutions are obliged to report cash transactions in excess of EUR 15.000 (European Union, 2005). Criminals are also aware of such thresholds and simply execute transactions just below those boundaries (‘structuring’) (Reuter and Truman, 2004; Takats, 2011). A risk-based approach is, in contrast, flexible and a reasonable designed risk management process enables to focus on customers and transactions that pose the highest risk for ML. Appropriate controls should be selected on basis of the risk assessment so that resources are allocated in the most efficient ways.

Controls are based on the so-called Know-Your-Customer principle and can be categorized whether they are performed a priori, during or a posteriori the business relationship of an individual with a financial institution or a non-financial business. In general, every AML strategy consists of multiple building blocks: a priori collection and analysis of personal data to derive implications regarding the expected risk of ML imposed by potential customers, collection and analysis of actual transaction data to detect suspicious activities and enrichment of customer profiles during the business relationship. This is complemented by a posteriori record keeping to provide audit trails for investigative purposes (see Table 11). It is important to determine how the implementation and application of prevailing controls is influenced by the factors of cryptocurrencies to identify the ML risks imposed.

Timepoint	Controls
A Priori	**Customer Identification Procedures** ▪ Identify and verify the identity of each customer/beneficial owner ▪ Develop customer profiles containing personal data ▪ Exclude certain potential customers
During	**Ongoing Account & Transaction Monitoring** ▪ Understanding of regular and reasonable activities ▪ Detection of unusual activity patterns ▪ Updating of customer profiles
A Posteriori	**Record Keeping** ▪ Provide audit trails

Table 11: Overview of Anti-Money Laundering Controls

3.3 Cryptocurrency Backed Money Laundering

As a first step to assess the risks posed by cryptocurrencies as possible ML instrument, this chapter focuses on the incentives of criminals to utilize cryptocurrencies for ML. Subsequently, a comparative analysis based on our conceptualization of the economic incentives of criminals to utilize a ML instrument is conducted.

3.3.1 Conceptualization: Provision of Incentives

Figure 14 illustrates the conceptualization for the analysis, which refers to the discussion of the ML process and AML controls in the previous sections. It is based on the economic incentives of criminals to utilize a ML instrument. In order to examine the behavior of the money launderer, it is important to set some basic assumptions.

Firstly, the individual is expected to act rational, which is equally defined for the legal as well as the criminal sphere (Geiger and Wuensch, 2007). In the classical economic theory, the main force which drives the behavior of an individual is maximization of utility. This depends on the expected costs and benefits of different choices that are available to the individual. A considerable part of the traditional economic analysis lays on this principle (e.g. Varian, 2010). The modern economic theory of crime and ML addresses criminals as rational beings and builds the analysis and policy implications upon the assumption, that a crime would be committed only of the expected utility from the gains of a criminal act exceeds the expected disutility caused by the costs of committing the given crime (Becker, 1968). Secondly, ML is considered as an offence independent from the initial criminal act. This implies for the analysis that the money launderer does not necessarily have to be the same individual as the offender of the initial crime. Therefore, this analysis does not include the decision whether to commit a crime in the first place. It is assumed that the criminal offence has already taken place and the process of ML needs to be executed. The aim of this simplification is to focus the analysis only on factors influencing the selection of the optimal ML instrument to be used.

Contextual and transactional factors that have effects on the execution of the ML process are identified. A distinction is drawn between direct and indirect effects. The direct impact of contextual and transactional factors on the conducting of transactions is defined as direct effects. They influence the efficiency and effectiveness of the ML process by making the process execution, for example, more cost-efficient, time-efficient or the system more robust against disturbances. Given that the ML process basically consists of a series of transactions, they affect honest individuals in conducting legal transactions as well as money launderers. Furthermore, money launderers also have to take indirect effects into account. They have an indirect impact on the execution of the ML process. Indirect effects influence the effectiveness of AML controls, which in turn alter the probability of being caught while laundering money. The direct and indirect effects of contextual and transactional factors on the execution of the

ML process provide positive or negative economic incentives, which eventually influences criminals in their decision to utilize an instrument for ML.

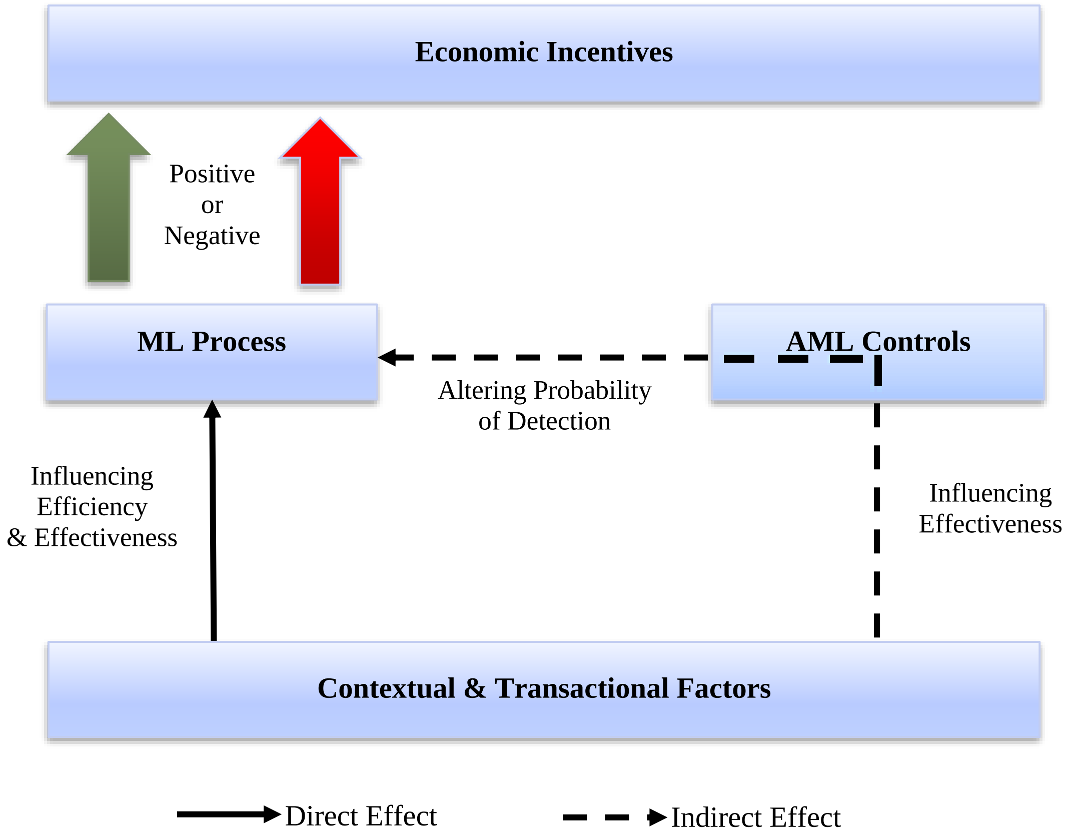


Figure 14: Conceptualization of the Analysis

3.3.2 Comparative Analysis of Money Laundering Related Factors

The identification of the conceptual and transactional factors took place in a two-step process. Firstly, literature of transnational organizations responsible for AML (e.g. United Nations Office on Drugs and Crime and Financial Action Task Force) considering the risks of ML through financial instruments and services was reviewed. This included general literature as well as literature specifically targeted at virtual currencies. It was complemented by the sparsely available academic literature about ML. Thus one is able to understand potential vulnerabilities of financial instruments and services, which are exploited by money launderers. Vulnerabilities are the result of certain design features (e.g. anonymity, irrevocable transactions, decentralization) and their implications (e.g. wide acceptance, borderless nature). Secondly, it was searched for academic and the vast, fragmented online literature addressing the extent to which cryptocurrencies exhibit these vulnerabilities. In doing so, contextual and transactional factors were identified, which are subsequently analyzed according to the conceptualization of how incentives for money launderers are provided.

Using the identified factors, the comparative analysis based on the conceptualization of the economic incentives of criminals to utilize a ML instrument was conducted. In order to facilitate ML, cryptocurrencies must be perceived relatively advantageous to other potential ML instruments (Mantel and McHugh, 2001). Therefore, cryptocurrencies are compared with traditional financial instruments and services as benchmark. Traditional financial instruments and services are the most important instruments for ML (Reuter and Truman, 2004; United Nations Office on Drugs and Crime, 2013). Generally, a financial service involves the transaction of a financial instrument or money within the financial system using financial institutions. For this purposes, currently used means of payment backed by conventional currencies are considered. They allow for the transfer of funds between accounts supported by financial institutions. Such a broad definition is deliberately chosen to account for a wide range of ML instruments (e.g. Credit Card, Online Money Transfer or PayPal) with common factors.

Afterwards, a discussion of the results and an overview over already evolving technological developments and regulatory approaches potentially affecting the economic incentives is given. Table 12 provides a summary of the methodological approach for the rest of this section. The results of the comparative analysis are described detailed below and presented in Table 13.

1. Identification of Factors	**Money Laundering Literature** ▪ Publications of transnational AML organizations (e.g. Financial Action Task Force, UNODC) ▪ Academic publications addressing ML ➢ Vulnerabilities of financial instruments and services **Cryptocurrency Literature** ▪ Academic and online literature ➢ If and how cryptocurrencies exhibit these vulnerabilities
2. Analysis of Factors	**Comparative Analysis** ▪ Analysis according to the conceptualization ▪ Benchmark: Traditional financial instruments and services
3. Implications	**Discussion of Results & Related Challenges**

Table 12: Methodological Approach for the Comparative Analysis

3.3.2.1 Acceptability

A growing number of merchants are offering cryptocurrencies as payment method for both real and digital goods and services. Thus, users are not necessarily required to exchange them for fiat currencies. Products and services range from clothing, electronics, groceries or travel services to games and online dating sites. One prominent example is the computer technology specialist Dell, who managed the switch towards cryptocurrencies (Dell, 2016). Furthermore, Ebay's payment unit PayPal allows digital goods merchants to accept Bitcoin payments (PayPal, 2014). The purchase of commodities and services is a common way for money launderers to enjoy their illegal profits, without necessarily drawing attention of government agencies. However, cryptocurrencies compared to traditional financial instruments and services currently are not nearly as widely accepted (Srinivas *et al.*, 2014). From a money launderer's perspective, this limits the channels to convert, move and integrate illicit funds. One important aspect is that limited market size reduces the extent to which large amounts of illicit value can be moved and restricts the utility of cryptocurrencies for smaller scale illicit activities (Australian Transaction Reports and Analysis Centre, 2012). Therefore, it is argued that limited acceptance currently has a direct effect on the execution of the ML process, providing negative incentives for money launderers to rely on cryptocurrencies. Even though this may evolve in the future, it is unlikely that they will gain greater acceptance than traditional financial instruments and services, which interact with a wide range of economic sectors (Dostov and Shust, 2014).

3.3.2.2 Administration

Despite the fact that intermediaries are not required to process transactions, there is also no central oversight body authorized to control the supply of cryptocurrencies and prevent certain individuals from account creation. This task is executed by the decentralized P2P network which, moreover, makes it impossible for law enforcing agencies to confiscate accounts containing ill-gotten funds due to the lack of a central repository (Financial Action Task Force, 2014). The accessibility of accounts is restricted to individuals knowing the corresponding private key. This is in contrast to financial institutions, with their ability to grant access to authorities for investigative purposes. It has an indirect effect, providing positive economic incentives for money launderers. High risk individuals, who are excluded from traditional financial instruments and services in AML regimes with effective customer identification procedures, need other channels to move illicit funds. Because of these low barriers to entry, cryptocurrencies are a particularly suitable instrument and they even permit to create several accounts without any restrictions including funding limits (United Nations Office on Drugs and Crime, 2014). The lack of a central authority prevents the applicability of a priori AML controls. This has an indirect effect on the execution of the ML process, providing positive incentives.

3.3.2.3 Authentication Level

Although the distributed ledger contains a public record of every transaction processed in the network, there is no identifying information of involved parties (Peck, 2012; Velde, 2013). Accountability is realized via asymmetric encryption, which allows for pseudonymously authentication. Following the privacy-terminology of Pfitzmann and Hansen (2010): “A pseudonym is an identifier of a subject other than one of the subject’s real names” (Pfitzmann and Hansen, 2010, p. 21). Therefore, without access to identifying information from outside the system connecting public keys with subjects, it is impossible to identify particular individuals (Reid and Harrigan, 2013). Additionally, multiple accounts can be opened by criminals to hide the true value of deposits. Pseudonymous authentication in connection with publicly accessible transaction histories is a double-edged sword with regard to the feasibility of AML controls. It prevents any successful customer identification procedures, as long as individuals do not interact with actors outside the network that collect personal identifying information (e.g. exchanges, online retailers). This is also addressed in the Financial Action Task Force recommendations, which explicitly require countries to give special attention to the risks arising from new or developing technologies that might facilitate transactions without disclosing personal identification (Financial Action Task Force, 2012). Today no AML software is available to monitor and report suspicious transaction patterns (Financial Action Task Force, 2014). Hence, the pseudonymous nature of cryptocurrencies has an indirect effect, providing positive incentives. At the same time, however, the public record allows to trace any transaction that has ever occurred. If a pseudonym is being associated with an individual, it is possible to identify suspicious activities in the transaction history (Möser *et al.*, 2013). That calls for new AML controls based on the analysis and enrichment of transaction graphs (e.g. Meiklejohn *et al.*, 2013; Ober *et al.*, 2013; Reid and Harrigan, 2013). Depending on their effectiveness, such controls may provide negative incentives for criminals to utilize cryptocurrencies for ML in the future.

3.3.2.4 Price Volatility

There exists a wide range of funding sources and withdrawal destinations for cryptocurrencies including: bank transfer, cash, other cryptocurrencies, payment cards or PayPal (European Central Bank, 2012; United Nations Office on Drugs and Crime, 2014). Cash acquired when committing predicate offences needs to be converted for cryptocurrencies and placed into the network through this channels. Money launderers will prefer funding sources that permit anonymous funding, like cash or third-party funding through exchangers that do not properly identify the funding source (Financial Action Task Force, 2014). The same holds in the opposite direction, in order to convert funds back into fiat currency after or while layering. Unlike financial instruments and services, cryptocurrencies are not backed by fiat currencies. Consequently, the exchange rates between cryptocurrencies and fiat currencies fluctuate over time. All cryptocurrencies suffer from a high level of price volatility, what is likely to discourage individuals to utilize them for transactions (Rogojanu and Badea, 2014; European Parliament Research Service, 2014). Funds may diminish in value during the layering stage, which requires money launderers to monitor the market continuously. This effort has to be added to the costs for the execution of the ML process and is of particular relevance for money launderers that may desire the flexibility to store their funds in cryptocurrencies. Hence, volatility has a direct effect on the execution of the ML process, providing negative economic incentives for money launderers.

3.3.2.5 Flexibility

It is possible to transfer cryptocurrencies globally, nearly instantaneously, with very low transaction fees. Accounts are not tied to any financial institution and the network processing transactions and transferring funds is a complex interconnected infrastructure. Several entities are involved, spread across different countries and one only needs an internet-supported device to participate. Since each node of the P2P network processes every transaction, and the difficulty of the mathematical problem to complete and publish blocks scales with the available computing capacity, the network only collapses when every node is disconnected (Nakamoto, 2008). Thus, there is no single point of failure, which makes the system robust against disturbances (Bryans, 2014). With financial instruments and services, the failure of a service provider negatively influences the processing of transactions. Flexibility has a direct effect, providing positive incentives to utilize cryptocurrencies compared to traditional financial instruments and services. Furthermore, it is essentially impervious for AML efforts to interrupt the ML process due to the systems flexibility. Therefore, flexibility also has an indirect effect, providing positive incentives for money launderers (Hochstein, 2014).

3.3.2.6 Irrevocability

Irrevocability of transactions is a property cryptocurrencies have in common with cash (beside interaction without necessary identification). Once confirmed, the protocol does not offer any functionality of having transferred funds charged back unless the receiver issues a new transaction (Hurlburt and Bojanova, 2014). That is the opposite of financial instruments and services, where it is possible to revoke transactions. Therefore, just like merchants offering legal goods or services, criminals benefit from this kind of fraud protection when committing predicate offences (Meiklejohn *et al.*, 2013; United Nations Office on Drugs and Crime, 2014). They profit even more, because no rational criminal would take legal action against someone involved in an illegal financial transaction, due to the risk of being prosecuted likewise. Irrevocability has a direct effect, decreasing the risk of payment fraud when offering illegal products and services, providing positive incentives for money launderers. Beyond that, irrevocability also has an indirect effect, providing positive incentives. Funds are outside of control of any authority after the completion of a transaction. It is impossible for law enforcement to reverse the transaction a posteriori (Shasky Calvery, 2013).

3.3.2.7 Payment Processing

Until the invention of cryptocurrencies online transactions required a trusted third party intermediary to verify payments and ensure that digital money could not be spent twice (double-spending problem). As mentioned, prevailing AML controls are based on transaction and user data being reported to law enforcement by these intermediaries (Financial Action Task Force, 2013). This situation can be modeled as agency problem, where the intermediary acts as agent on behalf the government and has an informal advantage. Incentives for monitoring and transaction reporting are provided by means of fines for false negatives (i.e. not reporting of transactions which are identified to be suspicious ex-post) (Takats, 2011). Unlike traditional financial instruments and services, cryptocurrencies do away with the need of interaction with third parties to process transactions by distributing the ledger among all users of the P2P network and offering irrevocable transactions (Brito and Castillo, 2013). This has an indirect effect on the execution of the ML process, providing positive incentives for criminals to utilize cryptocurrencies for ML. This is because current controls and their enforcement depend on agents implementing them (European Banking Authority, 2014).

3.3.2.8 Portability

Cryptocurrencies offer the opportunity to move large amounts of funds across national borders seamlessly without restrictions. The only requisite for this is an internet-supported device which grants access to the P2P network. ML is a transnational process in most cases, because the source of funds can be veiled more efficiently, when multiple jurisdictions are involved (Stessens 2000; Schott 2006). Practical experience indicates the particular difficulties when it comes to transaction monitoring across several jurisdictions, even when solely traditional financial instruments and services are involved (KPMG, 2014). It requires cooperation between authorities (with potentially diverging interests) on a global scale in order to develop a consistent approach, whilst it has traditionally been carried out in a localized manner (Dilley *et al.*, 2013). National borders nevertheless constitute a danger of being discovered, whether it be while smuggling large sums of cash through border controls or be it because of increasing reporting obligations of transnational capital flows (Basel Committee on Banking Supervision, 2014). This suggests the conclusion that the borderless international transferability of cryptocurrencies through global operating networks complicates monitoring of suspicious transactions. Thus, portability has an indirect effect on the execution of the ML process, providing positive incentives for money launderers. But portability has also a direct effect, providing positive incentives, because funds may be easily accessed from any remote location.

3.3.2.9 Rapidity

Scholars have long acknowledged the link between advances in information and communication technology and increasingly transnationally interconnected financial systems (Zagaris and MacDonald, 1992). One of the results of this globalization is the tendency towards instantaneous payment solutions. Rapidity is the speed with which transactions can occur. Cryptocurrency transactions are usually conducted in real time, which renders ongoing account and transaction monitoring very difficult and the suspension of suspicious transactions impossible. Another particular risk associated with near instantaneous transactions over the internet is, that they build up an extensive audit trail in a short space of time, requiring additional resources for near-time analysis (Philippsohn, 2001). This complicates the timely monitoring, investigation of suspicious transactions and also the freezing of funds (United Nations Office on Drugs and Crime, 2014). Rapidity has an indirect effect on the execution of the ML process, providing positive incentives for money launderers. Furthermore, instantaneous transaction processing increases the time-efficiency of the ML process (Federal Reserve Financial Services, 2013). This is why rapidity also has an indirect effect, providing positive incentives for money launderers.

3.3.2.10 Transaction Costs

The transaction costs of traditional financial instruments and services vary as a function of transaction value and charges policy of the respective service provider. They include for example currency conversion fees, effort for authorization through the intermediary or interchange fees. An overseas money transfer with Western Union, for example, incurs on average round about 10 percent of the monetary value transferred as transaction costs (Western Union, 2016). Cryptocurrencies serve as inexpensive funds-transfer systems potentially driving savings for merchants and users (Nathan *et al.*, 2014). Because the distributed P2P network enables transfers directly between accounts, the only transaction costs of cryptocurrencies are the operating costs for authorization and verification of payments (Financial Action Task Force, 2014). These costs are negligible at the moment, but may rise as operations scale up (Houy, 2014; Kashaloglu, 2014). Nevertheless, for the analysis it is assumed that the cost advantages will remain in the future. Costs associated with ML activities are transaction costs and have to be considered when choosing the instruments used. As stated by (Masciandaro, 1999) transaction costs for ML are the aggregated costs due to AML activities and the technical costs related to the specific ML instrument. In general, illicitly acquired funds require to go through multiple transactions and parties across different jurisdictions, aiming at reducing the risk of being discovered and prosecuted to an acceptable level. The lower the costs for conducting these transactions are, the higher the revenue of ML. For that reason, the cost advantage of cryptocurrencies over traditional financial instruments and services allows for a more cost-efficient ML process. It has a direct effect, providing positive incentives for money launderers (Federal Reserve Financial Services, 2013; European Banking Authority, 2014).

Instrument Factors		Financial Instruments & Services	Cryptocurrencies	Effect Provides (+/-) Incentives for ML	
				Direct Effect	Indirect Effect
Contextual	Acceptability	Widely Accepted	Limited Acceptance	-	
	Administration	Designated & Issued by a Central Authority	Decentralized Consensus & Storage		+
	Authentication Level	Identified Authentication	Pseudonymous Authentication		+
	Price Volatility	Relatively Stable	High Volatility	-	
Transactional	Flexibility	Transactions Depending on Service Provider	No Central Point of Failure	+	+
	Irrevocability	Revocable Transactions	Irrevocable Transactions	+	+
	Payment Processing	Based on Intermediaries	No Intermediaries Required		+
	Portability	Increasing Transnational AML Efforts	International Transferability	+	+
	Rapidity	Up to Several Days	Instantaneous Transactions	+	+
	Transaction Costs	Varying Fees & Charges	Low or not Existent Transaction Costs	+	
Examples		Credit Card, Online Money Transfer, Wire Transfer, PayPal, Other Monetary Instruments	Bitcoin, Litecoin, Dogecoin		

Table 13: Comparative Analysis

3.3.3 Results of the Comparative Analysis

Table 13 provides an overview of the main findings from the preceding comparative analysis. It is structured according to the differentiation, whether the identified contextual and transactional factors have a direct or indirect effect on the execution of the ML process and how they provide incentives for criminals (either positively or negatively). Without revising the respective factors explicitly, it can be summarized that the vast majority of them may provide positive incentives for criminals to utilize cryptocurrencies for ML. Limited acceptance and high price volatility of cryptocurrencies are identified as the only factors considered to provide negative incentives. The distribution between direct and indirect effects is fairly even. Five factors directly increase the efficiency and effectiveness of the ML process compared to conventional financial instruments and services. Additionally, this result supports the claim that cryptocurrencies provide positive economic incentives for honest individuals. Seven factors facilitate ML by limiting the applicability of prevailing AML controls. It confirms our assumption that both the direct and the indirect effects on the ML process shape the incentives of criminals.

The results do indicate that cryptocurrencies can be a driver for ML, which has implications on the design of DCSs in general and their applicability as EPSs. It is, for instance, at least questionable if an architecture without the possibility to revoke transactions is a desirable feature for a payment system. Even if a suspicious transaction is detected, it can not be prevented from being processed or reversed afterwards. The pseudonymous nature of cryptocurrencies is another characteristic of systems like Bitcoin that favors their use for ML, as it complicates to trace back individuals involved in illicit actions. The same can be stated for the decentralized administration, without even governmental authorities able to interfere and exclude individuals from misusing such systems. Therefore, these issues have to be considered in the course of assessing the suitability of DCSs in different use cases and also in their development.

3.3.4 Practical Scenarios

Having introduced and analyzed the factors that shape the incentives of criminal individuals to use cryptocurrencies for ML, these factors are subsequently applied to a set of practical scenarios. The section is intended to demonstrate the relevance of the factors for real world examples. A scenario considering transfers of illicitly acquired funds between different jurisdictions utilizing cryptocurrencies is examined in the following. Then, the case of misusing online casinos for ML is presented and it is elaborated on how cryptocurrencies can be implemented in this context by considering two concrete scenarios.

3.3.4.1 Transfers Between Different Jurisdictions

A common ML scenario involves the transfer of funds between different jurisdictions and institutions using complex financial transactions to disguise the illicit origin of funds. There are essentially two reasons explaining the frequent occurrence of this scenario. Besides moving funds to jurisdictions with lax AML regimes and, thereby, reducing the risk for detection, illegal funds are often not obtained within the same jurisdiction they are actually spend (Bauer and Ullmann, 2001). Therefore, money launderers need instruments that allow for a secure transmission of these proceeds. One commonly used approach is to smuggle currency in the form of cash or other valuable objects across state borders. This, however, requires the physical presence of a money launderer and is highly risky as they are faced with border controls. The emergence of instruments for the electronic transfer of funds opened up new possibilities for transferring digital representations of money, which are commonly misused by money launderers. A virtual currency that achieved dubious acclaim for being predominately used for illicit purposes is Liberty Reserve. It was a Costa Rica based service operated by the eponymous company and shut down in 2013 through an intervention of law enforcement authorities (Albergotti and Sparshott, 2013). Liberty Reserve is suspected of having processed 55 million transactions involving more than 1 million distinct users. It is assumed that funds up to the equivalent of 6 billion were laundered using the service (Stempel, 2015).

Figure 15 illustrates the ML schema facilitated by Liberty Reserve. The interlinkage with the real economy was accomplished through verified exchangers. Only they were able to obtain the Liberty Reserve virtual currency (LR) from the operator of the service. The exchange rate of LR was pegged to the value of the Euro or US-Dollar. Exchangers offered various payment options for their customers, such as PayPal or the credit cards American Express, MasterCard or Visa (Reuters, 2013). The LR were transferred into Liberty Reserve accounts, where the personal information users were required to enter were deliberately not checked for their validity (Rüdel, 2013). Thus, users have been able to anonymously and irrevocably transfer balances between Liberty Reserve accounts. Subsequently, they could use verified exchangers for the withdrawal of the funds. This practice rendered cash flows untraceable for public authorities (Richet, 2013).

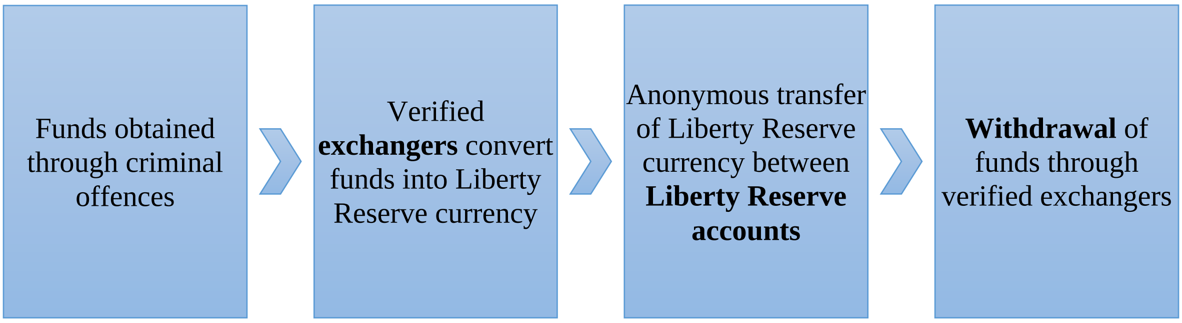

Funds obtained through criminal offences
Verified exchangers convert funds into Liberty Reserve currency
Anonymous transfer of Liberty Reserve currency between Liberty Reserve accounts
Withdrawal of funds through verified exchangers

Figure 15: Liberty Reserve Money Laundering Scheme

Even though Liberty Reserve is no longer running, the general scheme can be translated to the case of ML utilizing cryptocurrencies. In the scenario, a sender based in jurisdiction A wants to transfer funds to a receiver based in jurisdiction B, without causing suspicion and simultaneously not being linkable to the necessary transactions. Generally, this scenario requires exchangers that convert balances denominated in fiat currencies or other virtual currencies into the particular cryptocurrency without collecting personal information about its customers. Such exchange services potentially exist in different manifestations and include: ATMs, direct person-to-person exchanges or local retailers offering exchanges. The same holds true for the destination jurisdictions, where the cryptocurrency is converted back in balances denominated in a fiat currency. This approach enables the transfer of funds between jurisdictions without documenting their flow as depicted in Figure 16.

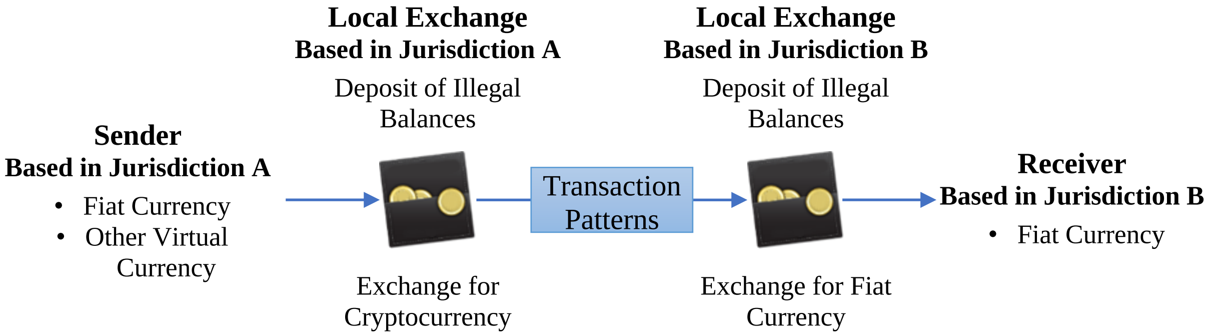


Figure 16: Scenario Transfer between Different Jurisdictions

In practice, certain transaction patterns that commonly occur when illegal funds are transferred between jurisdictions with the purpose of ML can be identified. One of these patterns, particularly used by drug cartels on the US-border to Mexico, is based on the creation of so-called funnel accounts. They are frequently used in combination with ML proceeds generated from illegal trade (FinCEN Advisory, 2014; Department of the Treasury, 2015). In the process of ML, accounts are created that are funded by proceeds originated from geographically distributed sources. These accounts are characterized by the fact that they are not used for daily business activities with regular cash flows (Department of the Treasury, 2015). Instead, they are funded with multiple deposits and the funds are withdrawn after a short period of time. Figure 17 illustrates the particular transaction pattern with cryptocurrencies.

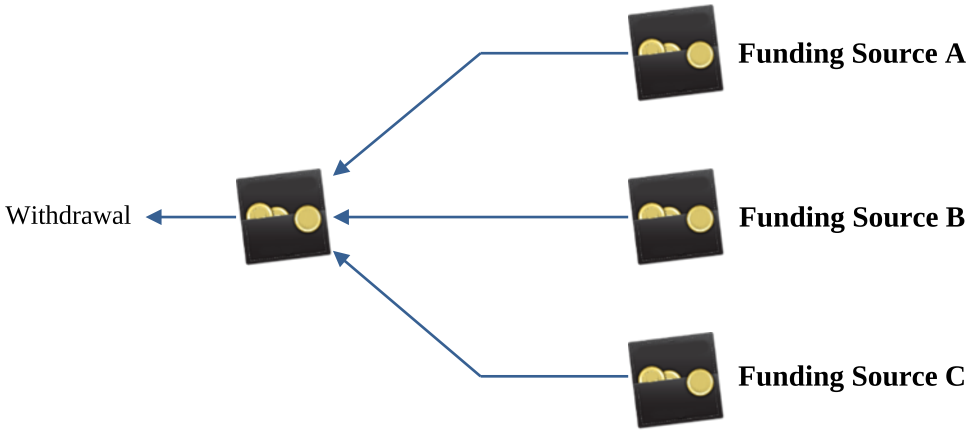


Figure 17: Transaction Pattern Funnel Accounts

Based on the analysis of ML related factors in section 3.3.2, Table 14 examines how and which of these factors influence the incentives of criminal individuals in the transfers between different jurisdictions scenario.

Factors		Explanation	Relevance
Contextual	Acceptability	As long as there are local exchanges that convert fiat currencies for cryptocurrencies and vice versa without collecting personal information, this scenario is feasible. Therefore, acceptability is only of low relevance for the transfers between different jurisdictions scheme.	Low
	Administration	The low barriers to entry of cryptocurrencies allow users to create accounts without restrictions. High risk individuals excluded from other funding options can use cryptocurrencies to create an unlimited number of accounts. This is especially important when funnel accounts are used, since it involves the creation of multiple accounts in order to store and transfer illicit funds.	High

	Authentication Level	Pseudonymous authentication of users supports money launderers to prevent the provision of identifying information. Utilizing exchange services that do not require users to verify themselves (or make it easy to transmit false information), it is difficult for investigative authorities to identify the source of balances.	High
	Price Volatility	Cryptocurrencies are utilized for the actual transfer of funds to be laundered between jurisdictions. Thereby, they are stored in multiple accounts and may remain there for a while. Price variations during this time period result in the risk of losses.	High
Transactional	**Flexibility**	The flexibility of cryptocurrency systems is an important factor for the examined scenarios, since dysfunctions of the network affect the whole process of ML.	High
	Irrevocability	Irrevocability of transactions is of no relevance for this scenario, as it does usually not involve any transacting parties except for the money launderer.	Not Relevant
	Payment Processing	The design feature of cryptocurrencies to refrain from implementing any central intermediaries to verify payments, makes it impossible to implement controls preventing the transfer of balances between several accounts This enables money launderers to unlimitedly transfer cryptocurrencies.	High
	Portability	Portability is an essential prerequisite for cryptocurrencies to be used in the scenario considered, because the transfer of funds between jurisdictions constitutes its overarching objective.	High
	Rapidity	The movement of capital occurs between several cryptocurrency accounts. Since disguising the illicit origin of funds involves multiple transactions, their nearly instantaneous settlement facilitates their timely availability at the place of destination.	High
	Transaction Costs	Transfers of funds between jurisdictions relies on transaction patterns consisting of multiple transactions. Therefore, low or not existent transaction costs dramatically increase the profitability of ML in this scenario. This factor gets even more relevant with a growing number of transactions required to launder proceeds without causing suspicion.	High

Table 14: Relevance of Factors Transfers between Different Jurisdictions Scenario

3.3.4.2 Online Gambling

The four large segments of the online gambling industry consist of sports betting, poker, casinos and bingo. The respective market has been calculated to a value of 35,52 billion US-Dollar for 2013 and a compound annual growth rate of 10,6 percent till 2018 was estimated (James Stocks & Co and KPMG, 2015). Similar to traditional casinos in the past, online gambling is now considered as one of the most favored methods for money launderers.

The reasons that gambling is of such a great relevance for ML are subsumed in Fiedler (2013):

- Gambling involves large transaction volumes and cashflows, which are essential for the concealment of ML
  - ➔ Reduces the risk of detection
- Gambling is not related to a physical product, which is why the traceability of cashflows is complicated
  - ➔ Reduces the risk of detection and allows to understate revenues and overstate costs with the purpose of avoiding taxes
- Profits from gambling are tax-free in many jurisdictions
  - ➔ Reduces the costs associated with ML

Two scenarios where gambling is utilized for ML can be generally distinguished (Fiedler, 2013):

1) The revenues of a preceding crime can be laundered by betting them and requesting a payout of the accruing profits subsequently. This is supported by the exterritorial character of many gambling services, which reduces the detection probability.
2) Gambling as payment method for illegal transactions, realized by transferring accruing profits to the gambling account of the seller of illegal goods and services.

The increasing digitization of business models naturally also affects the gambling industry, which turned the focus of its operators on the online market. This shift resulted in completely new opportunities for money launderers. In many areas, the market is characterized through its unregulated status and illegal nature (it is referred to (Swift, 2015) reporting on illegal sports betting in the United States and (Scherer, 2016) regarding illegal online-games operated by the Italian Mafia). Additionally, these services are internationally available and offer many different payment options. From this starting point, a series of new challenges for combating ML arises. Firstly, unlicensed gambling operators often refrain from verifying that the balances used for gambling are deposited from licensed sources and, correspondingly, are subject to applicable AML policies. Secondly, not all jurisdictions that issue licenses for gambling operators require balances to originate from licensed sources subject to AML policies (McAfee, 2014). This is exacerbated by the challenges related to the checking of deposits and withdrawals with cryptocurrencies affecting both licensed and unlicensed operators. Figure 18 presents the process of deposits and withdrawals in online gambling services.

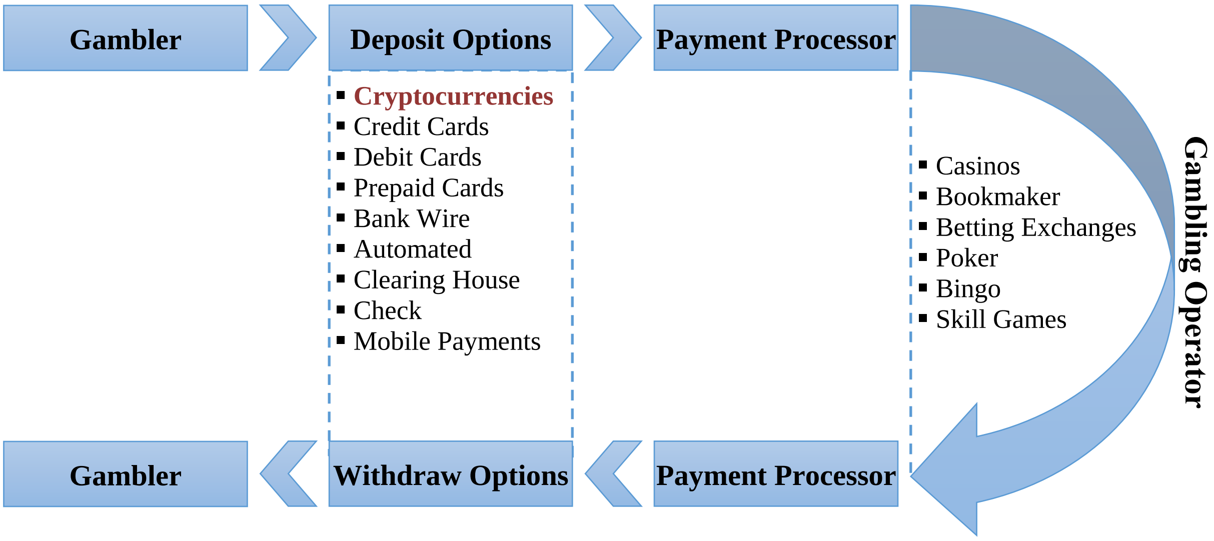


Figure 18: Process of Deposits and Withdrawals in Online Gambling[6]

The scenarios 1) and 2) defined above can be further substantiated by focusing on the concrete use of cryptocurrencies.

Scenario 1) considers a preceding criminal offence that accumulated illegitimate funds, which need to be integrated into the legitimate economy (see Figure 19). If the particular gambling operator is subject to regulation, a one-time payment from a bank account can be compulsory for the identification and verification of the user. The balance can also be used for the later argumentation that gambling proceeds occurred on the basis of this deposit. It is the first step

[6] Figure 18 is based on McAffee (2014)

and is potentially observable for investigative authorities, as payment flows from bank accounts underlie existing AML controls. Cryptocurrencies are used in the second step, where the illegal balances are deposited into the gambling account. The cryptocurrency should preserve the unlinkability of transactions, to prevent investigative authorities from tracing back balances in the gambling account to their illegal source. Finally, the balances within the gambling account are transferred to a bank account as apparently legal gambling proceeds (Fiedler, 2013).

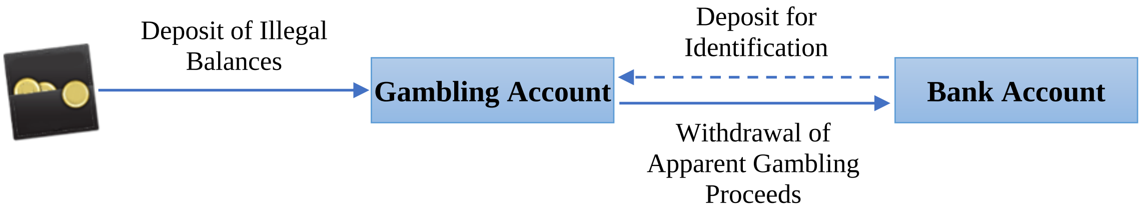

Deposit of Illegal Balances
Gambling Account
Deposit for Identification
Bank Account
Withdrawal of Apparent Gambling Proceeds

Figure 19: Online Gambling Money Laundering with Preceding Crime[7]

Scenario 2) where online gambling is used for the payment of illegal transactions is sketched in Figure 20. In this scenario, balances (which can be legally or illegally acquired) are deposited from gambler A into the corresponding gambling account. Gambler A is the person who proposes to buy an illegal good or service. Therefore, gambler A transfers the balances to a gambling account under the control of gambler B, who represents the provider of the illegal good or service. Eventually, gambler B is able to withdraw the balances apparently obtained via online gambling onto his or her bank account (Fiedler, 2013).

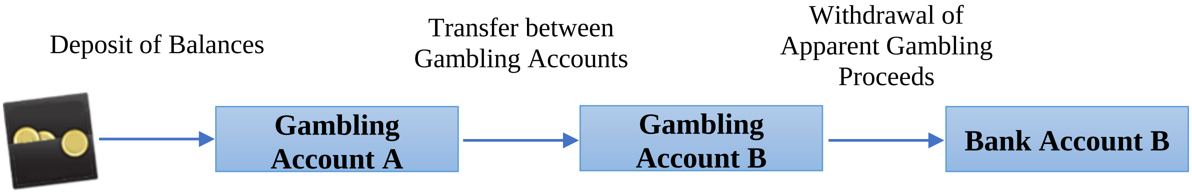

Deposit of Balances
Transfer between Gambling Accounts
Withdrawal of Apparent Gambling Proceeds
Gambling Account A
Gambling Account B
Bank Account B

Figure 20: Online Gambling for the Payment of Illegal Transactions[7]

In both presented scenarios it is also conceivable, that the ultimate withdrawal also occurs in the form of a cryptocurrency onto a respective account. Due to the currently wider acceptance of fiat currencies and their presumed larger utility for the receiver, only withdrawals on conventional bank accounts are assumed. The critical requirement for ML utilizing online gambling services are unregulated operators, which do not underlie any AML policies (Brooks, 2012). Moreover, they are also characterized by higher payment quotas than legally operating services (Fiedler, 2013).

[7] Figure 19 and Figure 20 are based on Fiedler (2013)

Drawn from the analysis of ML related factors in section 3.3.2, Table 15 explains how and which of these factors influence the incentives of criminal individuals in the online gambling scenario.

Factors		**Explanation**	**Relevance**
Contextual	**Acceptability**	Both online gambling scenarios rely on services accepting cryptocurrencies as deposit option. That is why the currently limited acceptance of cryptocurrencies may refrain money launderers from using this kind of money laundering schemes.	High
	Administration	The low barriers to entry of cryptocurrencies allow users to create accounts without restrictions. High risk individuals excluded from other funding options can use cryptocurrencies to deposit balances into gambling accounts.	High
	Authentication Level	Pseudonymous authentication of users supports money launderers to prevent the provision of identifying information. Utilizing online gambling services that do not require users to verify themselves (or make it easy to transmit false information), it is difficult for investigative authorities to identify the source of balances.	High
	Price Volatility	As cryptocurrencies get converted into the unit of account of the respective online gambling service when they are deposited into a gambling account, their price volatility does not constitute a relevant factor in both online gambling scenarios.	Low
Transactional	**Flexibility**	The flexibility of cryptocurrency systems is an important factor for the examined scenarios, since dysfunctions of the network affect the whole process of ML.	High
	Irrevocability	Irrevocability of transactions is of no relevance for both scenarios. Scenario 1) does not involve any transacting parties except for the money launder. Scenario 2) utilizes balances of gambling accounts to pay for illegal goods and services.	Not Relevant
	Payment Processing	The design feature of cryptocurrencies to refrain from implementing any central intermediaries to verify payments, makes it impossible to implement controls preventing deposits from cryptocurrencies into gambling accounts. This enables money launderers to unlimitedly use cryptocurrencies for the funding of gambling accounts.	High

	Portability	Online gambling services, often reside in offshore jurisdictions with lax or non-existent regulations. Portability is an important factor of cryptocurrencies allowing money launderers to use these services.	High
	Rapidity	Cryptocurrencies are solely used for the deposit (and theoretically withdrawal) of balances, while all other capital movements occur within gambling and bank accounts. Because of this, this rapidity of transactions only is a factor of minor relevance.	Low
	Transaction Costs	Since the concealment of the origin of illegal funds takes place by letting them appear as legal gambling proceeds, both scenarios do not rely on frequent capital movements. Therefore, it is not necessary to involve a large number of transactions between cryptocurrency accounts, which renders transaction costs to be a negligible factor.	Low

Table 15: Relevance of Factors in the Online Gambling Scenario

3.4 Available Risk Mitigation Measures

The preceding analysis aimed at providing a better understanding about the economic incentives of criminal individuals to misuse cryptocurrencies for ML based on factors resulting from their specific characteristics. It was identified that cryptocurrencies may indeed constitute an attractive instrument for money launderers from an economic point of view. These findings need to be taken into account for the design of further DCSs and the identification of possible use cases. However, as the analysis indicates, already evolving technological developments and regulatory approaches may also affect the economic incentives. Therefore, an overview of technological developments as well as regulatory approaches is given that are intended to mitigate the risks associated with already established DCSs like Bitcoin.

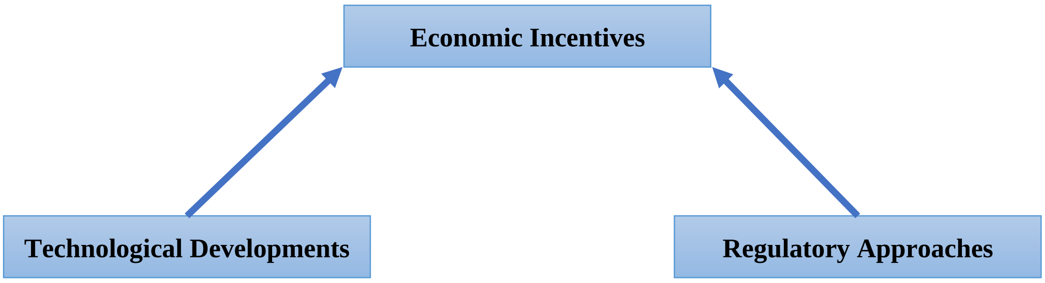


Figure 21: Risk Mitigation Approaches

3.4.1 Technological Developments

A large body of current research on ML with cryptocurrencies in computer sciences concentrates on statistical analysis and data mining to enable traceable transactions. As briefly mentioned above, pseudonymity is only guaranteed as long as an individual's public key cannot be linked to his true identity (Möser *et al.*, 2013). In particular, it is necessary to systematically evaluate available approaches to utilize context information based on the structure of the network inferred from the block-chain (e.g. transactions including amounts transferred over time) and the integration of data from outside the system (e.g. voluntary disclosures of identifying information in social networks). Some promising work has already been conducted in this area (e.g. Meiklejohn *et al.*, 2013; Ober *et al.*, 2013; Reid and Harrigan, 2013). Bonneau *et al.* (2015) provide a comprehensive overview about the anonymity and privacy of cryptocurrencies and evaluates available techniques intended to ensure anonymity.

Nevertheless, it remains unclear to what extent those approaches are appropriate to monitor transactions timely and indicate suspicions for ML. Especially when taking into account recent developments of mixing services or currencies, which aim at providing untraceable transactions (e.g. Sasson *et al.*, 2014; Bonneau *et al.*, 2015; Bonneau *et al.*, 2014; Ruffing *et al.*, 2014). Generally, there are three different approaches for enabling anonymous payments with cryptocurrencies: mixing services on a P2P basis or depending on third parties and cryptocurrency systems offering anonymity in terms of unlinkability of transactions (Bonneau *et al.*, 2015). As already explained as actor in the ecosystem, mixing services transfer payments from a set of input addresses to a set of output addresses in a way making it hard or impossible to trace which input address was intended to pay which output address (Heilman *et al.*, 2016). Mixcoin is an example for such a service to ensure unlinkability, however, the third party operating the service can violate users' privacy and steal coins (Bonneau *et al.*, 2014). Blindcoin is an extension to preserves users' privacy against the third party by using blind signatures similar to the ones used in e-cash (Valenta and Rowan, 2015). But it does not prevent the possibility of stealing coins for the third party. Mixing services on a P2P basis do away with the need for centralized third parties in the mixing process, by enabling users to combine their transactions on a P2P basis. Coinjoin (Maxwell, 2013) and CoinShuffle (Ruffing *et al.*, 2014) are examples for this kind of services. Cryptocurrencies providing unlinkability of transactions, like Zerocash (Sasson *et al.*, 2014) or Zerocoin (Miers *et al.*, 2013), constitute independent systems implementing a novel type of cryptographic proofs (ZK-SNARKs) (Heilman *et al.*, 2016). Unlike mixing services, they are based on their own distributed ledgers as well as protocols and do not directly interact with other systems.

The success of appropriate tools could imply a paradigm shift in AML controls, where monitoring of actual transactions gains more relevance compared to ex-ante customer identification procedures. This would clearly influence the economic incentives of money launderers too. If it becomes possible for law enforcement to link transactions to identities with a certain degree of precision, the probability of identifying suspicious transactions increases. That imposes additional costs on criminals, since they either need to implement more sophisticated laundering schemes or accept the higher risk of prosecution and conviction. To date, research addressing the suitability of cryptocurrencies for ML is primary targeted at Bitcoin. This is not surprising, since Bitcoin is the oldest and most prominent representative. However, it can be stated that criminal individuals will shift their attention to other implementations, the better Bitcoin is understood and observed. Therefore, an ongoing competition is expected between the developers of AML tools and money launderers utilizing new cryptocurrencies or services supporting the obfuscation of transaction flows. Additionally, possible privacy violations have to be considered due to derivations from the permanent public availability of transaction data (Androulaki *et al.*, 2013). Even if it would be technically feasible to trace back every transaction to real identities, this would hardly be in accordance with applicable law to oversee all transactions under general suspicion.

3.4.2 Regulatory Approaches

The regulatory perspective is also highly relevant, because cryptocurrencies are currently hardly regulated and not closely supervised or overseen by any public authority (European Central Bank, 2012). The rapidly evolving nature of technology and business models, with changing market roles and participants providing services, causes uncertainty regarding how regulation should be carried out in practice and needs to be addressed (Financial Action Task Force, 2014). Another challenge lies in tailoring regulation under consideration of the specific characteristics of cryptocurrencies (e.g. actors will be allocated in one jurisdiction and operate in another one). Furthermore, a level of regulation should be identified that minimizes ML risks by creating negative incentives for criminal individuals. At the same time, overregulation must be avoided. Only then it could be ensured that honest individuals do not hesitate from using cryptocurrencies.

This section presents regulatory approaches regarding virtual currencies and is structured according to different types of actions undertaken by governments. It includes the 11 countries with the highest concentration of reachable Bitcoin nodes, which together capture more than three quarters of the overall existing nodes (Bitnodes, 2016). The set of countries covered consists of: Australia, Canada, China, France, Germany, the Netherlands, Russia, Sweden, Switzerland, the United Kingdom and the United States. Table 16 provides an overview over the distribution of the different governmental action throughout January 2008 to September 2016. The detailed list can be found in the appendix of this dissertation. Thereby it is conspicuous that most warnings issued by the different Central banks primary focused on 2013 and 2014. In this time the public interest in the Bitcoin system increased significantly. However, this is also the time period of prominent incidents around the trading platform Mt. Gox and a highly-enhanced price-volatility of the cryptocurreny. Which is why these years are also related to high uncertainty for user and (service-) providers of virtual currencies as well as governmental regulators. The notion of virtual currencies is used hereafter, since part of the governmental actions are explicitly targeted at cryptocurrencies, while others also include other realizations of virtual currencies.

	Governmental Actions				
Year	**Classification**	**Regulation**	**Taxation Treatment**	**Warning**	**Sum**
2008-2010	0	0	1	0	**1**
2011	1	0	2	0	**3**
2012	1	1	0	0	**2**
2013	10	10	7	8	**35**
2014	4	29	9	10	**52**
2015	1	7	3	0	**11**
Jan. – Sep. 2016	1	6	1	1	**9**
Sum	**18**	**53**	**23**	**19**	**113**

Table 16: Overview of Governmental Actions per Year

3.4.2.1 Classification of Virtual Currencies

In Germany, the Federal Financial Supervisory Authority BaFIN classified Bitcoin as **private money** that can be used in “multilateral clearing circles” in accordance to the German Banking Act (BaFin, 2011). On the contrary, Bitcoin is neither regarded as money nor a foreign currency in Australia, but Bitcoin transactions are seen as a kind of **barter arrangement** (Walsh and Murphy, 2013; Australian Taxation Office, 2014a). Canada sees VC as **money service businesses** and clarified that they are not legal tender (The Law Library of Congress, 2014a). China clarified, that Bitcoin does not have legal status and should not be used as a currency and circulate in the market, in fact it is treated as **special virtual good** (Central Bank of China, 2013). France chooses to clarify that Bitcoin cannot be considered to be a real currency or means of payment (Bank of France 2013), because it is seen as property (Perkins, 2016). Sweden classifies Bitcoin as **another asset**, just as art, antiques, jewellery, stamps or copyrights and thus as an investment asset (Ek and Carlstrom, 2014). A court decision in the Netherlands implies that Bitcoin is a medium of exchange and an acceptable form of payment, but not a legal tender, common money, or electronic money (Siemers, 2014). This is in accordance with the United States approach from the Financial Crime Enforcement Network (FINCEN), where virtual currency is also classified as a medium of exchange that operates like a currency in some environments (Financial Crime Enforcement Network, 2013). As in the U.S. every state is responsible for the classification of virtual currencies, some states like the State of California already discuss the possibility of recognizing virtual currencies as **legal tender** (Ponsford, 2015). In Switzerland Bitcoin is no legal tender, because it is stated to not completely fulfill the three main functions of money (Swiss Federal Council, 2014). However, the Swiss Parliament asks for bitcoin to be treated as any other foreign currency in a postulate (Hajdarbegovic, 2013). In the United Kingdom, virtual currencies are seen as **single purpose voucher** (Gilson, 2013), whereby meanwhile there are also exist considerations to classify them as **private currency** (TMF, 2014). According to article 140 of the Russian Civil Code the use of bitcoins can be restricted as the Russian Ruble is the exclusive means of payment in Russia and all prices for financial transactions conducted in Russia have to be defined in Ruble. Virtual currencies are further seen as a **money surrogate**, not an official currency (The Law Library of Congress, 2014b). As seen, the classification of virtual currencies differs markedly among the investigated countries.

3.4.2.2 Regulation of Virtual Currencies

The use of virtual currencies is legal in Australia (Millet 2014). However, there is only a limited regulation of them: As barter money, virtual currencies do not fall under the Corporations Act 2001 and the Australian Securities and Investments Commission Act 2001 which only cover “financial products” (Australian Securities and Investments Commission, 2014). Further, virtual currencies are only sparsely affected by Australia’s current AML regulation that only applies if virtual currencies are exchanged for fiat currencies (or vice versa) and if a transaction intersects with banking or remittance services (Australian Government, 2015). However, the Australian Government recently revealed plans to bring domestic digital currency exchanges under existing Anti-Money-Laundering and Counter-Terrorist-Financing regulation (Buntinx, 2016).

Virtual currencies were exempt from the AML/CFT regulations in Canada for a while (Hamill, 2013) and Canadian regulators, as the Central Bank as well as the government, only monitored developments that involved virtual currencies (George-Cosh, 2014). After a decision of the House of Commons of Canada in 2014, the Canadian AML/CTF act applies to persons in Canada that are engaged in dealing virtual currencies as well as persons outside of Canada that provide such services to customers in Canada (Canadian Minister of Finance, 2014).

Individuals are free to use virtual currencies regarding buying and selling, but financial and payment institutions are subject to restrictive regulating approaches in China. In particular, these institutions are banned from virtual currencies and thus cannot be involved in related transactions (Hern, 2013a). Later, the People’s Bank of China extends the ban on accepting, using, or selling bitcoin as stated in earlier 2013 to third party payment providers. (Hern, 2013b). In addition, websites or exchanges that deal with virtual currencies as bitcoin need to register with appropriate regulatory agencies in China (Hern, 2013a). However, to date Bitcoin and virtual currencies remain legal in the People’s Republic of China (The Law Library of Congress, 2014b).

Already in 2012, French regulators approved a bitcoin exchange company operates as a bank, suggesting that VC companies respectively operate as payment services provider under French law (Lee, 2012). Further, a statement by the French Banking Federation indicates that the wiring of revenue from the sale of virtual currencies to a personal bank account desires the affected bank to file a declaration with the French AML agency (Adamovski, 2014). As the French public authorities see multiple opportunities in the development of virtual currencies, they released the plan to work on a "balanced regulatory framework" for the future (Schechner, 2014).

Contrary to the detailed and advanced approach regarding the classification or the taxation treatment of virtual currencies, Germany has no comprehensive regulatory approaches. In 2014 the German Financial Supervision Authority stated that mining, accepting or using bitcoins does not require bank supervisory licensing. Simultaneously, it is indicated that the commercial use of Bitcoin probably requires licenses (Münzer, 2013). Regarding the challenges of AML and terrorist financing, the German Federal Ministry of Education and Research together with the Austrian Federal Ministry for Transport, Innovation and Technology found a project called "Bitcrime" that investigates approaches for tackling Bitcoin-based crime (Das, 2016).

Because Russia classified virtual currencies as "money surrogates" and not the official currency, the release of virtual currencies is prohibited in Russia according to its federal law (The Law Library of Congress, 2014b). Beside the purchase goods and services using virtual currency, mining of virtual currencies as well as the operating of wallets and exchanges is made punishable. Even as the "distribution of information sufficient and necessary for issuance of money surrogates in media and information and communications networks" is prohibited (Forklog.net, 2015).

The Swiss regulating bodies made sure that no legal vacuum regarding the regulation of virtual currencies exists, as the commercial purchase and sale of virtual currencies as well as the operation of trading platforms are subject to the Swiss anti-money-laundering act (FINMA, 2014). Further, transactions using virtual currencies to buy goods or services as well as the non-commercial sale of virtual currencies in exchange for fiat money underlies the Swiss Code of Obligation. Providers who accept virtual currencies or administer virtual currencies holdings for their clients require banking licenses (Eidgenossenschaft, 2014). Moreover, Switzerland proceeds an innovative approach regarding virtual currencies: as the first administration in the world, the city of Zug accepts Bitcoins as means of payment in a pilot project started in 2016 (Aschwanden, 2016).

Officials from the UK treasury committee, which is amongst others responsible for the Bank of England, the tax authority as well as the financial regulators, stated that "Bitcoin should be regulated by the ordinary commercial business laws with no additional regulation" (Wong, 2014). However, the UK Government announced in 2015 that it will regulate Bitcoin exchanges under the AML-rules (Her Majesty Treasury, 2015).

As a federal regulating body, the FINCEN in the United States classifies virtual currencies as “money service businesses”. Therefore, they “have registration requirements and a range of AML, recordkeeping, and reporting responsibilities under FINCEN’s regulations” (Financial Crime Enforcement Network, 2013). Exchangers and administrators of virtual currencies are further seen as “money transmitters” according to the Bank Secrecy Act. Therefore, they have to implement an AML program and to comply with the recordkeeping, reporting, and transaction monitoring requirements according to FINCEN’s regulations. In addition to that, each money transmitter has to register at the FINCEN within 180 days after starting its business as an exchanger (Financial Crime Enforcement Network, 2015).

In the United States, each state has its own financial regulators laws and thus different regulatory approaches are applied (Coindesk.com, 2014). Hence, the U.S. Conference of State Bank Supervisors released a model regulatory framework for virtual currencies as a recommendation for state bank regulators (US Conference of State Bank Supervisors, 2015).

Whereas Sweden and the Netherlands have no specific regulation for virtual currencies, most countries adopted approaches leastwise covering AML as well as Counter-Terrorist-Financing or classified virtual currencies under existing legal regulation.

3.4.2.3 Taxation Treatment of Virtual Currencies

Australia has clarified the taxation treatment of virtual currencies in detail (Australian Taxation Office, 2014b): Due to the classification as barter money, transactions with virtual currencies are subject to goods and service tax. Further, the supply of bitcoins is an asset for capital gain tax purpose. If bitcoins are used for private transactions, any capital gain or loss from disposal will be disregarded if the cost of the bitcoin is at most 10.000 US-Dollar. If bitcoins are received in exchange for goods or services on the basis of commercial reason, the value is recorded as ordinary income. Any income that derives from bitcoin mining is included in the assessable income. However, the expenses occurred in connection with the mining activity can be used as a deduction, losses are subject to the non-commercial loss provision (Australian Taxation Office, 2014b).

The Canadian Revenue Agency clarified that Bitcoin is not exempt from taxes. However, barter transaction rules apply to bitcoins used for buying goods or services. If bitcoins are bought or sold as a commodity they are subject to capital gains taxes (Allen, 2013). The Internal Revenue Service of the United States of America published a notice regarding existing general tax principles applying to transactions with virtual currency (U.S. Internal Revenue Service 2014). Therefore, virtual currencies are capital assets in the hands of the taxpayer and thus subject to capital gains taxes. Moreover, mining activities are treated as immediate income.

In 2015, the European Court of Justice decided to exempt bitcoins that are exchanged for currency, bank notes and coins used as legal tender from the value-added tax in the European Union (Perez, 2015). The same applies for Switzerland, as the Swiss Federal Tax Administration confirmed considering the decision of the European Court of Justice (Btc-echo.de, 2015). However, the European states published additional taxation treatments. The French Ministry of Economy and Finance declared, that revenues from sales of virtual currencies are taxable income (Adamovski, 2014) and that they – after the classification as property - are subject to capital gains and asset taxes (Schechner, 2014). The German Ministry of Finance made several statements regarding the taxation of virtual currencies. Due to its classification and the use of virtual currencies in multilateral clearing circle, it suggested that it is taxed as capital (Perkins, 2016). However, virtual currencies that were held for more than one year will, in contrast to e.g. assets or bonds, not be subject to the capital gains tax (Eckert and Gotthold, 2013). Moreover, retailers that accept Bitcoins are subject to the value-added tax (Rizzo, 2014). In Sweden, the declaration of Bitcoin as "another asset" allows Sweden to charge capital gains taxes on any transactions using it (Ek and Carlstrom, 2014). In addition, the Swedish Enforcement Authority stated to "start to investigate and seize Bitcoin holdings when collecting funds from indebted individuals" (The Law Library of Congress, 2014b). Guidelines on the taxation of the mining of Bitcoins and other virtual currencies published by Sweden's Tax Authority clarified, that income generated from bitcoin mining activities is declared as income from employment. In Sweden, this incudes income from hobby activities, economic activity and capital (The Law Library of Congress, 2014b). In the Netherlands transactions with Bitcoin and other virtual currencies are taxable as the law stands regarding the income tax. Further this applies for the sales tax. Therefor the value of the virtual currencies has to be converted into Euros (Dutch Ministry of Finance, 2013).

In accordance to the Internal Revenue Service, virtual currencies are covered by the tax system in the United Kingdom. If virtual currencies are used to pay someone (a trader) for goods and services, the profits are taxable. Further, the traders have to convert the profits into sterling before they can enter them into their UK tax returns (Spaven, 2013).

For China, there is no specified regulation for virtual currencies or cryptocurrencies. However, the State Administration of Taxation answered to a request regarding the phenomenon of so-called gold-farmers in 2008. Gold-farmers are people that are employed to play online games in order to earn virtual currency (in-game currency) or equipment. The response implies that income obtained by individuals through selling a virtual currency is taxable incomes for individual income tax (Chu, 2008).

As to date the use of money substitutes, as virtual currencies are classified by the Central Bank of Russia, is prohibited and thus virtual currencies are considered illegal. There are no rules regarding the taxation treatment of virtual currencies in Russia (The Law Library of Congress, 2014b).

3.4.2.4 Warnings Regarding Virtual Currencies

In December 2013, several national Central Banks issued warnings regarding virtual currencies. The Reserve Bank of Australia suggested that Australia sees potential risk and volatility with Bitcoin (Southurst, 2013). After clarifying that bitcoins have no “real meaning”, the People’s Bank of China noted the lack of legal protection, of cryptocurrencies without a central authority. (Hern, 2013b). The warning issued by the Bank of France additionally mentioned further risks regarding the price volatility and difficulties to convert bitcoins to real money (Thomas and Pravin, 2013). Germanys financial supervisory authority issued a report including warnings with respect to the risk of the loss of money, the introduction of transaction fees, fluctuations in value, disputes respective adjustment within the system and that the internal structures of the Bitcoin system might become corrupted (Münzer, 2013).

Similar to the warnings stated above, the Dutch Central Bank warned user with respect to Bitcoins volatile exchange rates and a lack of central issuing institutions at the end of 2013 (Dutch Central Bank, 2013). In the following year, the Central Bank extended its warning to the user of virtual currencies in general, as they lack compensation policies and deposit guarantee systems (Dutch Central Bank, 2014). Even banks and payment institution should be aware of integrity risks derived from the processing of transactions with virtual currencies (Hajdarbegovic, 2014b).

The Swedish Central Bank considers virtual currencies not to be “subject to regulation and the issuers are not under national supervision” and sent a reminder that the consumer protection in this field is weak (Segendorf, 2014a). Only a few months later, the Swedish Central Bank issued a report dealing with the functionalities, benefit and risks of virtual currencies as bitcoins (Segendorf, 2014b). The Swiss Federal Council proposed that Bitcoin is used “for acquiring illegal products or as ransom in cases of extortion” and that Bitcoin can be “abused for ML purposes or stolen with relatively little risk”, wherefore it is seen as a rather high-risk object of speculation (Eidgenossenschaft, 2014).

In the United States, the Financial Stability Oversight Council issued a warning that Bitcoin (and blockchain technologies) are threats to financial stability (Financial Stability Oversight Council, FSOC, 2016). In contrast, the Bank of England stated that virtual currencies currently do not pose a risk to monetary or financial stability (Ali *et al.*, 2014). A dissent can also be seen in the statements from Russian authorities. The Central Bank of Russia regards transactions carried out with Bitcoin as “potentially suspicious” and as a “dubious activity” associated with ML and terrorism financing, wherefore individuals are recommended to refrain from transactions involving bitcoins in 2014 (Dillet, 2014). Which is conflicting with a recent plan of the Ministry of Finance to submit a report to Russian President Vladimir Putin containing the recommendation to promote the use of Bitcoin (Rizzo, 2016).

The European Banking Authority issued a warning dealing with various risks that are derived from buying, holding or trading virtual currencies. This risks occur due to the lack of regulation and contain the risk of losing money and that consumers could be liable for taxes if they use virtual currencies (European Banking Authority, 2013). In 2012 the ECB published a report dealing with virtual currencies, their potentials and risks. Thereby, the ECB curved out the feasible risks to the price and financial stability as well as the risks to the stability of the payment systems. Furthermore, the lack of regulation was dunned by the institution (European Central Bank, 2012). Three years later the ECB published another analysis regarding virtual currencies, which focuses on disadvantages for users due to certain intrinsic characteristics of virtual currencies. To this belong the anonymity, the high volatility and the risk of investment fraud as a consequence of a lack of transparency (European Central Bank, 2015).

3.5 Concluding Remarks

This chapter provided a first step towards a risk analysis of ML utilizing cryptocurrencies in addressing *RQ2: Does the system design of cryptocurrencies, especially Bitcoin, leads to risks in the context of money laundering? More precisely, what are the factors that shape the incentives for criminal individuals to utilize them for money laundering?* To this end, it was focused on the economic incentives of criminals to utilize cryptocurrencies as ML instrument. Only if cryptocurrencies are perceived as beneficial from a criminals' point of view, and for that reason are used as ML instrument, then the system design implemented by Bitcoin and other cryptocurrencies imposes risks for the financial system and society in this context.

This chapter firstly conceptualized cryptocurrencies as digital ecosystems to introduce the relevant actors emerging in their periphery in a structured form. These actors are of particular importance for interaction patterns involving the transfer of cryptocurrencies, therefore they need to be examined when analyzing the use of cryptocurrencies for ML. After an introduction into the economic literature of crime, the ML process was presented, an overview of AML controls was given and the analysis was conceptualized. Based on the conceptualization, this chapter identified and analyzed contextual and transactional factors that facilitate ML from the perspective of criminal individuals. It can be concluded from the results of this explorative analysis that the presented factors might indeed encourage the exploitation of cryptocurrencies by money launderers. This illustrates the risks arising from the specific characteristics of the Bitcoin reference implementation, which consequently need to be addressed. One approach to account for these risks is by mitigating them through technological developments and regulatory approaches applied to existing systems, as presented in the last part of the chapter. Another approach is to design DCSs with different characteristics, which do not exhibit the same vulnerabilities like Bitcoin and corresponding systems. Additionally, it has to be considered if there exist other promising application fields beside cryptocurrencies for such systems. Even though decentralized payments may not be the most suitable application for DCSs due to the arising risks, the concept of decentralized ledgers may be valuable for other use cases.

Consequently, the next chapter tackles the general architecture of DCSs. It firstly gives an overview of different application fields, where systems implementing a distributed ledger that provides transparency regarding transactions processed according to predefined rules may facilitate digital interactions. Subsequently, the common high-level purpose of DCSs is conceptualized. Then it compares the characteristics of so-called permissionless and permissioned types of systems. While Bitcoin is an example of the former type, the latter type accounts for the shortcomings of Bitcoin and similar implementations in some contexts such as payments. Afterwards a set of functional requirements DCSs need to posess is proposed.

4 Architecture of Decentralized Consensus Systems

The preceding chapters of this dissertation were solely concerned with DCSs building upon the Bitcoin characteristics and their application as cryptocurrencies, which facilitate payments between different parties and implement their own respective exchange medium. Since these respective tokens are independent of any form of governmental backed currency, it was discussed under which circumstances they may be regarded as money. Afterwards, cryptocurrencies were classified into existing forms of EPSs and the specific characteristics of Bitcoin got presented on the basis of a technical description. As the characteristics of cryptocurrencies enable transactions without the need to reveal any personal identifying data, their use is often associated with criminal behavior and especially ML. Against this background, a risk analysis of cryptocurrency backed ML was conducted to identify possible risks resulting from their design in this particular context. Consequently, after a general description of the various parties evolving in the ecosystem around these systems, their suitability for ML has been investigated. An economic approach was chosen to identify and analyze factors potentially providing incentives for criminal individuals to use cryptocurrencies for ML. As result, it was concluded that the specific characteristics of the Bitcoin design indeed lead to risks encouraging their misuse for ML.

The following parts of this thesis adopt a broader perspective by abstracting from systems designed like Bitcoin and their use as cryptocurrencies. This procedure allows to also analyze systems that are based on different characteristics than Bitcoin and accounts for application fields beside cryptocurrencies. The concept of distributed ledgers maintained through a collaborative consensus process is discussed as suitable to facilitate and support a wide range of business models and processes. Such a ledger provides transparency regarding the transaction history and is maintained by a distributed network ensuring its validity according to several rules. Systems based on this design approach are generally aggregated under the term DCSs, irrespective of their concrete application.

Tackling *RQ3a*, the first part of this chapter elaborates on the general architecture of DCSs by examining their basic functioning and intended use. To begin with, the relevance of key concepts in the context of DCSs is illustrated. Then, feasible application fields for DCSs are introduced according to an increasing degree of complexity[8]. A model is invented that conceptualizes the high-level purpose of agreeing on a common state between several entities. Subsequently, a classification of design approaches and consensus mechanisms in the context of DCSs is provided according to their specific characteristics. It differentiates between permissionless and permissioned types of systems, which both can be utilized to achieve this purpose. Whereby Bitcoin and other cryptocurrencies are examples for permissionless systems.

Addressing *RQ3b*, the remainder of this chapter identifies functional requirements for DCSs derived from a literature review consisting of relevant publications from actual and potential stakeholders. This ensures that requirements are in line with the stakeholders' objectives. Therefore, methods from Requirements Engineering (RE) are employed in order to develop requirements DCSs need to exhibit in order to be beneficial. It is necessary to define these kinds of systems as clear as possible without being too restrictive. This should prevent the concept of distributed ledgers from developing to a catchphrase for a phenomenon useful for every conceivable purpose. A comparable example is cloud computing, which describes a concept that has been overloaded with hopes and beliefs within the last years, whose feasibility has still to be demonstrated. Therefore, a brief introduction into RE is given and the research approach is presented. Afterwards, a schematic illustration of DCSs, their business environment and user-side is presented to clarify available interaction channels, to describe the relevant actors and reason about potential business models. Then the requirements elicited from the literature review are elaborated.[9]

4.1 Relevance of Key Concepts over Time

In order to get a quick glimpse regarding the evolving relevance of some of the key terms and concepts in the general context of DCSs, their search interest over time on Google is investigated. It is intended to illustrate the growing attention regarding uses beyond Bitcoin and cryptocurrencies. For reasons of clarity and significance, the results are restricted to the terms Bitcoin, cryptocurrency, blockchain and distributed ledger. The terms bitcoin blockchain and bitcoins are left out, because they are too specific and strongly connected to Bitcoin. Therefore, they do not provide any additional insights for the analysis. Cryptocurrency is selected as it

[8] Chapter 4.2 includes and extends parts of Brenig *et al.* (in review [b])

[9] Chapter 4.4 and 4.5 include an extension of Brenig *et al.* (in review [a]) and a part of Brenig *et al.* (2016)

constitutes the first abstraction level from Bitcoin. It accounts for additional representatives of EPSs inspired by Bitcoin, which may provide some modifications in their features. Another term of interest is blockchain, since it is solely tied to the technical foundation of Bitcoin and implies applications besides cryptocurrencies. Distributed ledger also encompasses systems that are only inspired by the philosophy behind Bitcoin, but can be designed completely different from a technical perspective. As an academic concept without a wider dissemination in the general public, the notion of DCS is excluded from the search interests examined.

Figure 22 provides an overview of the individual Google search interest in the four examined terms extracted via Google Trends (Google, 2016). The results of the different terms are not related to each other, hence it is not possible to compare the depicted graphs. The numbers represent the average indexed search interest of a keyword relative to the maximum value in the chart. In the event of the maximum number of queries for a specific keyword, the chart displays 100. Thus, these statements do not reflect the absolute search volume, but they are helpful to see how the interest on a specific topic changed over time. The tool Google Stats provides search queries since January 2004, however, the charts start at the month of the publication of the Bitcoin whitepaper in November 2008.

One can observe the maximum interest in Bitcoin was at the End of 2013 from the chart below. The number of search queries rapidly decreased in the following month and fluctuates between values ranging from just under 18 percent to 35 percent afterwards. Especially in the months around the maximum value of Bitcoin, the popularity of cryptocurrency sharply increases and is correlated with Bitcoin. It reaches the maximum of queries slightly delayed in February 2013. Cryptocurrency was also characterized by a decrease of interest in the month following, however, it was continuously increasing again to a value of 64 percent in September 2016 over the previous 15 months. The term blockchain was nearly irrelevant until December 2012. Then the search interest grew to values of around 20 percent of the maximum until Mai 2015. Since June 2015 the queries were constantly increasing with a maximum value reached in September 2016. The queries of distributed ledger have experienced a similar development as those of blockchain, with a maximum of 100 percent in September 2016 too. One can conclude from the graph that the interest in Bitcoin remained relatively stable from May 2014 till September 2016. However, this interest is on a level far below its maximum. On the contrary, the queries for all other terms increased significantly. This can be interpreted as a growing interest in applications of the technology apart from the concrete implementation Bitcoin.

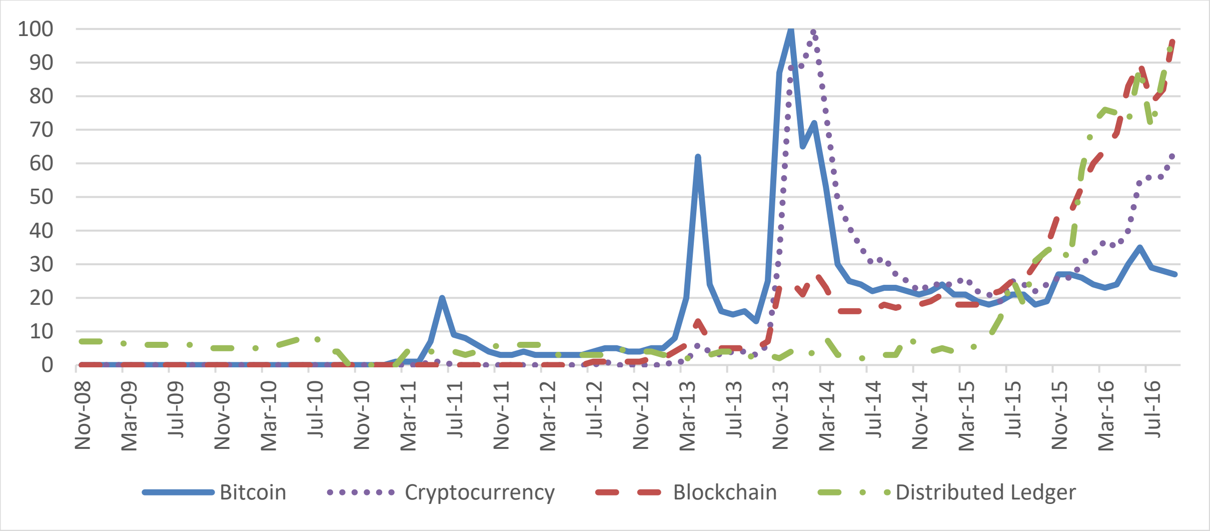


Figure 22: Individual Search Interest in Key Terms over Time

A comparison of the popularity of the four Google search queries is depicted in Figure 23. This feature of Google Trends is intended to provide an overview of how certain search terms perform to each other over time. One can immediately recognize that Bitcoin is by far more searched than the queries cryptocurrency, blockchain and distributed ledger, irrespective of the declining individual interest. Except for blockchain, the popularity of the other terms is so low that it is not measurable. Nevertheless, the chart provides the useful insight that Bitcoin is still the dominant search term in the context DCSs. What cannot be derived from the data is the intention behind the search queries. Do individuals search for Bitcoin because they are interested in the concrete system or is Bitcoin used as umbrella term for related but distinct concepts?

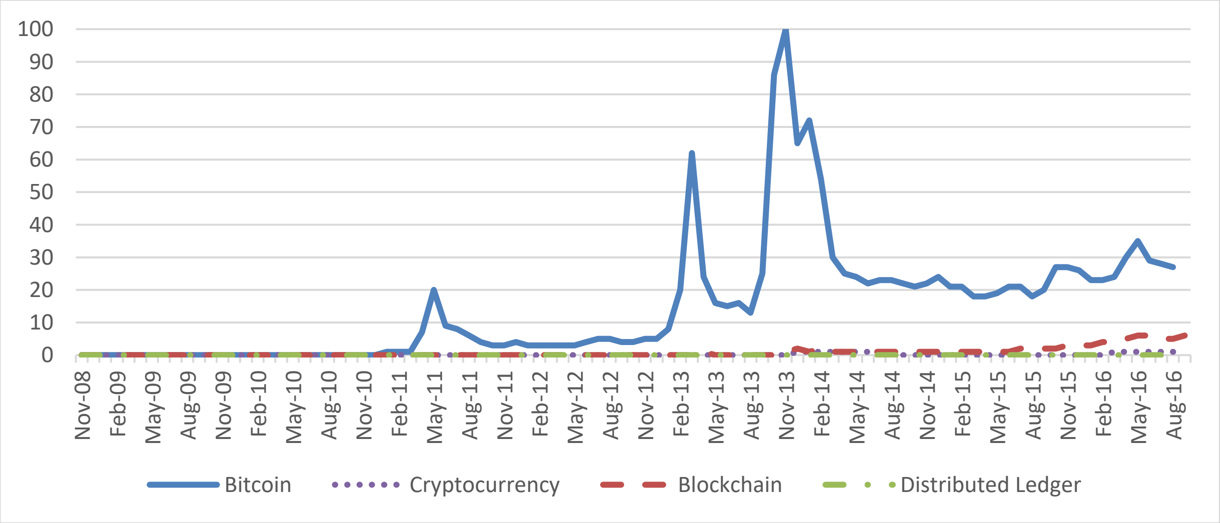
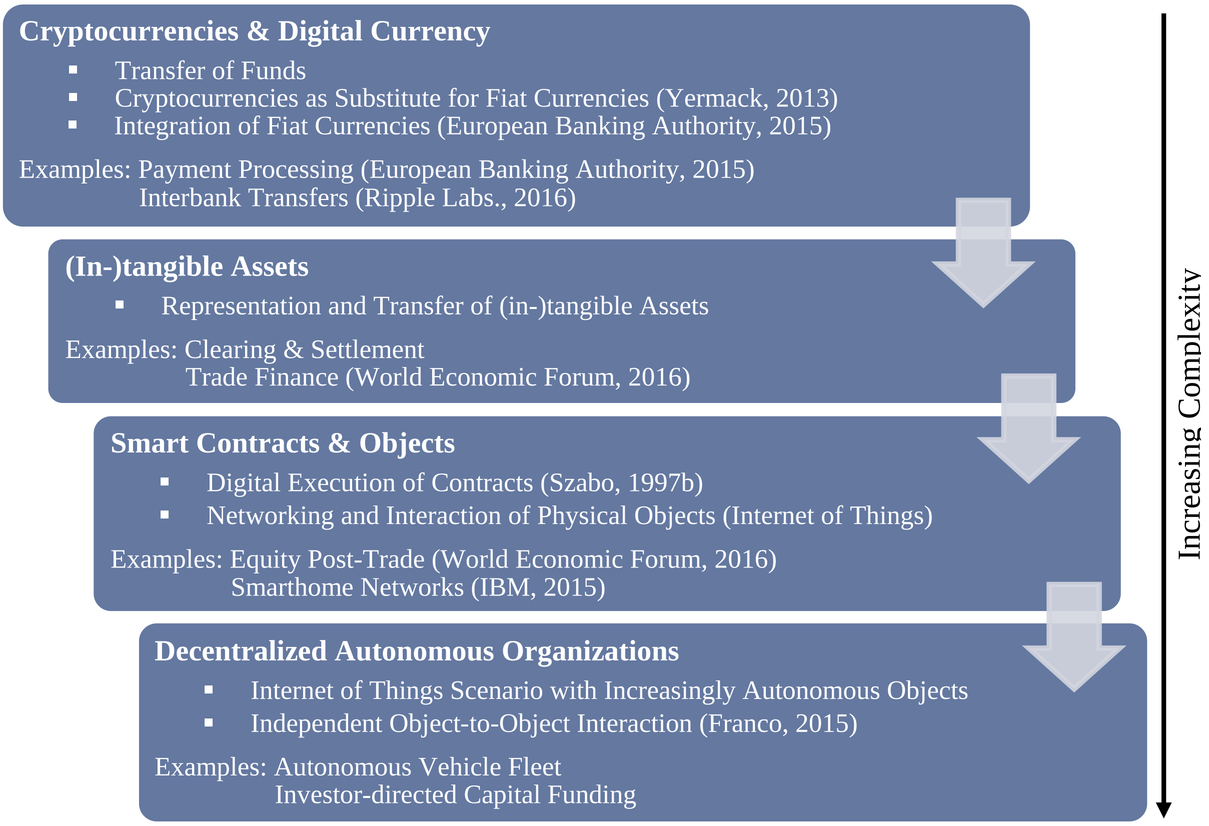


Figure 23: Comparison of Search Interest in Key Terms over Time

4.2 Development Towards Decentralized Consensus Systems

The fundamental idea of distributed ledgers providing transparency of transactions included based on certain rules is discussed in various application fields. Although the findings of the preceding chapter revealed the arising ML risks in the application of cryptocurrencies, DCSs may still be suitable to support other use cases. Figure 24 categorizes possible applications broadly according to the degree of complexity of their implementation.



Cryptocurrencies & Digital Currency

- Transfer of Funds
- Cryptocurrencies as Substitute for Fiat Currencies (Yermack, 2013)
- Integration of Fiat Currencies (European Banking Authority, 2015)

Examples: Payment Processing (European Banking Authority, 2015)
Interbank Transfers (Ripple Labs., 2016)

(In-)tangible Assets

- Representation and Transfer of (in-)tangible Assets

Examples: Clearing & Settlement
Trade Finance (World Economic Forum, 2016)

Smart Contracts & Objects

- Digital Execution of Contracts (Szabo, 1997b)
- Networking and Interaction of Physical Objects (Internet of Things)

Examples: Equity Post-Trade (World Economic Forum, 2016)
Smarthome Networks (IBM, 2015)

Decentralized Autonomous Organizations

- Internet of Things Scenario with Increasingly Autonomous Objects
- Independent Object-to-Object Interaction (Franco, 2015)

Examples: Autonomous Vehicle Fleet
Investor-directed Capital Funding

Figure 24: Application Fields According to Degree of Complexity

The category Cryptocurrencies & Digital Money encompasses all DCSs intended to facilitate the digital representation of money. As already explained in chapter 2, cryptocurrencies are part of the concept of virtual currencies, which according to the ECB is "a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money" (European Central Bank, 2015, p. 25). Their native asset (e.g. bitcoin, litecoin, dogecoin) serves as a unit of account and is independent of any government-issued currency. This opens up opportunities for cryptocurrencies to act as a substitute for conventional currency at least in some contexts, depending on the extent to which they fulfill the monetary functions medium of exchange, store of value and unit of account (e.g. Mankiw, 2016). If this holds true, it would “enable transactions across national borders and currency denominations without the interference of sovereign entities and central banks” (Lo and Wang, 2014, p. 2). Digital currency is an umbrella term covering any electronic form of currency (Financial Action Task Force, 2014), which accounts for efforts to integrate fiat currencies into DCSs in order to use them as payment networks. By maintaining a fixed exchange rate parity or directly supporting conventional currencies, DCSs may represent a challenge for centralized consumer and interbank payment infrastructures. Particularly, they offer resilient networks (Zohar, 2015), some of them privacy (Miers *et al.*, 2013) and theoretically reduced costs and entry barriers compared to conventional payment processes (European Banking Authority, 2015). A frequently discussed scenario are central banks acting as a backer of the native token.

(In-) tangible Assets describes the digital representation of heterogeneous types of assets beyond cryptocurrencies and digital money. By supporting heterogeneous types of assets, DCSs set up the infrastructure for a wider range of applications (Glaser and Bezzenberg, 2015). Financial institutions are interested in DCSs for issuing financial assets because of issues of consumer and regulator trust. NASDAQ, for instance, is running a pilot project in its private equity market (Hope and Casey, 2015). More generally, DCSs could provide decentralized infrastructures for any application relying on intermediaries to track ownership and enable the transfer of property (Fairfield, 2014). This enables direct transfers between two or more parties, by replacing functions of conventional trusted third parties with transparency and integrity of the stored data. The supported functions of such systems include the processing of transactions as well as record keeping for dispute resolution and mitigation of the risk of fraudulent behavior (Skevington and Hart, 1997). The role of third parties is limited to the verification of identities and the existence of (in-) tangible assets in this context (Mainelli and Smith, 2015). The respective applications can either be implemented as an additional layer on top of cryptocurrencies, where the native tokens represent (in-) tangible assets as so-called colored coins (Shomer, 2016) or they are integrated into specifically designed systems (Linux Foundation, 2015). DCSs are increasingly acknowledged as potentially improving existing business models and replace legacy systems for issues like clearing and settlement of transactions (for private and public equity, insurance policies, property titles, etc.) or post-trade operations (DTCC, 2016; Taylor, 2015).

Smart Contracts & Objects refers to the ability of DCSs to perform logical operations enabling the formalization of relationships between individuals and objects. Originating from Szabo (1997), smart contracts constitute computer protocols that aim to facilitate, verify and enforce the negotiation or performance of a contract. Thus, contractual terms are recorded in computer language instead of natural language and can be automatically executed (Government Office for Science, 2016). The definition is refined in conjunction with DCSs as "an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger" (Brown, 2015). Systems that facilitate the use of smart contracts provide functionalities exceeding the sole representation and transfer of (in-) tangible assets, by allowing for self-executing contracts regarding a priori determined agreements between contracting parties. To implement smart contracts, Turing-complete scripting languages are used by many DCSs in development (e.g. Clearmatics, 2016; Eris, 2016; Ethereum, 2015). This increases the complexity of applications, since the automatic fulfillment of contractual obligations can be conditional on the occurrence of external contract-related events sending information to the programmed contract.

Smart Objects are physical devices – such as sensors, actuators, tags, appliances etc. – that are able to network and interact with each other in a so-called Internet Of Things (IOT) scenario (Atzori *et al.*, 2010). Within certain companies in the high-tech industry, DCSs are envisaged as having the potential to constitute the infrastructure to connect billions of smart objects by providing a "framework facilitating transaction processing and coordination among interacting devices" (IBM, 2015, p. 11). In this IOT, users bind with devices such as washers, cars or thermostats using secure identification and authentication. The devices intelligently interact and communicate with each other by exchanging data and information (Uckelmann *et al.*, 2011). Thus, opportunities for completely new business models arise. As already acknowledged by IBM (2015), DCSs allow for a distributed, scalable and trustless form of coordination between intelligent devices. Contrarily, current IOT solutions rely on centralized clouds and server farms characterized by high costs for infrastructure, maintenance and service (Brenig *et al.*, 2016).

Decentralized Autonomous Organizations (DAOs) characterizes organizations consisting of autonomous agents operating without any human intervention, controlled by a predefined set of binding rules (Glaser and Bezzenberg, 2015). In DCSs, these binding rules can be formalized as contractual terms within smart contracts. Hence, choreographies of different smart contracts and their interrelations form the basis for DAOs (Norta, 2015). The transition from Smart

Contracts & Objects to “DAOs is blurry, as it is not clear when an adequate level of autonomy of an organization is achieved to act as a DAO. Especially it still describes a new design approach towards organizations without human supervision to ultimately “orchestrate human and non-human interaction in intelligent ways” (Glaser and Bezzenberg, 2015, p 2). First implementations from the real world include automated venture capital funds to disperse capital amongst projects without relying on centralized decision makers. Instead, the investors decide where funds are allocated to in a democratic voting process (The Economist, 2016).

4.3 High-Level Purpose: Agreement on a Common State

After having clarified the different application fields for DCSs according to their complexity, this section examines how they can be supported by these systems in general. The high-level purpose of every DCS is to enable an agreement between several entities participating within the network on a commonly accepted state. This commonly accepted state is achieved through a consensus process, whereby the entities utilize an instrument X which determines whether a given state is acceptable based on predefined rules. Instruments to define whether a given state is acceptable are consensus mechanisms. The foundation of consensus mechanisms for DCSs is that every interaction in digital economies is built upon the processing, recording and storing of transactions. To this belong the exchange of messages on social media platforms, online purchases, the representation of intangible assets or phone calls and smart electricity metering (IBM, 2015). Consensus mechanisms exploit the characteristic of DCSs to record every conducted transaction in distributed ledgers. On a fundamental level, transactions are thereby atomic changes to the actual state of the ledger.

4.3.1 Consensus via Decentralized Consensus Systems

Figure 25 presents a multi-layered structural model to illustrate the consensus-building via DCSs. The structural model distinguishes between two different layers: the design-layer and the system-layer. While the outer design-layer focuses on the process of determining the structure of an acceptable state, the inner system-layer relates to the technical dimension of the respective DCS.

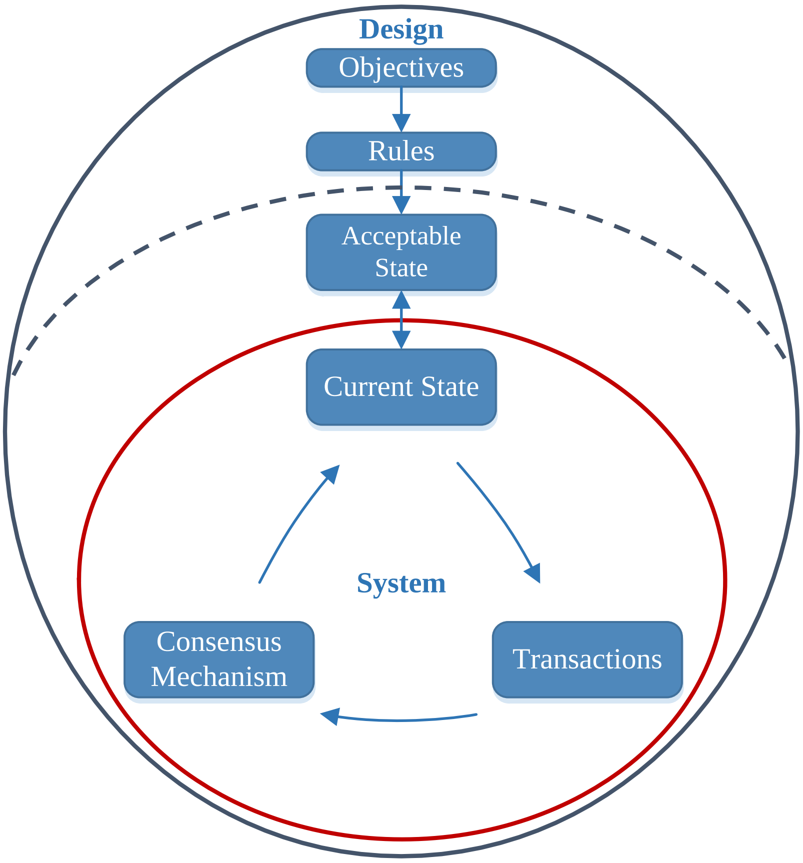


Figure 25: Multi-Layered Structural Model for DCSs

On the design-layer, stakeholders need to reach a consensus with respect to the objectives of a DCS. These objectives depend on the specific use case and include, among other things, statements about the nature of supported business models or the kind of transactions which should be facilitated by the system. It is important to note, that this upstream process of consensus finding depends on the organizational structure governing the intended DCS. Whether it is a community-driven project where various interests have to be considered, a consortium consisting of several independent entities or a profit-seeking enterprise with only a few decision makers, heavily influences the complexity of negotiations (Raiffa *et al.*, 2007). The process of specifying common objectives is not supported by a DCS, since it involves decisions how the system is to be designed. In the simplest case, entities implicitly agree on a set of objectives by using a particular DCS after its implementation. The identified objectives are subsequently used to derive concrete rules concerning the desired functionalities of the DCS. As a result, it is possible to determine the structure of an acceptable state. A state in this context is defined as acceptable, if it is in line with the previously set objectives.

On the system-layer, the technical implementation of a DCS is considered. Starting with a set of transactions, the consensus mechanism decides which of them are included into the ledger based on predefined rules. This rules for consensus mechanisms need to provide instructions regarding:

- Which transactions are qualified to be included into the ledger
- Which participants of the network are eligible to validate transactions
- How the validation process is actually carried out

The result is a current state of the ledger, which is replicated and shared among the participating nodes of the network. Originating from this current state, the loop represents an ongoing process of regular transactions which need to be taken into account. The consensus mechanism ensures that the ledger for all nodes is updated to the same current state. However, in order to fulfill the high-level purpose of coming to an agreement on a common state, the structure of the current state should be in accordance with the structure of the acceptable state and hence also with the objectives. A system can only be classified as DCS if this holds true. Requirements for DCSs must ensure that a system fulfills the high-level purpose.

4.3.2 Consensus in the Bitcoin System

For clarification, the structural model is exemplarily applied to the Bitcoin system as the arguably most well-known DCS. On the design layer, the objective of the Bitcoin developers was to provide “an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party” (Nakamoto, 2008, p. 1). The consensus about this objective was reached amongst the developers who wrote the introducing whitepaper in 2008. The growing number of network participants implicitly agree on this objective by using the system for transactions. However, an ongoing debate about an increase in the transaction processing capacity of the network illustrates the complexity of negotiations in community-driven project like Bitcoin (Priestley, 2016). The dispute boils down to the question, whether Bitcoin should compete with general payment networks like MasterCard or Visa. Given this objective, it is possible to derive at least two concrete rules relating to common issues in electronic cash systems: 1. the system must provide a proof of ownership of coins, 2. it must prevent double-spending of already transacted coins (Nakamoto, 2008). These issues are traditionally solved by using trusted third parties instead of a DCS (e.g. Chaum *et al.*, 1990). Accordingly, a state is acceptable in the

Bitcoin system when the ledger is just consisting of transactions which comply with the concrete rules.

On the system level, authentication is achieved by means of asymmetric encryption, which enables the pseudonymous transfer of Bitcoin coins. Actual transactions are carried out by signing a hash of the previous transaction where the particular coin was transferred combined with the public key of the intended recipient (Nakamoto, 2008). This should ensure that transactions are only qualified to be included into the ledger, if the sender is in possession of the private key. A proof of ownership of coins is provided in this way. The Hashcash POW algorithm, as already explained more detailed in section 2.3.4, is an approach to prevent attacks on a given system grounded on an economic rationale. It assumes that if a sufficiently high level of costs in terms of computing power is required to perform a successful attack, it induces rational individuals to behave honest. This may be a level of costs higher than the expected gains from an attack, or that the intended use of the system is the most profitable alternative. In the Bitcoin system, the distributed ledger evolves from including timestamped records of recent transactions into so-called blocks regularly broadcasted to and validated by all peers connected to the network. The POW mechanism determines which node in the network is authorized to broadcast the actual block of transactions. For this, nodes have to expend computing power to find a nonce value that, "when hashed with additional fields (i.e., the Merkle hash of all valid and received transactions, the hash of the previous block, and a timestamp), the result is below a given target value" (Karame *et al.*, 2012, p. 907). Whoever solves this computing intense trial and error puzzle first publishes the block and is rewarded with newly created coins and (voluntary) transaction fees. Every block refers to its predecessor, therefore, the distributed ledger is termed blockchain. The blockchain allows the participants to check if certain coins were already spent before and, if this is the case, the associated transactions are rejected from the shared ledger.

The current state in the Bitcoin system is the latest version of the blockchain the network peers agreed upon. As long as the system is secure against attackers, this current state includes all qualified transactions of coins, and only these, and is therefore in accordance with the acceptable state. Nevertheless, there may also be participating individuals pursing objectives which are not necessarily in accordance with the acceptable state (e.g. spend coins they do not own; exclude certain undesired transactions from processing). The chance of success of an attack on the system depends on the ability of such individuals to rewrite prior parts of the blockchain or to continue it in their own favor. In POW based system like Bitcoin this chance is positively correlated with the controlled computing power. If the majority of computing power is controlled by individuals who prefer to reach the acceptable state, the system remains secure against attacks (discussing security issues of Bitcoin in detail is out of the scope of this thesis, the interested reader is referred to the comprehensive body of literature available like (Bonneau *et al.*, 2015)).

4.4 Classification of Decentralized Consensus Systems & Mechanisms

This section provides an introduction and classification of design approaches and consensus mechanisms proposed in the context of DCSs. Having clarified the range of application fields as well as the high-level objective of DCSs, it needs to be elaborated on their architecture. Generally, it is distinguished between permissionless systems and permissioned systems (e.g. Government Office for Science, 2016; Swanson, 2015) to achieve the purpose of agreeing on a commonly accepted state of the ledger. The two types of systems describe opposite approaches for the design of DCSs and apply completely different paradigms regarding their openness as well as the toleration of centralized entities with exclusive rights. Systems between these extremes, which combine features from both approaches, are also conceivable. Permissionless and permissioned systems are compared and delimited from each other on the basis of several properties and their particular characteristics as summarized in Table 21. The properties correspond to those already introduced in section 2.3, covering the technical background and specific characteristics of Bitcoin. It constitutes the reference implementation for completely permissionless systems, therefore the explanations can be generalized and used for their understanding. Due to this, Tables 17-20 only present the characteristics of permissioned systems in detail. These characteristics account for the risks arising from permissionless implementations, as examined in chapter 3 of this dissertation. However, they also imply the reintroduction of some level of trust in centralized entities. The listing order deviates from Bitcoin’s description, because the explanations in this section are logical extensions of one another instead of providing a technical description of a concrete system.

Permissionless systems, sometimes termed public systems, grant an unrestricted permission for every entity to participate on the consensus process (i.e. the consensus mechanism has to consider every node in the network when updating the current state of the system). Unrestricted permission to participate on the consensus process allows nodes to use pseudonymous authentication methods. Permissioned systems, sometimes called private systems, restrict the permission for entities to participate on the consensus process (i.e. the consensus mechanism has to consider only a restricted number of nodes in the network when updating the current state of the system). Restricted permission to participate on the consensus process requires an identified authentication of nodes, which can also be held legally accountable for their actions (as already recommended by the European Banking Authority (European Banking Authority, 2004)).

Property	Characteristic	Explanation
System Participation	Permissioned	Access to the system is permissioned to authorized participants.
User Authentication	Identified	Participants need to provide personal information in order to authenticate at the system.
Consensus Participation	Restricted Permission	The consensus process is restricted to authorized entities only.

Table 17: Properties Permissioned Ledger User

The consensus process in permissioned systems can be controlled by one centralized entity, but also by a consortium consisting of several entities (Buterin, 2015; Government Office for Science, 2016). This implies that only permissionless systems fulfill the property of censorship resistance. The notion of censorship resistance can be understood as the ability to prevent a third party from imposing a particular set of transactions to be included into the ledger (e.g. Perng *et al.*, 2005). Due to the fact that the consensus participation in permissioned systems is restricted to identified designated authorities only, these entities have the capacity to exclude certain transactions and can be held accountable for transactions they include. In accordance with applicable AML regulation (e.g. European Union, 2005), designated authorities may be obliged to report suspicious transaction and prevent them from being processed.

Property	Characteristic	Explanation
Censorship Resistance	Unfulfilled	The possibility for third parties to prevent certain transactions from being included into the ledger.

Table 18: Property Permissioned Ledger Censorship Resistance

Resulting from the design decision to accommodate the use of pseudonyms, it is not possible to define different user roles in permissionless systems if accountability is a desired feature. Consequently, no means for the implementation of access controls are provided. The identified authentication in permissioned systems allows to specify concrete user roles. Governmental institutions, for instance, may get complete read permissions for the purpose of compliance checking, while the insights of conventional users are limited to transactions they are involved in. The properties already mentioned affect the available governance structures for DCSs. While projects implementing permisionless systems try to avoid centralized responsibilities by discussing major changes to the system within a community in a more or less democratic process, permissioned systems rely on a centralized governing organization. This centralized organization is required to authenticate users, determine restrictions for the consensus participation, to be held finally accountable and define appropriate roles for access controls. The two different types of DCSs rest upon opposing paradigms regarding the toleration and even desirability of central entities at the governance level as well as the consensus process level. The design approach of permissionless systems aims at circumventing any kind of central entities at both levels. In contrast, the proper functioning of permissioned systems relies on central entities responsible for the governance and consensus finding. The utilized type of system has considerable consequences on the applicability of alternative kinds of consensus mechanism. It is not the purpose of this dissertation to discuss stability related issues, which can be understood as the ability to continuously facilitate the agreement on a common state as the system grows in participants and novel attack vectors arise (Bonneau *et al.*, 2015). Instead, alternative concepts for consensus mechanisms are compared in terms of their properties and implications on the functionalities of DCSs.

Property	Characteristic	Explanation
Read Access	Access Control Feasible	The distributed ledger provides transparency regarding transactions to entities allowed to access this information.
Governance	Centralized	The system is governed by a centralized entity able to independently change the rules of the system.

Table 19: Properties Permissioned Ledger Access and Operation

Consensus mechanisms for permissionless systems are grounded on the principle that participation on the consensus process necessitates the expenditure of economic resources. A properly-functioning consensus mechanism realizes an incentive compatible Nash equilibrium, where deviating from the predefined rules does not result in a net gain (Kroll *et al.*, 2013). Therefore, a rational individual has no incentives to undermine the consensus by attacking the system. The Hashcash POW algorithm is the most prominent example for consensus mechanisms used in permissionless systems. Investments into hardware and infrastructure as well as the costs incurred for electricity are the common resources which are expended to compete for rewards in the form of coins and fees, although the protocols slightly differ between different implementations. Litecoin, for example, provides shorter periods for the creation of blocks than Bitcoin, which renders the verification of transactions faster (Litecoin, 2016). Furthermore, the used hash function varies between different systems, whereby SHA-256 (Dang, 2015) and Scrypt (Percival and Josefsson, 2012) are frequently used algorithms. Achieving consensus with POW, however, comes at the cost of an enormous amount of constantly consumed computing power, which constitutes a major drawback of such systems (Becker *et al.*, 2013). One attempt to address the issue is by extending the consensus mechanism with useful purposes, like incorporating obligations to store data files (Filecoin, 2014) or search for prime numbers (King, 2013) as part of the consensus process. Another approach substitutes computing power by other resources, which does away with the cost overhead for operating the system and is called Proof-of-Stake (POS) (Bonneau *et al.*, 2015). The first system that implemented POS for the consensus process was Peercoin (King and Nadal, 2012). It always boils down to some form of proof of ownership of the coins implemented in a permissionless system: The greater the share of coins in possession of one individual in the network, the larger is the probability that this individual publishes the next block. The argument in favor of POS from an economic point of view is that ensuring the proper operation of the system is incentive-compatible for a rational user with a high stake. Since consensus mechanisms in permissionless systems are based on the expenditure of resources, a native token is imperative for reconciling the incentives of individuals with the predefined rules determining an acceptable state. POW systems reward individuals with valuable coins to ensure honest behavior is incentive compatible and POS systems bind the consensus on the individual's stake of coins.

Crucial condition for the stability of permissionless systems is their ability to ensure that behaving according to predefined rules is incentive compatible for rational individuals. This condition also needs to be fulfilled, if individuals originally intend to pursue objectives not in line with the rules. In contrast, permissioned systems accept the presence of individuals with economic incentives to compromise the system. To nonetheless reach an acceptable state, centralized governance in combination with identified user authentication allows to restrict permissions for the consensus participation to a set of reliable parties. This parties need to be trusted to behave according to the predefined rules, because it is in their own interest (e.g. EY, 2016; International Monetary Fund, 2016). Even though all nodes participating on the consensus process in this scenario are assumed to be reliable, it needs a mechanism to maintain a consistent state of the distributed ledger shared between the network nodes. It may also be the case that some nodes have diverging interests despite restricted permissions or that nodes come to different states because of other failures. It is therefore essential for the consensus mechanism to tolerate a limited number of faulty nodes in the network. This class of failure, where nodes exhibit arbitrary behavior are defined as byzantine faults (Driscoll *et al.*, 2003). Consequently, the utilized consensus mechanism needs to guarantee the important distributed system correctness criteria of safety ("nothing bad happens") and liveness ("something good will eventually happen") in a network consisting of identified and permissioned nodes (Alpern and Schneider, 1987; Amir *et al.*, 2011). Consensus mechanisms to maintain a consistent state of a system like Byzantine Consensus protocols (e.g. Lamport, 1998) or Byzantine Fault Tolerance algorithms (e.g. Castro and Liskov, 1999) have been applied in distributed architectures for decades. These protocols already received considerable attention in the systems research literature for applications such as database systems (e.g. Garcia Molina *et al.*, 1986). Their use to coordinate the network for achieving a consensus on transactions in permissioned distributed ledgers, however, is a novel application. As consensus mechanisms in permissioned systems are not based resource expenditures, tokens are optional and not used for the consensus process.

Property	Characteristic	Explanation
Consensus Mechanism	Synchronization of Distributed Networks	Implemented to ensure that the actual state of the system is synchronized between the network participants.
Native Token	Optional	A native token can be optionally integrated into the system. However, it is not necessary for the provision of incentives in the consensus process.

Table 20: Properties Permissioned Ledger Consensus Process

After having compared permissionless and permissioned types of DCSs, Table 21 provides a final overview of their properties and the respective specific characteristics.

Type / Properties	**Permissionless System** ***Public System*** **Characteristics**	**Permissioned System** ***Private System*** **Characterstics**
System Participation	Permissionless	Permissioned
User Authentication	Pseudonymous	Identified
Consensus Participation	Unrestricted Permission	Restricted Permission
Censorship Resistance	Fulfilled	Unfulfilled
Read Access	No Access Control	Access Control
Governance	Community-Driven	Centralized
Consensus Mechanism	Underlying Principle: Expenditure of Resources ▪ Proof-of-Work ▪ Proof-of-Stake	Consensus Mechanisms in Distributed Networks: ▪ Byzantine Consensus ▪ Byzantine Fault Tolerance
Native Token	Imperative	Optional

Table 21: Types of Decentralized Consensus Systems

4.5 Requirements for Decentralized Consensus Systems

The classification of DCSs into permissionless and permissioned types (as well as solutions between these extremes) illustrated the different sets of characteristics such systems can possess. However, the requirements for the development of DCSs still remain vague. Addressing the issue, this section identifies functional requirements DCSs need to fulfill at the most fundamental level. As foundation for the elicitation of requirements, an agent-based framework consisting of the relevant actors of such systems is provided. The actual requirements are based on a review of industrial research and whitepapers concerned with distributed ledgers in order to reflect stakeholders' needs. They are intended to support academics in understanding the peculiarities of DCSs as well as practitioners in building DCSs that meet stakeholders' goals.

4.5.1 Requirements Engineering & Research Approach

In many system development projects, a discrepancy exists between operational needs and the actual design of IS (Castro *et al.*, 2002). A study conducted by PM Solutions identifies that unclear, imprecise, ambiguous and contradictory requirements belong to the five most important reasons why 37 percent of the IT projects - on average 74 million US-Dollar worth – of the companies examined are at risk of failing (PM Solutions Research, 2011). The case of BlackBerry illustrates the importance of clearly formulated and implemented requirements. Once the global market leader on the corporate mobile phone market, the company's market share was 0,3 percent in units of shipped smartphones in the second quarter of 2015 (IDC, 2015). BlackBerry offered secure solutions, but locked customers in with long-term contracts and server-based proprietary solutions. Concurrently, the targeted audience increasingly required flexibility, which was better served by devices running Apple's and Google's operating systems (Taulli, 2013). Given incidences like the BlackBerry example, it is not surprising that RE gained a of lot attention amongst academics as well as practitioners (e.g. Anton, 1996; Sadraei *et al.*, 2007). Nuseibeh and Easterbrook (2000) define RE as the process of discovering the purpose of a software system "by identifying stakeholders and their needs, and documenting these in a form that is amenable to analysis, communication, and subsequent implementation". (Nuseibeh and Easterbrook, 2000)

Although there is no generally accepted specification of the RE process, a set of core activities can be derived from existing literature:

- *Requirements Elicitation:* Derive system boundaries by determining what problems need to be solved; Identify the relevant stakeholders and their needs; Specify high level goals to denote the objectives a system must meet; Elicit concrete requirements (Nuseibeh and Easterbrook, 2000)
- *Requirements Negotiation:* Evaluation of Requirements; Risks are analyzed by stakeholders and alternatives are selected (van Lamsweerde, 2001)

- *Requirements Specification:* Requirements are formulated precisely and checked for issues such as inconsistencies and their feasibility (van Lamsweerde, 2001)
- *Requirements Validation:* Ensure that specifications correspond to stakeholders needs and are aligned with constraints set by organizations and their environment (Pohl, 1996)

This research focuses on the activities of requirements elicitation, since works that identify concrete requirements for DCSs are still missing at all. Instead, current studies are mainly focused on the potential benefits of using DCSs in different use cases, rather than providing guidance for the software design (e.g. WEF, 2016; Government Office for Science, 2016). RE can either be an iterative process or take place at an initial stage of the project, depending on the respective software development model employed (Pohl and Rupp, 2015). In agile models, requirements need to be constantly adjusted to changing environmental conditions or objectives (Nuseibeh and Easterbrook, 2000). Contrarily, defining requirements in the beginning of the project provides no possibilities of modifications throughout the actual development. The present dissertation assumes a sequential water-fall model, where the different phases of development (i.e. requirements formulation, design, implementation, verification and maintenance) build upon each other (Royce, 1987). It is chosen because it emphasizes on the extensive documentation of requirements before the actual design phase and regards RE as imperative prerequisite for all further development steps. RE contrasts functional with non-functional requirements, whereby the former defines the functions of a system and the latter cover constraints on the design and implementation in the form of qualities like security or reliability (Stellman and Greene, 2006).

The methodological approach for eliciting the requirements for DCSs is subsumed in Table 22. To elicit requirements capturing the needs of the stakeholders, a goal-oriented approach is employed. Goal-based methods for requirements engineering (GORE) emphasize on the relevant stakeholders' objectives. Based on the methods suggested by RE, the problems a system should solve need to be identified and restricted. This is done by means of a multi-layered structural model and a differentiation of systems, as already conducted in Section 4.3 and 4.4. In the next step, the goals and needs of the relevant stakeholders are examined. Therefore, a schematic illustration of DCSs is presented, which distinguishes between the system itself, the business environment consisting of organizations offering complementary applications and services and the end-users utilizing the system. The purpose of this contextualization is to divide DCSs and their environment into different layers and present available interaction channels. In this way, it is possible to examine the layers independently. This contextualization serves as basis for the development of a system context to model DCSs. A properly defined system context is important, as it influences how a DCS fits into its operational environment and, consequently, affects the objectives as well requirements that will eventually be elicited (Nuseibeh and Easterbrook, 2000). The system context for DCSs is visualized using *i** (Yu, 1997), which is an agent-oriented modeling framework supporting the documentation and analysis of goals in the form of actors and their dependencies (Lapouchnian, 2005). This provides the foundation for the subsequent elicitation of requirements from industrial research according to the actors and their particular intentions. These findings are used to derive the actual requirements explained below.

1. Operation of DCSs	**High-Level Objective & Classification of DCSs** ▪ Consensus via DCSs ▪ Classification of systems & corresponding consensus mechanisms ➢ Multi-layered structural model and differentiation of systems Already presented in section 4.3 and 4.4
2. Determination of Objectives	**Goals & Needs of Relevant Stakholders** ▪ Schematic illustration of DCSs to identify interaction channels ▪ Overview about the relevant literature to identify required functionalities and characteristics ➢ System context and clustering
3. Derivation of Requirements	**Functional Requirements for DCSs**

Table 22: Methodological Approach Requirements for DCSs

4.5.2 Schematic Illustration: DCS, Environment and User Side

Figure 26 presents the schematic illustration of a DCS in form of a contextualization by illustrating interactions with its ecosystem and end-users. Hence, it is distinguished between the layer of the DCS, the ecosystem and the end-users.

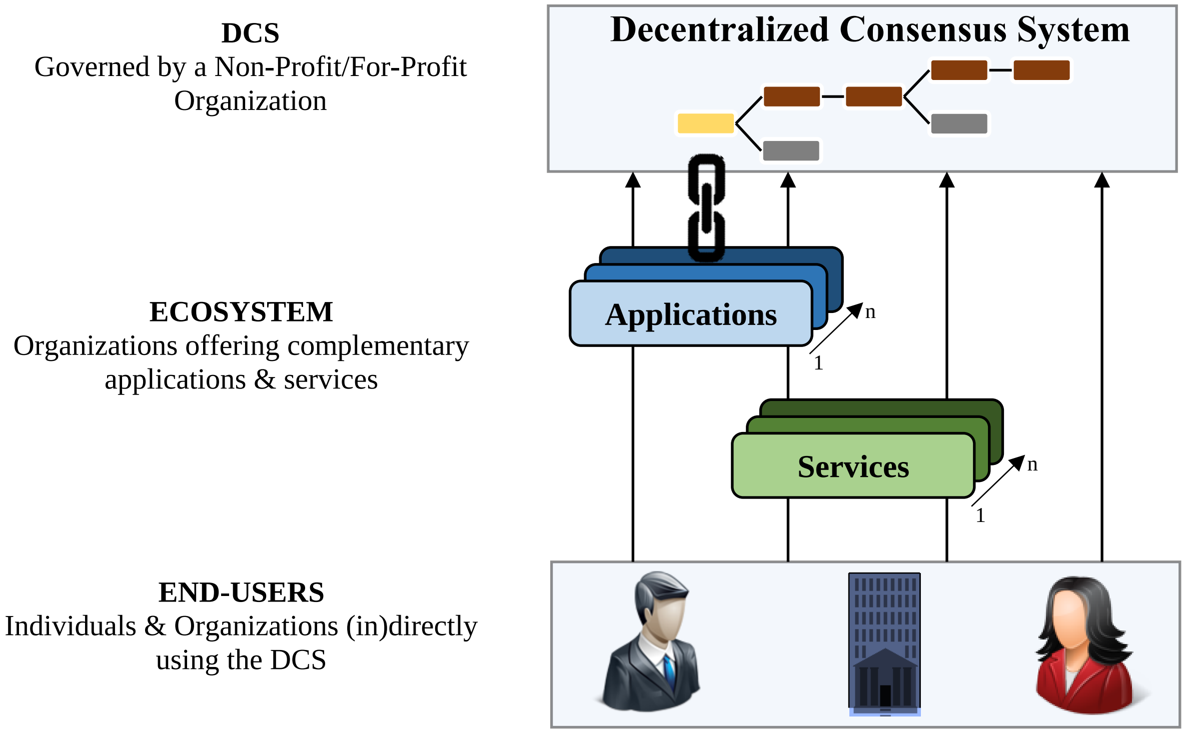

DCS
Governed by a Non-Profit/For-Profit Organization
ECOSYSTEM
Organizations offering complementary applications & services
END-USERS
Individuals & Organizations (in)directly using the DCS
Decentralized Consensus System
Applications
n
1
Services
n
1

Figure 26: Contextualization of Decentralized Consensus System

One can differentiate between DCSs governed by non-profit and for-profit organizations (Chesbrough *et al.*, 2006). Whilst non-profit organizations are predominantly foundations (e.g. Bitcoin Foundation, Ethereum Foundation), for-profit organizations are profit-seeking enterprises (e.g. Ripple Labs). From an organizational perspective, the term DCS is used when referring to the system as a whole, whereas the technical backbone of a DCS is the underlying distributed ledger. Beside Bitcoin there are various other DCSs already running live or in test modes. Litecoin implements an independent blockchain technically nearly identical to Bitcoin, but differs in some design features such as the maximum number of coins and the implemented hash algorithm. Ripple Labs introduces the eponymous DCS Ripple as "the world's first distributed exchange" and facilitates the decentralized transfer of any currency without restrictions (Gehring, 2014).

The evolving ecosystem around DCSs consists of organizations providing complementary applications or services for a DCS. In general, an economic ecosystem can be described as a business environment consisting of several entities and their corresponding relationships. It is characterized by competition and collaboration to pursue the overarching objective of generating added value (Henningsson and Hedman, 2014; Basole and Karla, 2011). Usually end-users are treated as an entity of the ecosystem, nevertheless they are examined independently owing to the complexity of DCSs. Although prevailing DCSs follow an open approach to encourage the participation of a community of developers providing applications and services, closed implementations without an ecosystem are also conceivable. For instance, nine of the largest investment banks, including GoldmanSachs and JPMorgan, recently announced a cooperation to develop common standards for DCSs to potentially reshape internal processes in the future (Stafford, 2015).

Applications are implemented on top of a given DCS to provide additional functionalities not initially available. They are related by a technical link to the system. Zerocoin is an application based on Bitcoin, which adds anonymity as functionality, since users' privacy is originally only protected through pseudonyms. The technical link to Bitcoin is established by exchanging the native asset bitcoin for zerocoins, which are then stored in the Bitcoin blockchain (Miers *et al.*, 2013). Ethereum encourages the development of applications for their DCS by providing a distributed ledger with a built-in Turing-complete programming language (Butterin, 2016). Contrary to applications, services do not require a technical link to a DCS. Instead, their legitimacy is determined by a DCS. They render the use of already existing functionalities of a system or application more convenient, but do not add any new functionalities. Consequently, the functionalities are in the center of the business models of service providers. BitPay offers payment processing as a service for enterprises who want to accept payments with bitcoin. Its business model consists of financial intermediation between these enterprises and their customers, by taking any volatility risk. Among the users of the service are major global players like Microsoft or PayPal (BitPay, 2015). Another service for DCSs are exchanges converting the respective exchange medium into fiat currencies (e.g. Bitstamp, Bitcoin.de or BTC China). Europe's largest bitcoin trading-platform Bitcoin.de cooperates with the FIDOR AG, which establishes a bridge to the financial industry and simplifies the clearing of transactions (Kannenberg, 2015).

End-users are entities that demand the functionalities offered by a DCS or a corresponding application. The end-user base consists of actual individuals as well as organizations like enterprises or governmental bodies. They get access to the DCS via different channels. Direct access describes the use of a DCS without any interposition of applications. Therefore, the available functionalities are restricted to those already implemented in the underlying system. Indirect access describes the use of a DCS supported by applications. In this case, it is possible to use functionalities not initially implemented in the distributed ledger backing a DCS. In the case of Bitcoin, this means that the use of privacy-enhancing applications like Zerocoin is possible. Irrespective of any applications, users may refer to services enhancing the convenience of functionalities.

4.5.3 Elicitation of Requirements

This section consolidates previous findings and presents an agent-based strategic dependencies model illustrating the system context. Thus, it provides a foundation for the requirements proposed afterwards.

4.5.3.1 System Context: Strategic Dependencies Model

As a prerequisite for the elicitation of requirements for DCSs, the intentions of the relevant stakeholders in the system context need to be identified and modeled (Castro et al., 2002). Only then it is possible to understand the problem domain subject to investigation, establish relationships between an envisioned DCS and its environment and to take the objectives of the different stakeholders into account. These insights are then used to identify the actual requirements for DCSs by implementing a goal-oriented analysis (Dardenne et al., 1993).

*i** is an agent-oriented framework commonly used for requirements engineering to model activities that take place before concrete requirements are formulated (e.g. Alencar *et al.*, 2009). A strategic dependencies model is used to visualize external relationships among actors (Yu, 1997). The central conceptual element for modeling with *i** are actors (individuals, hardware and software). They refer to an active entity capable of independent actions and are represented as nodes. Actors are assumed to be autonomous in the sense that their behavior is not fully anticipated and controllable, but intentions can be modelled by considering dependencies between actors. Nodes are connected to each other via links, indicating a dependency (dependum) between two actors (the depender and the dependee) (Alencar *et al.*, 2009). There are four different types of dependencies, describing how one actor depends on another actor for something. *Goals*, represented as rounded rectangles, are objectives an actor wants to be achieved by another actor. *Softgoals*, represented as clouds, are objectives in form of qualities like reliability or security and are often used to address non-functional requirements. *Tasks*, represented as hexagons, specify activities one actor wants to be performed by another actor. *Resources*, represented as rectangles, describe physical or informational entities one actor wants to be provided by another actor (Yu, 2009).

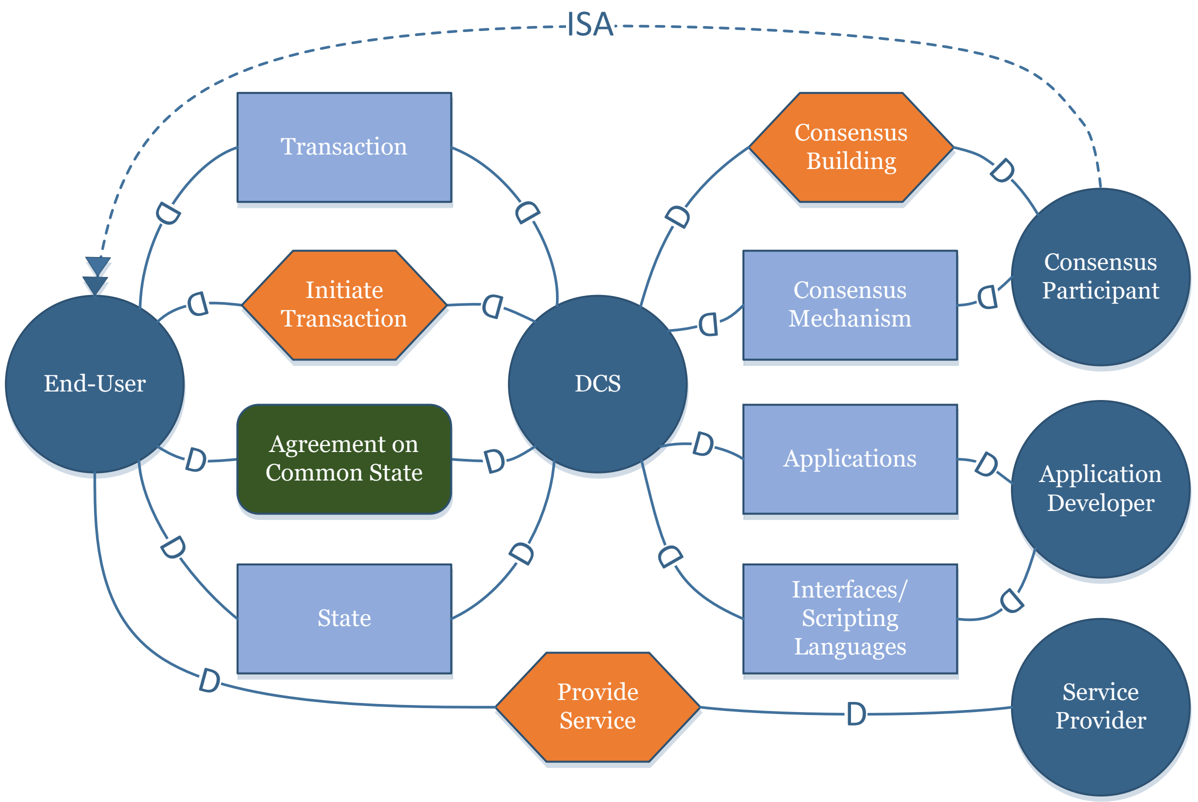


Figure 27: Strategic Dependency Model of Decentralized Consensus Systems

The strategic dependency model in Figure 27 presents the relevant actors in the context of a DCS and their external relationships. Overarching goal of the DCS is to facilitate an agreement on a common state between end-users in different application fields ranging from cryptocurrencies and electronic money, over any form of digitally represented (in-) tangible assets to smart contracts and objects. The representative end-user depends on the DCS to enable this agreement. To this end, the DCS relies on the end-user to perform the task of initiating transactions which results in the actual transactions represented as resources. The outcome of the subsequent consensus building is then provided as state to the end-user. The consensus building is carried out by the actor consensus participant, who is eligible to validate transactions utilizing the consensus mechanism. A consensus participant is either an end-user (represented by the dashed link) or an independent actor according to the design of the DCS. In permissionless systems they may belong to the end-users or form a separate group only involved in consensus building. Permissioned systems additionally allow consensus building to be carried out by the DCS operator itself. Application designers need interfaces and scripting languages to implement applications providing additional functionalities to the DCS. End-Users depend on the service provider for services.

4.5.3.2 Identification of Requirements

For the elicitation of requirements, a review of relevant literature concerning DCSs was conducted. The selection of the literature was undertaken by considering industrial studies and reports focusing on the concepts of "distributed ledger" and "blockchain technology" leading to a total of 34 relevant publications (as illustrated in Table 23 and 24). The literature predominantly consists of institutional and organizational research presenting use cases from the financial industry. The represented spectrum thereby includes the view of DCS developers, organizations from the financial industry, information technology companies, consulting firms as well as national and transnational governmental bodies and therefore potential stakeholders of such systems. Consequently, academic research was purposedly not taken into account, as the present work intends to unbiasedly reflect stakeholders' needs. This is in line with the methods of GORE, which propose documentations provided by potential stakeholders as appropriate source for collecting requirements (e.g. Pohl, 2010). Due to the reason that non-functional requirements for DCSs are commonly mentioned in the literature (e.g. EBA, 2015; DTCC, 2016), this dissertation is restricted to the identification of functional requirements. The review process was carried out by using perspective-based reading (PBR), where a document is read from predetermined perspectives (e.g. Shull et al., 2000). The literature was reviewed with regard to the functionalities a DCS requires from the perspective of the different actors in the strategic dependency model to identify their respective intentions and beliefs. For this purpose, it was searched for phrases like "the system should" or "it requires" and similar formulations describing something is desired. As result of this perspective based review, statements reflecting the views of various stakeholders were collected, which subsequently were clustered according to their content. The clustering enabled the elicitation of the functional requirements for DCSs. Table 23 and 24 provide an overview of the requirement clusters with reference to the literature.

Reference	Institution	Requirements			
		R.1: Authentication of End-Users	**R.2: Transparency of Transactions**	**R.3: Consistency of the Ledger**	
				R.3.1: Execution of the Consensus Process	***R.3.2: Rule-Conformity of Ledger Entries***
Accenture (2016)	Accenture	✓ (p. 15, 16)	✓ (p. 3)		✓ (p. 3)
Bogart and Rice (2015)	Needham & Company	✓ (p. 6)	✓ (p. 6)		
Cobben et. al (2015)	BlinkLane Consulting		✓ (p. 10)		
Deloitte (2016a)	Deloitte	✓ (p.7)	✓ (p. 5, 6, 8)	✓ (p.4)	
Deloitte (2016b)	Deloitte		✓ (p.12)	✓ (p.22)	
DTCC (2016)	DTCC		✓ (p. 10)		✓ (p. 6)
Duivestein et al. (2015)	Sogeti		✓ (p. 5, 11)	✓ (p.8)	✓ (p. 17)
EBA (2015)	European Banking Association			✓ (p. 6)	
Ethereum (2016)	Ethereum				
Euroclear & Wyman (2016)	Euroclear & Wyman	✓ (p. 6)	✓ (p. 7)	✓ (p. 6)	✓ (p. 6)
Evry (2015)	Evry	✓ (p.12)	✓ (p. 20)	✓ (p. 8,14)	
EY (2016)	EY		✓ (p. 7, 8)	✓ (p. 4)	
Fielder and Light (2015)	Accenture	✓ (p. 10)	✓ (p.3, 6, 8, 15, 16)	✓ (p. 16)	
Geiling (2016)	BaFin	✓	✓	✓	
Government Office for Science (2016)	UK Government	✓ (p. 34)	✓ (p. 22, 24)	✓ (p. 23,47)	
Greenspan (2015)	Multichain		✓ (p. 1)	✓ (p. 1)	
IBM (2015)	IBM	✓ (p. 11)	✓ (p. 11)	✓ (p. 11)	
IMF (2016)	International Monetary Fund		✓ (p. 1,18)		✓ (p. 9)
Innovalue and Locke Lord (2015)	Innovalue & Locke Lord		✓ (p. 7)	✓ (p. 6)	
Mainelli and Smith (2015)	EY		✓ (p. 5, 8)	✓ (p. 5)	
McKinsey (2015)	McKinsey	✓ (p. 5,9)	✓ (p. 9)	✓ (p. 5,9)	
Moody's (2016)	Moody's	✓ (p. 16)	✓ (p. 8)	✓ (p.16)	✓ (p. 4)
Mildner (2016)	Firstwaters				
Nakamoto (2008)	Bitcoin	✓(p. 8)	✓ (p. 2)	✓ (p. 3)	✓ (p. 4)
Robleh (2014)	Bank of England		✓ (p. 9)	✓ (p. 5)	
Ruecker (2015)	Deutsche Börse Group		✓	✓	
Santander (2015)	Anthemis Group				
Schwartz et al. (2014)	Ripple				✓ (p. 1)
Scott (2016)	United Nations	✓ (p. 15)	✓ (p. 11)		
Crosby et al. (2015)	Sutardja Center	✓ (p. 6)	✓ (p. 3, 6)	✓ (p. 3)	
Swanson (2015)	R3				
Taylor (2015)	Barclays		✓ (p.3, 4)		
UBS (2016)	UBS	✓ (p.33)	✓ (p.33)		
WEF (2016)	World Economic Forum		✓ (p.24)	✓ (p. 24)	

Table 23: Requirement Cluster Part 1

Reference	Institution	Requirements			
		R.4: Prevention of Unauthorized Modifications		**R.5: Enabling of External Applications**	
		R.4.1: Immutability of the Ledger	***R.4.2: Exclusive Rights for Reliable Parties***	***R.5.1: Provision of Application Programming Interfaces***	***R.5.2: Implementation of Scripting Languages***
Accenture (2016)	Accenture		✓ (p. 16)	✓ (p. 5)	✓ (p. 3)
Bogart and Rice (2015)	Needham & Company	✓ (p. 10,20)		✓ (p. 4)	
Cobben et. al (2015)	BlinkLane Consulting			✓ (p. 5)	✓ (p. 4)
Deloitte (2016a)	Deloitte				✓ (p. 6)
Deloitte (2016b)	Deloitte		✓ (p.22)		✓ (p.20)
DTCC (2016)	DTCC	✓ (p. 6,7)		✓ (p. 8)	
Duivestein et al. (2015)	Sogeti				
EBA (2015)	European Banking Association			✓ (p. 4)	
Ethereum (2016)	Ethereum				✓
Euroclear & Wyman (2016)	Euroclear & Wyman	✓ (p. 6)	✓ (p. 14)	✓ (p. 11)	✓ (p. 6)
Evry (2015)	Evry	✓ (p. 6)		✓ (p. 15, 27)	✓ (p. 16)
EY (2016)	EY			✓ (p. 3)	
Fielder and Light (2015)	Accenture	✓ (p. 5)	✓ (p. 6,16)	✓ (p. 16)	✓ (p. 16)
Geiling (2016)	BaFin		✓	✓	
Government Office for Science (2016)	UK Government	✓ (p. 47)	✓ (p. 35)	✓ (p. 35)	
Greenspan (2015)	Multichain		✓ (p. 5)	✓ (p. 11)	
IBM (2015)	IBM				✓ (p. 12)
IMF (2016)	International Monetary Fund				
Innovalue and Locke Lord (2015)	Innovalue & Locke Lord	✓ (p. 7)			
Mainelli and Smith (2015)	EY		✓ (p. 7,37)		✓ (p. 37)
McKinsey (2015)	McKinsey	✓ (p. 6)			✓ (p. 9)
Moody's (2016)	Moody's	✓ (p. 15, 16)			✓ (p. 12)
Mildner (2016)	Firstwaters	✓ (p.3)			✓ (p. 3)
Nakamoto (2008)	Bitcoin	✓ (p. 8)			
Robleh (2014)	Bank of England				
Ruecker (2015)	Deutsche Börse Group				
Santander (2015)	Anthemis Group				✓ (p. 15)
Schwartz et al. (2014)	Ripple				
Scott (2016)	United Nations	✓ (p. 11)			✓ (p. 11)
Crosby et al. (2015)	Sutardja Center	✓ (p. 3)		✓ (p. 4)	✓ (p. 4)
Swanson (2015)	R3		✓ (p. 5,21)		✓ (p. 23)
Taylor (2015)	Barclays	✓ (p. 4)	✓ (p. 3)		
UBS (2016)	UBS	✓ (p. 32)			
WEF (2016)	World Economic Forum	✓ (p. 24)			✓ (p. 29)

Table 24: Requirement Cluster Part 2

4.5.4 Examination of the Identified Requirements

An overview of the identified requirements and corresponding sub-requirements is presented in Table 25. They are ordered according to the addressed relationship between the stakeholders operating as actors in the strategic dependency model. Since exclusively functional requirements are taken into account, the DCS is always involved as actor. Furthermore, the affected resource dependencies are depicted and the table states whether a particular requirement applies to permissionless and/or permissioned systems. It is to be noted that bracketed checks indicate the conditional validity of a requirement discussed below.

Relationship with DCS	Requirement	Affected Resource Dependency	Perissionless System	Permissioned System
End-User	R.1: Authentication of End-Users	▪ Transactions ▪ State	✓	✓
Consensus Participants	R.2: Transparency of Transactions	▪ Transactions ▪ Consensus Mechanism	✓	(✓)
	R.3: Consistency of the Ledger	▪ Consensus Mechanism	✓	✓
	R.3.1: Execution of the Consensus Process		✓	✓
	R.3.2: Rule-Conformity of Ledger Entries		✓	✓
	R.4: Prevention of Unauthorized Modifications	▪ Consensus Mechanism	✓	✓
	R.4.1: Immutability of the Ledger		✓	✕
	R.4.2: Exclusive Rights for Reliable Parties		✕	✓
Application Developer	R.5: Enabling of External Applications	▪ Applications ▪ Interfaces / Scripting Languages	✓	(✓)
	R.5.1: Provision of APIs		✓	(✓)
	R.5.2: Implementation of Scripting Languages		✓	(✓)

Table 25: Overview of the Requirements

4.5.4.1 R.1: Authentication of End-Users

As with all transaction processing systems, a DCS must verify that the involved parties are who they claim to be (e.g. Fielder and Light, 2015; Evry, 2015; Government Office for Science, 2016). Accordingly, the requirement “Authentication of End-Users” expresses that the DCS should have processes in space allowing end-users to prove their identity. Authentication is a necessary precondition that only individuals who are entitled to do so are capable of exercising control over an asset. But authentication of end-users does not only cover natural persons. Devices tied to individuals and interacting based on user-defined rules should also be clearly identifiable (IBM, 2015). Therefore, the requirement is targeted at the relationship between the DCS and its end-users. The involved resource dependencies are the transactions and the state, because authenticated end-users can execute transactions and access the ledger.

Balancing between security and usability remains a critical challenge in the development of authentication schemes (e.g. Weir *et al.*, 2009). Artificially created obstacles are intended to prevent attackers from getting access to the system. These obstacles, however, shall not discourage legitimate users from participating. In DCSs, the authentication is realized via asymmetric encryption methods (Geiling, 2016; UBS, 2016). Possession of the respective private key serves as evidence that an end-user is the one who received or registered a particular asset. Furthermore, the associated recipient address is a public key derived from the private key. This permits the use of digital signatures, whereby the authenticity of a transaction can be verified by its receiver and other network participants (e.g. Müller *et al.*, 2003). In a logical order authentication precedes authorization, which is the process of granting access to the DCS conditional on an individuals’ identity (e.g. Bishop, 2005). In permissionless systems, the authentication with a certain key pair just affects the set of assets under control of an end-user, since there are no access controls and restrictions on the consensus participation. This is contrasted by the feasibility of different access rights and permissions for consensus participation in permissioned systems, which depend on the credentials assigned to an individual (Accenture, 2016; Bogart and Rice, 2015).

4.5.4.2 R.2: Transparency of Transactions

Transparency is frequently mentioned in the reviewed literature as an important characteristic of DCSs (e.g. Mainelli and Smith, 2015; Deloitte, 2016a; Duivestein *et al.*, 2015). The requirement “Transparency of Transactions” implies that the DCS should provide relevant stakeholders with access to transaction-related data. This data facilitates transaction processing and reduces associated risks for end-users (DTCC, 2016). Concurrently, consensus participants need transparency in order to verify the correctness of transactions (International Monetary Fund, 2016). The requirement consequently aims at the relationships between the DCS and its end-users as well as the DCS and the consensus participants. The affected resource dependencies are the transactions and the consensus mechanism. To achieve transparency, the system has to ensure traceability via a distributed ledger replicated on the nodes of the network (Cobben *et al.*, 2015). The ledger contains a permanent record of all transactions that have ever been conducted by any end-user (Accenture, 2016). Thereby, time-stamping allow chronological consideration of every transaction in a history, which is essential for the consensus process and conflict resolution in the event of a dispute (Evry, 2015). Traceability eliminates the need for trusted third parties, supports the detection of frauds like duplicated transactions and serves as basis to hold end-users accountable for their actions (EY, 2016). However, the requirement of transparency does not address any privacy-related problems in terms of the ability to link pseudonyms with real-world identities. The requirement is fulfilled, as long as a DCS establishes an unequivocal and verifiable connection of entities with transactions (DTCC, 2016).

The degree of transparency can vary depending on the type of system and different user roles (International Monetary Fund, 2016). Permissionless systems always achieve the highest degree of transparency for all individuals, which is owing to their public nature (Geiling, 2016). Every network node is able to access the full extent of data in the distributed ledger and is permitted to participate on the consensus process. In this way, each individual can trace the whole history of transaction-related data (Deloitte, 2016a; Duivestein *et al.*, 2015). In permissioned systems, access controls and restricted consensus participation make it possible that the degree of transparency depends on a specific user role (Government Office for Science, 2016). Consensus participants may have complete visibility of the distributed ledger, since it is necessary for the functioning of the consensus mechanism. The transparency for conventional end-users can be restricted to transactions they are involved in or may include activities of business partners they have a substantiated interest in (Bogart and Rice, 2015). However, this granular transparency involves a trade-off between transparency and trust (Cobben *et al.*, 2015). It limits the capacity to trace transactions for certain user groups, wherefore they rely on trusted parties with full transparency for the correctness of transactions.

4.5.4.3 R.3: Consistency of the Ledger

In order to facilitate digital interactions, it is crucial that the individuals involved possess the same information base (e.g. European Banking Authority, 2015; Euroclear & Wyman, 2016; Nakamoto, 2008). The requirement "Consistency of the Ledger" intends to ensure that all participants of the system share a common state of the ledger in accordance with predefined rules at any time. Consistency is reached by a decentralized consensus process, which obviates central governing authorities determining the systems' state (Deloitte, 2016a; Ruecker, 2015). Hence, there exists no single point of failure which promotes the resilience of the system in the event of disturbances (Fielder and Light, 2015). As consistency of the ledger is achieved by the consensus participants, the requirement refers to their relationship with the DCS and the impacted resource dependency is the consensus mechanism.

This leads to the sub-requirement ***R.3.1: "Execution of the Consensus Process"***, stating that the consensus process should independently be executed by consensus participants verifying transactions utilizing the implemented consensus mechanism. Independent verification of transactions is needed to avoid self-interested individuals from manipulating the ledger for their benefit and, thus, jeopardizing its overall consistency (IBM, 2015). As previously discussed in section 4.4 on the classification of DCSs and mechanisms, the available consensus mechanisms depend on the type of system under consideration. Permissionless systems require consensus mechanisms where the execution of the consensus process is based on the expenditure of economic resources. This is essential to align the incentives of consensus participants with the overall objective of agreeing on a common state (Robleh 2014; Swanson 2015). The ability to restrict permissions to identified nodes enlarges the number of available mechanisms in permissioned systems for protocols used in conventional distributed computing (Evry, 2015; McKinsey, 2015a).

Irrespective of the concretely used consensus mechanism, the sub-requirement ***R.3.2: "Rule-Conformity of Ledger Entries"*** requires ledger entries to conform to a set of predefined and incorruptible rules. Only if this holds, it is possible to discern the difference between correct and fraudulent transactions (Schwartz *et al.*, 2014). The consensus mechanism should enforce certain conditions or a particular behavior, by restricting transactions actually included into the ledger to those in accordance with the rules (International Monetary Fund, 2016). Although a DCS re-assigns digital assets based on predefined rules, it cannot ensure that changes to the ledger are enforced beyond the boundaries of the system. It is, for instance, impossible for a

DCS to enforce the transfer of physical objects, even if it involves an accepted transaction. This problem arises in connection with ***R.2*** and is mentioned as challenge, but it is object of investigation for regulations and does not constitute a functional requirement (DTCC, 2016; European Banking Authority, 2015).

4.5.4.4 R.4: Prevention of Unauthorized Modifications

The accuracy and consistency of data stored (Fielder and Light 2015) in the distributed ledger is a fundamental prerequisite for a DCS to be secure (e.g. Accenture, 2016; Innovalue & Locke Lord, 2015; UBS, 2016). Because of that, the requirement "Prevention of Unauthorized Modifications" claims that nobody who is not explicitly entitled to do so should be able to edit or delete ledger entries. Only a suitable selection of reliable entities authorized to modify data and the absence of technical vulnerabilities ensures that the data integrity of the system can be protected (Bishop, 2005). Since modifications have to be considered by the consensus mechanism, the requirement is related to the relationship between the DCS and consensus participants.

In permissionless systems, the issue is addressed by the sub-requirement ***R.4.1: "Immutability of the Ledger"***. It says that the DCS should prevent any entity from modifying data, once it has been included into the distributed ledger by the consensus participants. This results in a system where all transactions ever conducted are permanently recorded in the ledger to prevent malicious manipulations (Euroclear & Wyman, 2016; McKinsey, 2015a). The practical realization is based on the required expense of economic resources for modifying already processed transactions which increases over time. Somebody trying to alter a transaction has to redo the proof for all subsequent transactions and must also invest more resources than the rest of the consensus participants verifying present transactions (e.g. Karame *et al.*, 2012; Nakamoto, 2008). Immutability, however, has profound implications on the functionalities of the DCS. Firstly, it is impossible for end-users to revoke any incorrect or fraudulent transactions. Secondly, the operator or other designated authorities have no means to intervene whenever it is necessary. A system exhibiting the characteristic of immutability is called censorship-resistant, which is "the ability to prevent a third-party from imposing a particular distribution" (Perng *et al.*, 2005, p. 62).

In permissioned systems, the sub-requirement ***R.4.2: "Exclusive Rights for Reliable Parties"*** stipulates that the DCS should provide functionalities to assign exclusive rights for parties authorized to modify the distributed ledger. It is necessary for the reliability of the system in this context to make sure that these rights remain constrained on a specific group of users (Mainelli and Smith, 2015; Swanson, 2015). In order to blacklist end-users and delete transactions not compliant to applicable legal and organizational provisions, features facilitating controllability need to be incorporated (Taylor, 2015).

4.5.4.5 R.5: Enabling of External Applications

Extending a DCS with external applications increases the value of the system for end-users by providing additional functionalities not initially available (e.g. Cobben *et al.*, 2015; EY, 2016; Mildner, 2016). Hence, the requirement "Enabling of External Applications" addresses the issue that a DCS should implement means for developing such applications. In this context, the relationship between the DCS and application developers is of central concern and the requirement is relating to the resource dependencies applications and interfaces/scripting languages. By promoting the development of applications, the DCS operator utilizes knowledge from internal as well as outside sources to expand the value creation (Chesbrough and Appleyard, 2007). A publicly available source code is one of the opportunities to attract volunteers that contribute applications and even realize alternative systems (examples for open source projects are Bitcoin, Ethereum, Hyperledger or Ripple). As opposed to this open approach, a DCS following a closed strategy restricts the implementation of extended functionalities through external applications (Brenig *et al.*, 2016). Closed approaches are especially interesting for organizations intending to reshape their business processes by utilizing a permissioned system for interorganizational transactions between two or more affiliated parties (e.g. Greenspan, 2015). Whether a relationship between the DCS and application providers exists, and thus the validity the requirement, depends on the system operator's business model.

Applications are related by a technical link to the system. Concerning this matter, the sub-requirement ***R.5.1: "Provision of Application Programming Interfaces"*** states that the DCS should feature open interfaces allowing application developers to make use of the integrated functionalities. These interfaces may provide access to the distributed ledger and permit using as well as extending the implemented methods for updating it (Accenture, 2016; Bogart and

Rice, 2015). Thus, it becomes possible to harness network effects and profit from an already established system. But open interfaces may also ensure the interoperability of DCSs designed for the same or different purposes (e.g. one DCS used for derivatives trading and the other for processing payments) (Euroclear & Wyman, 2016; Evans-Greenwood *et al.*, 2016; Greenspan, 2015).

Logical operations formalized in smart contracts constitute functionalities exceeding passive data entries and can be considered as applications if they are sufficiently complex (e.g. Deloitte, 2016a; McKinsey, 2015a; Mildner, 2016). This is reflected in the sub-requirement ***R.5.2: "Implementation of Scripting Languages"***, which requires that DCSs should implement scripting languages to formalize logical operations (Santander, 2015). Additionally, the literature frequently demands that it fulfills the property of Turing Completeness (e.g. Mainelli and Smith, 2015; Swanson, 2015). A Turing Complete language is able to solve any computational problem, which qualifies application developers to realize a wider range of functionalities than a scripting language lacking this property (Turing, 1937).

4.6 Concluding Remarks

Chapter 4 elaborated on the architecture of DCSs in general and thereby addressed this dissertation's research questions *RQ3a* and *RQ3b*. Accordingly, The first part of this chapter investigated the research question *RQ3a: Based on the analysis of Bitcoin and similar cryptocurrencies, which implications result for the architecture of Decentralized Consensus Systems in general?* It adopted a broader perspective by considering DCSs apart from the permissionless design of Bitcoin and the context of payments, in order to facilitate the analysis of further systems and applications beyond cryptocurrencies. Originating from the specific characteristics of Bitcoin and the associated risks in the context of ML, it sketched the evolution of DCSs by means of possible application fields according to their degree of complexity. Even though the Bitcoin system might not be best suited for payments, the distributed ledger concept provides opportunities in a variety of use cases. Therefore, the high-level purpose of all DCSs, which is agreeing on a common state of the ledger, was explained afterwards. For this purpose, a multi-layered model introducing the structure of the consensus process via DCSs was invented. By distinguishing between permissionless and permissioned systems, two fundamentally different design approaches for DCSs were examined, which both exhibit a different set of characteristics. In general, these approaches can be delineated from each other based on whether they allow central instances to execute control or not.

The second research question tackled was *RQ3b: What are the functional requirements for Decentralized Consensus Systems?* While the classification of DCSs into permissionless and permissioned types illustrated the different sets of characteristics such systems can possess, the elicited requirements presented are intended to support the understanding of DCSs and provide assistance for their development. The method of GORE commonly used in RE was adopted to identify requirements in accordance with the relevant stakeholders' objectives. Therefore, a schematic illustration of DCSs, their business environment and user-side was presented to illustrate available interaction channel. Subsequently, a strategic dependency model that consolidates the previous findings and constituted the foundation for the requirement elicitation was postulated. The requirements were elaborated on basis of a literature review of industrial research and whitepapers.

Having examined the general architecture of DCSs and formulated functional requirements for their development, the subsequent chapter analyzes the the economic potentials of these systems. Therefore, it adapts the contextualization presented in section 4.5.2 and characterizes DCSs as platforms connecting different groups of users and which are characterized by network effects. This is followed by a framework to evaluate the economic value of DCSs, which incorporates different value concepts and utility theory. It allows to evaluate concrete realizations of DCSs and is exemplarily applied to the Bitcoin system. Further, the chapter assesses DCSs by providing a compliance perspective.

5 Economic Potentials of Decentralized Consensus Systems

The previous chapter investigated the architecture of DCSs, in order to take systems beyond the permissionless Bitcoin design and application fields beside cryptocurrencies into account. First of all, a classification of application fields according to their degree of complexity was provided. The subsequent section conceptualized the common high-level purpose of DCSs irrespective of concrete applications, which is an agreement on a common state of a system between the involved entities. Then DCSs and the corresponding consensus mechanism were classified into permissionless and permissioned systems, which purse a different philosophy regarding the toleration of central entities and the degree of openness they provide. The remainder of chapter 4 presented a set of fundamental requirements intended to support the development of DCSs.

In order to tackle *RQ4*, this chapter investigates the economic potentials of DCSs and provides means for the economic evaluation of specific systems. To begin with, the economic foundations justifying the use of DCSs for supporting digital interactions are examined in more detail. In this respect, a characterization of DCSs as Multi Sided platforms (MSPs) is presented, which extends the contextualization of interaction channels introduced in chapter 4.5.2 to reason about potential business models. The next part of this chapter presents a framework to evaluate the value of DCSs[10]. Starting point is the observation that innovative applications beyond payments already attract the attention of scholars and practitioners, whose works so far are mainly focused on explanatory issues. What is missing are approaches to evaluate the value of DCSs, taking into account the diversity of applications ranging from currencies to the decentralization of business operations. It is intended to provide a basis for the assessment of business models. The framework is then exemplarily applied to the Bitcoin system, which is evaluated according to various indicators such as venture capital investments, research or demand. Furthermore, this chapter provides a compliance perspective to assess the potentials of DCSs[11]. This interpretation provides a business perspective on DCSs and offers additional insights for elaborating on practicable applications. For this, the core elements of DCSs

[10] Chapter 5.2 consists of parts of Brenig *et al.* (2016)

[11] Chapter 5.3 consists of parts of Brenig *et al.* (in review [b])

supporting the realization of compliance are examined and illustrated by a use case from the financial industry.

5.1 Digital Interactions via Decentralized Consensus Systems

This section elaborates on the economic foundations that justify the use of DCSs for supporting digital interactions in more detail. Concretely, it relates the concepts of uncertainty, risk, trust and the role of intermediaries to each other and presents a business model for DCSs as Multi-Sided Platforms (MSPs). In doing so, the theoretical background to evaluate DCSs is established.

5.1.1 Economic Background: Uncertainty, Risk and Intermediation

Irrespective of the diversity of supported business models and concrete scenarios, interactions in digital environments are accompanied by uncertainty due to the missing physical presence of the involved parties and products or services offered. This is in line with findings of the social presence theory, which states that remote communication leads to uncertainties resulting from the inability to define the transaction partner as the one he, she or it claims to be (Gunawardena, 1995). The associated information asymmetry, usually studied in the context of the contract theory, is present when one side of the interaction possesses an information advantage regarding relevant decision parameters (Akerlof, 1970; Arrow, 2001). This has become a severe issue in the networked society to provide means for the ubiquitous exchange of information enabled by interconnections through IT (Castells, 2000). Research in that area suggests that the existence of information asymmetry prevents communication processes to be effective by leading them to uncertainty (e.g. Kajtazi, 2010; Bao, 2011). A concept related to uncertainty is risk. Whereby uncertainty refers solely to the probabilities of certain events to occur, risk also considers their impact (Hubbard, 2014). Consequently, digital interactions characterized by uncertainty lead to risks for the transacting parties, since they value possible outcomes differently. The range of conceivable outcomes can be categorized into transactions that ultimately fail, transactions where the actual outcome is not in the set of expected outcomes and transactions in a way that the outcome is expected.

Crucial requirement for entities to interact with each other in uncertain physical as well as digital environments is trust (Grandison and Sloman, 2000; Hoffman *et al.*, 1999). It is a construct getting relevant under conditions of risk and interdependence, where it implies that a trusting entity assesses the uncertainty of another party to act appropriately (Chen and Dhillon, 2003). The notion of trust in computer-mediated communication draws on sociological conceptualizations (e.g. Salam *et al.*, 2003; Kim and Koo, 2016) and is complemented by more technical approaches aiming at linking it to topics like privacy, security and reliability (e.g. Aljazzaf *et al.*, 2011; Tsiakis and Sthephanides, 2005). Despite the continuous scholarly attention of trust-related issues, due to its complex and multidisciplinary nature, there is no concise and universally accepted definition of trust. In the following, trust is conceptualized based on the definition of Gambetta as "a particular level of the subjective probability with which an agent will perform a particular action" (Gambetta, 2000, p. 4). By focusing on the probability of particular actions it is thus in accordance with the categorization of conceivable outcomes of transactions introduced above.

In order to increase the probability that an entity acts as expected, several measures can be implemented in the transaction process. For instance, measures like public key infrastructures established by trusted third parties (Blaze *et al.*, 1999) and mediating services that support the transactions process (Bakos, 1998) enforce that digital interactions conform to a set of predetermined rules. However, the usage of such measures involves a trade-off between the benefits of reduced uncertainty as well as risk and the associated costs for their implementation (Picot and Bortenlanger, 1997). DCSs constitute a novel type of measures, which facilitate digital interactions by substituting trust required in intermediaries for trust in the rules determined and enforced by the respective system. They are advantageous to already established solutions, if they induce entities to act as expected at lower costs.

5.1.2 Characterizing DCSs as Multi-Sided Platforms

The business model of DCS-providers can be characterized as MSP connecting different groups of end-users. The economic dimension of MSPs is a research field that receives much attention (e.g. Rochet and Tirole, 2003; Armstrong, 2006; Caillaud and Jullien, 2003; Hagiu and Wright, 2015). Generally, they can be defined as platforms "which get two or more sides on board and enable interactions between them" (Hagiu and Wright, 2015, p. 1). Early works on the topic commonly focused on platforms where two user groups interact (like credit card networks composed of cardholders and merchants (Rochet and Tirole, 2003)) and established the term "two-sided markets". The broader notion of MSPs is recently gaining more and more importance to describe interactions of two or more distinctive sides on a common platform (including smartphone operating systems that connect users, application developers, network operators or advertisers (Campbell-Kelly *et al.*, 2015)). Therefore, the term MSP is used in the following. Examples of successful MSPs are Airbnb, PayPal, Youtube and Facebook. Studies in this area deal with topics such as definitional aspects (Rysman, 2009), different pricing strategies (Armstrong and Wright, 2007), antitrust issues (Evans and Schmalensee, 2013) and operational decisions for platform operators (Rochet and Tirole, 2006) in a variety of industries ranging from newspapers to operating systems.

It is controversy discussed in the literature what the fundamental defining characteristics of a MSP are. The most popular approach identifies the existence of cross-group or indirect network effects between the sides using the platform as sufficient condition (e.g. Armstrong and Wright, 2007). While another approach defines MPSs as markets, where the volume of transactions can be affected by charging participating sides differently. Therefore, the price structure affects the economic outcome (Rochet and Tirole, 2006).

This thesis relates to Hagiu and Wright (2015), who define two fundamental key features of MSPs:

1. MSPs enable *direct interactions* between two or more distinct sides. Direct interaction describes that the sides using the platform control the decision variables of interaction, for example, throughout the processes of negotiation and settlement (Hagiu and Wright, 2015).
2. Each side is *affiliated* with the MSP. Affiliation characterizes platform-specific costs in terms of homing and switching costs incurring for each side to directly interact with one another (Staykova and Damsgaard, 2015). Whereby homing costs are investments for the adoption and continuous usage of a platform (Armstrong, 2006) and switching costs are expenses for migrating to another platform (Shapiro and Varian, 1999).

Central element of Figure 28 is a DCS as platform connecting application developers, service providers and different groups of end-users. As already explained in chapter 4.5.2, application developers implement applications on top of a DCS to provide functionalities not initially available. These functionalities may integrate additional types of assets not supported by the original system. Applications are therefore technically linked to a DCS. On the contrary, service providers render the use of existing functionalities more convenient by offering complementary services. Typical examples are service providers processing transactions on behalf of end-users.

Such services do not require a technical link to a DCS. Distinct groups of end-users consist of actual individuals as well as organizations like enterprises or governmental bodies, who are demanding the functionalities of the DCS or corresponding applications. In general, the broader the range of diverse functionalities covered, the greater the number of distinctive end-user groups connected on the platform. This is due to the fact that an increase in the variety of functionalities extends the available application fields, which, in turn, attracts additional user groups. Consequently, a DCS with a limited number of functionalities may connect users which only form a single user group (Staykova and Damsgaard, 2014). The system is governed by a platform operator, who can either be a non-profit or a for-profit organization adopting an open as well as a closed strategy to innovation (Brenig *et al.*, 2016). While an open strategy implies business models based on coordination and invention with a community (West and Gallagher, 2006), a closed strategy is characterized by ownership and control and the associated business models solely exploit knowledge from inside the organization (Chesbrough and Appleyard, 2007). The selected strategy influences the multi-sidedness of the respective platform. Operators pursing an open strategy may encourage third party involvement by providing open interfaces to develop applications. In the same way, operators following a closed strategy may purposely restrict the extent of functionalities and services offered. Consensus participants can also constitute a distinct user group depending on the design of the system. In permissionless systems they may belong to the end-users or form a separate group only involved in consensus building in order to compete for rewards. Permissioned systems additionally allow consensus building to be carried out by the DCS operator itself.

DCSs facilitate transactions within or between different groups of end-users, whereby every distinct group of end-users forms a side of the MSP. As noted above, the number of distinct groups, and simultaneously sides, increases with the provided functionalities of the DCS. Implementing the functionality to transfer currencies as assets potentially attracts the groups of merchants and customers to utilize a particular DCS for payments. The functionality to record the ownership of shares adds the group of equity traders as additional side. Irrespective of the particular functionality, every DCS fulfills the key feature of MSPs to enable direct interactions between distinct end-user groups. End-Users control the key terms of interactions by, for instance, setting prices in the payment example. Organizations have to integrate a DCS into their business operations, which is accompanied by the need to adapt existing business processes. Individuals must invest effort and time in terms of opportunity costs to properly use the system and understand possible risks (Burnham *et al.*, 2003). Application developers are provided with interfaces and tools to increase the functionalities of a DCS (e.g. Ripple, 2016a) and an evolution towards centralized application stores begins to emerge (e.g. Ethereum, 2016). These tendencies are similar to the development of Apple's 'App Store' and Google's 'Play Store', which provide applications for the respective operating system acting as a MSP (Campbell-Kelly *et al.*, 2015). Direct interactions between application developers and end-user groups exist, for instance, with regard to marketing activities or price negotiations. They are affiliated with a MSP by expending resources for gaining knowledge on how to develop applications for a specific platform. DCSs enable direct interactions between service providers and end-users, since services increase the convenience of use and do not provide any value on their own. Service providers and end-user groups are directly interacting by determining the nature and conditions of services offered. The affiliation of service providers is justified by their business models which are based on the existence of a DCS.

The existence of network effects, where the value of a platform for one user depends on the number of other present users, is an important characteristic of MSPs (e.g. Evans, 2003; Armstrong, 2006). One distinguishes between direct (same-side) and indirect (cross-side) network effects. Direct network effects presuppose that the value of a user in a group depends on the number of other users in the same group (Katz and Shapiro, 1985). They exist when utilizing DCSs for the private transfer of assets, since the roles of the sender and receiver are easily interchangeable. Indirect network effects are present if the value of a user in one group depends on how well the platform attracts users from another distinct group (Armstrong, 2006). With regard to the previous example, assuming fixed roles of sender and receiver in buyer-seller relationships results in indirect network effects between the users in this distinct groups. The indirect network effects flow in both directions in the present case, but the can also only go in one direction. Advertisers on the Facebook platform, for instance, are attracted by the large user base, but the users do not derive value from the number of companies placing advertisements (Staykova and Damsgaard, 2015). As noted in the preceding examples, direct as well as indirect network effects are present for end-users in the context of DCSs. Every interaction facilitated by DCSs is based on transactions between end-users, independent of the application field and the involved asset. Interactions between end-users within the same group are characterized by direct network effects, whereby the value of the system for a particular user increases with the number of available transaction partners. Following the same logic, interactions between end-users in distinct groups are characterized by indirect network effects flowing in both directions, because the value for a particular user in one group increases with the available transaction partners in another group. There are reciprocal indirect network effects flowing from end-users to application developers and in the other direction. Developers implementing applications for a DCS provide value for end-users by expanding the functionalities of the system, and additional end-users make developers better off by increasing the target group for applications. The same applies to the relationship between end-users and service providers. End-users profit from a wider range of services, while service providers appreciate additional end-users as potential consumers demanding their services.

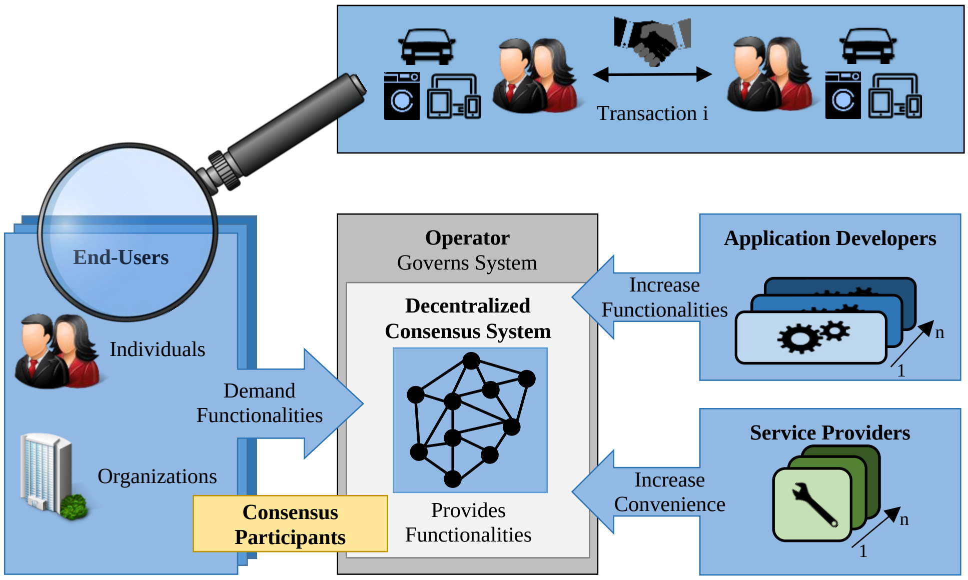


Figure 28: Decentralized Consensus System as Multi-Sided Platform

5.2 Economic Value of Decentralized Consensus Systems

The preceding section presented DCSs as digital infrastructures by characterizing them as MSPs to highlight their potentials. However, current literature lacks approaches that explain where and how the value of a DCS arises. After an introduction of the concept of value, a framework to evaluate the value of DCSs is presented. Table 26 summarizes the methodological approach for its development. The structure of the framework is derived from the layers already introduced in the schematic illustration of DCSs, their environment and the user-side in section 4.5.2. In particular, the concepts of value proposition and perceived value are included to determine the value created and captured by the ecosystem and the end-users of a specific DCS. The ecosystem consists of organizations offering complementary applications and services for a DCS. End-users utilize a DCS to track ownership and transfer of property, which may be supported by complementary applications and/or services. The framework is exemplarily applied to evaluate Bitcoin according to several indicators. It is intended to provide an initial step for the assessment of concrete business models.

1. Contextualization	**DCSs, Environment and User-Side** ▪ Literature regarding existing and planned systems (whitepaper, homepages) ▪ Industrial and institutional reports considering the economic potentials (e.g. European Banking Authority, 2015; IBM, 2015) ➢ The context of DCSs presented as schematic illustration Already presented in section 4.5.2
2. Analytical Framework	**Economic Value of DCSs** ▪ Identification of concepts for the determination / operationalization of value ▪ Characterization of DCSs as Multi-Sided Platforms (section 5.1.2) ➢ Framework based on contextualization and value concepts
3. Evaluation	**Evaluation of DCSs** ▪ Evaluation of Bitcoin with the framework

Table 26: Methodological Approach Value Framework

5.2.1 The Concept of Value

The notion of value describes a complex and abstract concept, which causes confusion around economists about its meaning and how it can be operationalized (e.g. Farber *et al.*, 2002; Payne and Holt, 2001). A variety of economic research is focused on how concepts like value, utility, quality and costs are related (e.g. Giddings, 1891; Grönroos, 2011). This results in a large number of differing definitions and uses of the value concept amongst academics (e.g. Salem Khalifa, 2004; Zott *et al.*, 2011). For the development of the evaluation framework the notion of 'value proposition' is adopted. Value proposition can be interpreted from two different perspectives. It is either referred to as a decision variable to gain a competitive advantage from a business perspective or the value created from a customer perspective (Antonopoulou *et al.*, 2014). Such a far-reaching definition is employed because it allows including the general value created and captured by the ecosystem and end-users. It is important to note that the concept of value proposition is not targeted at a specific entity, but instead captures the value provided for all entities on a certain layer.

Additionally, the framework is enriched by a value concept taken from marketing, which is usually referenced as 'perceived value' and allows for the inclusion of value captured by single individuals (e.g. Afuah, 2002; Tellis and Gaeth, 1990). This understanding is particular suited to study the benefits of DCSs, because it implies an interaction between single end-users and applications and/or services (Payne and Holt, 2001). For instance, an exchange offering its service for a particular currency creates value for the users. However, the service only provides perceived value for users demanding this currency. To put it differently, it is the perceived value an application or service offers that attracts customers (Chang and Wildt, 1994; Lo and Wang, 2014). The current thesis follows a uni-dimensional approach by using economic reasoning, operationalized as utility, to assess the benefits and costs associated with DCSs (Agarwal and Teas, 2004). It should be noted that the utility concept always refers to individuals. Therefore, it is provided for the stakeholders in case of an assessment of organizations. The utility concept is related to perceived value in economic terms as the "difference between the 'utility' provided by the attributes of a product and the 'disutility' represented by the price paid" (Sanchez-Fernandez and Iniesta-Bonillo, 2007, p.429).

5.2.2 Framework: Value of Decentralized Consensus Systems

Although all DCSs share the same fundamentals, i.e. their technical backbone is a distributed ledger facilitating decentralization, there are also differences. Depending on their organizational structure and business model, some DCSs encourage third-parties to provide complementary applications and services via open interfaces, while also proprietary systems are conceivable. Additionally, DCSs also differ regarding to their provided functionalities. Thus, the potential value of every concrete DCS needs to be assessed independently. Table 27 illustrates the proposed framework to evaluate the value of DCSs.

<table>
<tr><th colspan="5"><b>Infrastructure: Decentralized Consensus System</b>
Governed by Non-Profit/For-Profit Organization</th></tr>
<tr><td colspan="3"><b>Open Systems</b>
▪ Open Strategy: Business models based on invention and coordination with community (Chesbrough and Appleyard, 2007)
▪ Publicly available source code
▪ Promote the development of applications</td><td colspan="2"><b>Closed Systems</b>
▪ Closed Strategy: Business models based on ownership and control(Chesbrough and Appleyard, 2007)
▪ Privately kept source code
▪ Prevent external applications</td></tr>
<tr><td></td><td><b>Layer</b></td><td><b>Value Proposition</b></td><td><b>Measurements</b></td><td><b>Perceived Value</b></td></tr>
<tr><td><b>Value Capture</b></td><td><b>1. ECOSYSTEM</b>
Organizations offering complementary applications & services</td><td>▪ Higher return on business Activities (Chesbrough and Rosenbloom, 2002)
▪ Higher return on innovation activities & intellectual Property (West and Gallagher, 2006)</td><td>▪ Profit (Antonopoulou <i>et al.</i>, 2014)
▪ Market share (Antonopoulou <i>et al.</i>, 2014)
▪ Decreasing costs for information and processing (Brynjolfsson and Hitt, 2000)</td><td>$U_E = \sum_{i=1}^{n} u_i$</td></tr>
<tr><td></td><td><b>INTERACTIONS</b>
Between Ecosystem and End-Users</td><td>▪ Network effects (Armstrong, 2006; Evans, 2003)</td><td></td><td>$U_O(U_E, U_U)$</td></tr>
<tr><td><b>Value Creation & Value Capture</b></td><td><b>1. END-USERS</b>
Individuals and Organizations (in)directly using DCS</td><td>▪ Support of transaction phases
▪ Reduction of information asymmetries (Sambamurthy <i>et al.</i>, 2003)
▪ Organizational transformation and improvement (Sambamurthy et al.,</td><td>▪ Profit (Antonopoulou <i>et al.</i>, 2014)
▪ Decreasing costs for information processing (Brynjolfsson and Hitt, 2000)</td><td>$U_U = \sum_{j=1}^{m} u_j$</td></tr>
</table>

Table 27: Value Framework for Decentralized Consensus Systems

A distinction is drawn between two layers where value is provided. The ecosystem (layer 1) consists of organizations providing complementary applications and services for a DCS. End-users (layer 2) are individuals and organizations that demand the functionalities offered by a DCS or corresponding applications and use services. Layer 1 and layer 2 are interconnected, because value is not only provided out of the use of the DCS, but also by applications and services. Thereby the emerging value is not only depending on the DCS infrastructure, but also on the whole spectrum of applications and services that support a successful use of the DCS (Vargo and Lusch, 2004). DCSs are platforms connecting application developers, service providers and end-users. The existence of network effects, where the value for one user depends on the number of other present users, is an important characteristic of such MSPs as presented in section 5.1.2 (e.g. Armstrong, 2006; Evans, 2003). This is represented through interactions between the ecosystem and the end-users.

Value proposition and perceived value are included as concepts to measure the emerging value. Despite their close connection, the concepts of value proposition and perceived value should not be equated. Although a DCS, service or application may create value within one or more of the layers, it does not necessarily provide the same value for every single entity (Winkler and Dosoudil, 2011). That is because customers perceive value differently depending on their needs (Hassan, 2012). Utility functions are stated to model the perceived value for the individual stakeholders in the ecosystem and the end-users leading to the utility functions u_i (for the ecosystem) and u_j (for the end-users). The sum of the utility of the respective entities on the respective layer is stated as U_E (for the ecosystem) and U_U (for the end-users). It is assumed that the overall utility U_O depends on the different layers' utility levels. Through this general representation, it is possible to use proper types of utility functions (e.g. Cobb-Douglas or quasi-linear) to model the preferences of different individuals.

5.2.2.1 Business Strategies of Infrastructure Providers

Regardless of the organizational structure, i.e. a non-profit or for-profit organization governing a DCS, one can distinguish between open and closed systems. The former adopts an open approach to innovation, where the organization pursues a so-called open strategy. Building on works of Chesbrough (e.g. Chesbrough, 2003; Chesbrough *et al.*, 2006), open strategy addresses the challenge of aligning organizations' business strategy with the benefits of openness "as means of expanding value creation" (Chesbrough and Appleyard, 2007, p. 58).

This implies business models which are based on invention and coordination with a community. Thereby, organizations utilize knowledge from internal sources as well as outside sources (West and Gallagher, 2006). Open innovation is a common paradigm in the area of digital technologies, with open source software as its most popular example. The underlying open source code of Linux, for instance, is used by a large number of companies and volunteers contributing to the development of the operating system (Germonprez and Warner, 2013). The same holds true for most current DCSs, irrespective of whether they are governed by a non-profit organization (e.g. Ethereum Foundation, whose DCS Ethereum is open-source) or for-profit organization (e.g. Ripple Labs., whose DCS Ripple is open source). This aims at promoting the development of corresponding applications on layer 1. But also closed systems are conceivable, where organizations governing a DCS pursue a closed strategy. The associated business models are characterized by ownership and control, where only knowledge from inside the organization is exploited (Chesbrough and Appleyard, 2007). In this case, the source code is kept private, which prevents the development of applications by external organizations on layer 1. This type of system seems more appealing for DCSs governed by for-profit organizations, because innovation from outside sources is the “most beneficial choice for non-profits” (Hull and Lio, 2006, p. 62). How value is concretely captured by organizations governing a DCS requires the examination of specific business models, which are outside of the scope of this chapter. A differentiation between open and closed systems is nevertheless important to determine the value creation and capture on layer 1 and 2, since it determines the development of applications.

5.2.2.2 Ecosystem

The ecosystem consists of application and service providers, who capture value by extending the scope of a DCS or offering intermediary services. The former provide direct access to a DCS via executing complementary applications on top of the blockchain. Smart contracts, for instance, are able to automatically verify the interactions between parties and, thus, add additional functionality to the existing DCS (Peters *et al.*, 2015). By offering additional functionalities, application providers generate profits, which increase proportionally to the number of end-users that demand them. The latter support services by intermediation that renders the direct or indirect use of a DCS more convenient. Bitcoin payment processors, for example, provide ready-to-use online-shop solutions, which ease the access and implementation of the technology for the respective merchant (Chircu *et al.*, 2000).

5.2.2.3 End-Users

End-users create value by the use of the DCS, applications and/or services provided by entities on the first layer. Through the facilitation of certain transaction phases and the reduction of information asymmetries, new or altered business models are adopted and an adjustment of behavioural patterns takes place. By disintermediation and sometimes irreversibility of transactions, DCSs are potentially able to decrease the costs during the respective phase of a transaction, given that sufficient amount of network participants is not faulty. Property-ownership recording systems for any kind of high-value property lead to a substantial reduction of costs by relying on general public consensus instead of a trusted third-party like notaries. In particular, they enable transaction contracts to be precisely defined and automatically executed (Omohundro, 2014). Following Brynjolfsson and Hitt (2000), organizational transformation and improvement are achieved by the usage of IT innovation, which enables complementary organizational investments as well as productivity increases. NASDAQ, which makes use of a DCS to create a new private market platform that connects private companies with investors, needs to exert complementary organizational investments in order to offer this service for their customers. However, this platform will potentially increase profits as a growing number of customers profit from the new technology (MIT Technology Review, 2015).

5.2.2.4 Interactions

A comprehensive approach to assess the value of a DCS requires an integrated view on both layers and the associated indirect network effects between them. Those effects are present if the value of a user in one group depends on how well users from another distinct group are attracted (Armstrong, 2006). Application and service providers benefit from a wider range of end-users through increased turnover and potentially higher market share. Vice versa, end-users benefit from a greater amount of application and service providers owing to a wider choice and the possibility to maximize their utility.

Determining the overall value of a DCS requires the distinction of two scenarios. The first scenario is described by a DCS which is an open system and allows for coordination with the community and a publicly available source code. The openness of the system enables agents on layer 1 to develop application on basis of the source code and to create value through complementary innovation (Gawer and Henderson, 2007). Examples for open systems are

Bitcoin or Ripple, which release their source codes in order to benefit from the participation of the community. Consequently, the overall value depends on the value on both the first and second layer. The second scenario describes a DCS which is privately governed and prevents the development of complementary innovation through external applications. Accordingly, value is achieved through the services offered on the first layer as well as the usage of a DCS by entities on the second layer.

5.2.3 Exemplary Evaluation of Bitcoin

Most attempts to evaluate the economics of DCSs in general, and Bitcoin in particular, are of pure descriptive nature. Franco (2015) provides a comprehensive overview of the technical and economical co-development of Bitcoin and other DCSs. The role of intermediaries (i.e. exchanges, payment processors) in the Bitcoin ecosystem, especially how intermediation leads to centralization tendencies in the decentralized envisaged Bitcoin system, raised much attention (e.g. Böhme *et al.*, 2015; Gervais *et al.*, 2014). There are also more concrete economic analyses addressing a specific scenario like for example the suitability of Bitcoin ML (e.g. Brenig *et al.*, 2016; Dostov and Shust, 2014) or the incentive-compatibility of Bitcoin mining (e.g. Eyal and Sirer, 2014; Kroll *et al.*, 2013). The European Banking Authority published an opinion letter concerning the potential economic benefits and the causal drivers of risks regarding virtual currency schemes (European Banking Authority, 2014). This work was complemented by a report on the relevance of blockchains for organizations in transaction banking and payments (European Banking Authority, 2015). Kazan *et al.* (2015) propose a taxonomy of digital business models with focus on the value of Bitcoin for companies offering services. There is a body of literature focusing on the monetary aspects of the Bitcoin system, which refers to the question whether bitcoins are assets or currency units. The often cited work of Yermack (2013) draws the conclusion that Bitcoin fails to conform to the classical properties of a currency. This is mainly due to the excessive volatility, absent risk mitigation strategies, fixed monetary supply and security issues. These findings are supported by indications that Bitcoin is rather used as an asset than a currency (Glaser *et al.*, 2014b).

The price formation is the object of investigation of several empirical studies (e.g. D'Artis *et al.*, 2015; Bouoiyour and Selmi, 2014). The volatility of bitcoins in exchange for fiat currencies over the last few years and the unclear drivers of the price formation process of bitcoins render it a promising research objective (Dwyer, 2015). Most researchers look at the influences of supply and demand as well as micro- and macro-economic indicators (e.g. Glaser *et al.*, 2014a;

Kristoufek, 2015). Vockathaler (2015) illustrates the ambiguity of the results of previous works, showing that the significance of the variables differs considerably between various studies. Furthermore, it is shown that the price is driven by hitherto unknown sources.

Beside their descriptive nature, investigations of the economics of Bitcoin are primarily partial, meaning that they refer either to the first or second layer but do not include a broad perspective. A comprehensive evaluation of the value of Bitcoin as open system requires analysis of the value created and captured on both layers as well as the inclusion of interactions. However, an evaluation based purely on monetary measures is not feasible given a lack of appropriate data for both, the ecosystem and end-users of Bitcoin. For approximation, indicators are discussed according to the framework. The complete data collection is accessible in the appendix of this dissertation.

5.2.3.1 Bitcoin-Related Research

Within the ecosystem of Bitcoin, a further indicator for higher profits is academic and industrial research, which encourages innovation (Mansfield, 1991). In particular, knowledge and innovation have a substantial role in fostering business growth, technological performance and international competitiveness, leading to higher profits for companies in the ecosystem as well as general economic growth. Five different databases ares used as sources for the evaluation of Bitcoin-related research, which diverge with respect to their thematic orientation. While Science Direct, Springer and Web of Knowledge constitute sources for general academic literature, ACM as well as IEEE provide more specific data about publications in the research areas of computer science, business informatics and information technologies. Table 28 represents academic publications between 2011 and October 2015, which contain the keyword “Bitcoin”. Between 2011 and 2014, academic publication increased exponentially, indicating a growing interest in the field of Bitcoin and associated applications. For 2015, the data cover only the time period between January and October. Nevertheless, the number of academic publications within this time period already exceeds the previous years figure.

The existing academic literature is analyzed as a proxy not only for academic but also industrial and institutional research activities. In particular, it is assumed that the increasing activity in Bitcoin-related academic research reflects a growing interest also in the industrial as well as institutional sector. This assumption can be confirmed when analyzing existing literature in all three sectors. Accordingly, academic research is accompanied by a plenty of industrial research (e.g. IBM, 2015) and institutional research (e.g. European Banking Authority, 2014; European Banking Authority, 2015). Those data was excluded from the analysis due to the fact that industrial research is often held confidential and is not publicly available.

Database	**Keyword**	**2011**	**2012**	**2013**	**2014**	**2015** [Jan.-Oct.]	**Overall**
ACM, IEEE, Science Direct, Springer, Web of Knowledge	"Bitcoin"	11	59	151	335	349	905

Table 28: Temporal Development of Academic Publications

5.2.3.2 Venture Capital Investments

Application and service providers in the ecosystem capture value through higher profits and lower costs, respectively. Increased profits are achieved by their function as intermediary in the transaction process as well as higher returns on R&D activities and innovation as the market share and overall demand for their products and services is rising (Howells, 2006). However, there is little debate over the fact that Bitcoin is still in its infancy and early market stage, which is comprised of innovators and early adopters. Consequently, Bitcoin's ecosystem is characterized by plenty of private for profit start-ups, whereby cash-flows are typically negative and experience values are lacking (Damodaran, 2012). Thus, profits cannot serve as direct measurement for the value of Bitcoin. According to Brynjolfsson and Hitt (2000), investments into IT serve as proxy for business profits by assuming linkages to productivity gains and organizational transformation on the firm level. Given the uncertainties and risks related to the early market stage of Bitcoin, IT investments in the ecosystem are best described by looking at venture capital. These investments are typically employed in the context of high- risk, potentially high-reward projects (Gompers and Lerner, 2001).

For the analysis, venture capital investments in Bitcoin start-ups between January 2013 and October 2015 were extracted from (Coindesk, 2015). The data set was extended by using data from VentureSource, Crunchbase and Coinfilter and checked for their validity. As illustrated in

Figure 29, the amount of venture capital investments in US-Dollar per year has increased between 2013 and 2015, whereas the total number of investments per year has decreased during the same period. Less diversification of investments in the ecosystem of Bitcoin can be ascribed to capital syndication. Consequently, the aggregation of venture capital investments explains higher total investment sums. From a risk-reduction perspective capital syndication means that investors try to reduce their risk resulting from adverse selection and information asymmetry by changing the mean by which investments are made and a greater range of analytical skills among investors (Lockett and Wright, 2001). Figure 29 also illustrates the specialization of capital into different sectors within the Bitcoin ecosystem. Investors seem to identify the highest return on investment in the sector universal, capturing applications and services, which can be used for more than one purpose (e.g. full-service providers, wallet and exchange providers etc.). 21Inc., for instance, a start-up company in the ecosystem of Bitcoin, received one of the highest investment sums in 2015 (116 million US-Dollar.), based on their activities in developing an embeddable mining chip, which can be used in a wide range of applications (Casey, 2015). This argument is emphasized by the fact that in 2015, 92 percent of fundings were second or more rounds fundings (especially in the sectors universal, payment processor and mining), indicating either past return on venture capital or that investors expect future profits to arise (Mann and Sager, 2007).

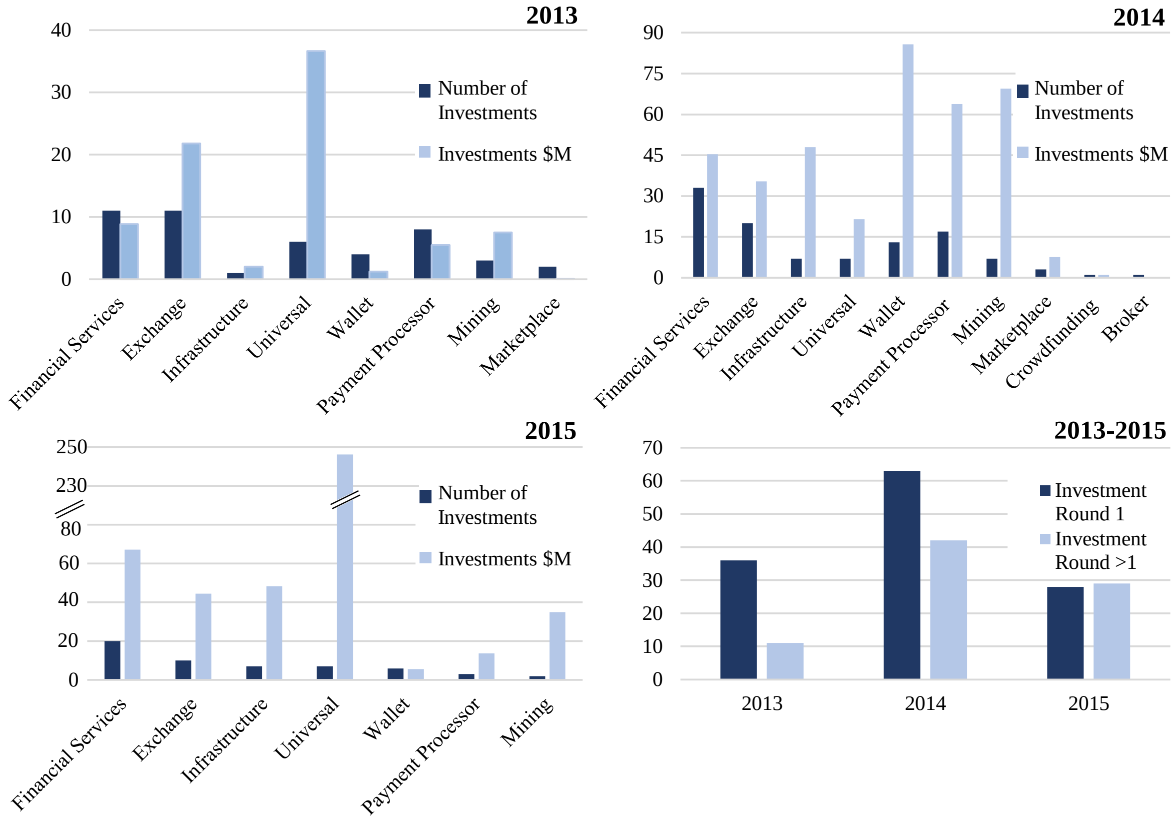


Figure 29: Temporal Development of Venture Capital Investments

5.2.3.3 Demand as Medium of Exchange

On layer 2, value is created by Bitcoin's ability to support different transaction phases and to reduce information asymmetries. Online retailers, for instance, derive advantages from reduced costs during the monitoring phase resulting from the irreversibility of payments and the associated impossibility of fraudulent chargebacks from end-users. More generally, individuals and organizations may benefit as end-users in a wide range of applications given Bitcoin's ability for disintermediation, due to the obsolescence of a trusted third-party within the transaction process. A complete set of data on cost reductions for information and processing of transactions, however, is not available. Nevertheless, given the cost reduction potential of Bitcoin, expect increasing demand for Bitcoin is expected assuming profit maximizing firms and individuals. Demand for Bitcoin is defined as the demand as medium of exchange. As an indicator for an increased demand a multi-dimensional proxy is used, comprising Bitcoin number of transactions, number of addresses and days destroyed. The latter is a measure of the level of activity and reflects the velocity of bitcoins within the system. It gives weight to a particular bitcoin depending on how long it has been in possession of an entity prior to its use in a transaction (a longer period of possession implies a greater weight).

The number of transactions has been increasing since the second half of 2012 (Blockchain.info, 2015). However, an increasing number of transactions alone is not a sufficient indicator for a growing demand of Bitcoin. Notably, raising transaction numbers may be caused by short-term purchases and sales effected by investors and for speculative purposes. For clarification, Figure 30 shows the number of unique addresses and Bitcoin days destroyed during the same time period. Bitcoin days destroyed is an indicator which gives an increasing weight to bitcoins involved in transactions depending on how long they have not been spent before. Transactions are largely conducted using bitcoins with short periods of possession, which implies that they are rather expended on a regular basis than hoarded. Furthermore, the increasing number of unique addresses shows a tendency towards a growing number of end-users. Unique addresses in this context are all existing addresses that hold account balances at a time. In combination with the steadily growing number of transactions, an increasing number of addresses as well as volatile but relatively stable low level of days destroyed emphasize that the demand for Bitcoin as a medium of exchange increases.

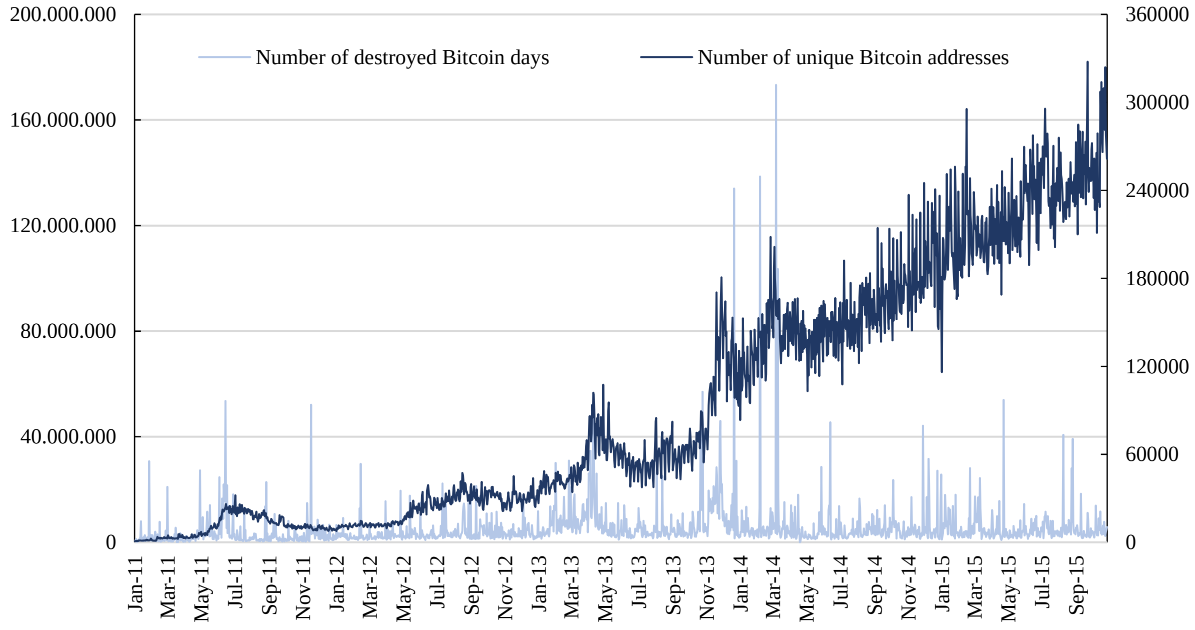


Figure 30: Unique Bitcoin Addresses and Destroyed Bitcoin Days

5.2.3.4 Media Attention

On the contrary to the indicators named above, media intention constitutes a negative indicator. According to (Garcia and Schweitzer, 2015), media attention is interpreted as the degree of word-of-mouth communication and approximated by Bitcoin-related data on Google trends as well as the Twitter mood. Those data were extended by looking at Wikipedia search queries, leading to the result of decreasing media attention for Bitcoin and consequently, declining public attention (stats.grok.se, 2015). This indicates a loss of relevance of Bitcoin as means of payment.

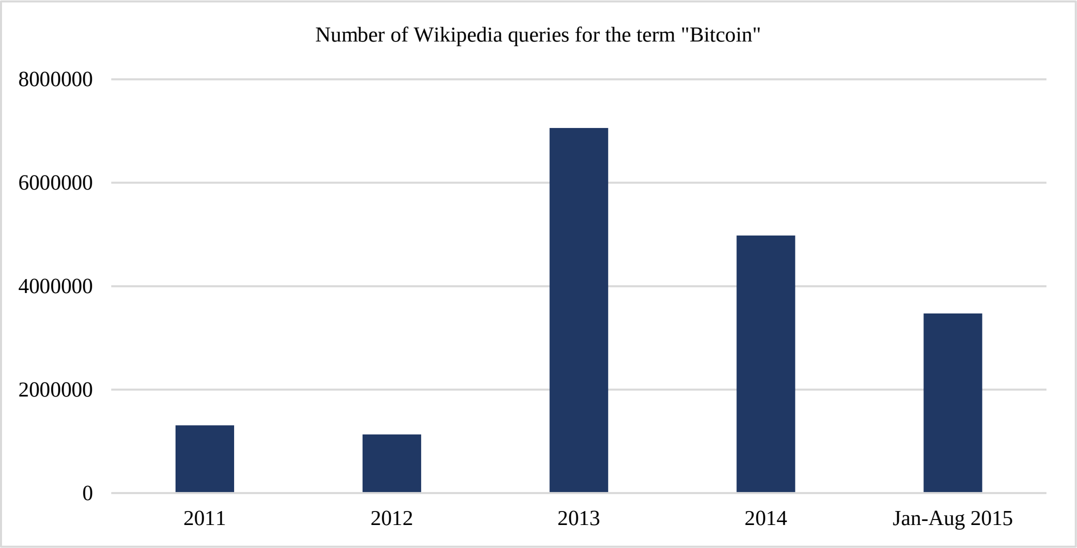


Figure 31: Wikipedia Queries for Bitcoin

5.2.4 Discussion of the Results

The analysis of the indicators concerning the value of Bitcoin is summarized in Table 29. Positive indicators suggest that Bitcoin provides value on the respective layer, whereas negative indicators point to the fact that entities in the ecosystem and end-users are not able to create and capture additional value by the use of the DCS. Referring to the ecosystem, venture capital syndication as well as the rising investment sum predicts future profits and indicates the value, which is captured by organizations offering complementary applications and services. Though it is possible to object that investments are made in a speculative bubble, it is argued that capital syndication leads to pareto-efficient portfolio selection. Based on complementary management skills and more efficient decision-making mechanism, it is concluded that venture capital is invested in sustainable business models and the technology underlying Bitcoin (Brander *et al.*, 2002). Moreover, Bitcoin-related research reflects the value of the DCS. Given the innovative potential of research, the findings are likely to be transformed into innovation, raising profits for application and service provider on the first layer. Demand for Bitcoin as medium of exchange illustrates the value created on the second layer. The growing use of bitcoins as an exchange medium indicates that individuals and companies identified potential for cost reductions through supported transactions and decreased information asymmetries. This conclusion is undermined by the decreasing development of the media attention, which can be interpreted as a loss of relevance for Bitcoin. Since crucial factors responsible for the price formation are still unclear, a restricted explanatory power for the bitcoin price as indicator is assumed. After peaking at over 1.000 US-Dollar at the end of 2013, the price of a bitcoin at exchanges fell steadily and fluctuated between 200 and 300 US-Dollar over the course of the first nine months in 2015 (Coindesk, 2015).

Layer	Positive Indicatior	Negative Indicator
1. ECOSYSTEM	▪ Venture Capital Investments ▪ Research	
2. END-USERS	▪ Demand as Medium of Exchange	▪ Media Attention ▪ (Bitcoin Price)

Table 29: Evaluation Results Bitcoin

5.3 A Compliance Perspective on Decentralized Consensus Systems

DCSs are envisaged to rearrange digital interactions by processing transactions through a decentralized network. Concretely, they provide mechanisms to execute transactions in accordance to predefined rules. The respective system enforces these rules and enables observability regarding performed transactions afterwards. The present section interprets these capabilities as a promising opportunity for compliance realization in digital interactions as outlined in Table 30. Thereby, DCSs may constitute platforms for improving existing business processes and implementing novel business models. Addressing this issue, such systems are classified into the concept of compliance. This interpretation provides a business perspective on DCSs and offers additional insights for elaborating on practicable applications. Therefore, the remainder of this chapter elaborates on the compliance process and shows how it can be ensured by DCSs before, during and after a transaction takes place. Afterwards, the core elements of DCSs regarding the realization of compliance are discussed in detail.

1. Compliance	**The Compliance Process** ▪ Introduction to the compliance phases with regard to their timing: before, during or after a particular transaction ▪ Specification of rules, conformance check and audit as parts of the compliance process ➢ Theoretical explanation of how compliance is realized
2. Implementation	**Compliance Facilitated by DCSs** ▪ Examination of how the compliance phases can be supported by the implementation of a DCS
3. Application	**Financial Asset Trading Infrastructure** ▪ Presentation of a use case from the financial industry ➢ Illustration with reference to the use case

Table 30: Methodological Approach DCSs as Compliance Instrument

5.3.1 The Compliance Process

Business compliance is the conformance of a company's activities and business practices with existing regulations, such as laws, best practices, contracts, agreements, and so on (Sackmann *et al.*, 2008). To ensure compliance, appropriate internal and external monitoring activities need to be implemented within business processes of the company (Scholte and Kirda, 2010). The aim of compliance requirements is to enhance transparency of business decision and to augment the accountability of responsibilities. Finally, compliance is protecting investors and stakeholders from fraud, corruption and corporate misconduct (Sackmann *et al.*, 2008).

Today, compliance management is an independent and autarchic management unit and includes all instruments and mechanisms that are necessary for the development, implementation as well as enforcement of requirements, principles and company values in the strategic and operative business (Scholte and Kirda, 2010). However, the realization of compliance requirements is not an easy task. For instance, regulations are imposed by external entities such as the government and implementing this rules is difficult as they are expressed at a high-level of abstraction and communicated in natural language. Consequently, the realization of compliance requires a process that makes existing regulations enforceable by the underlying technical infrastructure of every business / process (Sadiq *et al.*, 2007).

The process of compliance realization for any arbitrary chosen transaction *i* is depicted in Figure 32. In particular, the compliance realization process can be divided into three different phases referring to its timing and in regard to the point in time, when transaction *i* is executed. Assuming that all relevant compliance sources and requirements are identified (i.e. legal requirements, contractual obligations as well as external and internal business policies), the first phase of the compliance realization process comprises the specification of rules within the underlying IT infrastructure. The specification of rules requires the formal representation of existing compliance requirements in an appropriate policy language, such as EPAL or P3P. In particular, for the realization of compliance the specification of rules must be done before the execution of transaction *i*. During the execution, compliance is ensured through the enforcement of policy rules within the business process by means of internal compliance checking methods (Scholte and Kirda, 2010). This also includes the enforcement of corrective runtime actions (e.g. sending an alert), or the adjustment of internal policies (e.g. adjust inconsistent policies). The final realization of compliance is achieved after the execution of the transaction by means of appropriate detection methods and audit, such as data mining or root-cause analysis techniques that are applied to the data created during the execution of the transaction (Sackmann *et al.*, 2008; Sadiq *et al.*, 2007).

In general, conformance checking and audit mechanisms need to be context-specific, not only with respect to the particular business process, but also in terms of the underlying infrastructure. In the following, the three different phases of the compliance realization process will be further explained by assuming a DCS as underlying digital infrastructure for business process execution.

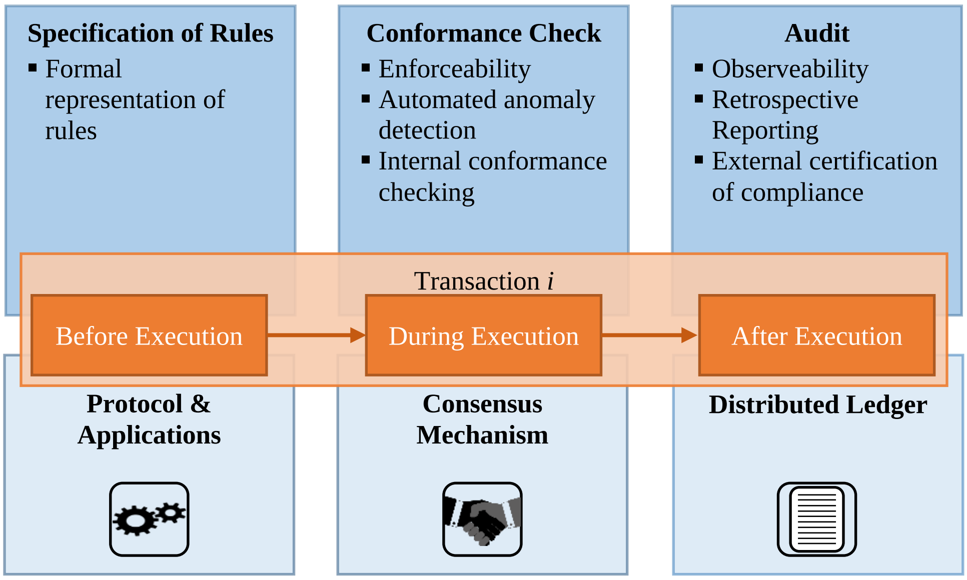


Figure 32: The Process of Compliance Realization

5.3.2 Compliance Facilitated by Decentralized Consensus Systems

This chapter is organized according to the different phases of compliance realization and explains how the process of compliance realization can be supported by DCSs. The compliance process is here defined as an integral approach, which links laws and regulations (e.g. the Sarbanes-Oxley Act or Basel II) with IT systems. Consequently, compliance is not only the non-technical adherence to laws, but must also consider the technical foundation of compliance realization, i.e. the implementation of mechanisms as well as the enforcement and control of rules within a DCS (Sackmann *et al.*, 2008). In this section, the focus lies on the technical specification, implementation, and realization of top-level compliance requirements through DCSs.

5.3.2.1 Pre-Execution Phase: Specification of Rules

Laws and regulations typically define a vague set of requirements describing what has to be done on a very abstract level. As any kinds of transactions are increasingly realized trough IT, these top-level compliance requirements must be transferred into machine-readable form in order to formulate control objectives on a technical layer. Thus, in order to monitor and enforce top-level requirements, first, a correct and complete specification and implementation of the desired rules must be realized, building the fundament of DCS and the decision criteria of decentralized consensus. The decision whether a transaction conducted utilizing a DCS is valid and, therefore, qualified to be included into the distributed ledger, is based on its conformance to a set of predefined rules. Two types of rules are of relevance in this context: general rules and contextual rules. As the naming suggests, they are distinguished according to their different scope. While general rules describe provisions applying to every transaction processed through a DCS irrespective of the respective use case, contextual rules are binding only to a set of similar transactions or even only a single transaction *i*.

General rules are embedded into the protocol of a DCS and determine the fundamental characteristics and features of the system. On the highest level, they define the degree of openness by setting the terms for participation. A typology is currently evolving in the practical context, which categorizes DCS into permissionless- and permissioned systems (e.g. Government Office for Science, 2016; McKinsey, 2015a). Permissionless systems grant public access to the distributed ledger and anyone can participate on the conformance-checking of transactions. Permissioned systems, in contrast, place restrictions upon user groups' rights to access certain features and are therefore understood to be private. The degree to which a particular system is assigned to one of these extremes depends on the concrete formulation of rules. They specify, for instance, which access controls are implemented prior to utilizing the DCS for digital interactions. It may be possible to create an unlimited number of pseudonyms (e.g. Bitcoin (Nakamoto, 2008), Ethereum (Butterin, 2016)) or that accounts are tied to personal identifying information (e.g. R3 (R3, 2016)). Beside rules controlling access to the system, it also needs to be formulated how assets are tied to accounts, which kinds of signatures are used to prove ownership and so on. Whether these general rules are loosely or tightly defining the system determines the range of transaction patterns, and with it functionalities, potentially facilitated by a DCS. A loose set of rules is limited to specifying minimum requirements on the structure and operation of correct transactions and composes a platform intended for multiple applications. Compared to this, a tightly set of rules limits the flexibility to implement extensive functionalities and is typical for a specialized system.

Contextual rules describe provisions not all transactions are obliged to conform to and which constitute the foundation for new functionalities added via applications. These applications are designed and provided by developers based on an open source code, application programing interfaces or scripting languages implemented into a DCS. One concept commonly mentioned to specify contextual rules are smart contracts, which constitute user-defined programs formalizing rules intended to govern transaction processing according to deliverables, responsibilities and operating parameters specified beforehand (Szabo, 1997). They function as self-executing contractual states autonomously reacting to events in a predefined way and are envisioned to enable “substantial improvements in compliance” (Government Office for Science, 2016, p. 18). With regard to digital interactions, smart contracts execute transactions between users or other smart contracts, once rules defined in the form of certain criteria are met. The concept is considered promising for integrating contextual rules into DCSs, since they promise to lower the technical bar of entry for users. However, in practice they have to be precisely designed in order to avoid security breaches, especially when valuable assets are involved (Delmolino *et al.*, 2016). Independent of their concrete realization, contextual rules can build applications and apply to all associated transactions or are only temporarily valid for a limited number of transactions between end-users.

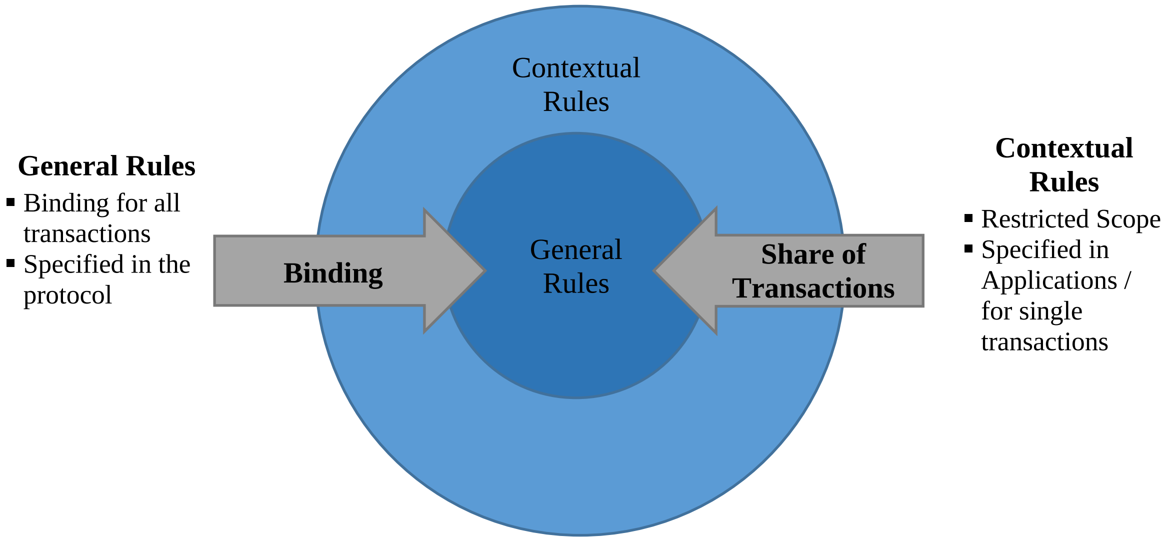

Contextual Rules
General Rules
General Rules
▪ Binding for all transactions
▪ Specified in the protocol
Binding
Share of Transactions
Contextual Rules
▪ Restricted Scope
▪ Specified in Applications / for single transactions

Figure 33: Binding of Types of Rules

5.3.2.2 Runtime Phase: Conformance Checking

Having specified the general and contextual rules a given transaction *i* has to comply with, mechanisms need to be implemented into the DCS in order to enforce them during execution. This is realized by simply adding only transactions to the distributed ledger, which are in conformance with the predefined rules. The major innovation of DCSs is that this consensus process is carried out in a decentralized fashion. Instead of trusting a third party checking the conformance of transactions, a distributed network of consensus participants agrees upon a common state of the systems. Therefore, they rely on a consensus mechanism technically ensuring this state to be finally reached.

Enforcing that only transactions according to predefined rules are processed by the DCS crucially depends on the composition of the network and varies significantly between the types of system implemented. As already mentioned above, permissionless systems are public and allow anyone to participate on the consensus process. To prevent deliberate violations against the rules by validating incorrect transactions, consensus participants are required to expend economic resources like computing power (POW) or they need to have a stake in the system (POS). It secures a DCS based on an economic rationale, where verifying transactions according to the rules need to be more favourable than compromising the system for every individual. Permissioned systems take a different approach, restricting consensus participation to entities known to and designated by the operator of the DCS. This procedure reintroduces some level of trust, varying with the number and diversity of entities appointed for verifying the rule conformity of transactions. The highest level of trust is required from end-users in a system with a single entity responsible for the consensus process. Theoretically, this entity is able to prevent correct transactions from being processed or insert additional transactions. The level of trust is gradually reduced the more entities are appointed to concurrently verify transaction and control each other. This applies especially in situations where the entities pursue diverging interests and though have no incentives to collude. DCSs with more than one preselected and independently operating entities participating in the consensus process are referred to as consortium systems (Buterin, 2015). In order to synchronize between these entities, such systems make use of consensus mechanisms already established in other distributed computing scenarios (Byzantine Consensus (Lamport *et al.*, 1982)).

5.3.2.3 Post-Execution Phase: Audit

Audit is a process of "after-the-fact" detection of compliance violations, often conducted by traditional audits and manual checks by consultants (Sackmann, 2008). In particular, evaluating the compliance state of a company means looking at how business has been performed, by checking whether the traces and evidences produced during the execution of the transaction actually conform to the specified compliance rules (Sackmann *et al.*, 2008). Mechanisms, which are applied in the context of the audit, can be summarized as retrospective reporting methods (Sackmann, 2008). However, the development of modern IT led to a blurring of boundaries and a shift of the audit process to the both the execution phase and the post-execution phase of a transaction. This is accomplished by so-called automated compliance through compliance checking software, which still is retrospective, or compliance by design approaches.

Compliance by design has a preventative focus on the enforcement of desired behaviour and the prevention of damaging events by implementing and refining regulations on all system layers. By this it is assumed that no damaging event can occur, irrespective of the type of fraud which is attempted (Sackmann, 2008).

Automated compliance, and especially, compliance by design led to significant cost reductions, not only in the area of personnel costs but also in terms of the time, which is needed to conduct the audit (Sadiq *et al.*, 2007). Despite this sounding more than promising, the existing compliance by design solutions are not sufficient to guarantee the adherence to regulations within the context of a transaction. Thus, additional retrospective detection methods must be implemented to assure and validate the rightness of every transaction (Sackmann, 2008). The necessity to implement additional methods of compliance by design is a consequence of different policy rules that need to be considered and require varying IT mechanisms. These policy rules are enforceable policy rules, whose violation can be prevented by appropriate IT mechanisms such as access control lists or workflow engines as well as observable policy rules that are sometimes also referred to as auditable rules, meaning that their compliance can be at least detected ex post by a monitor and through auditing logged event activities. Lastly, there are non-observable policy rules, where the adherence to the rule cannot be observed ex ante or ex post, for instance, if some actions are invisible to a monitor, such as ‘delete data after use’ actions. Non-observable policy rules constitute yet a major challenge on compliance and the associated audit process.

Using a DCS as digital infrastructure that facilitates the execution of transactions, a compliance by design approach is applied. As consensus will only be found over transactions that are in compliance with the rules specified within the DCS, non-compliance is likely to be technically impossible. However, the specification of rules in the consensus protocol must not only be correct, but also complete. Possibly, there are transactions within the system that are validated and executed through the decentralized consensus, although there are not mapped by the system through the general or contextual set of rules, e.g. due to the novelty or complexity of innovative, digital transactions. However, as indicated in Figure 32, information, which is processed by DCSs, is stored in a distributed ledger that is a shared database, which features transparency over transactions. Consequently, this allows ex post monitoring of transactions and their adherence to the pre-specified rules, leading to case-to-case decisions based on the existing set of policies and rules by the distributed network or a central entitiy, such as a network administrator.

5.3.2.4 Use Case: Financial Asset Trading Infrastructure

For the use case to which is referred to in the following, the application of a DCS in the context of a FATI is considered. The notion of financial asset was deliberately chosen in such a generic manner, as the depicted example is intended to cover a wide range of assets ranging from stocks or private equity up to the transmission of monetary value. Even though it might be conceivable to select any kind of interaction pattern for the development of the use case, it was purposely decided to pick the financial sector due to its actual practical relevance. This is expressed by the multitude and variety of projects the financial industry is working on. The US stock exchange NASDAQ, for instance, has already debuted a platform called Linq at the end of 2015. Linq initially only enabled trades on their private equity market, since it is characterized by a low level of regulatory complexity and provides valuable insights for other applications. The R3 distributed ledger consortium, a merger of more than 50 of the world's leading financial institutions (including amongst others Barclays, Credit Suisse or Deutsche Bank), aims at collaboration on the research, design and implementation of DCSs for supporting interbank processes (R3, 2016). Another DCS worth mentioning is the global settlement network Ripple. It is already running live and offers cross-border payments without any centralized financial intermediation (Ripple Labs., 2016). In a report examining the potentials of DCSs for financial industries, the World Economic Forum acknowledges financial trades as a high-potential use case (World Economic Forum, 2016).

The layers of financial systems are currently siloed and dominated by proprietary IS creating multiple versions of the truth. Additionally, the systems were predominantly architected decades ago and are not designed for continuous market operations needed in increasingly globalized markets. Expanding the view by an institutional dimension, it ultimately boils down to the issue to which extent one is willing to trust third parties (DTCC, 2016; Mainelli and Smith, 2015). Addressing these deficiencies, DCSs are envisaged as promising instruments to process financial transactions in a decentralized fashion and enhance the transparency of the underlying procedures (World Economic Forum, 2016). Figure 34 depicts the end-users present in the use case and their interactions with each other as well as with the system.

- *Issuer:* An entity that registers, distributes and sells a financial asset on the system
- *Investor:* An entity that is buying and holding financial asset
- *Financial Supervision:* An entity that is empowered to monitor activities and enforce actions

How the DCS ensures compliance in the transfer of financial assets between issuers and investors and how it supports financial supervisors is examined subsequently.

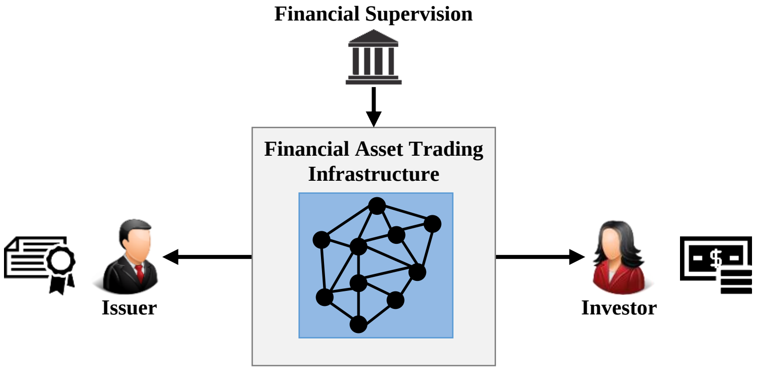


Figure 34: Interdependencies of a Financial Asset Trading Infrastructure

The FATI can be simplified characterized as an orchestration of general as well as contextual rules governing transactions executed by a DCS. Transactions in this use case facilitate the trading of financial assets between issuers and investors. Therefore, the two types of rules are responsible for managing the exchange of these assets and the corresponding payments. General rules define the overall functioning of the FATI and include: procedures for the registration of issuers to ensure emitted assets are legitimate, minimum requirements for information that need to be provided regarding an asset or conditions that a transaction has to fulfill in order to be valid. Contextual rules are specifically applied to a concrete business relationship. If, for example, the investor of a company should receive an extra dividend when certain business objectives are met, this could be formalized as contextual rule and automatically be executed. Therefore, the rule could reference to a reliable external source publishing relevant indicators like the turnover during a period or the profit.

It is designed as a consortium system operated by several financial institutions. The rationale behind this multilateral collaboration is the exploration and launching of innovative service solutions in the financial industry. Hereby, the FATI ensures that transactions successfully processed comply with the rules all involved financial institutions have agreed upon. Since these institutions are competing directly, they have strong incentives to control for the compliance of each other. Therefore, it might be reasonably assumed that the consensus mechanism works properly. Actual examples from practice provide evidence that DCSs operated by a consortium of organizations, especially from the IT and financial industry, constitute a realistic scenario. To this belong the Hyperledger Project, which is a collaborative project under the umbrella of the Linux Foundation concerned with establishing cross-industry standards for DCSs (Linux Fondation, 2016). Recently, a group of Russian financial companies announced to work together on the development of platforms utilizing the principles of distributed ledgers (Higgins, 2016).

An issuer and an investor that use the FATI must adhere to the general rules that are pre-specified by the trading platform. In fact, through the use of the DCS, a compliance by design approach is applied, since the issuer and the investor cannot violate the general rules due to the decentralized consensus. Moreover, the trading partners are able to specify their own contextual rules through the agreement on and execution of a smart contract, which again implies a compliance by design approach. Thus, the issuer and the investor cannot act against their own rules. As it necessary for decentralized consensus to have a transparent data structure, i.e. the distributed ledger, the decentralized asset trading infrastructure allows for complete transparency over executed transactions and the associated general and contextual rules. This enables not only the trading partners but also external supervisory authorities, e.g. such as the German financial supervisory authority or the United States Securities and Exchange Commission as well as other external monitors to check compliance. However, due to the complexity and novelty of certain financial assets and trading relationships (e.g. if there are more than two entities involved in the trading), there may be actions within the system that are validated and executed through the decentralized consensus, although there are not mapped by the system through the general or contextual set of rules. These kind of actions, however are still observable ex post such that supervisory authorities or other monitors are able to make individual case-to-case decisions based on the exiting set of policies and their own assessment. Notably, the conduction of non-observable rules within the decentralized infrastructure is no more feasible, which seems to solve one of the major problems of current audit.

5.3.3 Discussion

This section is intended to enrich the discussion of DCSs by a compliance perspective which has, to the best knowledge of the author, not considered before. The relevance of this perspective can be demonstrated by means of The DAO, a project showing existing technical as well as legal challenges and vulnerabilities of organizational structures completely depending on predefined rules. It was developed by the German start-up Slock.io to collect investments and distribute them to finance proposals for products and services voted on by its contributors. The DAO attracted a lot of attention due to a highly successful crowdfunding campaign raising 160 million US-Dollar and it has already offered the first proposals for selection. These proposals, however, could not be finalized since an attacker managed to exploit a vulnerability in the code defining the underlying rules and was able to drain a large number of funds. Fortunately, The DAO defined a time span which must elapse until it is possible for the attacker to actually access these funds. During this period, which has not been expired at the time of this writing, several solutions are discussed. One consists of agreeing on blacklisting transactions involving the funds by not forwarding them through the network. Another approach is more drastic and suggests to ignore existing rules and return the funds to their original owners through a discretionary intervention (Siegel, 2016).

More important than the concrete procedure in the present case are the general issues it demonstrates concerning DCSs. The discussion about potential solutions clarifies discrepancies regarding the extent to which a completely rule-driven system is desirable and where and how discretionary decision-makers can or need to be integrated into DCSs. Another challenge arises whether one is willing to take the risk of an incorrectly specified system, especially when it processes assets in the millions worth of value. This implies a controversy about how such systems have to be regulated from a legal point of view: the attacker has done nothing illegal based on the programmed rules, but the actions are certainly not in accordance with applicable law. Interpreting DCSs as instrument for compliance realization may offer additional insights for the identification and analysis of practicable application fields for DCSs. It provides a comprehensive economic view of such systems, including the definition of rules, their enforceability and observability, which is still missing right now and is required to tackle the issues mentioned above.

5.4 Concluding Remarks

The research question addressed in this chapter was *RQ4b: How can the economic potentials of Decentralized Consensus Systems be evaluated?* In order to lay the economic foundations, it was theoretically how DCSs facilitate digital interactions and they were characterized as MSPs to reason about possible business models. Based on this, an evaluation framework for the value of DCSs was provided. The concept of economic value was introduced and subdivided into the concepts value proposition and perceived value. This was necessary due to the complexity and abstractness of the term value. The value concepts constituted the theoretical foundation for the construction of the evaluation framework. The ecosystem (i.e. organizations offering complementary applications and services) and the end-users (i.e. individuals/organizations (in) directly using a DCS) were identified as layers, where value is created and captured. As a first use case, Bitcoin was evaluated with several indicators and it was concluded that Bitcoin indeed creates value on the mentioned layers. The proposed evaluation framework constitutes a first step to assess the value of DCSs. The presented evaluation focused on Bitcoin as the most prominent DCS, since there is the largest quantity of publicly available data. Due to its focus on payments, Bitcoin is not necessarily representative for all kinds of DCSs. It nevertheless serves as a nice application example for the evaluation framework and allows for comparing the results with other DCSs.

The remainder of this chapter provided an interpretation of DCSs as instrument for compliance realization to assess these systems. Consequently, the general compliance process was outlined and it was shown how the process could be supported by DCSs before, during and after a transaction takes place. Subsequently, the core elements of DCSs facilitating the realization of compliance were discussed. The use case of a FATI was presented as a practical example to illustrate the findings. This view was introduced as a new understanding of the functionalities offered by DCSs and to provide a basis for their further examination.

6 Conclusion & Outlook

The findings of the dissertation at hand are proposed as a contribution to analyze systems based on distributed ledgers and provide means for their development as well as economic evaluation. Therefore, it was structured into the five preceding chapters that addressed the successive research questions *RQ1* to *RQ4*. Naturally, various open research challenges and topics that are out of the scope of this dissertation remain. Consequently, this chapter firstly concludes with a summary and the main results. Based on the discussion of the main results, it suggests directions for future research on DCSs.

6.1 Summary & Main Results

The case study of bitcoins as digital representation of money was introduced in chapter 2 to tackle research question *RQ1*: *What are the specific characteristics of the Bitcoin system?* As chapter 2 clarifies, novel developments in payment systems are always driven by the promise of reductions in transaction costs associated with the transfer of assets. In this regard, Bitcoin constitutes a completely new type of decentralized payment system, implementing a convertible virtual currency called bitcoins. Consequently, different types of EPS were classified according to the type of money they support to transfer. Thereby, it was possible to clearly explain how Bitcoin, as well as other cryptocurrencies built upon its reference implementation, fit into the landscape of existing EPSs and to determine what their distinguishing features are. Finally, the different components of the Bitcoin system were examined on basis of its important elements to derive the specific characteristics of the Bitcoin system.

Originating from the specific characteristics of cryptocurrencies like Bitcoin, this dissertation analyzed risks arising from their design in the context of ML. Chapter 3 therefore tackled research question *RQ2: Does the system design of cryptocurrencies, especially Bitcoin, lead to risks in the context of money laundering? More precisely, what are the factors that shape the* *incentives for criminal individuals to utilize them for money laundering?* To begin with, chapter 3 conceptualized cryptocurrencies as digital ecosystems to introduce the relevant actors that emerged around them. These actors constitute an integral part of transaction patterns involving cryptocurrencies and have to be taken into account when analyzing the risks of cryptocurrencies for ML. A comprehensive overview of the current literature dealing with the justification of criminal activities from a microeconomic perspective was conducted to conceptualize the analysis. The results imply that the presented factors might indeed encourage the exploitation of cryptocurrencies by money launderers. This illustrates the risks arising from the specific characteristics of the Bitcoin reference implementation, which consequently need to be addressed. Moreover, technological developments and regulatory approaches were introduced as possible measures to mitigate these risks.

Having presented the specific characteristics of Bitcoin and analyzed potential risks of decentralized payments, the dissertation at hand investigated the resulting implications on the general architecture of DCSs and their applications. Consequently, this lead to the following research question *RQ3a: Based on the analysis of Bitcoin and similar cryptocurrencies, which implications result for the architecture of Decentralized Consensus Systems in general?* Broadly speaking, DCSs are systems implementing a distributed ledger, which can theoretically be used for a variety of applications in different scenarios. Due to the fast pace of developments, however, the range of possible use cases can only be guessed right now. Consequently, chapter 4 firstly provided a classification of different application fields according to their degree of complexity. Afterwards, the present thesis suggested a multi-layered structural model to conceptualize the consensus achieved by DCSs. Subsequently, chapter 4 provided a classification of different types of DCSs into permissionles and permissioned systems, which differ regarding their openness and the toleration of centralized entities. It refers to the characteristics of permissionless systems like Bitcoin already presented in chapter 2 and compares these findings to the characteristics of permissioned types of systems. Then chapter 4 elaborated on research question *RQ3b: What are the functional requirements for Decentralized Consensus Systems?* As foundation for the elicitation of requirements, an agent-based framework consisting of the relevant actors of such systems was provided. The actual requirements were based on a review of industrial research and whitepapers concerned with distributed ledgers in order to reflect stakeholders' needs. They are intended to support academics in understanding the peculiarities of DCSs as well as practitioners in building DCSs that meet stakeholders' goals.

Taking into account the general architecture of DCSs, chapter 5 addressed research question *RQ4: How can the economic potentials of Decentralized Consensus Systems be evaluated?* Accordingly, a framework was developed to evaluate the value of DCSs, in order to bridge the current gap of approaches to explain where and how the value of a DCS arises. The framework was exemplarily applied to the Bitcoin system, which was evaluated according to several indicators. The last sections of chapter 4 enriched the discussion of DCSs by a compliance perspective which has not considered before. It is based upon the observation that DCSs provide mechanisms to ensure compliance to a set of defined rules before, during and after transactions take. These mechanisms are grounded on the consensus process enforcing acceptable transactions to be included into the ledger and the transparency regarding conducted transactions facilitated by DCSs. This perspective offers means to assess DCSs from a compliance point of view.

6.2 Implications for Future Research

The previous section presented a summary of the identified research questions and explained this dissertation’s contributions addressing them. Nonetheless, a number of unanswered questions and challenges that are out of the scope of this thesis remain. Some of the limitations and open questions will be discussed in this section. It sketches some of the overarching challenges regarding DCSs arising in different fields of research and argues for a multidisciplinary research agenda.

A lot of developments in the concept of DCSs and a growing public as well as professional and academic attention can be noted since the inception of the Bitcoin system at the end of 2008. Many works on the topic, however, remain on a high-level and solely explain the promises of transparency and immutability provided by a distributed ledger which is not under control of a centralized entity. While this discussion offers fruitful insights into the potentials of a paradigm promoting the decentralization of a variety of business models and practices, it lacks clear guidelines of how the respective systems supporting its realization need to be designed in practice. Not to mention that it misses recommendations in which way such systems are successfully integrated into existing business processes, in order to facilitate the decentralization of concrete applications. Additionally, it is even unclear right now for which use cases DCSs really offer added value and in which contexts the concept is nothing more than a currently popular buzzword.

One viewpoint often heard is “Bitcoin works in practice, but not in theory”, which alludes to its still missing rigorous theoretical foundation (Bonneau *et al.*, 2015). This statement refers to the complexity issues arising in trying to thoroughly investigating security-related issues concerning Bitcoin and other DCSs. In addition, questions relating to the implementation of DCSs suitable for different applications belong to the existing challenges for researchers in the field of computer science, which should be subject to further investigation. Both sketched topics simultaneously preserve a strong connection to the fields of IS and economics. The security of a permissionless DCS is only guaranteed in practice as long as behavior according to the rules is more profitable than committing malicious attacks on the system. Or in other words, the participants of the decentralized network need to be incentivized for their correct conduct. As a consequence, the costs incurred for maintaining this type of system render the use of DCSs always more expensive than a comparable centralized solution. Even though it has to be clear that centralized systems also come at the price of trusting a third party. Potential cost reductions are one of the reasons that justify permissioned systems, which are somewhat opposing the original idea behind DCSs to avoid any centralization. The rationale backing the permissioned approach assumes a system to be secure as long as there are enough independent parties that control each other and reintroduces some form of trust. An example would be a consortium of banks jointly operating a DCS for the settlement of financial transactions. The idea sounds attractive but is based on purely theoretical considerations. Therefore, it remains an open how such systems can be implemented and whether the existence of independent actors disciplining each other will work in reality. Furthermore, many challenges remain unresolved that have to be tackled from the field of legal studies. Regulatory approaches that appreciate the specific characteristics of DCSs are just beginning to emerge. It is necessary to clarify which jurisdiction is (or jurisdictions are) responsible for overseeing globally operating decentralized systems with unclear responsibilities. It may also be a conceivable possibility to require operators of DCSs to provide certain institutions with exclusive access rights.

One cannot deny that it requires additional research integrating researchers from the fields of computer science, IS, economics and legal studies in a multidisciplinary research agenda towards the further examination of DCSs. This is not surprising, given that the notion describes a multifaceted concept with potentially severe impacts on business models and processes in a variety of industries, which may affect how digital interactions will be carried in the near future. However, the concept of DCSs could also turn out to be nothing more than an interesting idea without feasible real world applications. Against this unclear future prospects, the dissertation at hand has provided several contributions to facilitate the analysis of DCSs. It formulated the specific characteristics of permissionless systems like Bitcoin and illustrated risks arising in the context of payments. It elaborated on their general architecture by classifying different types of systems and elicitating functional requirements for DCSs. Furthermore, it developed frameworks and concepts to evaluate the economic value of DCSs.

Appendix

A: Overview of Governmental Actions Regarding Virtual Currencies

	Category	Date	Authority	Key findings
Australia	Classification	Jun-13	Australian Taxation Office	Bitcoin is expected to be understood as electronic payment system or money
		Dec-14	Australian Securities and Investments Commission	Digital Currencies themselves do not fit within the current legal definitions of a 'financial product'
		Dec-14	Australian Taxation Office	Bitcoin is neither money nor a foreign currency
		Aug-14	Australian Taxation Office	Bitcoin transactions are seen as a kind of barter arrangement.
	Regulation	Sep-14	Reserve Bank of Australia (Governor Glenn Steven)	Greater refinements to the details of existing regulatory structures is not feasible; People who seek returns and accept risks should be allowed to use Bitcoin
		Dec-14	Australian Securities and Investments Commission	As virtual currencies are not declared as a 'financial product', they do not fall under the regulation of the Corporations Act 2001 and the Australian Securities and Investments Commission Act 2001
		Dec-15	TRAction Fintech Pty Ltd (Directors Patricia Tsang and Sophie Gerber)	Virtual currencies are only sparsely affected by Australia's current AML/CTF regime. If they are exchanged for fiat currencies (or vice versa) or if a transaction intersects with banking or remittance services which are already regulated under the AML/CTF regime.
		May-16	The Australian Government	The Australian Government stated that the country has to bring domestic digital currency exchanges under existing AML and CTF rules.
	Taxation	Jun-13	Australian Taxation Office (Sen. Ass. Commissioner for the Cash Economy Michael Hardy)	Australian Taxation Office confirms that they monitor Bitcoin, is volatile, acceptance is interactions with conventional currencies through exchange mechanisms and international developments and the international development around the virtual currency. Consisting Tax rule for conventional transactions also apply for the use of modern payment systems. To this belong that items that are bought with Bitcoins are subject to goods and service tax (GST) or that recipients have to pay income tax if Bitcoins are part of their business or other income. Further speculators should keep records for capital gains taxes.

		Aug-14	Australian Taxation Office	Bitcoin transactions are seen as a kind of barter arrangement with corresponding tax consequences. Further the supply of Bitcoins is not a financial supply for GST purposes, but an asset for capital gain tax (CGT) purpose. If Bitcoins are used to for private transactions any capital gain or loss from disposal of the bitcoin will be disregarded if the cost of the bitcoin is at most $10,000. If Bitcoins are received for goods or services to commercial reason, the value is recorded as ordinary income. Simultaneous, the business may be charged GST on that bitcoin. Potentially even consequences from capital gains tax might emerge. Any income that derives from bitcoin mining is included in the assessable income. However, the expenses occurred in connection with the mining activity can be used as a deduction, losses are subject to the non-commercial loss provision.
		Mar-15	The Australian Department of Treasury	List of cryptocurrencies as bitcoin, focusing on determining how to appropriately tax companies and providing companies with the ability to relocate profits to minimize their tax payment
		May-16	The Australian Government	Due to the classification as barter money, digital currency are treated under GST law leading to a double taxation of consumers when using digital currency to buy things that are already subject to GST.The Australian government announced that it will back a legislative solution to this tax concerns.
	Warnings	Dec-13	Reserve Bank of Australia (Governor Glenn Steven)	Bank of Australia governor Glenn Stevens suggests that Australia sees potential risk and volatility with bitcoin, but no need to intent to regulate it.
	Intended Actions	May-16	Australian Government/Australian Transaction Reports and Analysis center	Extension of the Anti-Money Laundering and Counter-Terrorism Financing Act of 2006 to Bitcoin and cryptocurrency. Further GST taxation regulation should be changed to avoid doubled spending.
Canada	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Jan-14	Office of the Superintendent of Financial Institutions	Virtual Currencies are not “legal tender”.
		Jun-14	Governor General of Canada	Virtual Currencies are seen as "money service businesses" for the purposes of the anti-money laundering law.
	Regulation	May-13	Financial Transactions and Reports Analysis Centre	Bitcoin exchanges are exempt from Canadian money laundering laws.
		Jan-14	Canadian Government	Canadian regulators as the Central Bank as well as the government will continue to monitor developments involving virtual currencies.
		Feb-14	James Micheal Flaherty (Canadian Finance Minister)	Canadian government plans to introduce anti-money laundering and anti-terrorist financing regulations for virtual currencies such as Bitcoin.
		Mar-14	Canadian Parliament	The money laundering and terrorist financing act now applies to persons in Canada that are engaged in dealing virtual currencies as well as persons outside of Canada that provide such services to customers in Canada.

		Jun-15	Canadian Standing Senate Committee on Banking, Trade and Commerce	The Committee duns the limited regulatory control over digital currencies
		Jun-16	Bank of Canada	Bank of Canada stated that they have been experimenting with a digital fiat currency called "CAD-COIN".
	Taxation	Apr-13	Canada Revenue Agency	Bitcoin is not exempt from taxes. Accordingly, barter transaction rules apply to use of Bitcoin for goods or services and are subject to tax, and if bitcoins are bought or sold as a commodity they are subject to capital gains taxes.
China	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Dec-13	People's Bank of China	Bitcoin does not have the same legal status as a currency or monetary equivalent, and should not be used as a currency and circulate in the market. More likely, Bitcoin is a special kind of virtual good.
	Regulation	Dec-13	People's Bank of China	Individuals were free to use (buying and selling) bitcoin. Nevertheless, financial and payment institutions cannot be involved in bitcoin-related transactions, as they are banned from virtual currencies. Further websites or exchanges that deal with bitcoin need to register with appropriate regulatory agencies (e.g. exchanges with the Ministry of Industry and Information Technology and websites with the Telecommunications Bureau).
		Dec-13	People's Bank of China	The People's Bank of China extends the ban on accepting, using, or selling bitcoin as stated on the 5th December 2013 to third party payment providers. However, Bitcoin remains legal.
		Apr-14	People's Bank of China	Commercial banks and payment companies are directed to close bitcoin trading accounts within two weeks.
	Taxation	Sep-08	State Administration of Taxation (Beijing Local Taxation Bureau)	Answer regarding the phenomenon of “gold farmers”: Income obtained by individuals through selling the virtual currency are taxable incomes for individual income tax (as income from transfer of property).
	Warnings	Dec-13	People's Bank of China	Warning to Chinese financial institutions that Bitcoin has no "real meaning" and lacks legal protections, especially no central authority. Money laundering and other illegal uses are identified as potential problems relating to Bitcoin.
		Apr-14	People's Bank of China	The People's Bank of China urges Chinese banks to cut off all bitcoin-related business.
	Intended Actions	Jan-16	People's Bank of China	PBOC wants to launch its own virtual currency in the future.
France	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Dec-13	Bank of France	Under current French laws, Bitcoin cannot be considered a real currency or means of payment.

		Jul-14	French Ministry of Economy and Finance	Bitcoins are classified as property.
	Regulation	Dec-12	Bank of France	The Bitcoin exchange “Bitcoin Central“ got secured approval from regulators to operate as a bank respectively a payment services provider under French law.
		Apr-14	French Banking Federation	Indication that wiring revenue from the sale of virtual currencies to a personal bank account may desires the affected bank to file a declaration with the French anti-money-laundering agency.
		Jun-14	Senate Committee on Finance	Testimony regarding the development of currencies, with the conclusion, that virtual currencies can no longer be disregarded by public authorities and that despite from existing risks, there are multiple opportunities for the future wherefore public authorities should work on a balanced regulatory framework.
		Jul-14	French Ministry of Economy and Finance	Ministry plans to implement customer identity verification rules for bitcoin distributors and other platforms.
	Taxation	Apr-14	French Ministry of Economy and Finance	Revenue from sales of virtual currency is taxable income.
		Jul-14	French Ministry of Economy and Finance	After the classification of Bitcoin as property it s subject to capital gains and asset taxes.
	Warnings	Dec-13	Bank of France	Warnings regarding price volatility, difficulties to convert Bitcoins to real money, the misuse for money-laundering and financing of terrorism, legal and security risks as well as the absence of central regulatory authority.
Germany	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Dec-11	German financial supervisory authority	As Bitcoin not tied to legal tender currency it is exempt from the definition of e-money. However, it is seen as a commodity.
		Dec-14	German Finance Ministry	Virtual currency is not e-money or foreign currency but a financial instrument under German banking rules. VC is more akin to “private money” that can be used in “multilateral clearing circles” (according to the first sentence of section 1(11) of the German Banking Act).
		May-14	German Ministry of Finance	The commercial sale of bitcoin is a “miscellaneous service“.
	Regulation	Oct- 14	Government of Germany and Austria	The German Federal Ministry of Education and Research and the Austrian Federal Ministry for Transport, Innovation and Technology found a project called “Bitcrime“ that investigates approaches for Tackling Bitcoin-based Crime.
		Dec-14	German financial supervisory authority	The way bitcoins are currently given as payment, accepted as payment, or “mined” do not require bank supervisory licensing. However the report indicates that commercial use of BTC may require licensure and permission under various circumstances.
	Taxation	Dec-11	German financial supervisory authority	As a commodity Bitcoin is subject to taxation.

		Dec-11	German Finance Ministry	The use of VC in “multilateral clearing circles” suggest that it would be taxed as capital.
		Sep-13	German Government	The trading of Bitcoin is exempt from sales tax.
	Warnings	Dec-13	German financial supervisory authority	Overview of risks related to virtual currency.
		May-14	German Ministry of Finance	Retailers that accept bitcoin are taxed on the sale of goods (VAT) and upon selling any bitcoins they accept in purchases.
The Netherlands	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Jan-12	Supreme Court of the Netherlands	For the court, Bitcoins are seen as objects. Therefor public prosecution department can seize virtual currency from criminals legally.
		Dec-13	Jeroen Dijsselbloem (Dutch Minister of Finance)	Jeroen Dijsselbloem, the Dutch Minister of Finance, stated that Bitcoin does not qualify as electronic money within the meaning of the Dutch Financial Supervision Act (FSA), as it does not meet the existing legal requirements.
	Regulation	Jun-13	Dutch Minister of Finance	Bitcoin is not a financial product for the purposes of the Act on Financial Supervision.
		May-14	Dutch District Court (Overijssel)	Bitcoin is a medium of exchange and an acceptable form of payment in the Netherlands. However, it cannot be defined as legal tender, common money, or electronic money.
	Taxation	Jun-13	Dutch Minister of Finance	In the Netherlands transactions with Bitcoin and other virtual currencies are taxable as the law stands regarding the income tax. Further this applies for the sales tax. Therefor the value of the virtual currencies has to be converted into Euros.
		Dec-13	The Dutch Central Bank	Warning to consumers regarding the volatile exchange rates and the lack of central issuing institution.
		May-14	The Dutch Central Bank	Warning to consumers regarding amongst others the lack of compensation policies, deposit guarantee system and central party,
		Jun-14	The Dutch Central Bank	Banks and payment institutions should be aware of integrity risks derived from the processing of transactions with VC. Thereby VC are classified as financial products “with a very high risk profile”.
		Sep-14	Dutch Prosecuters	Priorization for deterrent action in the field of cryptocurrencies.
		Nov-14	Jakob Kamminga (Official from the Dutch Ministry of Finance)	Indication that the ministry of finance is considering the exemptation of bitcoin transactions from VAT.

	Intended Actions	Mar-16	The Dutch Central Bank	Dutch Central Bank has committed to experimentally create a prototype blockchain-based Currency.
Russia	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Aug-13	Russian law firm Tolkachev and Partners	According to article 140 of the Russian Civil Code the use of bitcoins could be restricted as the Russian ruble is the exclusive means of payment in Russia and all prices for financial transactions conducted in Russia have to be defined in rubles.
		Feb-14	Central Bank of Russia	Virtual Currencies are a money surrogate, not an official currency.
	Regulation	Jan-14	State Duma	The Security Committee in the lower house of parliament approved a counterterrorism bill which includes restrictions on anonymous transactions and thus also includes virtual currencies.
		Jan-14	Alexei Ulyukayev (Russian Economy Minister)	"We know regulators in some countries such as China and Japan are implementing restrictions. We'll monitor that carefully".
		Feb-14	Central Bank of Russia	According to Article 27 of the Federal Law "On the Central Bank of the Russian Federation", a release of Virtual currencies on the territory of the Russian Federation is prohibited, as they are money surrogates and not the official currency.
		Aug-14	The Finance Ministry	The prepared bill should prohibit the use of money substitutes including virtual currencies.
		Sep-14	Aleksey Moiseev (Deputy Finance Minister)	Announcement of a law that bans transactions in virtual currencies. Furthe the law includes penalties against miners of virtual currencies and bans access to exchanges as well as online stores accepting bitcoins.
		Oct-14	Ministry of Finance	Conducting transactions in Bitcoin is seen as misdemeanor. Fines for dealing with cyber-currencies and monetary surrogates are imposed.
		Dec-14	Aleksey Moiseev (Deputy Finance Minister)	Adaption of fines for individuals who disseminate money substitutes.
		Dec-15	State Duma	The submitted draft bill proposes a ban of virtual currencies as it prohibits not only the "malevolent issuance of money surrogates," which aims at miners as well as exchangers, but also the "assistance in money surrogates circulation," which includes virtual currency wallets, and ultimately the "circulation of money surrogates" which implies those who purchase goods and services using virtual currency. Furthermore, the advertisement of VC is prohibited as the "distribution of information sufficient and necessary for issuance of money surrogates in media and information and communications networks" is prohibited, too.
		Feb-16	Internet Advisor German Klimenko	Accepting Bitcoin Payments constitutes a crime in Russia

		Mar-16	The Russian Finance Ministry	Proposal of 7-Year Prison Sentences for Digital Currency Issuers
		Sep-16	Aleksey Moiseev (Deputy Finance Minister)	Moiseev announced that the ministry of finance will not be pushing for a direct blanket ban on Bitcoin in russia.
	Warning	Jan-14	Herman Gref (Former Russian Economy Minister)	A ban of virtual currencies in Russia would be a “colossal step backward” for what reason Gref sent letters to the Kremlin, the central bank, as well as the Finance Ministry.
		Feb-14	Central Bank of Russia	Transactions made with Bitcoin are seen as “potentially suspicious” and “dubious activity” associated with money laundering and terrorism financing. Individuals are recommended to refrain from transactions involving bitcoins.
		Nov-14	Alexey Moiseev (Deputy Finance Minister)	Maintaining the Ministry’s stance on bitcoin and further criminalize it is a danger to the banking system.
	Intended Actions	Aug-16	Ministry of Finance and the Central Bank of Russia	Representatives from amongst others the Ministry of Finance as well as the Central Bank of Russia are planning to submit a report to Russian President Putin containing the recommendation to Abandon Penalties for Bitcoin Use.
Sweden	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Oct-13	Swedish Tax Board	Bitcoin is treated as a currency.
		Jan-14	Swedish Tax Agency (Olof Wallin, Official)	Bitcoin and its competitors are rejected as a currency. Classification as "another asset", just as art, antiques, jewelry, stamps or copyrights and thus as an investment asset.
	Taxation	Aug-13	Swedish Tax Board	The trade in bitcoins is not subject to Swedish VAT. However, it is subject to the Financial Supervisory Authority regulations and treated as a currency.
		Jan-14	Swedish Tax Agency (Olof Wallin, Official)	The declaration of Bitcoin as "another asset" allows sweden to charge capital gains taxes on any transactions using it.
		Oct-14	Swedish Enforcement Authority	Swedish Enforcement Authority "will start to investigate and seize Bitcoin holdings when collecting funds from indebted individuals".
		Jun-14	Swedish high court/ Swedish Tax Authority	Sweden asked the European Court of Justice if the exchange of cryptocurrency for fiat currency is an transactions that should be subject to VAT, or whether exchange service should be exempt from VAT.
		Apr-15	Sweden’s Tax Authority	Publishing of guidelines on the Taxation of Mining of Bitcoins and Other Virtual Currencies, whereby income generated from bitcoin mining activities is declared as income from employment (which includes in sweden income from hobby activities, income from economic activity and income from capital).
	Warning	Jan-14	Sweden's Financial Markets Minister Peter Norman	“If we end up with artificial or virtual currencies, there is a risk that they could slip through the cracks and that would be serious. I don’t think Bitcoins are at that stage today, but if they were to grow into a big virtual currency that’s being used a lot, that would result in risks that we don’t want”.

		Jun-14	The Swedish Central Bank	“There are clear disadvantages with virtual currencies. Issuing these currencies is not subject to regulation and the issuers are not under national supervision. this means that consumer protection is weak in certain aspects and that the users may be exposed to risks.”
		Sep-14	The Swedish Central Bank	The article in the economic review journal of the Swedish Central Bank gives an overview of VC as Bitcoin, its benefits as well as risks.
Switzerland	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Dec-13	Swiss Parliament	The Swiss Parliament asks for bitcoin to be treated as any other foreign currency in a postulate.
		Jun-14	Swiss Federal Council	Bitcoin is not legal tender and does not completely fullfils the three main functions of money. This “seriously undermines it as a medium of exchange”.
	Regulation	Jun-14	Swiss Financial Market Supervisory Authority	The Bitcoin ATM operator SBEX gets permission to launch a network of machines as it is accepted as a member of the Association Romande des Intermédiaires Financiers, which is regulated by the Swiss Financial Market Supervisory Authority.
		Jun-14	Swiss Financial Market Supervisory Authority	The report straightens out that the commercial purchase and sale and the operation of Bitcoin trading platforms are subject to the Swiss AML act. Further, provider who accept bitcoins and administer bitcoin holdings for clients require a banking license.
		Jun-14	Swiss Federal Council	The report examines the economic significance, legal treatment and risks of virtual currencies. Referring to this the Swiss Federal Council sees no need for particulate regulation for VC. Transactions where goods and services are purchased with bitcoins as a means of payments as well as the sale of VC in exchange for fiat money fall under the Swiss Code of Obligations. This shall not apply for professional trade that generally come under the scope of the Anti-Money Laundering Act.
		Jul-16	City of Zug	The City of Zug becomes the first administration in the world that accepts bitcoin as means of payment in a pilot project.
	Taxation	May-15	Swiss Federal Tax Administration	Confirmation that bitcoin is exempt from Value Added Tax (VAT) in switzerland.
	Warning	Jun-14	Swiss Federal Council	"Bitcoin seems to be a rather high-risk object of speculation". "Bitcoin is used as a currency for acquiring illegal products or as ransom in cases of extortion. Moreover, bitcoins can be abused for money laundering purposes or stolen with relatively little risk."

	Category	Date	Authority	Key findings
The United Kingdom	Classification	Nov-13	Her Majesty Revenue and Customs (HMRC)	Classification as single purpose voucher.
		Jan-14	Her Majesty Revenue and Customs (HMRC)	Consideration to classify virtual currencies as a “private currency" instead of a tradable voucher.
	Regulation	Jun-13	Her Majesty Revenue and Customs (HMRC)	Bitcoin exchanges that are operating in the United Kingdom do not have to register with HMRC under money laundering regulations.
		Jan-14	Her Majesty Revenue and Customs (HMRC)	The consideration to categorize virtual currencies as a “private currency" would eliminate profits taxes and leaves a reduced Sales Tax liability.
		Dec-14	Steve Baker (UK Treasury Select Committee MP)	"Bitcoin should be regulated by the ordinary commercial business laws with no additional regulation." The treasury committee is responsible for amongst others the Bank of England, the tax authority as well as the financial regulator.
		Mar-15	Her Majesty Treasury	UK Government announces to regulate bitcoin exchanges under the anti-money laundering regulations.
	Taxation	Jun-13	Her Majesty Revenue and Customs (HMRC)	Digital currencies are covered by the UK tax system. Namely, if they are used to pay someone (a trader) for goods and services, the profits are taxable. Further, the traders have to convert the profits into sterling before they can enter them into their UK tax returns.
		Nov-13	Her Majesty Revenue and Customs (HMRC)	Classification as single purpose voucher comes with a 10-20% VAT.
	Warnings	Sep-14	Bank of England	Digital Currencies do not pose a risk to monetary or financial stability at the present moment.
The United States	**Category**	**Date**	**Authority**	**Key findings**
	Classification	Mar-13	Financial Crime Enforcement Network	“virtual” currency is a medium of exchange that operates like a currency in some environments.
		Aug-13	Texan Court	The judicial authority in Texas classified Bitcoin as “currency” or “form of money”.
		Mar-14	The Internal Revenue Service	Bitcoin Is Property, Not Currency which makes businesses and consumers subject to the same reporting requirements as any other payment made in property.
		Sep-15	United States Commodities Futures Trading Commission	For the first time Bitcoin is stated as a “commodity”. This is in contrast to FinCEN guidance which says that Bitcoin is no currency.
		Sep-16	Dorothy Hukill (Florida State Senator)	Suggestion that Bitcoin is stated as “money”.

	Regulation	Mar-13	Financial Crime Enforcement Network	FinCEN considers virtual currencies within the definition of money services businesses (MSBs). Therefor MSBs “have registration requirements and a range of anti-money laundering, recordkeeping, and reporting responsibilities under FinCEN’s regulations“. Further the guidance clarifice the notions of actors in a virtual currencies environment.
		May-13	United States Government Accountability Office	No additional rules specific to virtual currencies exist. However, “transactions within virtual economies or using virtual currencies could produce taxable income”. Regardless of the source the income is derived, taxpayers have to report and pay taxes on every income. Further VC pose Various Tax Compliance Risks like tax evasion.
		Apr-14	Janet Yellen (Federal Reserve Chair)	“The Fed doesn't have authority to supervise or regulate bitcoin in any way.”
		Jul-14	New York Department of Financial Services	As the first state in the US New York published rules and regulations that will be required for bitcoin businesses. Therefore, businesses that receive, transmit, store or convert virtual currency for customers; buy or sell virtual currency for customers, administer or issue a virtual currency; or perform exchange of virtual currency to other currencies have to be licensed to operate in New York. Merchants that accept bitcoin are excluded from this the rules and regulations.
		Oct-14	Benjamin Lawsky (Superintendent of the New York Department of Financial Services)	In contrast to financial intermediaries, developers, miners, and individuals using bitcoin do not fall under New Yorks BitLicense regulations.
		Aug-15	Financial Crime Enforcement Network	Exchangers and administrators of virtual currencies are stated that they are money transmitters under the Bank Secrecy Act. Therefore, they have to implement a anti-money laundering program to mitigate money laundering risk and further comply with the recordkeeping, reporting, and transaction monitoring requirements under FinCEN regulations. In addition to that, each money transmitter register with FinCEN within 180 days of starting to engage in convertible virtual currency transactions as an exchanger.
		Sep-15	US Conference of State Bank Supervisors	Model regulatory framework for digital currencies as a recommendation for state bank regulators.
	Taxation	Mar-13	The Internal Revenue Service	Notice regarding existing general tax principles that apply to transactions with virtual currency. Therefore, VC is a capital asset in the hands of the taxpayer and thus subject to capital gains taxes, whereby any disposition of these digital currencies (including trading and spending) is a tax event. Additionally mining is treated as immediate income.
	Warnings	Jul-13	U.S. Securities and Exchange Commission	We are concerned that the rising use of virtual currencies in the global marketplace may entice fraudsters to lure investors into Ponzi and other schemes in which these currencies are used to facilitate fraudulent, or simply fabricated, investments or transactions.

		May-14	U.S. Securities and Exchange Commission	Fraudulent use of Bitcoin with Ponzi Scheme
		Jun-16	Financial Stability Oversight Council	Warning that bitcoin and blockchain are threats to financial stability.
		May-14	Federal Reserve Board	Bitcoin is a potential threat "to the banking system, economic activity, or financial stability”.

B: Literature Review Industrial Research

Autor	Year	Title	Keyword Google
Accenture Research	2016	Blockchain-Enabled Distributed Ledgers: Are Investment Banks Ready	Distributed Ledger
Accenture Research	2015	Blockchain in the Investment Bank	
Accenture Research	2015	Distributed consensus ledgers for payments	
BaFin	2016	Distributed Ledger: The technology behind virtual currencies: the example of blockchain	
Bank of England	2014	Innovations in payment technologies and the emergence of digital currencies	
Barclays	2015	Blockchain: understanding the potential	
Bitcoin (Satoshi Nakamoto)	2008	Bitcoin: A Peer-to-Peer Electronic Cash System	
BlinkLane Consulting	2015	Creating Value from Distributed Ledgers Exploring the potential of the technology behind Bitcoin	
BIS	2015	Digital Currencies	
Deloitte	2015	State-Sponsored Cryptocurrency: Adapting the best of Bitcoin’s Innovation to the Payments Ecosystem	
Deutsche Börse Group	2015	Open Day 2015 - Blockchain technology	
DTCC	2016	Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape	
EBA	2015	Cryptotechnologies, a major IT innovation and catalyst for change	
EY	2016	Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)	
ESMA	2015	Investment using virtual currency or distributed ledger technology	
Ethereum	-	A Next-Generation Smart Contract and Decentralized Application Platform	
Evry	-	Blockchain: Powering the Internet of Value	
Firstwaters	2016	Distributed Ledger Technology in Finance - from Inception to Reality	
IBM	2015	Device Democracy	
Institute for International Finance	2015	Banking on the Blockchain: Reengineering the Financial Architecture	
International Monetary Fund	2016	Virtual Currencies and Beyond: Initial Considerations	
Locke Lord	2015	Blockchain and Financial Services Industry Snapshot and Possible Future Developments	
Needham & Company	2015	Th/e Blockchain Report: Welcome to the Internet of Value	

Autor	Year	Title	Keyword Google
NXT	2014	Nxt Whitepaper	Distributed Ledger
R3	2015	Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems	
Ripple (Schwartz et al.)	2014	The Ripple Protocol Consensus Algorithm	
Santander	2015	The Fintech 2.0 Paper: Rebooting Financial Services	
Sogeti	2015	Blockchain: cryptoplatform for a frictionless economy	
UK Government Chief Scientic Adviser	2016	Distributed Ledger Technology: beyond block chain	Blockchain Technology
McKinsey	2015	Beyond the Hype: Blockchains in Capital Markets	
Deloitte	2016	Blockchain - Enigma. Paradox. Opportunity.	
UBS	2016	Extreme automation and connectivity: The global, regional, and investment implications of the Fourth Industrial Revolution	
Multichain	2015	MultiChain White Paper: Understanding private blockchains and the MultiChain solution	
Euroclear	2016	Blockchain In Capital Markets - The Prize And The Journey	
EY	2016	Blockchain technology as a platform for digitization	
World Economic Forum	2016	The future of financial infrastructure An ambitious look at how blockchain can reshape financial services	
Deloitte	2016	Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality	
Moody's Investors Service	2016	Credit Strategy – Blockchain Technology: Robust, Cost-effective Applications Key to Unlocking Blockchain's Potential Credit Benefits	
Sutardja Center	2015	Blockchain Technology - Beyond Bitcoin	
IMF	2016	Virtual Currencies and Beyond: Initial Considerations	
UNRISD	2016	How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?	

C: Indicators Value Framework Evaluation Bitcoin

Bitcoin-Related Research (Time period: January 2011 till October 2015)

Date of access: 27. October 2015

Year	Publications per year
2011	11
2012	59
2013	151
2014	335
Jan. - Oct. 2015	349
Total	905

Year	Number
ACM	
2011	4
2012	18
2013	27
2014	58
2015	65
IEEE	
2011	2
2012	17
2013	51
2014	73
2015	49
Springer	
2011	1
2012	12
2013	28
2014	98
2015	99
Web of Knowledge	
2011	0
2012	3
2013	16
2014	56
2015	33
Science Direct	
2011	4
2012	9
2013	29
2014	50
2015	103

Venture Capital (Time period: January 2011 till October 2015)

Date of access: 27.October 2015

Total fundings	873,08
2015 (till 30.10.)	410,94
2014	377,95
2013	83,57
2012	0,63

No. Of enterprises receiving fundings per year	
2012	2
2013	37
2014	85
2015	47

Sum of investments in US$ per year	
2012	0,63
2013	83,57
2014	323,60
2015	410,94

Close Date	**Company**	**Classification**	**Funding ($m)**	**Cumulative Funding ($m)**	**Country**	**Currency**
06.10.2015	Orb	Financial Services	2,30	2,30	Japan	Multiple
02.10.2015	Coinplug	Universal	5,00	8,30	South Korea	Bitcoin
29.09.2015	Safe Cash Payment Technologies	Financial Services	1,12	1,12	United States	Multiple
17.09.2015	Pey	Infrastructure	0,34	0,34	Germany	Bitcoin
10.09.2015	Coinalytics	Financial Services	1,10	1,20	United States	Cryptotechnology
10.09.2015	Abra	Financial Services	12,00	14,00	United States	Multiple
10.09.2015	Case	Wallet	1,00	2,50	United States	Bitcoin
09.09.2015	Chain	Infrastructure	30,00	43,70	United States	Cryptotechnology
08.09.2015	ShapeShift	Exchange	1,60	2,13	Switzerland	Multiple
02.09.2015	Paymium	Payment Processor	1,12	1,12	France	Bitcoin
18.08.2015	Filament	Infrastructure	5,00	5,00	United States	Cryptotechnology
15.08.2015	BTC Trip	Marketplace	0,15	0,18	United States	Bitcoin
12.08.2015	BitFlyer	Exchange	4,00	6,90	Japan	Bitcoin
23.07.2015	Challenger Deep	Infrastructure	1,86	1,86	United Kingdom	Bitcoin
21.07.2015	BitX	Universal	4,00	4,82	Singapore	Bitcoin
10.07.2015	Airbitz	Wallet	0,45	0,45	United States	Bitcoin
09.07.2015	BitFury	Mining	20,00	60,00	The Netherlands	Bitcoin
24.06.2015	Ascribe	Financial Services	2,00	2,00	Germany	Cryptotechnology
24.06.2015	Vogogo	Payment Processor	12,50	21,00	Canada	Bitcoin
18.06.2015	Case	Wallet	1,50	1,50	United States	Bitcoin
16.06.2015	Reveal	Financial Services	1,50	1,50	United States	Multiple
11.06.2015	OpenBazaar	Financial Services	1,00	1,00	Unknown	Bitcoin
09.06.2015	Symbiont	Financial Services	1,25	1,25	United States	Cryptotechnology
03.06.2015	Mirror	Financial Services	8,80	12,80	United States	Bitcoin
20.05.2015	Bitbond	Financial Services	0,67	0,94	Germany	Bitcoin
19.05.2015	Ripple Labs	Financial services	28,00	34,40	United States	Ripple
08.05.2015	Satoshi Citadel Industries Inc.	Universal	0,10	0,10	Philippines	Bitcoin
07.05.2015	itBit	Exchange	25,00	28,25	United States	Bitcoin

07.05.2015	Cryex	Exchange	10,00	10,00	Sweden	Multiple
30.04.2015	Hedgy	Financial services	1,20	1,20	United States	Bitcoin
30.04.2015	Circle Internet Financial	Universal	50,00	76,00	United States	Bitcoin
02.04.2015	Gem	Financial services	1,30	4,90	United States	Multiple
31.03.2015	PeerNova	Infrastructure	5,00	13,60	United States	Cryptotechnology
30.03.2015	Bitt	Exchange	1,50	1,50	Barbados	Multiple
23.03.2015	Safello	Exchange	0,12	0,97	Sweden	Bitcoin
19.03.2015	Coinigy	Exchange	0,10	0,10	United States	Multiple
18.03.2015	Bitbank	Wallet	0,65	1,75	Japan	Bitcoin
13.03.2015	PayStand	Payment Processor	0,09	2,76	United States	Bitcoin
10.03.2015	21 Inc (21e6)	Universal	116,00	121,05	United States	Bitcoin
10.03.2015	ShapeShift	Exchange	0,53	0,53	Switzerland	Multiple
19.02.2015	Ledger	Wallet	1,50	1,50	France	Bitcoin
12.02.2015	TabTrader	Financial Services	0,07	0,07	The Netherlands	Multiple
09.02.2015	BitPesa	Payment Processor	1,10	1,10	Kenya	Bitcoin
04.02.2015	HashRabbit	Infrastructure	0,50	0,70	United States	Bitcoin
03.02.2015	KnCMiner	Mining	15,00	29,00	Sweden	Bitcoin
03.02.2015	NeuCoin	Financial Services	2,25	2,25	France	Neucoin
03.02.2015	Ziftr	Universal	0,85	0,85	United States	Multiple
02.02.2015	Bonafide (Bonifide.io)	Financial Services	0,85	0,95	United States	Bitcoin
29.01.2915	Tembusu	Financial Services	0,89	1,13	Singapore	Bitcoin
28.01.2015	BitFlyer	Exchange	1,10	2,93	Japan	Bitcoin
27.01.2015	Colu	Infrastructure	2,50	2,50	Israel	Bitcoin
22.01.2015	Anycoin Direct	Exchange	0,56	0,56	The Netherlands	Multiple
20.01.2015	Coinbase	Universal	75,00	106,71	United States	Bitcoin
20.01.2015	Trustatom	Financial Services	0,10	0,10	Canada	Cryptotechnology
15.01.2015	Ciphrex	Wallet	0,50	0,50	United States	Bitcoin
14.01.2015	BlockCypher	Infrastructure	3,10	3,50	United States	Cryptotechnology
07.01.2015	LibertyX	Financial Services	0,40	0,40	United States	Bitcoin
05.01.2015	GetGems	Financial Services	0,40	1,00	Israel	Bitcoin
30.12.2014	Bitreserve	Wallet	9,60	9,60	United States	Bitcoin
24.12.2014	BTCjam	Marketplace	6,10	7,30	United States	Cryptotechnology
17.12.2014	PeerNova	Mining	8,60	8,60	United States	Cryptotechnology
10.12.2014	Quoine	Exchange	2,00	2,00	Japan	Bitcoin
02.12.2014	ChangeTip	Financial Services	3,50	4,25	United States	Bitcoin
02.12.2014	DigiByte	Financial Services	0,25	0,25	United States	DigiByte
01.12.2014	GetGems	Financial Services	0,60	0,60	Israel	Bitcoin
27.11.2014	Purse.io	Financial Services	0,30	0,30	United States	Bitcoin
17.11.2014	Blockstream	Infrastructure	21,00	21,00	Canada	Cryptotechnology
16.11.2014	OneName	Financial Services	1,50	1,62	United States	Bitcoin
05.11.2014	Dogetipbot	Financial Services	0,50	0,50	United States	Dogecoin
14.01.2015	BlockCypher	Infrastructure	0,40	0,40	United States	Cryptotechnology
24.10.2014	Spondoolies-Tech	Mining	5,00	10,50	Israel	Bitcoin
24.10.2014	BitLendingClub	Financial Services	0,25	0,25	United States	Cryptotechnology
20.10.2014	Bitnet	Payment Processor	14,50	17,00	United States	Bitcoin
17.10.2014	AlphaPoint	Exchange	1,35	1,35	United States	Multiple
16.10.2014	Coinsetter	Exchange	1,30	3,10	United States	Bitcoin
10.10.2014	BitFlyer	Exchange	0,24	1,84	Japan	Bitcoin
10.10.2014	LibraTax	Financial Services	0,50	0,50	United States	Multi
10.10.2014	Melotic	Exchange	1,18	1,18	China	Bitcoin

09.10.2014	BitFury	Mining	20,00	40,00	The Netherlands	Bitcoin
08.10.2014	Coinplug	Universal	2,50	3,30	South Korea	Bitcoin
09.10.2014	Devign Lab	Universal	0,20	0,20	South Korea	Bitcoin
07.10.2014	Blockchain	Wallet	30,50	30,50	United Kingdom	Bitcoin
07.10.2014	SolidX	Financial Services	3,00	3,00	United States	Bitcoin
06.10.2014	SNAPCARD	Payment Processor	1,50	1,56	United States	Multiple
01.10.2014	HashRabbit	Infrastructure	0,20	0,20	United States	Bitcoin
30.09.2014	Coinapult	Wallet	0,78	0,78	Panama	Bitcoin
25.09.2014	Coinify	Universal	0,34	0,34	Denmark	Bitcoin
18.09.2014	CoinPlus	Payment Processor	0,17	0,38	Luxembourg	Bitcoin
17.09.2014	Koinify	Financial Services	1,00	1,45	United States	Cryptotechnology
17.09.2014	Gem	Financial Services	2,00	3,60	United States	Multiple
04.09.2014	KnCMiner	Mining	14,00	14,00	Sweden	Bitcoin
25.08.2014	Korbit	Exchange	3,00	3,60	South Korea	Bitcoin
20.08.2014	Chain	Infrastructure	9,50	13,70	United States	Cryptotechnology
20.08.2014	Chain	Infrastructure	4,20	4,20	United States	Cryptotechnology
19.08.2014	BitX	Universal	0,82	0,82	Singapore	Bitcoin
18.08.2014	BlockTrail	Infrastructure	0,65	0.65	The Netherlands	Bitcoin
13.08.2014	Bitbond	Financial Services	0,27	0,27	Germany	Bitcoin
11.08.2014	Unocoin	Universal	0,25	0,25	India	Bitcoin
05.08.2014	Vogogo	Payment Processor	8,50	8,50	Canada	Bitcoin
01.08.2014	Bitbank	Wallet	1,10	1,10	Japan	Bitcoin
01.08.2014	Stellar	Financial Services	3,00	3,00	United States	Stellar
23.07.2014	Volabit	Exchange	0,75	0,75	Mexico	Bitcoin
22.07.2014	BitFlyer	Exchange	1,60	1,60	Japan	Bitcoin
20.07.2014	Swarm	Crowdfunding	1,00	1,00	United States	Cryptotechnology
16.07.2014	OneName	Financial Services	0,12	0,12	United States	Bitcoin
16.07.2014	Bitaccess	Financial Services	1,00	11,00	Canada	Bitcoin
16.07.2014	Elliptic	Wallet	2,00	2,00	United Kingdom	Bitcoin
16.07.2014	Sfox	Broker	0,12	0,12	United States	Bitcoin
16.07.2014	Shift Payments	Payment Processor	0,12	0,12	United States	Multiple
16.07.2014	TradeBlock	Financial Services	2,80	2,80	United States	Bitcoin
14.07.2014	PayStand	Payment Processor	0,10	2,58	United States	Bitcoin
10.07.2014	Safello	Exchange	0,25	0,85	Sweden	Bitcoin
08.07.2014	Xapo	Wallet	20,00	40,00	United States	Bitcoin
01.07.2014	37Coins	Wallet	0,50	0,53	United States	Bitcoin
01.07.2014	Expresscoin	Financial Services	0,15	0,15	United States	Multiple
28.06.2014	Bitstash	Wallet	0,50	0,50	United States	Bitcoin
26.06.2014	BlockScore	Financial Services	2,00	2,03	United States	Multiple
17.06.2014	BitPagos	Payment Processor	0,60	0,74	United States	Bitcoin
16.06.2014	BitGo	Infrastructure	12,00	14,00	United States	Bitcoin
12.06.2014	HashPlex	Mining	0,40	0,40	United States	Bitcoin
11.06.2014	PayStand	Payment Processor	0,30	2,48	United States	Bitcoin
06.06.2014	Coinfloor	Exchange	0,34	0,49	United Kingdom	Bitcoin
05.06.2014	BTCjam	Marketplace	1,20	1,20	United States	Cryptotechnology
01.06.2014	BlockScore	Financial Services	0,03	0,03	United States	Multiple
30.05.2014	BitFury	Mining	20,00	20,00	The Netherlands	Bitcoin
30.05.2014	Bitex.la	Exchange	2,00	4,00	Argentina	Multiple
15.05.2014	CoinPlus	Payment Processor	0,21	0,21	Luxembourg	Bitcoin
13.05.2014	BitPay	Payment Processor	30,00	32,51	United States	Bitcoin
07.05.2014	Mirror	Financial Services	4,00	4,00	United States	Bitcoin
07.05.2014	Vaurum	Financial Services	4,00	6.00	United States	Bitcoin

05.05.2014	ChangeTip	Financial Services	0,75	0,75	United States	Bitcoin
21.04.2014	Coinalytics	Financial Services	0,10	0,10	United States	Bitcoin
21.04.2014	Neuroware	Wallet	0,10	0,10	United States	Bitcoin
21.04.2014	Monetsu	Payment Processor	0,10	0,10	United States	Bitcoin
03.04.2014	Coinplug	Universal	0,40	0,80	South Korea	Bitcoin
02.04.2014	PayStand	Payment Processor	2,00	2,18	United States	Bitcoin
01.04.2014	BTC.sx	Financial Services	0,30	0,45	Singapore	Bitcoin
27.03.2014	Coinsetter	Exchange	0,78	1,79	United States	Bitcoin
26.03.2014	GoCoin	Payment Processor	1,50	2,05	Singapore	Bitcoin
26.03.2014	Circle Internet Financial	Universal	17,00	26,00	United States	Bitcoin
26.03.2014	Hive	Wallet	0,19	0,19	China	Bitcoin
25.03.2014	Payward, Inc. (Kraken)	Exchange	5,00	5,00	United States	Multiple
25.03.2014	Koinify	Financial Services	0,45	0,45	United States	Cryptotechnology
20.03.2014	CoinPass	Financial Services	0,50	0,50	Japan	Cryptotechnology
17.03.2014	Bex.io / Spawngrid	Financial Services	0,55	1,05	Canada	Bitcoin
16.03.2014	OKCoin	Exchange	10,00	11,00	China	Bitcoin
15.03.2014	37Coins	Wallet	0,03	0,03	United States	Bitcoin
13.03.2014	Xapo	Wallet	20,00	20.00	United States	Bitcoin
12.03.2014	Tembusu	Financial Services	0,24	0,24	Singapore	Bitcoin
07.03.2014	CoinSimple	Payment Processor	0,18	0,18	China	Bitcoin
25.02.2014	CoinZone	Payment Processor	1,40	1,40	United Kingdom	Bitcoin
18.02.2014	Coinsetter	Exchange	0,51	1,01	United States	Bitcoin
17.02.2014	Safello	Exchange	0,60	0,60	Sweden	Bitcoin
12.02.2014	LedgerX	Exchange	1,50	1,50	United States	Multi
11.02.2014	Gem	Financial Services	1,50	1,60	United States	Multiple
10.02.2014	Tealet	Marketplace	0,24	0,26	United States	Bitcoin
04.02.2014	BitSim	Wallet	0,50	0,50	China	Bitcoin
01.02.2014	Cryptopay	Payment Processor	0,08	0,08	United Kingdom	Bitcoin
01.02.2014	Spondoolies-Tech	Mining	1,50	5,50	Israel	Bitcoin
31.01.2014	Gliph	Financial Services	0,03	0,41	United States	Bitcoin
30.01.2014	Bitnet	Payment Processor	2,50	2,50	United States	Bitcoin
30.01.2014	Bonafide (Bonifide.io)	Financial Services	0,10	0,10	United States	Bitcoin
21.01.2014	Gem	Financial Services	0,10	0,10	United States	Multiple
21.01.2014	Bitaccess	Financial Services	10,00	10,00	Canada	Bitcoin
21.01.2014	Tangible Cryptography (BitSimple)	Exchange	0,60	0,60	United States	Bitcoin
20.01.2014	Korbit	Exchange	0,40	0,60	South Korea	Bitcoin
15.01.2014	Bitex.la	Exchange	2,00	2,00	Argentina	Multiple
31.12.2013	Coinfirma	Mining	0,50	0,50	United States	Bitcoin
27.12.2013	PayStand	Payment Processor	0,75	0,75	United States	Bitcoin
18.12.2013	Gliph	Financial Services	0,13	0,38	United States	Bitcoin
12.12.2013	Coinbase	Universal	25,00	31,71	United States	Bitcoin
01.12.2013	CoinJar Pty	Wallet	0,50	0.52	Australia	Bitcoin
01.12.2013	SNAPCARD	Payment processor	0,06	0,06	United States	Multiple
01.12.2013	Bex.io / Spawngrid	Financial Services	0,50	0,50	Canada	Bitcoin
25.11.2013	Coinplug	Universal	0,40	0,40	South Korea	Bitcoin

18.11.2013	BTC China (Shanghai Satuxi Network)	Exchange	5,00	5,00	China	Bitcoin
17.11.2013	21 Inc (21e6)	Universal	5,05	5,05	United States	Bitcoin
12.11.2013	Ripple Labs	Financial Services	3,50	6,40	United States	Ripple
11.11.2013	itBit	Exchange	3,25	3,25	United States	Bitcoin
08.11.2013	BitPagos	Payment Processor	0,11	0,14	United States	Bitcoin
07.11.2013	GoCoin	Payment Processor	0,55	0,55	Singapore	Bitcoin
31.10.2013	Bitstamp	Exchange	10,00	10,00	United Kingdom	Bitcoin
31.10.2013	Circle Internet Financial	Universal	9.00	9,00	United States	Bitcoin
09.10.2013	GogoCoin	Financial Services	0,11	0,11	United States	Bitcoin
25.09.2013	Bitbox	Universal	0,07	0,07	United States	Bitcoin
19.09.2013	Gliph	Financial Services	0,20	0,25	United States	Bitcoin
18.09.2013	Buttercoin	Exchange	0,25	1,25	United States	Bitcoin
08.09.2013	Coinfloor	Exchange	0,16	0,16	United Kingdom	Bitcoin
04.09.2013	OKCoin	Exchange	1,00	1,00	China	Bitcoin
01.09.2013	BTC Trip	Marketplace	0,03	0,03	United States	Bitcoin
01.09.2013	LatinCoin	Exchange	0,03	0,03	Argentina	Bitcoin
01.09.2013	BitPagos	Payment Processor	0,03	0,03	United States	Bitcoin
01.09.2013	Armory Technologies	Wallet	0,60	0,60	United States	Bitcoin
19.08.2013	Buttercoin	Exchange	1,00	1,00	United States	Bitcoin
19.08.2013	Digital Currencies FinTech	Financial Services	1,25	1,25	United States	Bitcoin
15.08.2013	SpectroCoin	Financial Services	0,11	0,11	Lithuania	Bitcoin
01.08.2013	Korbit	Exchange	0,20	0,20	South Korea	Bitcoin
01.08.2013	Spondoolies-Tech	Mining	4,00	4,00	Israel	Bitcoin
23.07.2013	Avalon Clones	Mining	3,00	3,00	United States	Bitcoin
18.05.2013	Bitinstant	Payment Processor	1,50	1,50	United States	Bitcoin
18.05.2013	Gliph	Financial Services	0,02	0,05	United States	Bitcoin
16.05.2013	BitPay	Payment Processor	2,00	2,51	United States	Bitcoin
14.05.2013	Ripple Labs	Financial Services	1,40	2,90	United States	Ripple
01.05.2013	CoinJar Pty	Wallet	0,02	0,02	Australia	Bitcoin
26.04.2013	Coinbase	Universal	6,11	6,71	United States	Bitcoin
11.04.2013	Ripple Labs	Financial Services	1,50	1,50	United States	Ripple
09.04.2013	Coinsetter	Exchange	0,50	0,50	United States	Bitcoin
12.03.2013	Tealet	Marketplace	0,02	0,02	United States	Bitcoin
01.03.2013	BTC.sx	Financial Services	0,15	0,15	Singapore	Bitcoin
01.03.2013	Coinkite	Wallet	0,12	0,12	Canada	Multiple
01.03.2013	TradeHill	Exchange	0,40	0,40	United States	Multiple
01.03.2013	BitGo	Infrastructure	2,00	2,00	United States	Bitcoin
07.01.2013	BitPay	Payment Processor	0,51	0,51	United States	Bitcoin
01.09.2012	Coinbase	Universal	0,60	0,60	United States	Bitcoin
01.03.2012	Gliph	Financial Services	0,03	0,03	United States	Bitcoin

Demand and Supply (Time period: January 2011 till Ocotber 2015)

Date of access: 27. October 2015

Source: www.blockchain.info

Date	Number of unique Bitcoin addresses	Number of destroyed Bitcoin days	Number of transactions (Top-100 adresses excluded)	Date2	Number of unique Bitcoin addresses2	Number of destroyed Bitcoin days2	Number of transactions (Top-100 adresses excluded)2	Date3	Number of unique Bitcoin addresses3	Number of destroyed Bitcoin days3	Number of transactions (Top-100 adresses excluded)3
01.01.2011	775,00	545395	594,00	10.08.2012	29288,00	2127704	13747,00	20.03.2014	141026,00	8077114	65858,00
02.01.2011	779,00	382668	593,00	11.08.2012	27985,00	1854574	14506,00	21.03.2014	155285,00	5503403	64789,00
03.01.2011	956,00	1218375	853,00	12.08.2012	30165,00	1476377	13552,00	22.03.2014	137388,00	15266748	59005,00
04.01.2011	943,00	576014	1242,00	13.08.2012	41509,00	2428462	17446,00	23.03.2014	131768,00	1346701	49799,00
05.01.2011	1064,00	155624	1192,00	14.08.2012	34362,00	3160076	15631,00	24.03.2014	155589,00	2833682	57982,00
06.01.2011	950,00	741235	850,00	15.08.2012	36444,00	3490176	14665,00	25.03.2014	145432,00	5567422	62131,00
07.01.2011	887,00	352517	880,00	16.08.2012	47362,00	4338173	24045,00	26.03.2014	146464,00	1927480	61430,00
08.01.2011	1267,00	968855	1392,00	17.08.2012	45775,00	11627721	24396,00	27.03.2014	158999,00	6333260	63326,00
09.01.2011	1110,00	482275	1193,00	18.08.2012	41427,00	13615115	21679,00	28.03.2014	163425,00	5554495	62230,00
10.01.2011	1209,00	1523883	1358,00	19.08.2012	32820,00	14724429	15126,00	29.03.2014	126941,00	3500882	48911,00
11.01.2011	1185,00	1882630	1262,00	20.08.2012	34086,00	11742290	16526,00	30.03.2014	150155,00	4284850	48087,00
12.01.2011	1084,00	7990981	1233,00	21.08.2012	40498,00	3228810	20195,00	31.03.2014	137342,00	3155846	55077,00
13.01.2011	1150,00	754963	1271,00	22.08.2012	39189,00	5272495	18217,00	01.04.2014	157020,00	2903188	58640,00
14.01.2011	1134,00	1699704	1285,00	23.08.2012	34809,00	2682449	18003,00	02.04.2014	152718,00	2367084	60114,00
15.01.2011	1094,00	1556845	932,00	24.08.2012	34511,00	3097632	16869,00	03.04.2014	137224,00	14030081	61093,00
16.01.2011	1250,00	512425	1027,00	25.08.2012	33067,00	1708532	16349,00	04.04.2014	144468,00	1652514	57563,00
17.01.2011	1080,00	1973965	816,00	26.08.2012	28168,00	1689500	13231,00	05.04.2014	135497,00	11164185	52538,00
18.01.2011	1200,00	573352	870,00	27.08.2012	30516,00	14821671	13916,00	06.04.2014	163904,00	2584550	41548,00
19.01.2011	1281,00	2676277	967,00	28.08.2012	32138,00	6030621	13018,00	07.04.2014	134360,00	7262542	51594,00
20.01.2011	1125,00	1930344	847,00	29.08.2012	32378,00	2515391	14755,00	08.04.2014	148772,00	1778659	59906,00
21.01.2011	1354,00	556606	1047,00	30.08.2012	26377,00	1280245	11990,00	09.04.2014	144875,00	2938453	55882,00
22.01.2011	1742,00	591597	1431,00	31.08.2012	37505,00	21148402	17651,00	10.04.2014	165795,00	13481561	60009,00
23.01.2011	1397,00	1604043	1073,00	01.09.2012	39715,00	1628783	17919,00	11.04.2014	146801,00	6536699	59225,00
24.01.2011	1682,00	1871248	1334,00	02.09.2012	28708,00	1219950	12876,00	12.04.2014	124543,00	1296218	46197,00
25.01.2011	1282,00	901405	965,00	03.09.2012	29237,00	2279484	11042,00	13.04.2014	150009,00	1577317	41146,00
26.01.2011	1192,00	2046511	985,00	04.09.2012	31358,00	2670006	13895,00	14.04.2014	146634,00	2859160	55962,00
27.01.2011	1184,00	30722527	900,00	05.09.2012	33850,00	1393632	18105,00	15.04.2014	166401,00	3236911	65835,00
28.01.2011	1329,00	962084	1036,00	06.09.2012	38202,00	3057905	18987,00	16.04.2014	142870,00	18065220	63308,00
29.01.2011	1642,00	1257856	1290,00	07.09.2012	31911,00	2139353	14184,00	17.04.2014	141012,00	3545679	60301,00
30.01.2011	2494,00	2835376	2203,00	08.09.2012	30088,00	1204829	14589,00	18.04.2014	123771,00	5144347	50198,00
31.01.2011	2162,00	575318	1815,00	09.09.2012	33631,00	3990338	16682,00	19.04.2014	127435,00	0	50045,00
01.02.2011	1311,00	2370735	985,00	10.09.2012	28826,00	21390336	13071,00	20.04.2014	149260,00	287469	43670,00
02.02.2011	1283,00	2714200	1004,00	11.09.2012	36043,00	1354218	17028,00	21.04.2014	124225,00	1708052	53398,00
03.02.2011	975,00	669159	777,00	12.09.2012	29944,00	1581070	14146,00	22.04.2014	150856,00	3210814	67222,00
04.02.2011	1134,00	817293	918,00	13.09.2012	27663,00	2750128	11905,00	23.04.2014	134126,00	5769459	67166,00
05.02.2011	1094,00	779722	887,00	14.09.2012	30426,00	1350770	13751,00	24.04.2014	129810,00	3496658	62271,00
06.02.2011	1060,00	1696657	857,00	15.09.2012	26871,00	3719666	12227,00	25.04.2014	157853,00	2158048	71984,00
07.02.2011	1094,00	4038080	911,00	16.09.2012	24913,00	1412322	12149,00	26.04.2014	131955,00	1756096	53383,00
08.02.2011	1053,00	1359070	842,00	17.09.2012	26956,00	8668494	10967,00	27.04.2014	147987,00	1651652	45405,00
09.02.2011	1387,00	388789	1033,00	18.09.2012	31239,00	6777806	15454,00	28.04.2014	133142,00	1788238	56288,00
10.02.2011	2797,00	1976742	1866,00	19.09.2012	32351,00	6048941	14795,00	29.04.2014	145888,00	4104753	58686,00
11.02.2011	3757,00	3020519	2433,00	20.09.2012	41220,00	6295199	19585,00	30.04.2014	137816,00	2424249	57558,00
12.02.2011	2918,00	702300	1903,00	21.09.2012	29455,00	5975936	11290,00	01.05.2014	134499,00	2092532	56146,00
13.02.2011	2608,00	406609	1841,00	22.09.2012	22976,00	4796622	9799,00	02.05.2014	128157,00	1853121	53800,00
14.02.2011	2838,00	747255	1978,00	23.09.2012	22048,00	2650154	9671,00	03.05.2014	103028,00	1238226	48488,00
15.02.2011	3046,00	7793427	2267,00	24.09.2012	26499,00	6508692	10979,00	04.05.2014	138218,00	1313176	45157,00
16.02.2011	2466,00	439593	2062,00	25.09.2012	31768,00	3522175	14273,00	05.05.2014	113712,00	3002374	55470,00
17.02.2011	3096,00	203931	2255,00	26.09.2012	37569,00	4132527	17172,00	06.05.2014	144937,00	1943272	67980,00
18.02.2011	3034,00	661917	2086,00	27.09.2012	32067,00	3474441	14752,00	07.05.2014	137586,00	2770349	64083,00
19.02.2011	2542,00	825856	1773,00	28.09.2012	35047,00	2929865	15794,00	08.05.2014	140822,00	2493114	61626,00
20.02.2011	2492,00	551738	1698,00	29.09.2012	29803,00	10911367	15930,00	09.05.2014	140925,00	1618870	61323,00
21.02.2011	2857,00	771844	1969,00	30.09.2012	25781,00	2189009	10929,00	10.05.2014	119139,00	1313942	55633,00
22.02.2011	3143,00	990024	2152,00	01.10.2012	29541,00	2987961	11524,00	11.05.2014	143525,00	1753223	48439,00
23.02.2011	3480,00	673460	2394,00	02.10.2012	35169,00	2866101	16185,00	12.05.2014	130988,00	1673014	63435,00
24.02.2011	2847,00	519567	1957,00	03.10.2012	35365,00	4144257	17520,00	13.05.2014	125036,00	1438594	63900,00
25.02.2011	3067,00	1555819	2134,00	04.10.2012	35434,00	7443107	13985,00	14.05.2014	131116,00	7179368	63119,00
26.02.2011	2901,00	4422223	1964,00	05.10.2012	34539,00	2732842	13434,00	15.05.2014	151809,00	2464462	68081,00
27.02.2011	3198,00	1916207	2261,00	06.10.2012	34398,00	1403860	12842,00	16.05.2014	127748,00	1603546	62685,00
28.02.2011	2706,00	755051	1932,00	07.10.2012	30653,00	1774322	10787,00	17.05.2014	115383,00	1187134	50924,00

01.03.2011	2494,00	21019413	1660,00	08.10.2012	37625,00	11110521	12409,00	18.05.2014	151855,00	2132629	45521,00
02.03.2011	4755,00	1122183	2974,00	09.10.2012	37794,00	1619555	13691,00	19.05.2014	127935,00	1525211	55903,00
03.03.2011	4099,00	354593	3002,00	10.10.2012	37830,00	4143772	13797,00	20.05.2014	153007,00	1556387	64563,00
04.03.2011	2996,00	844996	2119,00	11.10.2012	32004,00	2334714	13414,00	21.05.2014	145579,00	3228546	65595,00
05.03.2011	2839,00	529146	1946,00	12.10.2012	32832,00	3434996	12965,00	22.05.2014	129318,00	3559296	62786,00
06.03.2011	2750,00	1180849	1918,00	13.10.2012	33228,00	1185349	12101,00	23.05.2014	155129,00	2966589	66578,00
07.03.2011	2990,00	304160	2120,00	14.10.2012	30494,00	6354668	11302,00	24.05.2014	113362,00	11454254	52616,00
08.03.2011	3547,00	816938	2530,00	15.10.2012	32370,00	4197375	12844,00	25.05.2014	159903,00	5538872	50254,00
09.03.2011	2833,00	256808	1787,00	16.10.2012	31951,00	1953644	11214,00	26.05.2014	136252,00	4488778	58215,00
10.03.2011	2388,00	300189	1491,00	17.10.2012	33554,00	11601741	14024,00	27.05.2014	145771,00	3964607	60714,00
11.03.2011	2834,00	267689	2107,00	18.10.2012	34489,00	4706927	15835,00	28.05.2014	161438,00	28569355	66749,00
12.03.2011	2600,00	1877887	2812,00	19.10.2012	32236,00	3143603	15934,00	29.05.2014	143379,00	2880431	58932,00
13.03.2011	2494,00	841701	2475,00	20.10.2012	31187,00	1842021	13230,00	30.05.2014	137258,00	5606324	61119,00
14.03.2011	2388,00	3132325	2981,00	21.10.2012	31535,00	5862916	10212,00	31.05.2014	123216,00	6115853	50349,00
15.03.2011	2660,00	1259156	2499,00	22.10.2012	29410,00	1826164	11321,00	01.06.2014	164472,00	3791769	48238,00
16.03.2011	2581,00	5512025	3237,00	23.10.2012	33577,00	2620540	11068,00	02.06.2014	140278,00	2954722	56625,00
17.03.2011	2663,00	2121396	3188,00	24.10.2012	33269,00	2022041	13163,00	03.06.2014	162366,00	5227838	64508,00
18.03.2011	2802,00	108002	2759,00	25.10.2012	27911,00	7404129	13525,00	04.06.2014	154092,00	2953035	62282,00
19.03.2011	2697,00	693155	3114,00	26.10.2012	29737,00	5007913	14132,00	05.06.2014	148891,00	3869249	61399,00
20.03.2011	2378,00	93947	2674,00	27.10.2012	22726,00	5700471	10196,00	06.06.2014	150478,00	3963135	59197,00
21.03.2011	5496,00	483141	7322,00	28.10.2012	21318,00	1346475	9694,00	07.06.2014	127246,00	2117008	49794,00
22.03.2011	3504,00	1285344	2301,00	29.10.2012	21429,00	2137126	9161,00	08.06.2014	153084,00	2482747	43445,00
23.03.2011	5598,00	1532840	4368,00	30.10.2012	26964,00	4027731	10291,00	09.06.2014	128287,00	2463912	52697,00
24.03.2011	3802,00	3445384	2218,00	31.10.2012	26412,00	3686639	11056,00	10.06.2014	150796,00	12113329	59436,00
25.03.2011	3624,00	700177	2087,00	01.11.2012	23811,00	3095946	10842,00	11.06.2014	141736,00	14000924	58166,00
26.03.2011	3808,00	3046723	2987,00	02.11.2012	26334,00	3416200	10731,00	12.06.2014	140825,00	10598764	58229,00
27.03.2011	3565,00	788382	2272,00	03.11.2012	26548,00	1436767	10952,00	13.06.2014	151052,00	45489504	61667,00
28.03.2011	5102,00	1522833	3420,00	04.11.2012	22368,00	2827474	9755,00	14.06.2014	136421,00	1878374	51974,00
29.03.2011	4182,00	375102	2915,00	05.11.2012	27968,00	2916321	10585,00	15.06.2014	156871,00	1071047	44881,00
30.03.2011	2870,00	218206	1625,00	06.11.2012	28560,00	2440659	10983,00	16.06.2014	144825,00	3390638	55333,00
31.03.2011	3692,00	482674	2206,00	07.11.2012	34011,00	2485436	12076,00	17.06.2014	157183,00	1977642	61902,00
01.04.2011	2785,00	471003	1573,00	08.11.2012	30564,00	4491055	12054,00	18.06.2014	153204,00	2419526	62754,00
02.04.2011	2915,00	289974	1804,00	09.11.2012	28883,00	2796632	11892,00	19.06.2014	127162,00	3020069	56372,00
03.04.2011	2708,00	434826	1603,00	10.11.2012	24961,00	1048185	9649,00	20.06.2014	142279,00	2382716	55889,00
04.04.2011	3887,00	2359957	2327,00	11.11.2012	21483,00	3368638	8038,00	21.06.2014	131691,00	1369531	49007,00
05.04.2011	3741,00	2390112	2272,00	12.11.2012	26835,00	4882612	9925,00	22.06.2014	166479,00	2618573	45909,00
06.04.2011	3149,00	1372337	1768,00	13.11.2012	23713,00	1753493	8793,00	23.06.2014	125908,00	2936308	53514,00
07.04.2011	3057,00	674878	1842,00	14.11.2012	27765,00	5043121	10839,00	24.06.2014	149893,00	8819431	59866,00
08.04.2011	2897,00	894889	1700,00	15.11.2012	34437,00	3002754	14067,00	25.06.2014	150209,00	1909173	57849,00
09.04.2011	3078,00	350683	1749,00	16.11.2012	33886,00	6925545	14493,00	26.06.2014	141973,00	4186204	57187,00
10.04.2011	2843,00	212963	1653,00	17.11.2012	45125,00	3178654	13070,00	27.06.2014	143429,00	2503022	56295,00
11.04.2011	3040,00	454615	1879,00	18.11.2012	32677,00	2191750	12069,00	28.06.2014	123855,00	1212926	52183,00
12.04.2011	3398,00	1571815	2019,00	19.11.2012	34545,00	3907579	13291,00	29.06.2014	159773,00	13746308	44675,00
13.04.2011	3759,00	1336535	2480,00	20.11.2012	34632,00	2179889	15204,00	30.06.2014	136152,00	4809434	57408,00
14.04.2011	5390,00	1059114	2968,00	21.11.2012	34618,00	3121044	13398,00	01.07.2014	163651,00	3009945	64855,00
15.04.2011	3050,00	3072779	2001,00	22.11.2012	32823,00	2464723	16262,00	02.07.2014	152310,00	7570274	62842,00
16.04.2011	3115,00	2422178	1980,00	23.11.2012	26731,00	2183170	12915,00	03.07.2014	142946,00	5099209	59392,00
17.04.2011	3531,00	1238981	2320,00	24.11.2012	27215,00	3008030	13245,00	04.07.2014	128352,00	2961896	57102,00
18.04.2011	3997,00	2695691	2711,00	25.11.2012	27411,00	2224723	11687,00	05.07.2014	107662,00	1812041	43684,00
19.04.2011	5118,00	2009633	3567,00	26.11.2012	28774,00	5359954	12105,00	06.07.2014	163209,00	1480468	47739,00
20.04.2011	4676,00	1516506	3173,00	27.11.2012	31418,00	4499584	14655,00	07.07.2014	136897,00	2199542	56650,00
21.04.2011	3310,00	491546	1912,00	28.11.2012	33542,00	3872342	13339,00	08.07.2014	192201,00	1802689	65142,00
22.04.2011	3723,00	3003385	2262,00	29.11.2012	32816,00	2085482	13420,00	09.07.2014	160879,00	6395980	64396,00
23.04.2011	3399,00	1952865	2100,00	30.11.2012	27705,00	4319586	12121,00	10.07.2014	149129,00	3012272	58507,00
24.04.2011	4082,00	4591453	2496,00	01.12.2012	29164,00	3157935	11156,00	11.07.2014	145718,00	1638317	57127,00
25.04.2011	4110,00	1989477	2516,00	02.12.2012	21186,00	1478522	9133,00	12.07.2014	145144,00	1859387	51347,00
26.04.2011	4431,00	1217124	2753,00	03.12.2012	23333,00	2493671	10120,00	13.07.2014	165376,00	1356456	48085,00
27.04.2011	6329,00	2191095	4550,00	04.12.2012	26758,00	17834778	12593,00	14.07.2014	133673,00	1771043	53369,00
28.04.2011	5619,00	3069801	3618,00	05.12.2012	32849,00	8394451	15540,00	15.07.2014	151679,00	1710420	61612,00
29.04.2011	5505,00	27239019	3474,00	06.12.2012	29988,00	2712317	13587,00	16.07.2014	151081,00	2595225	60139,00
30.04.2011	6324,00	3370468	4022,00	07.12.2012	29236,00	9363068	13173,00	17.07.2014	146474,00	3261528	61928,00
01.05.2011	7135,00	2609081	4648,00	08.12.2012	29214,00	1774420	12347,00	18.07.2014	141439,00	3074604	57314,00
02.05.2011	4268,00	3371529	2519,00	09.12.2012	29112,00	2248202	10771,00	19.07.2014	132003,00	3499686	52995,00
03.05.2011	5240,00	3756035	3235,00	10.12.2012	26865,00	4479391	11427,00	20.07.2014	176955,00	3253549	50857,00
04.05.2011	5204,00	9534308	2967,00	11.12.2012	28917,00	4774963	13765,00	21.07.2014	135230,00	3410173	57612,00
05.05.2011	5773,00	1138735	3399,00	12.12.2012	30888,00	6824595	15571,00	22.07.2014	134257,00	4788189	62921,00
06.05.2011	5690,00	2579885	3249,00	13.12.2012	33996,00	4609420	16338,00	23.07.2014	155345,00	2846298	65037,00
07.05.2011	6110,00	3440541	3889,00	14.12.2012	33491,00	7337808	15409,00	24.07.2014	150217,00	9011417	60982,00
08.05.2011	4744,00	2518873	2777,00	15.12.2012	27511,00	2785572	12963,00	25.07.2014	151416,00	3107498	59317,00
09.05.2011	6323,00	2246657	3560,00	16.12.2012	28933,00	2830742	12799,00	26.07.2014	130299,00	2001091	51209,00
10.05.2011	5425,00	2824118	3147,00	17.12.2012	32044,00	1934277	14162,00	27.07.2014	163986,00	2662136	49062,00
11.05.2011	5921,00	5846208	3272,00	18.12.2012	38406,00	3113418	17697,00	28.07.2014	135674,00	3560245	56163,00
12.05.2011	4914,00	11597997	2636,00	19.12.2012	36002,00	3390321	15423,00	29.07.2014	147327,00	5056271	60770,00

13.05.2011	7624,00	7054448	4404,00	20.12.2012	30200,00	6481924	13466,00	30.07.2014	151806,00	4254734	59532,00
14.05.2011	7463,00	2872402	4349,00	21.12.2012	32608,00	3706681	14440,00	31.07.2014	152214,00	3106130	62647,00
15.05.2011	7124,00	4897291	3990,00	22.12.2012	43693,00	2410198	17745,00	01.08.2014	146378,00	7982377	61823,00
16.05.2011	9243,00	2189938	4160,00	23.12.2012	32573,00	1127849	13381,00	02.08.2014	133227,00	2931814	55899,00
17.05.2011	9093,00	14095084	4355,00	24.12.2012	29026,00	2316909	12446,00	03.08.2014	155660,00	1875001	49287,00
18.05.2011	9918,00	2324178	4997,00	25.12.2012	25045,00	1367122	10601,00	04.08.2014	122118,00	6716938	59112,00
19.05.2011	11265,00	4789626	5131,00	26.12.2012	24110,00	1606864	10482,00	05.08.2014	166966,00	16612551	67774,00
20.05.2011	9419,00	2916753	4803,00	27.12.2012	27812,00	1520708	11889,00	06.08.2014	175244,00	13135345	71825,00
21.05.2011	9193,00	4656426	4822,00	28.12.2012	31561,00	2406201	13908,00	07.08.2014	153189,00	4451508	65231,00
22.05.2011	9823,00	1228059	5447,00	29.12.2012	30563,00	2201831	13470,00	08.08.2014	151292,00	2181508	62814,00
23.05.2011	10157,00	1350381	5775,00	30.12.2012	35482,00	1846915	16611,00	09.08.2014	130400,00	2663606	58049,00
24.05.2011	10691,00	1195519	5562,00	31.12.2012	29019,00	11795538	12793,00	10.08.2014	176751,00	1933041	53617,00
25.05.2011	12928,00	4136891	6172,00	01.01.2013	26713,00	2928461	13424,00	11.08.2014	161536,00	2441094	65330,00
26.05.2011	12180,00	3133931	6818,00	02.01.2013	33739,00	2053182	16176,00	12.08.2014	172608,00	2908954	72854,00
27.05.2011	9863,00	3026199	5491,00	03.01.2013	38262,00	2940399	16404,00	13.08.2014	173743,00	5223944	69312,00
28.05.2011	9834,00	1595206	5054,00	04.01.2013	37428,00	3812690	17256,00	14.08.2014	168931,00	3020590	75480,00
29.05.2011	9270,00	697189	4725,00	05.01.2013	41926,00	3538133	17789,00	15.08.2014	155144,00	3814262	63678,00
30.05.2011	10010,00	2520990	4835,00	06.01.2013	33185,00	1370929	14625,00	16.08.2014	161700,00	3385801	70469,00
31.05.2011	12252,00	2462533	6203,00	07.01.2013	39233,00	2055052	18091,00	17.08.2014	180542,00	2664071	54894,00
01.06.2011	11219,00	1280720	6069,00	08.01.2013	36996,00	4355310	17259,00	18.08.2014	146537,00	6921439	63950,00
02.06.2011	12768,00	4077259	7157,00	09.01.2013	40935,00	5712860	18753,00	19.08.2014	172107,00	2748508	70875,00
03.06.2011	14800,00	24645102	8374,00	10.01.2013	43702,00	5207166	18846,00	20.08.2014	163890,00	2755557	69785,00
04.06.2011	16750,00	3097601	8773,00	11.01.2013	48496,00	2662429	21326,00	21.08.2014	176373,00	5234521	71266,00
05.06.2011	14944,00	8895799	8161,00	12.01.2013	37486,00	2375902	16729,00	22.08.2014	156481,00	7721693	66732,00
06.06.2011	17688,00	10724343	9808,00	13.01.2013	40823,00	3375071	17120,00	23.08.2014	135772,00	5050379	57973,00
07.06.2011	15812,00	1689044	8704,00	14.01.2013	32734,00	2975712	11472,00	24.08.2014	183565,00	5786670	52680,00
08.06.2011	20730,00	16588929	11394,00	15.01.2013	46112,00	4157737	18811,00	25.08.2014	148320,00	5112947	63222,00
09.06.2011	22272,00	16054550	12167,00	16.01.2013	45312,00	3288830	20222,00	26.08.2014	163922,00	4199026	71269,00
10.06.2011	21061,00	8901992	11233,00	17.01.2013	42042,00	5076600	18114,00	27.08.2014	160858,00	3067223	69521,00
11.06.2011	20896,00	21938305	11162,00	18.01.2013	44445,00	5034996	19684,00	28.08.2014	166074,00	10772107	66527,00
12.06.2011	21909,00	16890554	11668,00	19.01.2013	38673,00	2898542	17522,00	29.08.2014	145588,00	3477188	65314,00
13.06.2011	22918,00	15580070	12238,00	20.01.2013	34725,00	2199697	15397,00	30.08.2014	145985,00	9941580	61887,00
14.06.2011	23877,00	53532635	12602,00	21.01.2013	32882,00	3403001	15108,00	31.08.2014	172302,00	3985272	56915,00
15.06.2011	26175,00	20536752	14172,00	22.01.2013	37266,00	13624749	17719,00	01.09.2014	162588,00	2932817	61965,00
16.06.2011	22537,00	5329505	11777,00	23.01.2013	36782,00	6218530	15664,00	02.09.2014	153606,00	6227104	66497,00
17.06.2011	22736,00	21641611	11548,00	24.01.2013	39004,00	7538617	18028,00	03.09.2014	148218,00	2717307	66433,00
18.06.2011	23543,00	3500241	12025,00	25.01.2013	39799,00	6777706	17666,00	04.09.2014	152304,00	3616314	67680,00
19.06.2011	23804,00	7006559	11478,00	26.01.2013	40491,00	6508467	18247,00	05.09.2014	155908,00	4932965	63656,00
20.06.2011	23113,00	13712116	11278,00	27.01.2013	40004,00	11895873	15128,00	06.09.2014	143414,00	12260199	62897,00
21.06.2011	19981,00	2213245	9152,00	28.01.2013	42353,00	4054864	15506,00	07.09.2014	214360,00	2930649	55736,00
22.06.2011	24881,00	1697123	11810,00	29.01.2013	41643,00	13876541	16885,00	08.09.2014	151689,00	3876634	67638,00
23.06.2011	22014,00	2331781	10512,00	30.01.2013	36938,00	12158261	15686,00	09.09.2014	173414,00	5985520	76384,00
24.06.2011	22763,00	2559619	11134,00	31.01.2013	34477,00	13098273	16186,00	10.09.2014	164564,00	8953363	72396,00
25.06.2011	19107,00	1601867	9517,00	01.02.2013	47420,00	30089741	18874,00	11.09.2014	147710,00	3478134	65134,00
26.06.2011	20531,00	1382669	10298,00	02.02.2013	45504,00	13601580	17383,00	12.09.2014	148941,00	2897576	64582,00
27.06.2011	24689,00	8625037	11438,00	03.02.2013	41758,00	3216828	16161,00	13.09.2014	136734,00	2960064	60353,00
28.06.2011	22877,00	18188877	10892,00	04.02.2013	41685,00	8514241	17821,00	14.09.2014	203940,00	2030025	58907,00
29.06.2011	21640,00	2168932	10158,00	05.02.2013	48193,00	7320496	23359,00	15.09.2014	161269,00	4939347	68187,00
30.06.2011	20088,00	3262597	9885,00	06.02.2013	42634,00	4384327	19299,00	16.09.2014	186658,00	2501232	82881,00
01.07.2011	25731,00	1601270	9450,00	07.02.2013	44112,00	4981165	20178,00	17.09.2014	164215,00	3572281	75113,00
02.07.2011	31999,00	886321	9454,00	08.02.2013	46037,00	9066863	20369,00	18.09.2014	168204,00	5491126	76196,00
03.07.2011	19140,00	1112033	7973,00	09.02.2013	39368,00	3998375	18174,00	19.09.2014	149539,00	7356464	69166,00
04.07.2011	20364,00	861964	9495,00	10.02.2013	45554,00	10179608	19316,00	20.09.2014	142592,00	14032476	60173,00
05.07.2011	17861,00	4543668	8481,00	11.02.2013	41240,00	3535977	17988,00	21.09.2014	172794,00	4539848	58629,00
06.07.2011	23786,00	2884920	11053,00	12.02.2013	41227,00	6219088	18081,00	22.09.2014	175943,00	1397004	65891,00
07.07.2011	20579,00	1313169	9392,00	13.02.2013	40152,00	8244990	16313,00	23.09.2014	166664,00	3918311	68439,00
08.07.2011	19803,00	1083716	8211,00	14.02.2013	39268,00	6400894	16942,00	24.09.2014	171434,00	2966974	75798,00
09.07.2011	20921,00	758174	8397,00	15.02.2013	39955,00	9950207	17649,00	25.09.2014	167940,00	2652472	74180,00
10.07.2011	25941,00	1270279	8057,00	16.02.2013	37901,00	17246033	15330,00	26.09.2014	149986,00	5243090	69279,00
11.07.2011	20304,00	6034880	9867,00	17.02.2013	36500,00	7837205	14033,00	27.09.2014	145374,00	1815678	61574,00
12.07.2011	20971,00	735356	8795,00	18.02.2013	36918,00	5887010	16973,00	28.09.2014	213832,00	3335096	56893,00
13.07.2011	24854,00	996321	9575,00	19.02.2013	39259,00	6249436	17047,00	29.09.2014	152629,00	9374718	68262,00
14.07.2011	25498,00	956043	8419,00	20.02.2013	39597,00	6399108	18258,00	30.09.2014	184554,00	5355053	75290,00
15.07.2011	21025,00	693014	8630,00	21.02.2013	42228,00	8342099	17339,00	01.10.2014	184739,00	4088537	74675,00
16.07.2011	21029,00	464355	7821,00	22.02.2013	43549,00	5461297	18252,00	02.10.2014	161404,00	3839984	69812,00
17.07.2011	22354,00	881543	9110,00	23.02.2013	41330,00	5059053	17279,00	03.10.2014	150641,00	7763379	67817,00
18.07.2011	19515,00	13063137	8185,00	24.02.2013	41919,00	5223336	16568,00	04.10.2014	137659,00	7026753	65139,00
19.07.2011	23514,00	2246135	9863,00	25.02.2013	43083,00	30992629	18098,00	05.10.2014	207383,00	23652527	62133,00
20.07.2011	21109,00	4736132	8545,00	26.02.2013	45961,00	5581467	19601,00	06.10.2014	151236,00	9947756	70344,00
21.07.2011	22713,00	421822	8608,00	27.02.2013	44197,00	6645610	18868,00	07.10.2014	178444,00	5729066	74334,00
22.07.2011	21044,00	488297	8437,00	28.02.2013	43778,00	20746704	19200,00	08.10.2014	165335,00	6093968	73207,00
23.07.2011	19698,00	567402	8034,00	01.03.2013	51127,00	6177637	21567,00	09.10.2014	156106,00	8088954	73307,00
24.07.2011	20708,00	696956	7866,00	02.03.2013	40918,00	5889036	17227,00	10.10.2014	164414,00	7979839	73889,00

25.07.2011	22766,00	824690	9555,00	03.03.2013	34273,00	3759036	12300,00	11.10.2014	152027,00	1404404	61934,00
26.07.2011	21078,00	791042	8401,00	04.03.2013	40375,00	3981903	15604,00	12.10.2014	206084,00	6767047	59581,00
27.07.2011	20882,00	640812	8329,00	05.03.2013	45553,00	11463803	19608,00	13.10.2014	181872,00	4419814	70036,00
28.07.2011	22225,00	1865533	7818,00	06.03.2013	52412,00	16362552	22628,00	14.10.2014	174859,00	5003542	75953,00
29.07.2011	20440,00	847466	7460,00	07.03.2013	51281,00	18164723	21927,00	15.10.2014	175952,00	7279236	73184,00
30.07.2011	18672,00	1776355	6854,00	08.03.2013	48391,00	5368543	20934,00	16.10.2014	163270,00	4409323	70193,00
31.07.2011	20480,00	1800072	7429,00	09.03.2013	41355,00	9723727	17139,00	17.10.2014	157782,00	4373652	69098,00
01.08.2011	21414,00	1125450	8032,00	10.03.2013	45331,00	3261583	21266,00	18.10.2014	156631,00	1689556	64669,00
02.08.2011	19473,00	1519296	8813,00	11.03.2013	42498,00	5575288	16740,00	19.10.2014	211493,00	2296311	58026,00
03.08.2011	15703,00	2087153	8054,00	12.03.2013	39137,00	7165690	16281,00	20.10.2014	155800,00	2158560	71465,00
04.08.2011	15681,00	1187052	8251,00	13.03.2013	54264,00	8856162	21149,00	21.10.2014	175051,00	1404294	76716,00
05.08.2011	18013,00	3361298	7308,00	14.03.2013	47557,00	6934457	20098,00	22.10.2014	171845,00	3779735	74600,00
06.08.2011	18171,00	1798043	7080,00	15.03.2013	51067,00	5012939	21347,00	23.10.2014	163026,00	4438411	71289,00
07.08.2011	17200,00	3250893	6725,00	16.03.2013	42592,00	5636980	18570,00	24.10.2014	165243,00	7898167	74677,00
08.08.2011	18130,00	3148989	7110,00	17.03.2013	41008,00	3499190	17059,00	25.10.2014	189654,00	3002971	66299,00
09.08.2011	20864,00	667313	8638,00	18.03.2013	42920,00	6179988	19061,00	26.10.2014	183560,00	1099320	66113,00
10.08.2011	16769,00	761570	8382,00	19.03.2013	52355,00	8358526	24469,00	27.10.2014	181920,00	2318987	74641,00
11.08.2011	16032,00	834290	8116,00	20.03.2013	49153,00	6446598	22659,00	28.10.2014	177816,00	2808275	80037,00
12.08.2011	14031,00	659033	7064,00	21.03.2013	51230,00	10648179	23501,00	29.10.2014	175287,00	4215908	79347,00
13.08.2011	15861,00	949401	7386,00	22.03.2013	58318,00	14193600	26754,00	30.10.2014	175625,00	2068461	80386,00
14.08.2011	19243,00	487546	7621,00	23.03.2013	50716,00	14496356	22002,00	31.10.2014	174925,00	3182640	79609,00
15.08.2011	16500,00	1316917	8347,00	24.03.2013	57950,00	8002473	24811,00	01.11.2014	146848,00	5695988	67184,00
16.08.2011	16666,00	468794	9259,00	25.03.2013	51092,00	11718611	25336,00	02.11.2014	236884,00	3808661	64662,00
17.08.2011	16997,00	1178375	8128,00	26.03.2013	56598,00	11371172	24343,00	03.11.2014	157911,00	2622697	73300,00
18.08.2011	18383,00	1278380	7457,00	27.03.2013	56615,00	9441164	27647,00	04.11.2014	184888,00	3212542	80673,00
19.08.2011	20161,00	921109	7787,00	28.03.2013	65540,00	10100397	33459,00	05.11.2014	171401,00	5186515	79327,00
20.08.2011	19019,00	877894	7125,00	29.03.2013	69638,00	8576370	30749,00	06.11.2014	173515,00	2815695	80971,00
21.08.2011	18708,00	314731	7355,00	30.03.2013	60390,00	16326590	27579,00	07.11.2014	163094,00	17115606	78705,00
22.08.2011	21602,00	1095403	7924,00	31.03.2013	49192,00	3780046	19367,00	08.11.2014	144394,00	6296139	67080,00
23.08.2011	21892,00	514253	7425,00	01.04.2013	55367,00	9211119	22408,00	09.11.2014	223383,00	5468754	63268,00
24.08.2011	17886,00	683896	7333,00	02.04.2013	70819,00	26113352	31282,00	10.11.2014	176533,00	3672387	75820,00
25.08.2011	18626,00	13596409	7082,00	03.04.2013	85804,00	24086368	35162,00	11.11.2014	168913,00	2903664	79449,00
26.08.2011	19914,00	6262864	7479,00	04.04.2013	86046,00	23576222	37870,00	12.11.2014	179505,00	4920049	82662,00
27.08.2011	16681,00	22831821	6988,00	05.04.2013	82343,00	34693218	35319,00	13.11.2014	197029,00	6671112	95109,00
28.08.2011	16239,00	684416	5453,00	06.04.2013	68732,00	9661063	28056,00	14.11.2014	200490,00	6362912	80812,00
29.08.2011	17103,00	3352388	7807,00	07.04.2013	74149,00	9201496	25164,00	15.11.2014	156976,00	3462904	69581,00
30.08.2011	14933,00	656852	7846,00	08.04.2013	93700,00	15825007	33728,00	16.11.2014	220218,00	2080611	67707,00
31.08.2011	14550,00	490704	7280,00	09.04.2013	85063,00	21890887	41823,00	17.11.2014	171933,00	1886032	78525,00
01.09.2011	13820,00	620014	7222,00	10.04.2013	102016,00	52694515	51455,00	18.11.2014	176768,00	4513359	79411,00
02.09.2011	13891,00	2273146	6917,00	11.04.2013	100830,00	38783212	49131,00	19.11.2014	175445,00	4737987	81149,00
03.09.2011	12731,00	458109	6325,00	12.04.2013	87352,00	14405332	38328,00	20.11.2014	177646,00	3160588	79495,00
04.09.2011	14161,00	434634	6612,00	13.04.2013	72076,00	10676727	30827,00	21.11.2014	174282,00	5900906	76668,00
05.09.2011	15971,00	2473421	7281,00	14.04.2013	57080,00	5905214	23968,00	22.11.2014	166491,00	1461794	71779,00
06.09.2011	15194,00	3360323	7705,00	15.04.2013	80731,00	11671398	26933,00	23.11.2014	224922,00	1284407	67599,00
07.09.2011	14446,00	2934569	7178,00	16.04.2013	79311,00	26044894	33725,00	24.11.2014	163316,00	1931815	73842,00
08.09.2011	13362,00	1550330	6481,00	17.04.2013	84698,00	7625994	33619,00	25.11.2014	169442,00	3424247	78211,00
09.09.2011	13930,00	6691451	7266,00	18.04.2013	72737,00	6097391	28920,00	26.11.2014	180983,00	2412033	84534,00
10.09.2011	13186,00	1844114	6453,00	19.04.2013	87326,00	5099989	35933,00	27.11.2014	178381,00	4374762	77335,00
11.09.2011	12955,00	10769893	6301,00	20.04.2013	61190,00	4730462	26957,00	28.11.2014	175185,00	44189193	80741,00
12.09.2011	12932,00	2165748	6422,00	21.04.2013	59238,00	10660362	24533,00	29.11.2014	166646,00	12072220	76097,00
13.09.2011	13053,00	6386033	6564,00	22.04.2013	77777,00	5339100	27512,00	30.11.2014	245004,00	2763653	72338,00
14.09.2011	13152,00	2851952	6515,00	23.04.2013	72900,00	10450354	31495,00	01.12.2014	174232,00	4596775	86252,00
15.09.2011	11956,00	1177980	6040,00	24.04.2013	85420,00	6683370	33712,00	02.12.2014	205483,00	5837936	94405,00
16.09.2011	12058,00	1517145	6042,00	25.04.2013	73729,00	13392759	31457,00	03.12.2014	199881,00	4387633	92810,00
17.09.2011	12148,00	1534108	6181,00	26.04.2013	74621,00	3383214	28632,00	04.12.2014	186491,00	3522369	88683,00
18.09.2011	11736,00	376498	5775,00	27.04.2013	62711,00	6405801	24689,00	05.12.2014	194141,00	17119943	86128,00
19.09.2011	12541,00	801936	6272,00	28.04.2013	107554,00	3273131	22796,00	06.12.2014	173360,00	2451010	75452,00
20.09.2011	18459,00	1913594	7420,00	29.04.2013	73687,00	5306881	27314,00	07.12.2014	232300,00	1515620	72640,00
21.09.2011	13872,00	736553	8078,00	30.04.2013	60887,00	3919949	25564,00	08.12.2014	183776,00	31650645	80024,00
22.09.2011	14757,00	764978	6808,00	01.05.2013	61672,00	7617711	24530,00	09.12.2014	191539,00	22903887	86078,00
23.09.2011	17019,00	1215758	5820,00	02.05.2013	67744,00	6499154	27688,00	10.12.2014	190602,00	5891045	87315,00
24.09.2011	17662,00	633908	6231,00	03.05.2013	70210,00	14873997	26506,00	11.12.2014	187113,00	3653390	82901,00
25.09.2011	17523,00	261754	5671,00	04.05.2013	56115,00	4044481	18242,00	12.12.2014	177462,00	1685095	76365,00
26.09.2011	17160,00	3051776	5917,00	05.05.2013	55974,00	4527940	21113,00	13.12.2014	174655,00	3638935	75799,00
27.09.2011	16854,00	1524821	6055,00	06.05.2013	64381,00	2729247	24879,00	14.12.2014	231376,00	1399010	68435,00
28.09.2011	11610,00	651664	5795,00	07.05.2013	89457,00	4669155	27551,00	15.12.2014	215842,00	2639315	88535,00
29.09.2011	10806,00	347003	5709,00	08.05.2013	95352,00	2536036	25395,00	16.12.2014	204914,00	3749097	90848,00
30.09.2011	11409,00	1356970	5762,00	09.05.2013	70728,00	3786891	25416,00	17.12.2014	203993,00	3328855	88560,00
01.10.2011	10969,00	1319649	5584,00	10.05.2013	72244,00	5053019	25530,00	18.12.2014	225354,00	4981190	95565,00
02.10.2011	10163,00	980016	5145,00	11.05.2013	67240,00	7316599	21238,00	19.12.2014	160502,00	4494426	86754,00
03.10.2011	11545,00	499542	6273,00	12.05.2013	61435,00	2304224	19684,00	20.12.2014	240775,00	1790614	84341,00
04.10.2011	10079,00	769034	5316,00	13.05.2013	65440,00	2068169	23179,00	21.12.2014	204217,00	4231400	75527,00
05.10.2011	12453,00	715372	6218,00	14.05.2013	68323,00	3069549	26812,00	22.12.2014	195624,00	5495943	85763,00

06.10.2011	11909,00	8170252	6004,00	15.05.2013	70212,00	7402098	28149,00	23.12.2014	210726,00	3800448	93782,00
07.10.2011	11289,00	663161	5509,00	16.05.2013	67246,00	3112026	26773,00	24.12.2014	174711,00	27154619	84662,00
08.10.2011	10939,00	1289094	5604,00	17.05.2013	64560,00	2614963	26882,00	25.12.2014	147374,00	2160920	65198,00
09.10.2011	10976,00	2158599	5623,00	18.05.2013	55716,00	6760613	22985,00	26.12.2014	145412,00	1759008	67031,00
10.10.2011	10553,00	1146543	5530,00	19.05.2013	51111,00	1993973	19778,00	27.12.2014	188604,00	1288478	74575,00
11.10.2011	11523,00	1373684	5846,00	20.05.2013	56966,00	2177603	22790,00	28.12.2014	236392,00	1196849	68015,00
12.10.2011	12312,00	1475436	6498,00	21.05.2013	63976,00	1868880	25688,00	29.12.2014	159314,00	3589855	72823,00
13.10.2011	9294,00	797229	4739,00	22.05.2013	65369,00	2135736	26186,00	30.12.2014	181005,00	16810168	80010,00
14.10.2011	10647,00	1256284	5676,00	23.05.2013	65171,00	2894274	27539,00	31.12.2014	157377,00	25682967	74288,00
15.10.2011	11551,00	878179	6080,00	24.05.2013	67558,00	2988329	28073,00	01.01.2015	116012,00	1044937	53529,00
16.10.2011	9706,00	498650	4878,00	25.05.2013	60147,00	14865869	23552,00	02.01.2015	168563,00	2072541	66773,00
17.10.2011	11136,00	4881096	5593,00	26.05.2013	52307,00	965754	21292,00	03.01.2015	207571,00	3328615	75473,00
18.10.2011	10981,00	4900131	5562,00	27.05.2013	59395,00	1448306	23700,00	04.01.2015	206228,00	7294529	79818,00
19.10.2011	9684,00	3719688	4810,00	28.05.2013	56871,00	4252774	23738,00	05.01.2015	193982,00	5575923	83904,00
20.10.2011	8801,00	1604516	4708,00	29.05.2013	66689,00	4210870	28087,00	06.01.2015	179154,00	5277899	79804,00
21.10.2011	10518,00	774758	5357,00	30.05.2013	63212,00	4960431	26318,00	07.01.2015	180992,00	17968831	86052,00
22.10.2011	9425,00	2946421	4820,00	31.05.2013	62386,00	8397401	26691,00	08.01.2015	186319,00	11659229	89016,00
23.10.2011	10417,00	625118	5451,00	01.06.2013	59033,00	2626027	24158,00	09.01.2015	201458,00	6049004	93280,00
24.10.2011	11390,00	577297	5919,00	02.06.2013	50677,00	2684924	22684,00	10.01.2015	251092,00	7926712	96782,00
25.10.2011	10830,00	411436	5282,00	03.06.2013	58321,00	3140875	24959,00	11.01.2015	209755,00	6553567	84038,00
26.10.2011	10204,00	1639365	5307,00	04.06.2013	63518,00	2368577	27841,00	12.01.2015	185802,00	3013565	89969,00
27.10.2011	9527,00	2127148	4739,00	05.06.2013	67477,00	14045052	25027,00	13.01.2015	199744,00	13119490	94090,00
28.10.2011	9752,00	722106	5111,00	06.06.2013	60098,00	8957143	26401,00	14.01.2015	228898,00	12550448	97287,00
29.10.2011	11058,00	829626	5826,00	07.06.2013	60504,00	4705195	26978,00	15.01.2015	212403,00	6793862	105562,00
30.10.2011	9259,00	2243811	4888,00	08.06.2013	51054,00	3932971	23662,00	16.01.2015	219873,00	12372752	104844,00
31.10.2011	9725,00	379673	4956,00	09.06.2013	45062,00	8892211	20904,00	17.01.2015	254267,00	3213825	83315,00
01.11.2011	10403,00	2216727	5885,00	10.06.2013	48672,00	1834324	20896,00	18.01.2015	223392,00	2798596	79371,00
02.11.2011	10673,00	408186	5750,00	11.06.2013	57169,00	4362852	23454,00	19.01.2015	197559,00	2641519	82018,00
03.11.2011	10207,00	3587743	5746,00	12.06.2013	52722,00	3547709	21852,00	20.01.2015	194860,00	2877498	87331,00
04.11.2011	11518,00	2528474	6662,00	13.06.2013	53645,00	1734384	22741,00	21.01.2015	197159,00	13762971	90542,00
05.11.2011	12548,00	570239	6575,00	14.06.2013	60855,00	2812255	26342,00	22.01.2015	188687,00	4077520	87136,00
06.11.2011	9641,00	286792	5021,00	15.06.2013	52008,00	5384873	21840,00	23.01.2015	179966,00	2223875	81067,00
07.11.2011	10269,00	334690	5329,00	16.06.2013	37955,00	3822006	17372,00	24.01.2015	172854,00	3706748	78100,00
08.11.2011	10896,00	1545422	5748,00	17.06.2013	45693,00	1455866	20835,00	25.01.2015	256121,00	1397733	72746,00
09.11.2011	12174,00	14875242	6627,00	18.06.2013	48967,00	1679554	23077,00	26.01.2015	236920,00	18020965	95324,00
10.11.2011	11557,00	6283628	6364,00	19.06.2013	55778,00	2757006	25385,00	27.01.2015	204121,00	3611594	91044,00
11.11.2011	10074,00	730366	5439,00	20.06.2013	54530,00	2234427	26140,00	28.01.2015	165874,00	3459853	85017,00
12.11.2011	10156,00	4342142	5346,00	21.06.2013	58295,00	1727293	26165,00	29.01.2015	171619,00	3823613	87193,00
13.11.2011	9589,00	369418	5088,00	22.06.2013	49708,00	1954581	21857,00	30.01.2015	167768,00	2523572	85068,00
14.11.2011	10726,00	4539422	5620,00	23.06.2013	41462,00	1981250	18203,00	31.01.2015	239182,00	3590169	82179,00
15.11.2011	11798,00	4146264	6442,00	24.06.2013	48326,00	3003280	21748,00	01.02.2015	208727,00	1774688	77506,00
16.11.2011	10639,00	52127501	5855,00	25.06.2013	50770,00	5172031	24782,00	02.02.2015	185554,00	3959118	81679,00
17.11.2011	10600,00	3121487	5596,00	26.06.2013	54518,00	4179178	26087,00	03.02.2015	207461,00	4546822	92194,00
18.11.2011	9438,00	5101809	4818,00	27.06.2013	51936,00	4194626	24892,00	04.02.2015	198955,00	2586867	89353,00
19.11.2011	8745,00	3541108	3927,00	28.06.2013	53524,00	4556438	26147,00	05.02.2015	181629,00	5882362	89051,00
20.11.2011	8068,00	3508423	3404,00	29.06.2013	55499,00	6895564	23586,00	06.02.2015	186259,00	3483740	81964,00
21.11.2011	8487,00	3282663	3607,00	30.06.2013	41271,00	3974842	19434,00	07.02.2015	180449,00	1814435	78776,00
22.11.2011	8795,00	5973371	3999,00	01.07.2013	49206,00	12991760	24137,00	08.02.2015	251391,00	1824963	73463,00
23.11.2011	8805,00	1393328	4161,00	02.07.2013	56769,00	9614523	29925,00	09.02.2015	197636,00	2775715	85756,00
24.11.2011	8310,00	3272310	3737,00	03.07.2013	53642,00	5503193	25803,00	10.02.2015	189629,00	3897878	87201,00
25.11.2011	9336,00	3982593	3973,00	04.07.2013	53347,00	7776154	26097,00	11.02.2015	189188,00	1974889	87389,00
26.11.2011	8122,00	3558624	3724,00	05.07.2013	47699,00	5762453	22418,00	12.02.2015	202264,00	3929339	86100,00
27.11.2011	8141,00	2570610	3508,00	06.07.2013	46957,00	5660865	22481,00	13.02.2015	256202,00	4291966	95533,00
28.11.2011	9939,00	8603686	4567,00	07.07.2013	37506,00	2590565	17764,00	14.02.2015	243646,00	2983381	90182,00
29.11.2011	11164,00	5591484	5331,00	08.07.2013	47647,00	1978383	23029,00	15.02.2015	295507,00	4217029	80391,00
30.11.2011	10512,00	1263353	4830,00	09.07.2013	54846,00	2723814	26041,00	16.02.2015	223579,00	2205958	87415,00
01.12.2011	11715,00	6505257	5198,00	10.07.2013	55835,00	8151396	26244,00	17.02.2015	226216,00	2533282	91708,00
02.12.2011	10589,00	1441619	4961,00	11.07.2013	56988,00	3090130	29490,00	18.02.2015	223247,00	1688999	95051,00
03.12.2011	9426,00	1135469	4169,00	12.07.2013	69663,00	5732529	33625,00	19.02.2015	181312,00	9163144	87029,00
04.12.2011	9094,00	4560606	3899,00	13.07.2013	57072,00	6363795	25977,00	20.02.2015	194679,00	2860483	87583,00
05.12.2011	10411,00	2970889	4689,00	14.07.2013	38740,00	1908589	17989,00	21.02.2015	248310,00	28112219	86038,00
06.12.2011	11341,00	1508497	5580,00	15.07.2013	46589,00	2048499	21699,00	22.02.2015	223159,00	1607521	77520,00
07.12.2011	10988,00	2434287	5695,00	16.07.2013	53761,00	3032388	25421,00	23.02.2015	215517,00	3351031	88993,00
08.12.2011	9481,00	6624823	4203,00	17.07.2013	54355,00	4000127	26069,00	24.02.2015	196851,00	3924482	97226,00
09.12.2011	9524,00	1211888	4090,00	18.07.2013	54308,00	3048957	26312,00	25.02.2015	194596,00	6289079	97116,00
10.12.2011	9793,00	687854	4234,00	19.07.2013	48100,00	2456794	24401,00	26.02.2015	189240,00	3612636	89371,00
11.12.2011	8549,00	2623714	3694,00	20.07.2013	44457,00	2902194	20029,00	27.02.2015	199935,00	3134154	93947,00
12.12.2011	8547,00	4755326	3475,00	21.07.2013	43487,00	2737885	21524,00	28.02.2015	238834,00	7196553	79240,00
13.12.2011	9008,00	791091	3910,00	22.07.2013	46082,00	3119065	22602,00	01.03.2015	229461,00	3372037	77863,00
14.12.2011	9943,00	1199161	3602,00	23.07.2013	54206,00	2870681	26085,00	02.03.2015	213896,00	17359481	92924,00
15.12.2011	8700,00	1596556	3972,00	24.07.2013	54521,00	2596908	26735,00	03.03.2015	216316,00	13756603	99109,00
16.12.2011	8365,00	2871455	3874,00	25.07.2013	51978,00	3639587	26580,00	04.03.2015	211468,00	8149254	96428,00
17.12.2011	7780,00	895149	3386,00	26.07.2013	55955,00	2641241	27299,00	05.03.2015	195590,00	7566509	87646,00

18.12.2011	7873,00	618547	3297,00	27.07.2013	42750,00	1465542	21881,00	06.03.2015	199410,00	10737128	90351,00
19.12.2011	8828,00	6701570	3845,00	28.07.2013	37554,00	2051227	18416,00	07.03.2015	222227,00	7702042	85542,00
20.12.2011	10966,00	5997430	5116,00	29.07.2013	54397,00	6300665	26191,00	08.03.2015	213398,00	17079274	75981,00
21.12.2011	9328,00	1606610	4158,00	30.07.2013	55581,00	4652952	27480,00	09.03.2015	201698,00	10987858	86735,00
22.12.2011	9669,00	1228793	4263,00	31.07.2013	69550,00	5676468	33198,00	10.03.2015	210072,00	4265199	101305,00
23.12.2011	9685,00	1023275	4255,00	01.08.2013	82370,00	3867734	31084,00	11.03.2015	208179,00	24380041	95980,00
24.12.2011	7849,00	1518191	3302,00	02.08.2013	84776,00	5208974	33698,00	12.03.2015	193924,00	12841387	92444,00
25.12.2011	8775,00	813670	3773,00	03.08.2013	53305,00	32422936	25934,00	13.03.2015	198297,00	7510415	87615,00
26.12.2011	9053,00	3079677	3868,00	04.08.2013	46413,00	1627222	20226,00	14.03.2015	219463,00	1228391	80884,00
27.12.2011	9312,00	889486	4149,00	05.08.2013	57924,00	4185528	25770,00	15.03.2015	222639,00	2383368	73041,00
28.12.2011	8289,00	2509289	3564,00	06.08.2013	61468,00	2112225	27939,00	16.03.2015	206461,00	3273818	85728,00
29.12.2011	8731,00	1643701	3703,00	07.08.2013	64048,00	2854526	28170,00	17.03.2015	199845,00	5031826	93255,00
30.12.2011	8353,00	1397811	3544,00	08.08.2013	61019,00	3932917	28609,00	18.03.2015	191204,00	5308744	89818,00
31.12.2011	8668,00	1113701	3779,00	09.08.2013	57904,00	3348040	25338,00	19.03.2015	190851,00	5358786	89798,00
01.01.2012	7701,00	6562833	3052,00	10.08.2013	52564,00	2089614	23776,00	20.03.2015	198449,00	3011239	93346,00
02.01.2012	9669,00	3718986	4239,00	11.08.2013	43679,00	3419148	19500,00	21.03.2015	218099,00	3813896	83857,00
03.01.2012	9207,00	1654156	3966,00	12.08.2013	70581,00	4578669	27001,00	22.03.2015	214152,00	2024403	76544,00
04.01.2012	9255,00	2276381	4012,00	13.08.2013	75208,00	25193134	33947,00	23.03.2015	221091,00	2524861	92109,00
05.01.2012	11542,00	3409898	5125,00	14.08.2013	60659,00	4532415	31876,00	24.03.2015	185435,00	3327068	88390,00
06.01.2012	11043,00	3348300	5175,00	15.08.2013	66433,00	6341354	32388,00	25.03.2015	182792,00	3765986	88646,00
07.01.2012	9902,00	2339391	4186,00	16.08.2013	69457,00	2508367	32176,00	26.03.2015	188107,00	3180340	89463,00
08.01.2012	10516,00	1945637	4472,00	17.08.2013	58546,00	5850534	28976,00	27.03.2015	202290,00	4879560	94188,00
09.01.2012	10229,00	3393232	4323,00	18.08.2013	42791,00	2372792	25899,00	28.03.2015	208232,00	1945972	83161,00
10.01.2012	11080,00	2226356	4859,00	19.08.2013	65506,00	3070676	29673,00	29.03.2015	228699,00	1334060	78466,00
11.01.2012	12031,00	3581516	5299,00	20.08.2013	69460,00	3123578	35589,00	30.03.2015	202713,00	2820249	92978,00
12.01.2012	11184,00	2471006	5002,00	21.08.2013	70761,00	5894709	37681,00	31.03.2015	203189,00	2076885	98965,00
13.01.2012	11096,00	9261642	5197,00	22.08.2013	70737,00	3533664	37527,00	01.04.2015	241041,00	5454483	115358,00
14.01.2012	10567,00	2271629	4846,00	23.08.2013	68764,00	3474402	34078,00	02.04.2015	214884,00	12206603	104713,00
15.01.2012	11200,00	2697420	4941,00	24.08.2013	54649,00	1850930	27218,00	03.04.2015	195509,00	9519647	94497,00
16.01.2012	11207,00	2029204	4816,00	25.08.2013	48105,00	1162536	24835,00	04.04.2015	228536,00	2082078	84096,00
17.01.2012	11033,00	3190623	4725,00	26.08.2013	57471,00	3053308	31010,00	05.04.2015	222020,00	1410388	81030,00
18.01.2012	11962,00	2767022	5311,00	27.08.2013	71151,00	2891789	36873,00	06.04.2015	189967,00	1897220	88792,00
19.01.2012	10970,00	1391607	4664,00	28.08.2013	72494,00	2924753	36209,00	07.04.2015	220417,00	2597994	102214,00
20.01.2012	11045,00	3023294	4863,00	29.08.2013	67844,00	10583999	32714,00	08.04.2015	214628,00	3708696	101474,00
21.01.2012	10759,00	993760	4714,00	30.08.2013	72629,00	4271283	35621,00	09.04.2015	203465,00	5018546	103426,00
22.01.2012	8918,00	867978	3496,00	31.08.2013	82290,00	4539244	33954,00	10.04.2015	215133,00	3050381	105399,00
23.01.2012	10161,00	1392832	4095,00	01.09.2013	49046,00	3879262	27222,00	11.04.2015	243573,00	9920298	96631,00
24.01.2012	11338,00	1009730	5103,00	02.09.2013	52118,00	4571007	28807,00	12.04.2015	193479,00	3351575	88884,00
25.01.2012	12942,00	2267439	6243,00	03.09.2013	54757,00	5550075	32641,00	13.04.2015	232236,00	3392506	96153,00
26.01.2012	11098,00	3500305	4843,00	04.09.2013	58274,00	4871485	34303,00	14.04.2015	219510,00	3150050	101712,00
27.01.2012	10852,00	1722206	4931,00	05.09.2013	63542,00	2777562	37741,00	15.04.2015	190441,00	15676397	95743,00
28.01.2012	10498,00	1966085	4323,00	06.09.2013	57620,00	2098478	35505,00	16.04.2015	196262,00	3429711	95847,00
29.01.2012	10772,00	1349666	4611,00	07.09.2013	56635,00	3076006	34405,00	17.04.2015	191876,00	2421062	93893,00
30.01.2012	10175,00	1696857	4139,00	08.09.2013	43712,00	1996776	26077,00	18.04.2015	225102,00	1268569	89058,00
31.01.2012	11376,00	1559872	4637,00	09.09.2013	53474,00	3024540	33571,00	19.04.2015	168858,00	896722	77576,00
01.02.2012	11855,00	1411727	5071,00	10.09.2013	55161,00	8414363	34709,00	20.04.2015	253148,00	1547926	104049,00
02.02.2012	12071,00	2590868	5113,00	11.09.2013	58672,00	2881307	35535,00	21.04.2015	205286,00	2936001	114061,00
03.02.2012	12407,00	1305632	5156,00	12.09.2013	65300,00	4463375	38697,00	22.04.2015	222085,00	4728504	106012,00
04.02.2012	12959,00	1824316	5774,00	13.09.2013	59829,00	6986801	34662,00	23.04.2015	212819,00	53954298	101207,00
05.02.2012	11232,00	1165811	5084,00	14.09.2013	48712,00	5404479	28979,00	24.04.2015	205205,00	2055625	102383,00
06.02.2012	10914,00	2040204	4576,00	15.09.2013	42924,00	2870683	28348,00	25.04.2015	242148,00	2003605	94093,00
07.02.2012	10983,00	1616906	5090,00	16.09.2013	52304,00	2331655	33155,00	26.04.2015	226263,00	3614064	86025,00
08.02.2012	11209,00	1191800	5078,00	17.09.2013	61057,00	3311134	42021,00	27.04.2015	203028,00	5121156	101588,00
09.02.2012	11806,00	850106	5536,00	18.09.2013	65538,00	6402238	43705,00	28.04.2015	218502,00	2564413	106587,00
10.02.2012	12310,00	2079160	6905,00	19.09.2013	66398,00	11008778	41152,00	29.04.2015	207741,00	3895363	106124,00
11.02.2012	12079,00	1417483	6032,00	20.09.2013	65306,00	2171813	40460,00	30.04.2015	215077,00	2049652	108264,00
12.02.2012	11301,00	12901438	5663,00	21.09.2013	58758,00	2746292	36353,00	01.05.2015	197072,00	2340154	97071,00
13.02.2012	12245,00	1633027	5857,00	22.09.2013	53993,00	4132847	33215,00	02.05.2015	238390,00	1365131	86271,00
14.02.2012	14695,00	29745958	8100,00	23.09.2013	62037,00	2455737	38353,00	03.05.2015	212123,00	1720175	79473,00
15.02.2012	14215,00	1783444	7802,00	24.09.2013	65845,00	3457666	41262,00	04.05.2015	190201,00	4538615	88545,00
16.02.2012	14299,00	1690353	7743,00	25.09.2013	66539,00	3129874	40337,00	05.05.2015	219068,00	3466805	107830,00
17.02.2012	11991,00	2305049	5566,00	26.09.2013	63157,00	3679305	38352,00	06.05.2015	219506,00	1887906	107858,00
18.02.2012	11605,00	2589055	5024,00	27.09.2013	66494,00	2902645	36560,00	07.05.2015	227324,00	2700742	107329,00
19.02.2012	10536,00	982196	4286,00	28.09.2013	60434,00	1632110	31425,00	08.05.2015	261673,00	2796155	101732,00
20.02.2012	10712,00	1135312	4510,00	29.09.2013	54587,00	2875775	28026,00	09.05.2015	199251,00	2360970	92434,00
21.02.2012	11125,00	1137600	4767,00	30.09.2013	61734,00	2708390	32223,00	10.05.2015	213909,00	1630861	83644,00
22.02.2012	12333,00	1599707	5474,00	01.10.2013	69975,00	3742086	39079,00	11.05.2015	215628,00	6185156	96515,00
23.02.2012	13080,00	1817974	6051,00	02.10.2013	77571,00	7379002	42584,00	12.05.2015	233523,00	4242824	109297,00
24.02.2012	12673,00	1953427	5558,00	03.10.2013	72720,00	7610109	41357,00	13.05.2015	211323,00	2689446	101967,00
25.02.2012	11532,00	2904644	4910,00	04.10.2013	64698,00	1587524	35360,00	14.05.2015	201739,00	2433288	93903,00
26.02.2012	10278,00	871877	4227,00	05.10.2013	55710,00	2066846	31381,00	15.05.2015	209999,00	3818660	99964,00
27.02.2012	11131,00	1347437	4684,00	06.10.2013	48783,00	3832244	26177,00	16.05.2015	236081,00	1617558	85085,00
28.02.2012	11726,00	1645416	5029,00	07.10.2013	58652,00	11620203	30100,00	17.05.2015	216412,00	1485375	77481,00

29.02.2012	12087,00	1185771	5096,00	08.10.2013	60475,00	9320239	34291,00	18.05.2015	197816,00	2037401	90495,00
01.03.2012	12079,00	7097686	5123,00	09.10.2013	69133,00	5924464	38692,00	19.05.2015	207126,00	4961633	99347,00
02.03.2012	13152,00	2245600	6031,00	10.10.2013	65216,00	4764026	36547,00	20.05.2015	221491,00	2585580	101313,00
03.03.2012	10220,00	3274616	4378,00	11.10.2013	67974,00	2140026	37937,00	21.05.2015	203159,00	2394648	95717,00
04.03.2012	11319,00	2074557	4531,00	12.10.2013	58649,00	2815544	33344,00	22.05.2015	207671,00	2209801	94416,00
05.03.2012	12425,00	1248054	5305,00	13.10.2013	57180,00	2098856	31479,00	23.05.2015	194783,00	8345933	83932,00
06.03.2012	11913,00	1456010	4916,00	14.10.2013	74721,00	3794965	36518,00	24.05.2015	246182,00	1715057	81001,00
07.03.2012	11591,00	1343998	4828,00	15.10.2013	70171,00	3568751	37753,00	25.05.2015	206424,00	1727715	96824,00
08.03.2012	12250,00	1680063	4983,00	16.10.2013	74562,00	6232447	39527,00	26.05.2015	222322,00	4188824	100829,00
09.03.2012	11826,00	1381641	4806,00	17.10.2013	68607,00	11623202	35519,00	27.05.2015	221553,00	3776426	102986,00
10.03.2012	10915,00	2248267	4443,00	18.10.2013	69519,00	5097023	42341,00	28.05.2015	220123,00	4578889	104001,00
11.03.2012	9925,00	2234383	3726,00	19.10.2013	75457,00	7459764	40260,00	29.05.2015	237083,00	4454491	112775,00
12.03.2012	10385,00	1072259	4053,00	20.10.2013	64030,00	4166087	33432,00	30.05.2015	269743,00	14494770	125827,00
13.03.2012	12352,00	1959196	5183,00	21.10.2013	73341,00	38920639	40197,00	31.05.2015	238007,00	2588787	90007,00
14.03.2012	12273,00	2011571	5482,00	22.10.2013	89356,00	19994442	47416,00	01.06.2015	252174,00	5065880	109364,00
15.03.2012	12046,00	2205914	5130,00	23.10.2013	87179,00	15404789	42721,00	02.06.2015	257275,00	6185215	126303,00
16.03.2012	11928,00	3882634	5036,00	24.10.2013	88605,00	12140540	46979,00	03.06.2015	239702,00	3432415	114926,00
17.03.2012	13116,00	1642471	5670,00	25.10.2013	82770,00	57050042	43703,00	04.06.2015	240222,00	3146840	117311,00
18.03.2012	10606,00	3890866	4248,00	26.10.2013	67249,00	4417519	34869,00	05.06.2015	232715,00	2869997	103094,00
19.03.2012	11743,00	1905569	5057,00	27.10.2013	54418,00	3788068	30090,00	06.06.2015	244636,00	1283152	93425,00
20.03.2012	11698,00	2418829	4964,00	28.10.2013	63786,00	4236872	34629,00	07.06.2015	225189,00	3014378	84280,00
21.03.2012	12291,00	3265569	5376,00	29.10.2013	70275,00	7081000	38140,00	08.06.2015	188952,00	2234200	91751,00
22.03.2012	12360,00	1529387	5184,00	30.10.2013	77520,00	4222302	38560,00	09.06.2015	208925,00	2849521	111830,00
23.03.2012	10829,00	3889295	4796,00	31.10.2013	77578,00	5687660	38478,00	10.06.2015	267864,00	4860855	123557,00
24.03.2012	11385,00	2230373	4929,00	01.11.2013	72946,00	5695578	35575,00	11.06.2015	258189,00	3716028	116693,00
25.03.2012	10821,00	1343850	4515,00	02.11.2013	69196,00	3910908	35652,00	12.06.2015	247460,00	8957078	113864,00
26.03.2012	11226,00	1501218	4874,00	03.11.2013	63309,00	2302430	30351,00	13.06.2015	246532,00	3135500	104241,00
27.03.2012	11432,00	1823193	4990,00	04.11.2013	77104,00	7376880	38141,00	14.06.2015	223880,00	3741570	94046,00
28.03.2012	12371,00	1507640	5550,00	05.11.2013	93462,00	19598967	45732,00	15.06.2015	277522,00	2675609	112459,00
29.03.2012	12719,00	1846014	6073,00	06.11.2013	101631,00	11701348	48151,00	16.06.2015	241825,00	7429264	117904,00
30.03.2012	12480,00	15554864	5688,00	07.11.2013	104142,00	16520300	53470,00	17.06.2015	256567,00	6877483	125228,00
31.03.2012	11040,00	1360996	4799,00	08.11.2013	107930,00	13955926	53584,00	18.06.2015	233829,00	4480226	113931,00
01.04.2012	9586,00	971741	4221,00	09.11.2013	108461,00	15516547	53728,00	19.06.2015	247406,00	8912165	115154,00
02.04.2012	10766,00	1264807	4676,00	10.11.2013	97886,00	10975129	44438,00	20.06.2015	246533,00	7170780	100133,00
03.04.2012	13073,00	4956464	5962,00	11.11.2013	86543,00	11266570	44441,00	21.06.2015	224267,00	10036801	85165,00
04.04.2012	12774,00	3051368	5980,00	12.11.2013	95747,00	16771019	48485,00	22.06.2015	204152,00	2120377	105432,00
05.04.2012	11946,00	1586323	5552,00	13.11.2013	100090,00	11581259	51452,00	23.06.2015	271463,00	3530451	121894,00
06.04.2012	12300,00	4124362	5402,00	14.11.2013	113020,00	21247342	56284,00	24.06.2015	218529,00	5394402	110435,00
07.04.2012	11003,00	1802835	4755,00	15.11.2013	97415,00	19209754	50247,00	25.06.2015	199310,00	2580697	107281,00
08.04.2012	10863,00	1028625	4577,00	16.11.2013	97096,00	14448648	44994,00	26.06.2015	240437,00	4022541	111419,00
09.04.2012	10799,00	4201922	4610,00	17.11.2013	86411,00	14674476	40401,00	27.06.2015	258833,00	2875684	100268,00
10.04.2012	13688,00	2407006	6883,00	18.11.2013	130894,00	20030471	62847,00	28.06.2015	230750,00	1894427	89826,00
11.04.2012	13265,00	3908686	6055,00	19.11.2013	170367,00	28434094	85571,00	29.06.2015	224321,00	3488404	110573,00
12.04.2012	14415,00	7157253	6776,00	20.11.2013	141505,00	25393951	68797,00	30.06.2015	261770,00	5659018	144779,00
13.04.2012	12853,00	2712908	6243,00	21.11.2013	124584,00	10953014	63432,00	01.07.2015	250536,00	4327533	143673,00
14.04.2012	13306,00	1612221	6457,00	22.11.2013	140082,00	17036226	67820,00	02.07.2015	254259,00	4121324	130719,00
15.04.2012	12285,00	2492187	5919,00	23.11.2013	134532,00	16304778	65874,00	03.07.2015	270019,00	7824449	127989,00
16.04.2012	13624,00	3175684	6426,00	24.11.2013	103353,00	8883132	49377,00	04.07.2015	250207,00	1556735	104771,00
17.04.2012	14357,00	2184400	6827,00	25.11.2013	117870,00	39270729	60652,00	05.07.2015	241519,00	4038837	96444,00
18.04.2012	13860,00	2241347	6626,00	26.11.2013	145494,00	45989474	70916,00	06.07.2015	276989,00	9793057	143911,00
19.04.2012	13885,00	2042819	6306,00	27.11.2013	164541,00	26162062	85164,00	07.07.2015	295662,00	9532418	195298,00
20.04.2012	13626,00	2443497	6559,00	28.11.2013	180643,00	18768124	93911,00	08.07.2015	273054,00	11635298	197841,00
21.04.2012	14018,00	2215558	6260,00	29.11.2013	160752,00	22045193	83714,00	09.07.2015	263045,00	8600871	179359,00
22.04.2012	11561,00	2618295	5218,00	30.11.2013	150747,00	9682583	73917,00	10.07.2015	273833,00	7383926	213672,00
23.04.2012	12471,00	2315141	5268,00	01.12.2013	125448,00	8224263	61331,00	11.07.2015	278810,00	5189277	171529,00
24.04.2012	12541,00	2007917	5874,00	02.12.2013	144106,00	11841215	69250,00	12.07.2015	271999,00	9885963	204511,00
25.04.2012	13879,00	2653091	5710,00	03.12.2013	149257,00	8692444	71611,00	13.07.2015	232590,00	3703187	176542,00
26.04.2012	14567,00	19537035	5807,00	04.12.2013	150637,00	6047589	72687,00	14.07.2015	229381,00	3049779	119332,00
27.04.2012	12887,00	2333965	5582,00	05.12.2013	164289,00	8713087	78591,00	15.07.2015	234754,00	3616094	116425,00
28.04.2012	12306,00	1373341	5206,00	06.12.2013	140744,00	8175966	66006,00	16.07.2015	228231,00	4186749	111183,00
29.04.2012	12863,00	1008124	5285,00	07.12.2013	143645,00	10748912	68497,00	17.07.2015	214161,00	8148349	110715,00
30.04.2012	14525,00	4203520	5775,00	08.12.2013	95996,00	3707906	44771,00	18.07.2015	219461,00	3022172	105710,00
01.05.2012	15610,00	2179617	6009,00	09.12.2013	127647,00	3258274	54531,00	19.07.2015	242814,00	1592948	129223,00
02.05.2012	14824,00	1864622	5960,00	10.12.2013	128388,00	3875617	60322,00	20.07.2015	216715,00	2939104	105702,00
03.05.2012	17151,00	1945705	6624,00	11.12.2013	129666,00	8122054	60671,00	21.07.2015	240028,00	8168341	117682,00
04.05.2012	17877,00	2342666	7340,00	12.12.2013	113825,00	3074233	52110,00	22.07.2015	270355,00	2235904	143934,00
05.05.2012	16679,00	1362277	5582,00	13.12.2013	120982,00	5220155	53311,00	23.07.2015	207134,00	2826418	107076,00
06.05.2012	15598,00	2343484	5374,00	14.12.2013	113263,00	4427843	50023,00	24.07.2015	217981,00	2319273	106528,00
07.05.2012	19235,00	6081933	6812,00	15.12.2013	103782,00	7031942	47577,00	25.07.2015	201269,00	4212933	99402,00
08.05.2012	19674,00	1859026	6998,00	16.12.2013	137337,00	14075870	55917,00	26.07.2015	244803,00	3942039	85399,00
09.05.2012	20332,00	2925838	6874,00	17.12.2013	139023,00	5662288	65237,00	27.07.2015	229418,00	3646875	108188,00
10.05.2012	17330,00	2912658	6232,00	18.12.2013	153222,00	18384616	72219,00	28.07.2015	240969,00	3180408	113425,00
11.05.2012	17977,00	2063025	6418,00	19.12.2013	134257,00	6465511	61379,00	29.07.2015	255290,00	4459915	132097,00

12.05.2012	21047,00	1484870	5599,00	20.12.2013	125004,00	4504023	59721,00	30.07.2015	247799,00	2527083	128885,00
13.05.2012	16837,00	17657803	5044,00	21.12.2013	110306,00	134084959	49099,00	31.07.2015	232699,00	3332717	124065,00
14.05.2012	26853,00	5559397	7296,00	22.12.2013	98559,00	1464744	42186,00	01.08.2015	275871,00	4100425	156306,00
15.05.2012	22051,00	4717841	6782,00	23.12.2013	105307,00	4947159	44607,00	02.08.2015	248553,00	2227637	93462,00
16.05.2012	20909,00	1861385	6147,00	24.12.2013	135360,00	3382734	48392,00	03.08.2015	226079,00	2606815	114769,00
17.05.2012	17048,00	4855754	5647,00	25.12.2013	120437,00	30883621	48430,00	04.08.2015	265834,00	2682764	129710,00
18.05.2012	20911,00	3347920	6235,00	26.12.2013	97504,00	2759956	41892,00	05.08.2015	250494,00	5552656	127347,00
19.05.2012	28460,00	4121009	5229,00	27.12.2013	115404,00	9732296	47287,00	06.08.2015	247781,00	1877936	129396,00
20.05.2012	25560,00	3054837	5209,00	28.12.2013	95474,00	2284141	40315,00	07.08.2015	242234,00	3144410	119389,00
21.05.2012	23727,00	3155344	5527,00	29.12.2013	93084,00	2621601	39438,00	08.08.2015	233508,00	7690993	99688,00
22.05.2012	22830,00	5480705	6701,00	30.12.2013	130692,00	1696030	47795,00	09.08.2015	218499,00	40746164	82199,00
23.05.2012	23849,00	3802939	6460,00	31.12.2013	108166,00	2797668	46174,00	10.08.2015	220994,00	8034558	103390,00
24.05.2012	22814,00	1261258	5904,00	01.01.2014	83356,00	2076517	33625,00	11.08.2015	227498,00	4038934	110280,00
25.05.2012	24436,00	3301470	6180,00	02.01.2014	103246,00	3954542	42112,00	12.08.2015	232055,00	3173876	109091,00
26.05.2012	21295,00	3236377	5509,00	03.01.2014	125864,00	3991406	56617,00	13.08.2015	226126,00	3627874	111008,00
27.05.2012	19795,00	2278812	4970,00	04.01.2014	103502,00	12073956	46386,00	14.08.2015	220370,00	6544553	104109,00
28.05.2012	24424,00	2016790	5358,00	05.01.2014	106688,00	7537719	48192,00	15.08.2015	245458,00	2945460	101858,00
29.05.2012	26445,00	1978490	7487,00	06.01.2014	152700,00	3824590	60826,00	16.08.2015	228284,00	5647310	84478,00
30.05.2012	23184,00	1695022	6679,00	07.01.2014	121152,00	4240526	55344,00	17.08.2015	230212,00	5437215	105299,00
31.05.2012	21952,00	1270202	7082,00	08.01.2014	129583,00	8066486	55054,00	18.08.2015	244699,00	3745384	116238,00
01.06.2012	23238,00	15009488	6637,00	09.01.2014	114730,00	2415052	50774,00	19.08.2015	247961,00	8515347	119064,00
02.06.2012	18762,00	1586776	5625,00	10.01.2014	112691,00	2679764	49153,00	20.08.2015	222182,00	6782670	113433,00
03.06.2012	22565,00	2191149	5991,00	11.01.2014	110670,00	4180310	48970,00	21.08.2015	235230,00	4180310	113062,00
04.06.2012	32189,00	4579599	6048,00	12.01.2014	98958,00	13517660	42175,00	22.08.2015	259239,00	4191219	104099,00
05.06.2012	34449,00	2677442	7516,00	13.01.2014	110334,00	4725219	47711,00	23.08.2015	247407,00	2910619	88760,00
06.06.2012	20500,00	3008873	6916,00	14.01.2014	133541,00	3999478	49932,00	24.08.2015	237850,00	28078520	111842,00
07.06.2012	26044,00	1793527	7171,00	15.01.2014	115087,00	9212176	51934,00	25.08.2015	245539,00	7718331	117845,00
08.06.2012	23625,00	2107069	7227,00	16.01.2014	110024,00	4891360	49623,00	26.08.2015	243215,00	39189034	120364,00
09.06.2012	24654,00	1403658	6554,00	17.01.2014	113632,00	3332107	49365,00	27.08.2015	232198,00	7006227	111998,00
10.06.2012	26535,00	871671	6338,00	18.01.2014	95634,00	2084893	44588,00	28.08.2015	243840,00	4383864	114654,00
11.06.2012	27456,00	2189550	6356,00	19.01.2014	94782,00	3235536	41985,00	29.08.2015	250584,00	3402426	106197,00
12.06.2012	18916,00	2375955	7020,00	20.01.2014	144276,00	4515816	51466,00	30.08.2015	229116,00	4504434	88602,00
13.06.2012	35054,00	2974287	7098,00	21.01.2014	136930,00	4156436	60309,00	31.08.2015	238504,00	3019431	109165,00
14.06.2012	37395,00	2472316	7606,00	22.01.2014	131062,00	5453349	58564,00	01.09.2015	272866,00	5549818	130024,00
15.06.2012	39031,00	1596967	8641,00	23.01.2014	127975,00	2629008	55005,00	02.09.2015	230707,00	5052749	132339,00
16.06.2012	34580,00	2602425	9429,00	24.01.2014	127984,00	5272225	59895,00	03.09.2015	249811,00	6477807	134325,00
17.06.2012	30521,00	1454846	10008,00	25.01.2014	108098,00	3840341	47710,00	04.09.2015	209983,00	4435944	90818,00
18.06.2012	31363,00	2987414	9884,00	26.01.2014	107203,00	1439134	46710,00	05.09.2015	284893,00	2406262	127176,00
19.06.2012	30103,00	2800322	8462,00	27.01.2014	145032,00	4037745	54329,00	06.09.2015	253777,00	2613743	101418,00
20.06.2012	25912,00	4000836	8463,00	28.01.2014	135152,00	4152514	61216,00	07.09.2015	238459,00	3489547	108880,00
21.06.2012	22814,00	4662364	8018,00	29.01.2014	124466,00	4371707	56810,00	08.09.2015	280276,00	2898789	123535,00
22.06.2012	23645,00	2730087	8403,00	30.01.2014	129214,00	3252381	55026,00	09.09.2015	265428,00	4068814	125800,00
23.06.2012	22670,00	1520029	8191,00	31.01.2014	132531,00	2350012	56192,00	10.09.2015	235288,00	18401319	120592,00
24.06.2012	21800,00	6410212	7179,00	01.02.2014	123558,00	4865914	50171,00	11.09.2015	252398,00	2183400	161565,00
25.06.2012	25287,00	2625483	9685,00	02.02.2014	112877,00	2191838	44915,00	12.09.2015	258271,00	1590446	150249,00
26.06.2012	30371,00	3222222	13495,00	03.02.2014	152868,00	1827417	51992,00	13.09.2015	279964,00	1611945	133887,00
27.06.2012	29665,00	1527051	14690,00	04.02.2014	140332,00	4210232	59321,00	14.09.2015	234525,00	1734158	159347,00
28.06.2012	27355,00	2316724	12121,00	05.02.2014	139743,00	13208015	62067,00	15.09.2015	263932,00	4330831	161192,00
29.06.2012	25246,00	1297001	12605,00	06.02.2014	142991,00	138634893	63678,00	16.09.2015	261990,00	3109638	165564,00
30.06.2012	27258,00	1913905	13953,00	07.02.2014	143818,00	6307031	65766,00	17.09.2015	250985,00	2865606	238266,00
01.07.2012	23260,00	1472890	11476,00	08.02.2014	131014,00	1959709	57867,00	18.09.2015	273195,00	2354306	180020,00
02.07.2012	30158,00	1616916	15888,00	09.02.2014	112334,00	3469666	52019,00	19.09.2015	230379,00	2820318	114515,00
03.07.2012	26804,00	2198875	12608,00	10.02.2014	155591,00	4147602	61132,00	20.09.2015	264443,00	1961529	101659,00
04.07.2012	24790,00	2291148	11814,00	11.02.2014	121449,00	5932979	57955,00	21.09.2015	285612,00	4371241	119372,00
05.07.2012	22083,00	2673476	9812,00	12.02.2014	121999,00	6004871	56760,00	22.09.2015	327724,00	11204308	132321,00
06.07.2012	22262,00	2324401	9044,00	13.02.2014	130490,00	2542128	59093,00	23.09.2015	250674,00	8766719	128069,00
07.07.2012	26033,00	2338224	14531,00	14.02.2014	148377,00	4638184	67449,00	24.09.2015	239053,00	2123435	119219,00
08.07.2012	22403,00	6281904	9436,00	15.02.2014	127810,00	2765394	55413,00	25.09.2015	255255,00	3364706	126908,00
09.07.2012	24678,00	2870465	11769,00	16.02.2014	110198,00	4110418	48370,00	26.09.2015	249080,00	1805978	115045,00
10.07.2012	30219,00	3123715	14253,00	17.02.2014	114626,00	2463685	50026,00	27.09.2015	251247,00	2109848	101501,00
11.07.2012	27370,00	22273956	12621,00	18.02.2014	163002,00	4964235	56375,00	28.09.2015	246314,00	5308320	126552,00
12.07.2012	27972,00	1616187	14729,00	19.02.2014	142987,00	5980716	59290,00	29.09.2015	267985,00	2546750	135138,00
13.07.2012	24266,00	3876820	12350,00	20.02.2014	159962,00	4535355	63613,00	30.09.2015	272223,00	4356216	136404,00
14.07.2012	24426,00	15859221	12889,00	21.02.2014	165370,00	5557046	67627,00	01.10.2015	247211,00	4154593	132272,00
15.07.2012	24339,00	1841186	11599,00	22.02.2014	132542,00	1428208	53496,00	02.10.2015	254192,00	3316045	132606,00
16.07.2012	28370,00	3741008	12849,00	23.02.2014	142019,00	1866988	52230,00	03.10.2015	234800,00	3746627	129718,00
17.07.2012	33380,00	15404081	15490,00	24.02.2014	167219,00	7588410	62090,00	04.10.2015	261675,00	1773092	98648,00
18.07.2012	27537,00	4810063	12195,00	25.02.2014	208180,00	12955451	77494,00	05.10.2015	226632,00	3981539	115131,00
19.07.2012	28008,00	4539221	11908,00	26.02.2014	166920,00	3006261	66512,00	06.10.2015	249199,00	3895081	140787,00
20.07.2012	28822,00	2364798	14058,00	27.02.2014	164199,00	3388086	65279,00	07.10.2015	239250,00	13892084	136497,00
21.07.2012	31248,00	3687205	15535,00	28.02.2014	145830,00	11339608	64477,00	08.10.2015	265540,00	4892644	136722,00
22.07.2012	28132,00	2390146	14143,00	01.03.2014	151446,00	9888843	58109,00	09.10.2015	211096,00	2700805	117816,00
23.07.2012	35299,00	2726280	16667,00	02.03.2014	139563,00	5061433	51306,00	10.10.2015	278854,00	2949225	127194,00

24.07.2012	29817,00	2523647	13623,00	03.03.2014	187106,00	7155425	65711,00	11.10.2015	234919,00	2564806	104281,00
25.07.2012	26521,00	2237551	12535,00	04.03.2014	201394,00	6905567	80405,00	12.10.2015	232117,00	9050528	124371,00
26.07.2012	25872,00	3695236	11699,00	05.03.2014	180104,00	7366268	66518,00	13.10.2015	235683,00	5332716	130340,00
27.07.2012	25871,00	1879028	11425,00	06.03.2014	171560,00	3511814	64869,00	14.10.2015	228578,00	4639614	133248,00
28.07.2012	31154,00	2568552	13889,00	07.03.2014	154757,00	173297972	63687,00	15.10.2015	307247,00	11641425	152540,00
29.07.2012	26862,00	1927607	11567,00	08.03.2014	154394,00	3644391	64748,00	16.10.2015	275882,00	3335756	139120,00
30.07.2012	30168,00	2949976	12850,00	09.03.2014	155361,00	3041495	56901,00	17.10.2015	313859,00	4500652	137027,00
31.07.2012	37314,00	4118769	17125,00	10.03.2014	164890,00	103622683	62205,00	18.10.2015	274902,00	2882514	116380,00
01.08.2012	38959,00	2478577	19278,00	11.03.2014	152037,00	17158834	69747,00	19.10.2015	266086,00	4415616	134440,00
02.08.2012	32741,00	3495048	15951,00	12.03.2014	165460,00	4012246	70451,00	20.10.2015	290886,00	6335003	135153,00
03.08.2012	29197,00	5087997	14362,00	13.03.2014	165883,00	6103123	70141,00	21.10.2015	309724,00	3125674	154119,00
04.08.2012	28179,00	4179002	14934,00	14.03.2014	139218,00	3346363	64302,00	22.10.2015	289944,00	7772552	146034,00
05.08.2012	28698,00	2030424	14297,00	15.03.2014	128219,00	1729680	61481,00	23.10.2015	281281,00	4002726	138481,00
06.08.2012	33954,00	3899731	16076,00	16.03.2014	121995,00	2002129	53512,00	24.10.2015	323968,00	2368270	137519,00
07.08.2012	32197,00	3497351	15315,00	17.03.2014	140722,00	3127371	60315,00	25.10.2015	278147,00	4012513	122953,00
08.08.2012	35918,00	7076636	15584,00	18.03.2014	140518,00	5343136	54012,00	27.10.2015	261476,00	5779483	125020,00
09.08.2012	34940,00	2710487	17203,00	19.03.2014	130586,00	4849642	58408,00				

Wikipedia Queries (Time period: January 2011 till August 2015)

Source: stats.grok.se

Per month	
Jan 10	335
Feb 10	514
Mar 10	503
Apr 10	1343
May 10	1335
Jun 10	2716
Jul 10	16263
Aug 10	1165
Sep 10	1177
Oct 10	1069
Nov 10	953
Dec 10	8449
Jan 11	6920
Feb 11	21664
Mar 11	30454
Apr 11	30561
May 11	183107
Jun 11	457542
Jul 11	155827
Aug 11	123432
Sep 11	65955
Oct 11	105622
Nov 11	74262
Dec 11	54987
Jan 12	112813
Feb 12	77329
Mar 12	65875
Apr 12	79557
May 12	71813
Jun 12	75428
Jul 12	84976
Aug 12	107139
Sep 12	150690
Oct 12	103632
Nov 12	74262
Dec 12	130059
Jan 13	160259
Feb 13	215498
Mar 13	624785
Apr 13	1346386
May 13	498762
Jun 13	75428
Jul 13	277149
Aug 13	266001
Sep 13	196280
Oct 13	588964
Nov 13	1318561
Dec 13	1491697
Jan 14	1046868
Feb 14	941499
Mar 14	885530
Apr 14	360928
May 14	259011
Jun 14	274419
Jul 14	216177
Aug 14	194422
Sep 14	224400
Oct 14	173454
Nov 14	224789
Dec 14	176937
Jan 15	176936
Feb 15	157646
Mar 15	2187508
Apr 15	183357
May 15	194172
Jun 15	274419
Jul 15	147993
Aug 15	151259

Per year	
2010	35822
2011	1310333
2012	1133573
2013	7059770
2014	4978434
Jan-Aug 2015	3473290

References

Abel, A.B., Bernanke, B. and Croushore, D. (2013), *Macroeconomics: Student Value Edition*, Pearson College Div.

Accenture (2016), *Blockchain-Enabled Distributed Ledgers: Are Investment Banks Ready?*

Adamovski, J. (2014), *France: Bitcoin Revenues Must be Declared to Tax Authorities*, available at: http://www.coindesk.com/france-bitcoin-revenues-must-declared-tax-authorities/ (accessed 9 September 2016).

Adams, C., Cain, P., Pinkas, D. and Zuccherato, R. (2001), *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, Network Working Group Category: Standards Track.

Adner, R. and Kapoor, R. (2010), "Value creation in innovation ecosystems: how the structure of technological interdependence affects firm performance in new technology generations", *Strategic Management Journal*, Vol. 31 No. 3, pp. 306–333.

Afuah, A. (2002), "Mapping technological capabilities into product markets and competitive advantage: the case of cholesterol drugs", *Strategic Management Journal*, Vol. 23 No. 2, pp. 171–179.

Agarwal, S. and Teas, R.K. (2004), "Cross-national applicability of a perceived risk-value model", *Journal of Product & Brand Management*, Vol. 13 No. 4, pp. 242–256.

Akerlof, G.A. (1970), "The Market for "Lemons". Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84 No. 3, p. 488.

Al Kawasmi, E., Arnautovic, E. and Svetinovic, D. (2015), "Bitcoin-Based Decentralized Carbon Emissions Trading Infrastructure Model", *Systems Engineering*, Vol. 18 No. 2, pp. 115–130.

Albergotti, R. and Sparshott, J. (2013), "U.S. Says Firm Laundered Billions. Digital-Currency Group Is Accused of Moving Illicit Cash for Hackers, Drug Dealers and Others", available at: http://www.wsj.com/articles/SB10001424127887323855804578511121238052256.

Alencar, F., Marín, B., Giachetti, G., Pastor, O., Castro, J. and Pimentel, J.H. (2009), "From i* Requirements Models to Conceptual Models of a Model Driven Development Process", in van der Aalst, W., Mylopoulos, J., Sadeh, N.M., Shaw, M.J., Szyperski, C., Persson, A. and Stirna, J. (Eds.), *The Practice of Enterprise Modeling*, *Lecture Notes in Business Information Processing*, Vol. 39, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 99–114.

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014), *The economics of digital currencies*.

Aljazzaf, Z.M., Perry, M. and Capretz, M.A.M. (2011), "Towards a unified trust framework for trust establishment and trust based service selection", Niagara Falls, ON, Canada.

Allen, B. (2013), *Bitcoins aren't tax exempt, Revenue Canada says*, available at: http://www.cbc.ca/news/business/bitcoins-aren-t-tax-exempt-revenue-canada-says-1.1395075.

Alpern, B. and Schneider, F.B. (1987), "Recognizing safety and liveness", *Distributed Computing*, Vol. 2 No. 3, pp. 117–126.

Aluko, A. and Bagheri, M. (2012), "The impact of money laundering on economic and financial stability and on political development in developing countries", *Journal of Money Laundering Control*, Vol. 15 No. 4, pp. 442–457.

Amazon (2016), "Amazon Coins", available at: http://www.amazon.de/gp/feature.html?ie=UTF8&docId=1000749413 (accessed 1 August 2016).

Amir, Y., Coan, B., Kirsch, J. and Lane, J. (2011), "Prime. Byzantine Replication under Attack", *IEEE Transactions on Dependable and Secure Computing*, Vol. 8 No. 4, pp. 564–577.

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S. (2013), "Evaluating User Privacy in Bitcoin", in Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G. and Sadeghi, A.-R. (Eds.), *Financial Cryptography and Data Security*, *Lecture Notes in Computer Science*, Vol. 7859, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 34–51.

ANSI (2005), *X9 X9.95-2005: Trusted Time Stamp Management and Security*.

Anton, A.I. (1996), "Goal-Based Requirements Analysis", in *Proceedings of the Second International Conference on Requirements Engineering: April 15-18, 1996, Colorado Springs, Colorado*, IEEE Computer Society Press, Los Alamitos, Calif.

Antonopoulos, A.M. (2015), *Mastering bitcoin: Unlocking digital cryptocurrencies,* First edition, O'Reilly, Sebastopol, CA.

Antonopoulou, K., Nandhakumar, J. and Panourgias, N. (2014), "Value Proposition for Digital Technology Innovations of Uncertain Market Potential", in *Twenty Second European Conference on Information Systems, Tel Aviv 2014*.

Apple (2016a), "Apple Pay - Official Website", available at: https://www.apple.com/apple-pay/ (accessed 22 July 2016).

Apple (2016b), "Apple Pay security and privacy overview", available at: https://support.apple.com/en-us/HT203027 (accessed 25 July 2017).

Apreda, R., Bonaccorsi, A., Fantoni, G. and Gabelloni, D. (2013), "Functions and failures: how to manage technological promises for societal challenges", *Technology Analysis & Strategic Management*, Vol. 26 No. 4, pp. 369–384.

Argentiero, A., Bagella, M. and Busato, F. (2008), "Money Laundering in a Two Sector Model: Using Theory for Measurement", *SSRN Electronic Journal*.

Aristoteles and Rackham, H. (1944), *Aristotle, The Loeb classical library*, Vol. 264, Reprinted with corrections, Harvard University press, Cambridge (Mass.), London.

Armstrong, M. (2006), "Competition in two-sided markets", *The RAND Journal of Economics*, Vol. 37 No. 3, pp. 668–691.

Armstrong, M. and Wright, J. (2007), "Two-sided Markets, Competitive Bottlenecks and Exclusive Contracts", *Economic Theory*, Vol. 32 No. 2, pp. 353–380.

Arrow, K.J. (2001), "Uncertainty and the Welfare Economics of Medical Care", *Journal of Health Politics, Policy and Law*, Vol. 26 No. 5, pp. 851–883.

Aschwanden, E. (2016), *Stadt Zug wird weltweit zum Bitcoin-Pionier*, available at: http://www.nzz.ch/schweiz/crypto-valley-zukunftsmodell-oder-marketing-gag-ld.22911 (accessed 9 September 2016).

Asokan, N., Janson, P.A., Steiner, M. and Waidner, M. (1997), "The state of the art in electronic payment systems", *Computer*, Vol. 30 No. 9, pp. 28–35.

Atzori, L., Iera, A. and Morabito, G. (2010), "The Internet of Things. A survey", *Computer Networks*, Vol. 54 No. 15, pp. 2787–2805.

Australian Government (2015), *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Australian Securities and Investments Commission (2014), *Senate inquiry into digital currency*.

Australian Taxation Office, A.T. (2014a), *ATO delivers guidance on Bitcoin*.

Australian Taxation Office, A.T. (2014b), *Tax treatment of crypto-currencies in Australia – specifically bitcoin*, available at: https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia--specifically-bitcoin/.

Australian Transaction Reports and Analysis Centre (2012), *Typologies and Case Studies Report 2012*, Australian Transaction Reports and Analysis Centre.

Back, A. (2002), *Hashcash - A Denial of Service Counter-Measure*.

Baddeley, M. (2004), "Using E-Cash in the New Economy: An Economic Analysis of Micropayment Systems", *Journal of Electronic Commerce Research*, Vol. 5 No. 4, pp. 239–253.

BaFin (2011), "Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz", available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html.

Bagella, M., Busato, F. and Argentiero, A. (2009), "Money Laundering in a Microfounded Dynamic Model: Simulations for the U.S. and the EU-15 Economies", *Review of Law & Economics*, Vol. 5 No. 2.

Bakos, Y. (1998), "The emerging role of electronic marketplaces on the Internet", *Communications of the ACM*, Vol. 41 No. 8, pp. 35–42.

Bank for International Settlements (2003), *A glossary of terms used in payments and settlement systems,* rev. ed., Bank for International Settlements, Basel.

Bank of Greece (2014), *Information on the use of virtual currency*.

Bao, J. (2011), "The analysis and strategy of information asymmetry in e-commerce", Shanghai, China.

Barber, S., Boyen, X., Shi, E. and Uzun, E. (2012), "Bitter to Better — How to Make Bitcoin a Better Currency", in Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G. and Keromytis, A.D. (Eds.), *Financial Cryptography and Data Security*, *Lecture Notes in Computer Science*, Vol. 7397, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 399–414.

Basel Committee on Banking Supervision (2014), *Sound management of risks related to money laundering and financing of terrorism,* Jan. 2014, Bank for International Settlements, Basel.

Basole, R.C. and Karla, J. (2011), "On the Evolution of Mobile Platform Ecosystem Structure and Strategy", *Business & Information Systems Engineering*, Vol. 3 No. 5, pp. 313–322.

Bauer, P. and Ullmann, R. (2001), "Understanding the Wash Cycle", *Economic Perspectives*, Vol. 6 No. 2, pp. 19–23.

Beck, R., Stenum Czepluch, J., Lollike, N., Malone, S. and (Keine Angabe) (2016), "Blockchain - The Gateway to Trust-Free Cryptographic Transactions", in *ECIS 2016 Completed Research Papers 2016*.

Becker, G. (1968), "Crime and Punishment: An Economic Approach", *The Journal of Political Economy*, Vol. 76 No. 2, pp. 169–217.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H.P. and Böhme, R. (2013), "Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency", in Böhme, R. (Ed.), *The Economics of Information Security and Privacy*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 135–156.

Beckers, K., Faßbender, S., Heisel, M. and Paci, F. (2013), "Combining Goal-Oriented and Problem-Oriented Requirements Engineering Methods", in Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Cuzzocrea, A., Kittl, C., Simos, D.E., Weippl, E. and Xu, L. (Eds.), *Availability, Reliability, and Security in Information Systems and HCI*, *Lecture Notes in Computer Science*, Vol. 8127, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 178–194.

Bentham, J. (1843), *Principles of penal law.*, W.Tait.

Berentsen, A. (2006), "On the private provision of fiat currency", *European Economic Review*, Vol. 50 No. 7, pp. 1683–1698.

Bishop, M. (2005), *Introduction to computer security*, Addison-Wesley, Boston.

bitcoinwiki (2016), "Controlled supply", available at: https://en.bitcoin.it/wiki/Controlled_supply#cite_note-2 (accessed 15 July 2016).

Bitnodes (2016), *Concentration of reachable Bitcoin nodes per Country*, available at: https://bitnodes.21.co/ (accessed 6 September 2016).

BitPay (2015), "BitPay - Website", available at: https://bitpay.com/ (accessed 12 September 2016).

Blanchard, O. and Johnson, D.R. (2013), *Macroeconomics,* 6. ed., Global ed., Pearson, Boston.

Blaze, M., Feigenbaum, J. and Keromytis, A.D. (1999), "KeyNote: Trust Management for Public-Key Infrastructures", in Goos, G., Hartmanis, J., van Leeuwen, J., Christianson, B., Crispo, B., Harbison, W.S. and Roe, M. (Eds.), *Security Protocols*, *Lecture Notes in Computer Science*, Vol. 1550, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 59–63.

Blizzard Entertainment (2015), "World of Warcraft - Die Konsequenzen des Goldkaufs", available at: http://eu.battle.net/wow/de/shop/anti-gold/ (accessed 6 April 2015).

Blizzard Entertainment (2016), "World of Warcraft - Offizielle Webseite", available at: http://eu.battle.net/wow/de/?- (accessed 1 August 2016).

Blockchain.info (2015), "Number of Transactions excluding Popular Adresses", available at: https://blockchain.info/charts/n-transactions-excluding-popular (accessed 14 October 2015).

Bogart, S. and Rice, K. (2015), *The Blockchain Report: Welcome to the Internet of Value*.

Böhle, K. and Riehm, U. (1998), "Elektronisches Geld und Internet-Zahlungssysteme - Innovationen, Mythen, Erklärungsversuche", *TA-Datenbank-Nachrichten*, No. 2, pp. 40–54.

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015), "Bitcoin. Economics, Technology, and Governance", *Journal of Economic Perspectives*, Vol. 29 No. 2, pp. 213–238.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A. and Felten, E.W. (2015), "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", San Jose, CA, USA.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A. and Felten, E.W. (2014), "Mixcoin: Anonymity for Bitcoin with Accountable Mixes", in Christin, N. and Safavi-Naini, R. (Eds.), *Financial Cryptography and Data Security*, *Lecture Notes in Computer Science*, Vol. 8437, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 486–504.

Borenstein, S., Jaske, M. and Rosenfeld, A. (2002), *Dynamic Pricing, Advanced Metering, and Demand Response in Electricity Markets*.

Bouckaert, B. and Geest, G. de (1992), *Bibliography of Law and Economics*, Springer Netherlands, Dordrecht.

Bouoiyour, J. and Selmi, R. (2014), "What Does Crypto-currency Look Like? Gaining Insight into Bitcoin Phenomenon", *Munich Personal RePEc Archive*.

Brandenburger, A.M. and Stuart, H.W. (1996), "Value-based Business Strategy", *Journal of Economics & Management Strategy*, Vol. 5 No. 1, pp. 5–24.

Brander, J.A., Amit, R. and Antweiler, W. (2002), "Venture-Capital Syndication. Improved Venture Selection vs. The Value-Added Hypothesis", *Journal of Economics Management Strategy*, Vol. 11 No. 3, pp. 423–452.

Brenig, C., Accorsi, R. and Müller, G. (2015), "Economic Analysis of Cryptocurrency Backed Money Laundering", in *ECIS 2015 Completed Research Papers*, Paper 20.

Brenig, C., Schwarz, J. and Rückeshäuser, N. (2016), "Value of Decentralized Consensus Systems - Evaluation Framework", in *ECIS 2016 Completed Research Papers 2016*.

Brenig, C., Schwarz, J. and Nolte, C.-G. (in review [a]), "Requirements for Decentralized Consensus Systems". *Submitted to ECIS2017 and currently in the review process.*

Brenig, C., Rückeshäuser, N. and Schwarz, J. (in review [b]), "Assessing the Potentials of Decentralized Consensus Systems: A Compliance Perspective". *Submitted to ECIS2017 and currently in the review process.*

Brezo, F. and Bringas, P.G. (2012), "Issues and Risks Associated with Cryptocurrencies such as Bitcoin", in Berntzen, L. and Dini, P. (Eds.), *SOTICS 2012: The second international conference on social eco-informatics, October 21-26, Venice, Italy*, IARIA, [S. l.], pp. 20–26.

Brito, J. and Castillo, A. (2013), *Bitcoin: A Primer for Policymakers*.

Brooks, G. (2012), "Online gambling and money laundering. "views from the inside"", *Journal of Money Laundering Control*, Vol. 15 No. 3, pp. 304–315.

Brown, R. (2015), "A Simple Model for Smart Contracts", available at: http://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/ (accessed 8 September 2016).

Bryans, D. (2014), "Bitcoin and Money Laundering: Mining for an Effective Solution", *Indiana Law Journal*, Vol. 89 No. Iss. 1, p. Article 13.

Brynjolfsson, E. and Hitt, L.M. (2000), "Beyond Computation: Information Technology, Organizational Transformation and Business Performance", *Journal of Economic Perspectives*, Vol. 14 No. 4, pp. 23–48.

Brynjolfsson, E. and McAfee, A. (2014), *The second machine age: Work, progress, and prosperity in a time of brilliant technologies,* First Edition, W. W. Norton & Company.

Btc-echo.de (2015), *Die Schweiz hat entschieden: Bitcoin unterliegt keiner Mehrwertsteuer*, available at: https://www.btc-echo.de/schweiz-bitcoin-unterliegt-keiner-mehrwertsteuer_2015061301/ (accessed 9 September 2016).

Buntinx, J.P. (2016), *Australian Regulators to Bring Bitcoin Under AML Laws*, available at: http://www.newsbtc.com/2016/05/05/australian-regulators-bring-bitcoin-aml-laws/.

Burnham, T.A., Frels, J.K. and Mahajan, V. (2003), "Consumer Switching Costs. A Typology, Antecedents, and Consequences", *Journal of the Academy of Marketing Science*, Vol. 31 No. 2, pp. 109–126.

Buterin, V. (2015), "On Public and Private Blockchains", available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed 9 September 2016).

Butterin, V. (2016), "Ethereum White Paper", available at: https://github.com/ethereum/wiki/wiki.

Caillaud, B. and Jullien, B. (2003), "Chicken & Egg. Competition among Intermediation Service Providers", *The RAND Journal of Economics*, Vol. 34 No. 2, p. 309.

Camp, L.J., Sirbu, M. and Tygar, J.D. (1995), "Token and notational money in electronic commerce", in *Usenix Workshop on Electronic Commerce*.

Campbell-Kelly, M., Garcia-Swartz, D., Lam, R. and Yang, Y. (2015), "Economic and business perspectives on smartphones as multi-sided platforms", *Telecommunications Policy*, Vol. 39 No. 8, pp. 717–734.

Canadian Minister of Finance (2014), *BILL C-31*, HOUSE OF COMMONS OF CANADA, available at: http://publications.gc.ca/collections/collection_2014/parl/XB412-31-1.pdf.

Capgemini and Royal Bank of Scotland (2014), *World Payments Report 2014*.

Casey, M.J. (2015), "Big Names Put Cash In Bitcoin Startup 21 Inc.", available at: http://www.wsj.com/articles/big-names-put-cash-in-bitcoin-startup-21-inc-1426029318 (accessed 29 October 2015).

Castells, M. (2000), *The information age,* 2. ed., Blackwell, Oxford, Malden, MA.

Castro, J., Kolp, M. and Mylopoulos, J. (2002), "Towards requirements-driven information systems engineering. The Tropos project", *Information Systems*, Vol. 27 No. 6, pp. 365–389.

Castro, M. and Liskov, B. (1999), "Practical Byzantine fault tolerance", in Seltzer, M. (Ed.), *Proceedings of the third symposium on Operating systems design and implementation*, USENIX Association, Berkeley, CA, pp. 173–186.

Central Bank of China (2013), "Prevention of Risks Associated with Bitcoin", available at: https://exchange.btcc.com/page/bocnotice2013.

Centre for Retail Research (2007), "Cheque Use and Payment Systems in UK Retailing", available at: http://www.retailresearch.org/downloads/PDF/Cheque%20Use%20and%20Payment%20Systems%20in%20UK%20Retailing.pdf (accessed 17 June 2016).

Chang, T.-Z. and Wildt, A.R. (1994), "Price, Product Information, and Purchase Intention: An Empirical Study", *Journal of the Academy of Marketing Science*, Vol. 22 No. 1, pp. 16–27.

Chaum, D. (1983), "Blind Signatures for Untraceable Payments", in Chaum, D., Rivest, R.L. and Sherman, A.T. (Eds.), *Advances in Cryptology*, Springer US, Boston, MA, pp. 199–203.

Chaum, D., Fiat, A. and Naor, M. (1990), "Untraceable Electronic Cash", in Goldwasser, S. (Ed.), *Advances in Cryptology — CRYPTO' 88*, *Lecture Notes in Computer Science*, Vol. 403, Springer New York, New York, NY, pp. 319–327.

Chen, M.-S., Wu, K.-L. and Yu, P.S. (1992), "Efficient decentralized consensus protocols in a distributed computing system", 9-12 June 1992, Yokohama, Japan.

Chen, S.C. and Dhillon, G.S. (2003), "Interpreting Dimensions of Consumer Trust in E-Commerce", *Information Technology and Management*, Vol. 4 No. 2/3, pp. 303–318.

Chesbrough, H. and Rosenbloom, R.S. (2002), "The role of the business model in capturing value from innovation. Evidence from Xerox Corporation's technology spin-off companies", *Industrial and Corporate Change*, Vol. 11 No. 3, pp. 529–555.

Chesbrough, H.W. (2003), "The Era of Open Innovation", *MIT Sloan Management Review*, Vol. 44 No. 3, pp. 35–41.

Chesbrough, H.W. and Appleyard, M.M. (2007), "Open Innovation and Strategy", *California Management Review*, Vol. 50 No. 1, pp. 57–76.

Chesbrough, H.W., Vanhaverbeke, W. and West, J. (2006), *Open innovation: Researching a new paradigm*, Oxford University Press, Oxford.

Chester, J. (2016), "Why Companies Like Orange Silicon Valley Are Working With Private Blockchain Startups", available at: http://www.forbes.com/sites/jonathanchester/2016/02/17/beyond-bitcoin-why-companies-like-orange-silicon-valley-are-working-with-blockchain-startups/#1534044b5ad4 (accessed 12 September 2016).

Chircu, A., Davis, G. and Kauffmann, R. (2000), "Trust, Expertise, and E-Commerce Intermediary Adoption", *AMCIS 2000 Proceedings, Paper 405*, pp. 710–716.

Christin, N. (2013), "Traveling the silk road: a measurement analysis of a large anonymous online marketplace", in Schwabe, D. (Ed.), *Proceedings of the 22nd international conference on World Wide Web*, International World Wide Web Conferences Steering Committee, [S.l.], pp. 213–224.

Chu, P. (2008), *Virtual currency: regulation and taxation issues*.

Clearmatics (2016), "Clearmatics - Official Website", available at: http://www.clearmatics.com/ (accessed 8 September 2016).

Clemons, E.K., Croson, D.C. and Weber, B.W. (1996), "Reengineering Money. The Mondex Stored Value Card and Beyond", *International Journal of Electronic Commerce*, Vol. 1 No. 2, pp. 5–31.

Cobben, M., Hofman, R. and van Santen, F. (2015), *Creating Value from Distributed Ledgers: Exploring the potential of the technology behind Bitcoin*.

Coindesk (2015), "Bitcoin Venture Capital", available at: http://www.coindesk.com/bitcoin-venture-capital/ (accessed 14 October 2015).

Coindesk.com (2014), *Is bitcoin legal?*, available at: http://www.coindesk.com/information/is-bitcoin-legal/ (accessed 9 September 2016).

Coindesk (2015). Bitcoin Price Index Chart. URL: http://www.coindesk.com/price/ (accessed 02 September 2015).

Coindesk.com (2016), *Australian Government Seeks End to Double Taxation of Bitcoin*, available at: http://www.coindesk.com/australian-government-seeks-end-to-double-taxation-of-bitcoin/ (accessed 9 September 2016).

CoinMarketCap (2016), "Crypto-Currency Market Capitalizations", available at: http://coinmarketcap.com/all/views/all/ (accessed 7 September 2016).

Dahlman, C. (2007), "Technology, globalization and international competitiveness: Challenges for developing Countries", in *Industrial Development for the 21st Century*, pp. 29–83.

Damodaran, A. (2012), *Investment valuation: Tools and techniques for determining the value of any asset, Wiley finance series,* 3rd ed., Wiley, Hoboken, New Jersey.

Dang, Q.H. (2015), *Secure Hash Standard*, National Institute of Standards and Technology.

D'Artis, K., Pavel, C. and Rajcaniova, M. (2015), *The Digital Agenda of Virtual Currencies: Can BitCoin Become a Global Currency?*, Publications Office of the European Union.

Dardenne, A., van Lamsweerde, A., Fickas, S. (1993): Goal-directed requirements acquisition. In: *Science of Computer Programming 20 (1-2)*, S. 3–50. DOI: 10.1016/0167-6423(93)90021-G.

Das, S. (2016), *Germany & Austria Fund a Bitcoin Financial Crime Research Project* (accessed 13 September 2016).

Davies, G. (2002), *A history of money: From ancient times to the present day,* 3rd ed., with revisions, University of Wales Press, Cardiff.

Dell (2016), "Dell now accepts bitcoin", available at: http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing?c=us&l=en&s=corp (accessed 29 August 2016).

Delmolino, K., Arnett, M., Kosba, A., Miller, A. and Shi, E. (2016), "Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab", in *3rd Workshop on Bitcoin and Blockchain Research (BITCOIN 2016)*, Barbados, February 2016.

Deloitte (2016a), *Blockchain: Enigma. Paradox. Opportunity*. Deloitte.

Deloitte (2016b), *Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality*, Deloitte.

Dennehy, J. (2015), "Ecuador launches new digital currency – but most residents know little about it", available at: https://www.theguardian.com/world/2015/feb/26/ecuador-digital-currency-dollar-rafael-correa (accessed 26 August 2016).

Department of the Treasury (2015), *National Money Laundering Risk Assessment 2015*.

Descôteaux, D. (2014), *How should Bitcoin be regulated?: Economic Note*.

Deutsche Bundesbank (2015), *Zahlungsverkehrs- und Wertpapierabwicklungsstatistiken in Deutschland 2010 - 2014*.

Diffie, W. and Hellman, M. (1976), "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol. 22 No. 6, pp. 644–654.

(2013), *Digital Signature Standard (DSS)*, National Institute of Standards and Technology.

Dillet, R. (2014), *Russia Says Bitcoin Should Be Avoided*, available at: https://techcrunch.com/2014/02/07/russia-bans-bitcoin/ (accessed 9 September 2016).

Dilley, B., Dawson, N. and Schutze, J. (2013), *Virtually Unregulated: Countering Virtual Currency Money Laundering in the 21st Century*.

Dini, P., Rathbone, N., Vidal, M., Hernandez, P., Ferronato, P., Briscoe, G. and Hendryx, S. (2005), *The Digital Ecosystems Research Vision: 2010 and Beyond*.

Dostov, V. and Shust, P. (2014), "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?", *Journal of Financial Crime*, Vol. 21 No. 3, pp. 249–263.

Douceur, J. (2002), "The Sybil Attack", in *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*.

Driscoll, K., Hall, B., Sivencrona, H. and Zumsteg, P. (2003), "Byzantine Fault Tolerance, from Theory to Reality", in Goos, G., Hartmanis, J., van Leeuwen, J., Anderson, S., Felici, M. and Littlewood, B. (Eds.), *Computer Safety, Reliability, and Security*, *Lecture Notes in Computer Science*, Vol. 2788, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 235–248.

DTCC (2016), *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*.

Duivestein, S., van Doorn, M., van Manen, T., Bloem, J. and van Ommeren, E. (2015), *Blockchain: cryptoplatform for a frictionless economy*.

Dutch Central Bank (2013), *Consumers should be aware of the risks of virtual currencies*.

Dutch Central Bank (2014), *Virtual currencies are not a viable alternative*.

Dutch Ministry of Finance (2013), *Reply of the Minister of Finance on questions asked by Nijboer (PvdA) to the Minister of Finance on the rise of Bitcoin and digital payments*.

Dwyer, G.P. (2015), "The economics of Bitcoin and similar private digital currencies", *Journal of Financial Stability*, Vol. 17, pp. 81–91.

Eckert, D. and Gotthold, K. (2013), *Bitcoin-Geschäfte nach einem Jahr steuerbefreit*, available at: https://www.welt.de/print/die_welt/finanzen/article117487737/Bitcoin-Geschaefte-nach-einem-Jahr-steuerbefreit.html (accessed 13 September 2016).

Eidgenossenschaft, S. (2014), *Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates*.

Ek, V. and Carlstrom, J. (2014), *Bitcoin Turns Into Art as Sweden Rejects Creative Currency*, available at: http://www.bloomberg.com/news/articles/2014-01-21/bitcoin-becomes-art-as-swedish-taxman-rejects-creative-currency (accessed 9 September 2016).

El Sawy, O.A. and Pereira, F. (Eds.) (2013), *Business Modelling in the Dynamic Digital Space, SpringerBriefs in Digital Spaces*, Springer Berlin Heidelberg, Berlin, Heidelberg.

Emiliy Flitter (2013), *U.S. accuses currency exchange of laundering $6 billion*, Reuters.

Eris (2016), "Eris - Official Website", available at: https://erisindustries.com/ (accessed 8 September 2016).

Ethereum (2015), "Ethereum - Official Website", available at: https://www.ethereum.org/ (accessed 8 September 2016).

Ethereum (2016), "State of the DApps", available at: http://dapps.ethercasts.com/ (accessed 12 September 2016).

Euroclear & Wyman (2016), *Blockchain in Capital Markets: The Prize and the Journey*.

European Banking Authority (2013), "EBA warns consumers on virtual currencies", available at: http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies (accessed 7 October 2014).

European Banking Authority (2014), "EBA Opinion on ‘ virtual currencies ’", No. July.

European Banking Authority (2015), *Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios 4 categories, 4 applications and 4 scenarios: An exploration for transaction banking and payments professionals*, EBA Working Group on Electronic and Alternative Payments.

European Central Bank (2012), *Virtual currency schemes*, European Central Bank, Frankfurt-on-Main.

European Central Bank (2015), *Virtual currency schemes: A further analysis*, European Central Bank, Frankfurt am Main.

European Central Bank (2016a), "Electronic Money", available at: https://www.ecb.europa.eu/stats/money/aggregates/emon/html/index.en.html (accessed 27 July 2016).

European Central Bank (2016b), “The ECB’s definition of euro area monetary aggregates”, available at: https://www.ecb.europa.eu/stats/money/aggregates/aggr/html/hist.en.html (accessed 7 June 2016).

European Parliament Research Service (2014), “Bitcoin: market, economics and regulation (Briefing)”, available at: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI%282014%29140793_REV1_EN.pdf (accessed 31 August 2016).

European Union (2005), “DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005. on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing”, *Official Journal of the European Union*, No. L 309/17.

European Union (2009), “DIRECTIVE 2009/110/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic moneyinstitutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC”, *Official Journal of the European Union*, No. L 267/7.

European Union (2012), “Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. 2012/C 326/01”, *Official Journal of the European Union*, Vol. 55.

Evans, D. (2003), “The antitrust economics of multi-sided platform markets”, *Yale Journal of Regulation*, Vol. 20 No. 2, pp. 325–381.

Evans, D.S. and Schmalensee, R. (2013), “The Antitrust Analysis of Multi-Sided Platform Businesses”, in Blair, R. and Sokol, D. (Eds.), *Oxford Handbook on International Antitrust Economics*, Oxford University Press, Forthcoming, p. University of Chicago Institute for Law & Economics Olin Research Paper No. 623.

Evans-Greenwood, P., Hillard, R., Harper, I. and Williams, P. (2016), *Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality*.

Evry (2015), *Blockchain: Powering the Internet of Value*.

EY (2016), *Blockchain technology as a platform for digitization: Implications for the insurance industry*.

Eyal, I. and Sirer, E.G. (2014), “Majority Is Not Enough: Bitcoin Mining Is Vulnerable”, in Christin, N. and Safavi-Naini, R. (Eds.), *Financial Cryptography and Data Security*, *Lecture Notes in Computer Science*, Vol. 8437, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 436–454.

Facebook (2011), “Expanding Facebook Credits”, available at: https://developers.facebook.com/blog/post/416 (accessed 20 March 2015).

Facebook (2012), “Introducing subscriptions and local currency pricing”, available at: https://developers.facebook.com/blog/post/2012/06/19/introducing-subscriptions-and-local-currency-pricing/ (accessed 20 March 2015).

Fairfield, J.A. (2014), “Smart Contracts, Bitcoin Bots, and Consumer Protection”, *Washington and Lee Law Review Online*, Vol. 71 No. 2.

Farber, S.C., Costanza, R. and Wilson, M.A. (2002), “Economic and ecological concepts for valuing ecosystem services”, *Ecological Economics*, Vol. 41 No. 3, pp. 375–392.

FBI (2012), *(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*, Federal Bureau of Investigation: Cyber Intelligence Section and Criminal Intelligence Section.

Federal Financial Institutions Examination Council (2014), *Bank Secrecy Act/ Anti-Money Laundering Examination Manual*, Federal Financial Institutions Examination Council.

Federal Reserve Financial Services (2013), *Payment System Improvement - Public Consultation Paper*, Federal Reserve Financial Services.

Federal Reserve System (2005), *The Federal Reserve System: Purposes and Functions*, Board of Governors of the Federal Reserve System, Washington D.C.

Ferwerda, J. (2009), “The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime?”, *Review of Law & Economics*, Vol. 5 No. 2.

Fiedler, I. (2013), “Online Gambling as a Game Changer to Money Laundering?”, *SSRN Electronic Journal*.

Fielder, S. and Light, J. (2015), *Distributed consensus ledgers for payments: How banks can realize the full opportunities of cryptocurrency technologies, including the blockchain, in payments*.

Filecoin (2014), “Filecoin: A Cryptocurrency Operated File Storage Network”, available at: http://filecoin.io/filecoin.pdf (accessed 8 September 2016).

Financial Action Task Force (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*.

Financial Action Task Force (2013), *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*.

Financial Action Task Force (2014), *Virtual Currencies Key Definitions and Potential AML/CFT Risks: FATF Report*.

Financial Crime Enforcement Network (2013), *FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities*.

Financial Crime Enforcement Network (2015), *Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals*.

Financial Stability Oversight Council, FSOC (2016), *Financial Stability Oversight Council*.

Financial Times (2016), "Definition of market capitalisation", available at: http://lexicon.ft.com/Term?term=market-capitalisation (accessed 4 August 2016).

FinCEN Advisory (2014), *Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML: FIN-2014-A005*.

Finextra (2016), "It's time to take a stand against all the blockchain crap out there", available at: http://www.finextra.com/news/fullstory.aspx?newsitemid=28328 (accessed 14 September 2016).

FINMA (2014), *Enforcement report 2014*.

Forklog.net (2015), *A Draft Bill Implying Bitcoin Legalization Introduced in the Russian Parliament*, available at: http://forklog.net/a-draft-bill-implying-bitcoin-legalization-introduced-in-the-russian-parliament/ (accessed 9 September 2016).

Franco, P. (2015), *Understanding bitcoin: Cryptography, engineering and economics, The Wiley finance series*, John Wiley & Sons, Chichester, West Sussex.

Frank, U. (2006), *Towards a Pluralistic Conception of Research Methods in Information Systems Research: ICB Research Report No.7*.

Frow, P., McColl-Kennedy, J.R., Hilton, T., Davidson, A., Payne, A. and Brozovic, D. (2014), "Value propositions. A service ecosystems perspective", *Marketing Theory*, Vol. 14 No. 3, pp. 327–351.

Gambetta, D. (2000), "Can We Trust Trust?", in Gambetta, D. (Ed.), *Trust: Making and Breaking Cooperative Relations*, pp. 213–237.

Garcia, D. and Schweitzer, F. (2015), "Social signals and algorithmic trading of Bitcoin", *Royal Society open science*, Vol. 2 No. 9, p. 150288.

Garcia Molina, H., Pittelli, F. and Davidson, S. (1986), "Applications of Byzantine agreement in database systems", *ACM Transactions on Database Systems*, Vol. 11 No. 1, pp. 27–47.

Garoupa, N.M. (1999), "Optimal Law Enforcement and Criminal Organization", *SSRN Electronic Journal*.

Gawer, A. and Henderson, R. (2007), "Platform Owner Entry and Innovation in Complementary Markets. Evidence from Intel", *Journal of Economics & Management Strategy*, Vol. 16 No. 1.

Gehring, B. (2014), "How Ripple Works", available at: https://ripple.com/knowledge_center/how-ripple-works/ (accessed 2 October 2015).

Geiger, H. and Wuensch, O. (2007), "The fight against money laundering", *Journal of Money Laundering Control*, Vol. 10 No. 1, pp. 91–105.

Geiling, L. (2016), *Distributed Ledger: The technology behind virtual currencies: the example of blockchain*.

George-Cosh, D. (2014), *Canada Says Bitcoin Isn't Legal Tender*, available at: http://blogs.wsj.com/canadarealtime/2014/01/16/canada-says-bitcoin-isnt-legal-tender/ (accessed 9 September 2016).

Germonprez, M. and Warner, B. (2013), "Organisational Participation in Open Innovation Communities", in Eriksson Lundström,Jenny S. Z, Wiberg, M., Hrastinski, S., Edenius, M. and Ågerfalk, P.J. (Eds.), *Managing Open Innovation Technologies*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 35–52.

Gervais, A., Karame, G.O., Capkun, V. and Capkun, S. (2014), "Is Bitcoin a Decentralized Currency?", *IEEE Security & Privacy*, Vol. 12 No. 3, pp. 54–60.

Giaglis, G.M. and Kypriotaki, K.N. (2014), "Towards an Agenda for Information Systems Research on Digital Currencies and Bitcoin", in Abramowicz, W. and Kokkinaki, A. (Eds.), *Business Information Systems Workshops*, *Lecture Notes in Business Information Processing*, Vol. 183, Springer International Publishing, Cham, pp. 3–13.

Giddings, F.H. (1891), "The Concepts of Utility, Value and Cost", in *Publications of the American Economic Association*, ½, pp. 41–43.

Gilson, D. (2013), *Bitcoin in the UK: HMRC suggests bitcoins are 'taxable vouchers'*, available at: http://www.coindesk.com/bitcoin-uk-hmrc-suggests-bitcoins-taxable-vouchers/ (accessed 9 September 2016).

Gischer, H., Herz, B. and Menkhoff, L. (2012), *Geld, Kredit und Banken*, Springer Berlin Heidelberg, Berlin, Heidelberg.

Glaser, F. and Bezzenberg, L. (2015), "Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems", in *23rd European Conference on Information Systems (ECIS), Münster, Germany, 2015*.

Glaser, F., Haferkorn, M., Moritz, C. and Zimmermann, K. (2014a), "How to price a digital currency? empirical insights on the influence of media coverage on the Bitcoin bubble", *Banking and information technology BIT; a strategic report for top management*, No. 15.2014, 1, pp. 21–32.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M.C. and Siering, M. (2014b), "Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions", in *Proceedings of the 22nd European Conference on Information Systems; Tel Aviv, Israel*.

GluuFederation (2016), “Yet to see a use case for blockchain that can’t be solved with an existing simpler technology Adi Shamir #RSAC, Twitter post”, available at: https://twitter.com/gluufederation/status/705125001880403968 (accessed 14 September 2016).

Gompers, P. and Lerner, J. (2001), “The Venture Capital Revolution”, *Journal of Economic Perspectives*, Vol. 15 No. 2, pp. 145–168.

Goodhart, C.A.E. (1989), *Money, information, and uncertainty,* [2nd ed.], MIT Press, Cambridge, Mass.

Google (2016), “Google Trends”, available at: https://www.google.de/trends/ (accessed 8 September 2016).

Goos, G., Hartmanis, J., van Leeuwen, J., Becker, E., Buhse, W., Günnewig, D. and Rump, N. (Eds.) (2003), *Digital Rights Management, Lecture Notes in Computer Science*, Springer Berlin Heidelberg, Berlin, Heidelberg.

Government Office for Science (2016), *Distributed Ledger Technology: beyond block chain: A report by the UK Government Chief Scientific Adviser*.

Grandison, T. and Sloman, M. (2000), “A survey of trust in internet applications”, *IEEE Communications Surveys & Tutorials*, Vol. 3 No. 4, pp. 2–16.

Greenspan, G. (2015), *MultiChain Private Blockchain - Whitepaper*.

Grönroos, C. (2011), “A service perspective on business relationships: The value creation, interaction and marketing interface”, *Industrial Marketing Management*, Vol. 40 No. 2, pp. 240–247.

Gruber, S. (2013), “Trust, Identity and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion”, *Quinnipiac L. Rev*, Vol. 32 No. 135.

Gunawardena, C.N. (1995), “Social Presence Theory and Implications for Interaction and Collaborative Learning in Computer Conferences”, *International Journal of Educational Telecommunications*, Vol. 1 No. 2, pp. 147–166.

Haber, S. and Stornetta, W. (1991), “How to time-stamp a digital document”, *Journal of Cryptology*, Vol. 3 No. 2.

Hagiu, A. and Beach, N. (2014), “Bitcoin: The Future of Digital Payments?”, *Harvard Business School Case 714-519*.

Hagiu, A. and Wright, J. (2015), “Multi-sided platforms”, *International Journal of Industrial Organization*, Vol. 43, pp. 162–174.

Hahn, F. (1973), “On Transaction Costs, Inessential Sequence Economies and Money”, *The Review of Economic Studies*, Vol. 40 No. 4, pp. 449–461.

Hajdarbegovic, N. (2013), *Swiss Lawmakers Propose Treating Bitcoin as Foreign Currency*, available at: http://www.coindesk.com/swiss-lawmakers-bitcoin-foreign-currency/ (accessed 1 January 2016).

Hajdarbegovic, N. (2014a), *Lawsky: Bitcoin Developers and Miners Exempt from BitLicense*, available at: http://www.coindesk.com/lawsky-bitcoin-developers-miners-exempt-bitlicense/ (accessed 9 September 2016).

Hajdarbegovic, N. (2014b), *Netherlands Issues Bitcoin Warning to Financial Institutions*, available at: http://www.coindesk.com/netherlands-issues-bitcoin-warning-banks-financial-institutions/ (accessed 9 September 2016).

Hamill, J. (2013), *Canadian regulators welcome US Bitcoin refugees with open arms*, available at: http://www.theregister.co.uk/2013/05/20/canada_welcomes_bitcoin_traders_fintrac_letter/ (accessed 9 September 2016).

Hankerson, D.R., Vanstone, S.A. and Menezes, A.J. (2003), *Guide to elliptic curve cryptography, Springer professional computing*, Springer, New York.

Hassan, A. (2012), “The Value Proposition Concept in Marketing: How Customers Perceive the Value Delivered by Firms– A Study of Customer Perspectives on Supermarkets in Southampton in the United Kingdom”, *International Journal of Marketing Studies*, Vol. 4 No. 3.

Hayek, F.A.v. (1990), *Denationalisation of money: The argument refined an analysis of the theory and practice of concurrent currencies,* 3rd ed., Institute of Economic Affairs, London.

Heilman, E., Baldimsti, F. and Goldberg, S. (2016), “Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions”, *3rd Workshop on Bitcoin and Blockchain Research (BITCOIN’16) at FC’16, Barbados, February 2016*.

Heller, W.P. and Starr, R.M. (1976), “Equilibrium with Non-Convex Transactions Costs: Monetary and Non-Monetary Economies”, *The Review of Economic Studies*, Vol. 43 No. 2, pp. 195–215.

Henningsson, S. and Hedman, J. (2014), “Transformation of Digital Ecosystems: The Case of Digital Payments”, in Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Kobsa, A., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Terzopoulos, D., Tygar, D., Weikum, G., Linawati, Mahendra, M.S., Neuhold, E.J., Tjoa, A.M. and You, I. (Eds.), *Information and Communication Technology*, *Lecture Notes in Computer Science*, Vol. 8407, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 46–55.

Her Majesty Treasury (2015), *Digital currencies: response to the call for information*.

Hern, A. (2013a), *Bitcoin plummets as China's largest exchange blocks new deposits*, available at: https://www.theguardian.com/technology/2013/dec/18/bitcoin-plummets-china-payment-processors-digital-cryptocurrency (accessed 9 September 2016).

Hern, A. (2013b), *Bitcoin price tumbles after warning from Chinese central bank*, available at: https://www.theguardian.com/technology/2013/dec/05/bitcoin-price-tumbles-chinese-central-bank-warning (accessed 9 September 2016).

Hevner, A. and Chatterjee, S. (2010), "Design Science Research in Information Systems", in Hevner, A. and Chatterjee, S. (Eds.), *Design Research in Information Systems*, *Integrated Series in Information Systems*, Vol. 22, Springer US, Boston, MA, pp. 9–22.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design Science in Information Systems Research", *MIS Quarterly*, Vol. 28 No. 1, p. 75.

Hicks, J.R. (1935), "A Suggestion for Simplifying the Theory of Money", *Economica*, Vol. 2 No. 5, p. 1.

Higgins, S. (2014), *New York Reveals BitLicense Framework for Bitcoin Businesses*, available at: http://www.coindesk.com/new-york-reveals-bitlicense-framework-bitcoin-businesses/ (accessed 9 September 2016).

Higgins, S. (2016), "Russian Finance Firms Form Blockchain Consortium", available at: http://www.coindesk.com/russian-finance-firms-form-blockchain-consortium/ (accessed 9 September 2016).

Hochstein, M. (2014), "Why Bitcoin Matters for Bankers", American Banker, available at: http://www.americanbanker.com/magazine/124_02/why-bitcoin-matters-for-bankers-1065590-1.html (accessed 31 August 2016).

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999), "Building consumer trust online", *Communications of the ACM*, Vol. 42 No. 4, pp. 80–85.

Holdgaard, L. (2014), "An Exploration of the Bitcoin Ecosystem", Master Thesis, Copenhagen Business Institute, Copenhagen Business School, Copenhagen, 2014.

Holland, J.H. (1995), *Hidden order: How adaptation builds complexity, Helix books*, Addison-Wesley, Reading, Mass.

Houy, N. (2014), *The Economics of Bitcoin Transaction Fees*, Working Paper GATE 2014-07.

Howells, J. (2006), "Intermediation and the role of intermediaries in innovation", *Research Policy*, Vol. 35 No. 5, pp. 715–728.

Hubbard, D.W. (2014), *How to measure anything: Finding the value of intangibles in business,* Third edition, John Wiley & Sons, Inc, Hoboken, New Jersey.

Hubbard, R.G., Garnett, A.M., Lewis, P.E.T. and O'Brien, A.P. (2014), *Microeconomics,* 3rd edition, Pearson Australia, Frenchs Forest, N.S.W.

Hubbard, R.G. and O'Brien, A.P. (2014), *Money, banking, and the financial system,* Second edition, Pearson, Boston.

Hull, C.E. and Lio, B.H. (2006), "Innovation in non-profit and for-profit organizations: Visionary, strategic, and financial considerations", *Journal of Change Management*, Vol. 6 No. 1, pp. 53–65.

Hurlburt, G.F. and Bojanova, I. (2014), "Bitcoin: Benefit or Curse?", *IT Professional*, Vol. 16 No. 3, pp. 10–15.

ibi research (2014), *Gesamtkosten von Zahlungsverfahren – Was kostet das Bezahlen im Internet wirklich?*, ibi research an der Universität Regensburg GmbH, Regensburg.

IBM (2015), *Device democracy - Saving the future of the Internet of Things: Executive Report*.

IDC (2015), "Smartphone OS Market Share, 2015 Q2", available at: http://www.idc.com/prodserv/smartphone-os-market-share.jsp (accessed 4 February 2016).

IEEE (1990), *Standard Glossary of Software Engineering Terminology*, IEEE, Piscataway, NJ, USA.

IfH Köln (2015), "Welches Zahlungsverfahren haben Sie bei Ihrem letzten Online-Kauf eingesetzt?", available at: http://de.statista.com/statistik/daten/studie/384666/umfrage/umfrage-zu-zahlungsmethoden-beim-online-einkauf-nach-ausgabenanteil/ (accessed 18 March 2015).

Innovalue & Locke Lord (2015), *Blockchain and Financial Services: Industry Snapshot and Possible Future Developments*.

International Monetary Fund (2014), "The IMF and the Fight Against Money Laundering and the Financing of Terrorism", available at: http://www.imf.org/external/np/exr/facts/pdf/aml.pdf.

International Monetary Fund (2016), *Virtual Currencies and Beyond: Initial Considerations*.

James Stocks & Co and KPMG (2015), "Red Roses and Slain Dragons", available at: http://www.kpmg.com/GI/en/IssuesAndInsights/ArticlesPublications/Events/eSummit-2015/Documents/Tim-Stocks.pdf (accessed 1 September 2016).

Jevons, W.S. (1893), *Money and mechanism of exchange*, D. Appleton, New York.

Johnson, D., Menezes, A. and Vanstone, S. (2001), "The Elliptic Curve Digital Signature Algorithm (ECDSA)", *International Journal of Information Security*, Vol. 1 No. 1, pp. 36–63.

Kajtazi, M. (2010), "Information asymmetry in the digital economy", in *2010 International Conference on Information Society: I-Society 2010 28-30 June 2010, London, England*, [IEEE], [Piscataway, N.J.], pp. 135–142.

Kannenberg, A. (2015), ""Express-Handel": Bitcoin.de kooperiert mit Onlinebank Fidor", available at: http://www.heise.de/newsticker/meldung/Express-Handel-Bitcoin-de-kooperiert-mit-Onlinebank-Fidor-2557630.html (accessed 12 September 2016).

Kannenberg, A. (2016), ""Utility Settlement Coin": Vier Großbanken wollen eigene Kryptowährung entwickeln", available at: http://www.heise.de/newsticker/meldung/Utility-Settlement-Coin-Vier-Grossbanken-wollen-eigene-Kryptowaehrung-entwickeln-3304631.html (accessed 26 August 2016).

Karame, G.O., Androulaki, E. and Capkun, S. (2012), "Double-spending fast payments in bitcoin", *CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 906-917.

Kashaloglu, K. (2014), "Near Zero Bitcoin Transaction Fees Cannot Last Forever", *The International Conference on Digital Security and and Forensics, Technical University of Ostrava, Czech Republic*, pp. 91–99.

Kaskaloglu, K. (2014), "Near zero Bitcoin transaction fees cannot last forever", in *The International Conference on Digital Security and Forensics (DigitalSec 2014)*, pp. 91–99.

Katz, J. and Lindell, Y. (2015), *Introduction to modern cryptography, Chapman & Hall/CRC cryptography and network security,* Second edition, CRC Press/Taylor & Francis, Boca Raton.

Katz, M.L. and Shapiro, C. (1985), "Network Externalities, Competition, and Compatibility", *The American Economic Review*, Vol. 75 No. 3 (Jun., 1985), pp. 424–440.

Kazan, E., Tan, C.-W. and Lim, E.T. (2015), "Value Creation in Cryptocurrency Networks: Towards A Taxonomy of Digital Business Models for Bitcoin Companies", in *PACIS 2015 Proceedings. Paper 34.*

Kelly, J. (2015), *R3 blockchain group adds five banks, brings in technology heavyweights*, Reuters.

Keynes, J.M. (2008), *The general theory of employment, interest, and money*, BN Pub, [Place of publication not identified].

Kim, G. and Koo, H. (2016), "The causal relationship between risk and trust in the online marketplace. A bidirectional perspective", *Computers in Human Behavior*, Vol. 55, pp. 1020–1029.

Kim, J.-H., West, M., Scholte, E. and Narayanan, S. (2008), "Multiscale consensus for decentralized estimation and its application to building systems", Seattle, WA.

Kim, H.-W., Xu, Y. and Koh, J. (2004), "A Comparison of Online Trust Building Factors between Potential Customers and Repeat Customers", *Journal of the Association for Information Systems*, Vol. 5 No. 10, Article 13.

King, S. (2013), "Primecoin: Cryptocurrency with Prime Number Proof-of-Work", available at: http://primecoin.io/bin/primecoin-paper.pdf.

King, S. and Nadal, S. (2012), "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", available at: https://peercoin.net/assets/paper/peercoin-paper.pdf (accessed 8 September 2016).

Kiyotaki, N. and Wirght, R. (1993), "A Search-Theoretic Approach to Monetary Economics", *The American Economic Review*, Vol. 83 No. 1.

Klein, B. (1974), "The Competitive Supply of Money", *Journal of Money, Credit and Banking*, Vol. 6 No. 4, p. 423.

KPMG (2014), *Global Anti-Money Laundering Survey – 2014*.

Kristoufek, L. (2015), "What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis", *PloS one*, Vol. 10 No. 4, pp. e0123923.

Kroll, J.A., Davey, I.C. and Felten, E.W. (2013), "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", in *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, Washington, DC, June 11-12, 2013.

Krugman, P.R. (1984), "The International Role of the Dollar: Theory and Prospect", in Bilson, J.F.O. and Marston, R.C. (Eds.), *Exchange rate theory and practice: [papers presented at a Conference held in Jan. 1982 at the Rockefeller Foundation's BallagioConference Center*, *A National Bureau of Economic Research. Conference Report*, The University of Chicago Press, Chicago, London, pp. 261–278.

Laidler, D. (1969), "The Definition of Money. Theoretical and Empirical Problems", *Journal of Money, Credit and Banking*, Vol. 1 No. 3, p. 508.

Lamport, L. (1998), "The part-time parliament", *ACM Transactions on Computer Systems*, Vol. 16 No. 2, pp. 133–169.

Lamport, L., Shostak, R. and Pease, M. (1982), "The Byzantine Generals Problem", *ACM Transactions on Programming Languages and Systems*, Vol. 4 No. 3, pp. 382–401.

Lapouchnian, A. (2005), *Goal-Oriented Requirements Engineering: An Overview of the Current Research*.

Lee, T.B. (2012), *Bitcoin going mainstream? Exchange approved to operate as a bank*, available at: http://arstechnica.com/tech-policy/2012/12/bitcoin-going-mainstream-exchange-approved-to-operate-as-a-bank/ (accessed 9 September 2016).

Liberty Reserve (2016), “Liberty Reserve Website. web.archive.org”, available at: http://web.archive.org/web/20130423093118/https://www.libertyreserve.com/ (accessed 3 August 2016).

Linden Lab (2016), “Second Life - Official Website”, available at: http://secondlife.com/ (accessed 3 August 2016).

Linux Fondation (2016), “Hyperledger Project - Official Website”, available at: https://www.hyperledger.org (accessed 20 July 2016).

Linux Foundation (2015), *Linux Foundation Unites Industry Leaders to Advance Blockchain Technology*, San Francisco.

Litecoin (2016), “Comparison between Litecoin and Bitcoin/Alternative work in progress version”, available at: https://litecoin.info/Comparison_between_Litecoin_and_Bitcoin/Alternative_work_in_progress_version (accessed 8 September 2016).

Lo, S. and Wang, C. (2014), “Bitcoin as Money?”, *Boston Federal Reserve, Current Policy Perspectives [Internet]*, Vol. 14 No. 4.

Lockett, A. and Wright, M. (2001), “The syndication of venture capital investments”, *Omega*, Vol. 29 No. 5, pp. 375–390.

Mainelli, M. and Smith, M. (2015), “Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)”, *The Journal of Financial Perspectives: FinTech*, Vol. 3 No. 3.

Malhotra, K., Gardner, S. and Patz, R. (2007), “Implementation of Elliptic-Curve Cryptography on Mobile Healthcare Devices”, 2007 IEEE International Conference on, London, 15–17 April 2007, pp. 239–244.

Mankiw, N.G. (2016), *Macroeconomics,* Ninth edition, Worth Publishers, New York.

Mann, R.J. and Sager, T.W. (2007), “Patents, venture capital, and software start-ups”, *Research Policy*, Vol. 36 No. 2, pp. 193–208.

Mansfield, E. (1991), “Academic research and industrial innovation.“”, *Research Policy*, Vol. 20 No. 1, pp. 1–12.

Mantel, B. and McHugh, T. (2001), “Competition and Innovation in the Consumer e-Payments Market? Considering the Demand, Supply, and Public Policy Issues”, *Federal Reserve Bank of Chicago Pub-lic Policy Working Paper No. EPS-2001-4.*

Marley, G. (2015), *Ethereum Blockchain as a Service now on Azure*.

Masciandaro, D. (1998), “Money Laundering Regulation: The Micro Economics”, *Journal of Money Laundering Control*, Vol. 2 No. 1, pp. 49–58.

Masciandaro, D. (1999), “Money Laundering: the Economics of Regulation”, *European Journal of Law and Economics*, Vol. 7 No. 3, pp. 225–240.

Masciandaro, D. and Barone, R. (2008), “Worldwide Anti-Money Laundering Regulation: Estimating Costs and Benefits”, *SSRN Electronic Journal*.

Maxwell, G. (2013), “CoinJoin: Bitcoin privacy for the real world”, available at: https://bitcointalk.org/index.php?topic=279249.0 (accessed 31 August 2016/).

McAfee (2014), *Jackpot! Money Laundering Through Online Gambling*.

McCusker, R. (2007), “Transnational organised cyber crime: distinguishing threat from reality”, *Crime, Law and Social Change*, Vol. 46 No. 4-5, pp. 257–273.

McDowell, J. and Novis, G. (2001), “The Consequences of Money Laundering and Financial Crime”, *Economic Perspectives*, Vol. 6 No. 2, pp. 6–8.

McKinsey (2015a), *McKinsey Working Papers on Corporate & Investment Banking | No. 12: Beyond the Hype: Blockchains in Capital Markets*.

McKinsey (2015b), *The Internet of Things: Mapping the Value Beyond the Hype*.

McLeay, M., Radia, A. and Thomas, R. (2014), “Money in the modern economy: an introduction”, *Bank of England Quarterly Bulletin*, Vol. 54 No. 1, pp. 4–13.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S. (2013), “A fistful of bitcoins”, Barcelona, Spain.

Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A. (1997), *Handbook of applied cryptography, CRC Press series on discrete mathematics and its applications*, CRC Press, Boca Raton.

Menger, K. (1892), “On the Origin of Money”, *The Economic Journal*, Vol. 2 No. 6, p. 239.

Merkle, R.C. (1988), “A Digital Signature Based on a Conventional Encryption Function”, in Goos, G., Hartmanis, J., Barstow, D., Brauer, W., Brinch Hansen, P., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmüller, G., Stoer, J., Wirth, N. and Pomerance, C. (Eds.), *Advances in Cryptology — CRYPTO ’87, Lecture Notes in Computer Science*, Vol. 293, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 369–378.

Microsoft (2016), “Hinzufügen von Guthaben zum Microsoft-Konto mit Bitcoin”, available at: https://support.microsoft.com/de-de/help/13942/microsoft-account-add-money-with-bitcoin (accessed 29 August 2016).

Miers, I., Garman, C., Green, M. and Rubin, A.D. (2013), “Zerocoin: Anonymous Distributed E-Cash from Bitcoin”, Berkeley, CA.

Mildner, M. (2016), *Distributed Ledger Technology in Finance - from Inception to Reality*.

Mises, L. von and Batson, H.E. (2009), *The theory of money and credit,* New ed. enl. with an essay on monetary reconstruction, Signalman Pub, Orlando.

Mishkin, F.S. (2013), *The economics of money, banking, and financial markets, Pearson series in economics,* Eleventh edition, Pearson, Boston.

MIT Technology Review (2015), "Why Nasdaq is Betting on Bitcoin's Blockchain", available at: https://www.technologyreview.com/s/539171/why-nasdaq-is-betting-on-bitcoins-blockchain/ (accessed 13 September 2016).

Moody's (2016), *Credit Strategy -- Blockchain Technology: Robust, Cost-effective Applications Key to Unlocking Blockchain's Potential Credit Benefits*, Moody's.

Monnet, C. (2002), *Optimal Public Money*, European Central Bank Working Paper 159.

Moore, J.F. (1993), "Predators and Prey: A New Ecology of Competition", *Harvard Business Review*, Vol. 71 No. 3, pp. 75–86.

Möser, M. and Böhme, R. (2015), "Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees", in Brenner, M., Christin, N., Johnson, B. and Rohloff, K. (Eds.), *Financial Cryptography and Data Security*, *Lecture Notes in Computer Science*, Vol. 8976, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 19–33.

Möser, M., Böhme, R. and Breuker, D. (2013), "An inquiry into money laundering tools in the Bitcoin ecosystem", San Francisco, CA, USA.

Möser, M., Böhme, R. and Breuker, D. (2014), "Towards Risk Scoring of Bitcoin Transactions", in Böhme, R., Brenner, M., Moore, T. and Smith, M. (Eds.), *Financial Cryptography and Data Security*, *Lecture Notes in Computer Science*, Vol. 8438, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 16–32.

Müller, G. (2009), "Was the Internet the Only Option? Which Way Should Business and Information Systems Engineering Go?", *Business & Information Systems Engineering*, Vol. 1 No. 1, pp. 46–52.

Müller, G., Eymann, T. and Kreutzer, M. (2003), *Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft, Lehrbücher Wirtschaftsinformatik*, Oldenbourg, München.

Münzer, J. (2013), *Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer*.

Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, available at: https://bitcoin.org/bitcoin.pdf (accessed 4 February 2016).

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016), *Bitcoin and Cryptocurrency Technologies: Draft - Feb 9, 2016*.

NASDAQ (2015), *Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology*, New York.

Nathan, A., Currie, J., Ursua, J., Wilson, D. and Leaf, R. (2014), *Top of Mind: All About Bitcoin*.

Norta, A. (2015), "Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations", in Matulevičius, R. and Dumas, M. (Eds.), *Perspectives in Business Informatics Research*, Springer International Publishing, Cham, pp. 3–17.

Nuseibeh, B. and Easterbrook, S. (2000), "Requirements engineering", Limerick, Ireland.

Ober, M., Katzenbeisser, S. and Hamacher, K. (2013), "Structure and Anonymity of the Bitcoin Transaction Graph", *Future Internet*, Vol. 5 No. 2, pp. 237–250.

Olshavsky, R.W. and Spreng, R.A. (1996), "An Exploratory Study of the Innovation Evaluation Process", *Journal of Product Innovation Management*, Vol. 13 No. 6, pp. 512–529.

Omohundro, S. (2014), "Cryptocurrencies, Smart Contracts, and Artificial Intelligence", *AI Matters*, Vol. 1 No. 2, pp. 19–21.

Ostroy, J.M. and Starr, R.M. (1990), "Chapter 1 The transactions role of money", in *Handbook of Monetary Economics*, Vol. 1, Elsevier, pp. 3–62.

O'Sullivan, A. and Sheffrin, S.M. (2003), *Economics: Principles in action*, Prentice Hall, Needham, Mass.

Panurach, P. (1996), "Money in electronic commerce. Digital cash, electronic fund transfer, and Ecash", *Communications of the ACM*, Vol. 39 No. 6, pp. 45–50.

Párhonyi, R., Nieuwenhuis, L.J.M. and Pras, A. (2005), "Second generation micropayment systems: lessons learned", in Funabashi, M. and Grzech, A. (Eds.), *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government*, *IFIP International Federation for Information Processing*, Vol. 189, Kluwer Academic Publishers, Boston, pp. 345–359.

Paul, G., Sarkar, P. and Mukherjee, S. (2014), "Towards a More Democratic Mining in Bitcoins", in Prakash, A. and Shyamasundar, R. (Eds.), *Information Systems Security*, *Lecture Notes in Computer Science*, Vol. 8880, Springer International Publishing, Cham, pp. 185–203.

Payne, A. and Holt, S. (2001), "Diagnosing Customer Value: Integrating the Value Process and Relationship Marketing", *British Journal of Management*, Vol. 12 No. 2, pp. 159–182.

PayPal (2014), "PayPal Payments Hub", available at: https://www.paypal.com/webapps/mpp/paymentshub (accessed 15 October 2014).

PayPal (2016), “FORM 8-K. Filed 04/27/16 for the Period Ending 04/27/16”, available at: http://files.shareholder.com/downloads/AMDA-4BS3R8/1964234858x0xS1633917-16-158/1633917/filing.pdf (accessed 25 July 2016).

Peck, M.E. (2012), “The cryptoanarchists’ answer to cash”, *IEEE Spectrum*, Vol. 49 No. 6, pp. 50–56.

Percival, C. and Josefsson, S. (2012), *The scrypt Password-Based Key Derivation Function*.

Perez, Y.B. (2015), *Bitcoin is Exempt from VAT, Rules European Court of Justice*, available at: http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/ (accessed 9 September 2016).

Perkins, C. (2016), *Digital Currencies: International Actions and Regulations*, available at: https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#Germany (accessed 9 September 2016).

Perng, G., Reiter, M.K. and Wang, C. (2005), “Censorship Resistance Revisited”, in Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Barni, M., Herrera-Joancomartí, J., Katzenbeisser, S. and Pérez-González, F. (Eds.), *Information Hiding*, *Lecture Notes in Computer Science*, Vol. 3727, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 62–76.

Peters, G., Panayi, E. and Chapelle, A. (2015), *Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective*, arXiv:1508.04364.

Pfitzmann, A. and Hansen, M. (2010), *Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology: Version 0.34*.

Philippsohn, S. (2001), “Money Laundering on the Internet”, *Computers & Security*, Vol. 20 No. 6, pp. 485–490.

Picot, A. and Bortenlanger, C. (1997), “Organization of Electronic Markets. Contributions from the New Institutional Economics”, *The Information Society*, Vol. 13 No. 1, pp. 107–123.

PM Solutions Research (2011), *Strategies for Project Recovery: A PM Solutions Research Report*.

Pohl, K. (1996), *Process-centered requirements engineering, Advanced software development series*, Vol. 5, Research Studies Press; Wiley, Taunton, Somerset, England, New York.

Pohl, K. (2010), *Requirements engineering: Fundamentals, principles, and techniques*, Springer, Heidelberg, New York.

Pohl, K., Rupp, C. (2015), *Basiswissen Requirements Engineering. Aus- und Weiterbildung zum "Certified Professional for Requirements Engineering"*; Foundation Level nach IREB-Standard. 4., überarb. Aufl. Heidelberg: dpunkt-Verl.

Polinsky, A.M. and Shavell, S. (2000), “The Economic Theory of Public Enforcement of Law”, *Journal of Economic Literature*, Vol. 38 No. 1, pp. 45–76.

Ponsford, M.P. (2015), *A comparative analysis of Bitcoin and other decentralized virtual currencies: legal regulation in the People’s Republic of China, Canada and the United States*, available at: http://jolt.law.harvard.edu/digest/bitcoin/a-comparative-analysis-of-bitcoin-and-other-decentralized-virtual-currencies-legal-regulation-in-the-peoples-republic-of-china-canada-and-the-united-states (accessed 9 September 2016).

Popper, N. (2016), “A Bitcoin Believer’s Crisis of Faith”, available at: http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html (accessed 15 July 2016).

Pranata, I., Skinner, G. and Rukshan, A. (2012), “A Holistic Review on Trust and Reputation Management Systems for Digital Environments”, *International Journal of Computer and Information Technology*, Vol. 01 No. 01.

Priestley, T. (2016), “Bitcoin Declared An “Inescapable Failure””, available at: http://www.forbes.com/sites/theopriestley/2016/01/15/bitcoin-declared-an-inescapable-failure/#4a4cdd2f9bf8 (accessed 16 February 2016).

Putland, P.A., Hill, J. and Tsapikidis, D. (1997), “Electronic payment systems”, *BT Technology Journal*, Vol. 15 No. 2, pp. 32–38.

R3 (2016), “R3 Official Website”, available at: http://r3cev.com/ (accessed 9 September 2016).

Radford, R.A. (1945), “The Economic Organisation of a P.O.W. Camp”, *Economica*, Vol. 12 No. 48, p. 189.

Raeesi, R. (2015), “The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?”, *Glendon Journal of International Studies*, Vol. 8 No. 2.

Raiffa, H., Richardson, J. and Metcalfe, D. (2007), *Negotiation analysis: The science and art of collaborative decision making*, Belknap, Cambridge, Mass., London.

Raymond, N. (2015), *Accused Silk Road operator convicted on U.S. drug charges*, Reuters, New York.

Reichenbach, M. (2001), *Individuelle Risikohandhabung elektronischer Zahlungssysteme: Nutzerorientierte Abwicklung von Internet-Zahlungen, Gabler Edition Wissenschaft. Markt- und Unternehmensentwicklung,* 1. Aufl., Deutscher Universitäts-Verlag; Gabler, Wiesbaden, Wiesbaden.

Reid, F. and Harrigan, M. (2013), “An Analysis of Anonymity in the Bitcoin System”, in Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N. and Pentland, A. (Eds.), *Security and Privacy in Social Networks*, Springer New York, New York, NY, pp. 197–223.

Renda, A., Schrefler, L., Luchetta, G. and Zavatta, R. (2013), *Assessing the Costs and Benefits of Regulation: Study for the European Commission, Secretariat General*, Brussels.

Reuter, P. and Truman, E.M. (2004), *Chasing dirty money: Progress on anti-money laundering*, Institute for International Economics, Washington, DC.

Reuters (2016), *Dutch arrest 10 men suspected of using Bitcoin to launder money*, Reuters, available at: http://www.reuters.com/article/us-netherlands-crime-bitcoin-idUSKCN0UY0V8 (accessed 03 November 2016).

Reuters (2013), *Ermittler sprengen milliardenschweren Geldwäschering*, Reuters, available at: http://de.reuters.com/article/usa-cyberkriminalitt-idDEBEE94S00O20130529 (accessed 03 November 2016).

Richet, J.-L. (2013), *Laundering Money Online: A review of cybercriminals' methods: Tools and Resources for Anti-Corruption Knowledge - June, 01, 2013 - United Nations Office on Drugs and Crime (UNODC)*.

Ripple (2014), “The Ripple Protocol: A Deep Dive for Finance Professionals”, available at: http://www.the-blockchain.com/docs/Ripple%20Protocol%20-%20Deep%20Dive%20For%20Financial%20Professionals.pdf (accessed 25 August 2016).

Ripple (2015), “Ripple Consensus Ledger”, available at: https://wiki.ripple.com/Ripple_Consensus_Ledger.

Ripple (2016a), “Ripple Developer Center”, available at: https://ripple.com/build/ (accessed 9 March 2016).

Ripple (2016b), “The Ledger”, available at: https://ripple.com/build/ledger-format/ (accessed 25 August 2016).

Ripple Labs. (2016), “Ripple - Official Website”, available at: https://ripple.com/ (accessed 8 September 2016).

Rivest, R.L., Shamir, A. and Adleman, L. (1978), “A method for obtaining digital signatures and public-key cryptosystems”, *Communications of the ACM*, Vol. 21 No. 2, pp. 120–126.

Rizzo, P. (2016), *Report: Russian Government to Abandon Penalties for Bitcoin Use*, available at: http://www.coindesk.com/russian-bitcoin-penalties-abandon-report/ (accessed 9 September 2016).

Robleh, A., Barrdear, J., Clews, R. and Southgate, J. (2014), *Innovations in payment technologies and the emergence of digital currencies*, Bank of England.

Rochet, J.-C. and Tirole, J. (2003), “Platform Competition in Two-Sided Markets”, *Journal of the European Economic Association*, Vol. 1 No. 4, pp. 990–1029.

Rochet, J.-C. and Tirole, J. (2006), “Two-sided markets. A progress report”, *The RAND Journal of Economics*, Vol. 37 No. 3, pp. 645–667.

Rogojanu, A. and Badea, L. (2014), “The issue of competing currencies. Case study - Bitcoin”, *Theoretical and Applied Economics*, Vol. 21 No. 1, pp. 103–114.

Royce, W. W. (1987), Managing the development of large software systems: concepts and tech-niques. In: ICSE '87 Proceedings of the 9th international conference on Software Engineering. New York: Institute of Electrical and Electronics Engineers, S. 328–338.

Rüdel, N. (2013), “Schlag gegen Liberty Reserve. Geldwäsche à la Al Capone”, available at: http://www.handelsblatt.com/finanzen/maerkte/boerse-inside/schlag-gegen-liberty-reserve-geldwaesche-a-la-al-capone/8269912.html (accessed 3 September 2016).

Ruecker, G. (2015), “Open Day 2015 Blockchain technology”, available at: http://www.mds.deutsche-boerse.com/blob/10304/649c21aa656ba788026f9d371caa557f/blockchain-technology-data.pdf (accessed 12 September 2016).

Ruffing, T., Moreno-Sanchez, P. and Kate, A. (2014), “CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin”, in Kutyłowski, M. and Vaidya, J. (Eds.), *Computer Security - ESORICS 2014*, *Lecture Notes in Computer Science*, Vol. 8713, Springer International Publishing, Cham, pp. 345–364.

Ruiz-Martínez, A., Reverte, Ó.C. and Gómez-Skarmeta, A.F. (2012), “Payment frameworks for the purchase of electronic products and services”, *Computer Standards & Interfaces*, Vol. 34 No. 1, pp. 80–92.

Rysman, M. (2009), “The Economics of Two-Sided Markets”, *Journal of Economic Perspectives*, Vol. 23 No. 3, pp. 125–143.

Sackmann, S. (2008), “Automatisierung von Compliance”, *HMD Praxis der Wirtschaftsinformatik*, Vol. 45 No. 5, pp. 39–46.

Sackmann, S., Kähmer, M., Gilliot, M. and Lowis, L. (2008), “A Classification Model for Automating Compliance”, Arlington, VA, USA.

Sadeghi, A.-R. and Schneider, M. (2003), “Electronic Payment Systems”, in Goos, G., Hartmanis, J., van Leeuwen, J., Becker, E., Buhse, W., Günnewig, D. and Rump, N. (Eds.), *Digital Rights Management*, *Lecture Notes in Computer Science*, Vol. 2770, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 113–137.

Sadiq, S., Governatori, G. and Namiri, K. (2007), “Modeling Control Objectives for Business Process Compliance”, in Alonso, G., Dadam, P. and Rosemann, M. (Eds.), *Business Process Management*, *Lecture Notes in Computer Science*, Vol. 4714, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 149–164.

Sadraei, E., Aurum, A., Beydoun, G. and Paech, B. (2007), “A field study of the requirements engineering practice in Australian software industry”, *Requirements Engineering*, Vol. 12 No. 3, pp. 145–162.

Salam, A.F., Rao, H.R. and Pegels, C.C. (2003), “Consumer-perceived risk in e-commerce transactions”, *Communications of the ACM*, Vol. 46 No. 12, p. 325.

Salem Khalifa, A. (2004), “Customer value: a review of recent literature and an integrative configuration”, *Management Decision*, Vol. 42 No. 5, pp. 645–666.

Sambamurthy, V., Bharadwaj, A.S. and Grover, V. (2003), “Shaping Agility Through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms”, *MIS Quarterly*, Vol. 27 No. 2, pp. 237–263.

Sanchez-Fernandez, R. and Iniesta-Bonillo, M.A. (2007), “The concept of perceived value: a systematic review of the research”, *Marketing Theory*, Vol. 7 No. 4, pp. 427–451.

Santander (2015), *The Fintech 2.0 Paper: Rebooting Financial Services*.

Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. and Virza, M. (2014), “Zerocash: Decentralized Anonymous Payments from Bitcoin”, Berkeley, CA, USA.

Schechner, S. (2014), *France Plans Transparency Rules For Bitcoin Businesses*, available at: http://blogs.wsj.com/digits/2014/07/11/france-plans-transparency-rules-for-bitcoin-businesses/?mg=id-wsj (accessed 9 September 2016).

Scherer, S. (2016), *Italy arrests 11 in illegal online gaming ring involving mafia*, Reuters, Rom.

Schneider, F. and Windischbauer, U. (2008), “Money laundering: some facts”, *European Journal of Law and Economics*, Vol. 26 No. 3, pp. 387–404.

Schneier, B. (1996), *Applied cryptography: Protocols, algorithms, and source code in C,* 2nd ed., Wiley, New York.

Scholte, T. and Kirda, E. (2010), “Achieving Life-Cycle Compliance of Service-Oriented Architectures: Open Issues and Challenges”, in Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Garcia-Alfaro, J., Navarro-Arribas, G., Cuppens-Boulahia, N. and Roudier, Y. (Eds.), *Data Privacy Management and Autonomous Spontaneous Security*, *Lecture Notes in Computer Science*, Vol. 5939, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 253–267.

Schumpeter, J.A. (2009), *Geschichte der ökonomischen Analyse, UTB Wirtschaftswissenschaften*, Vol. 8411, Vandenhoeck & Ruprecht, Göttingen.

Schwartz, D., Youngs, N. and Britto, A. (2014), “The Ripple Protocol Consensus Algorithm”, available at: https://ripple.com/files/ripple_consensus_whitepaper.pdf (accessed 25 August 2016).

Scott, B. (2016), How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?, Working Paper 2016-1, United Nations Research Institute for Social Development.

Segendorf, B. (2014a), *Have virtual currencies affected the retail payments market?*

Segendorf, B. (2014b), *What is Bitcoin?*, available at: http://www.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_artikel_4_1400918_eng.pdf.

Selander, L., Henfridsson, O. and Svahn, F. (2010), “Transforming Ecosystem Relationships in Digital Innovation”, in *ICIS 2010 Proceedings*, p. Paper 138.

Shapiro, C. and Varian, H.R. (1999), *Information rules: A strategic guide to the network economy*, Harvard Business School Press, Boston, Mass.

Shasky Calvery, J. (2013), *Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury: Before the United States Senate Committee on Homeland Security and Government Affairs*.

Shin, L. (2015), “Bitcoin’s Shared Ledger Technology: Money’s New Operating System”, available at: http://www.forbes.com/sites/laurashin/2015/09/09/bitcoins-shared-ledger-technology-moneys-new-operating-system/#22caca80c4fc (accessed 23 March 2016).

Shomer, A. (2016), “The Colored Coins Protocol”, available at: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Data%20Storage%20Methods (accessed 28 February 2016).

Shull, F., Rus, I. and Basili, V. (2000), “How perspective-based reading can improve requirements inspections”, *Computer*, Vol. 33 No. 7, pp. 73–79.

Siegel, D. (2016), “Understanding The DAO Attack”, available at: http://www.coindesk.com/understanding-dao-hack-journalists/ (accessed 11 July 2016).

Siemers, B. (2014), *Bitcoin does not qualify as currency, but as medium of exchange*, available at: https://www.eaccny.com/news/bitcoin-does-not-qualify-as-currency-but-as-medium-of-exchange/ (accessed 9 September 2016).

Skevington, P.J. and Hart, T.P. (1997), “Trusted third parties in electronic commerce”, *BT Technology Journal*, Vol. 15 No. 2, pp. 39–44.

Smith, A. (1775), *An inquiry into the nature and causes of the wealth of Nations*, Modern Library, New York: Random House.

Southurst, J. (2013), *Central Banks in New Zealand and Australia Issue Bitcoin Warning*, available at: http://www.coindesk.com/central-bank-new-zealand-australia-bitcoin-warning/ (accessed 9 September 2016).

Spaven, E. (2013), *IRS targets bitcoin*, available at: http://www.coindesk.com/irs-targets-bitcoin/ (accessed 9 September 2016).

Srinivas, V., Piscini, E. and Dillion, D. (2014), *Bitcoin: The new gold rush?*, Deloitte Center for Financial Services.

Stafford, P. (2015), "Blockchain initiative backed by 9 large investment banks", available at: http://www.ft.com/cms/s/0/f358ed6c-5ae0-11e5-9846-de406ccb37f2.html (accessed 12 September 2016).

Stalder, F. (2002), "Failures and Successes. Notes on the Development of Electronic Cash", *The Information Society*, Vol. 18 No. 3, pp. 209–219.

Statista (2011), "Umsatz im Social Games Markt bei Facebook weltweit in 2010 und Prognose bis 2014", available at: http://de.statista.com/statistik/daten/studie/205427/umfrage/weltweiter-umsatz-mit-social-games-bei-facebook/ (accessed 20 March 2015).

stats.grok.se (2015), "Wikipedia article traffic statistics", available at: http://stats.grok.se/ (accessed 14 October 2015).

Staykova, K. and Damsgaard, J. (2014), "A Model of Digital Payment Infrastructure Formation and Development: The EU Regulator´s Perspective", in *2014 International Conference on Mobile Business*, p. Paper 14.

Staykova, K.B.S. and Damsgaard, J.B.S. (2015), *A Typology of Multi-sided Platforms: The Core and the Periphery*, University of Münster, Münster, Germany.

Stellman, A.; Greene, J. (2006), Applied software project management. Sebastopol, CA: O'Reilly.

Stempel, J. (2015), *Liberty Reserve founder must face $6 bln laundering case in U.S.*, New York.

Stokes, R. (2012), "Virtual money laundering: the case of Bitcoin and the Linden dollar", *Information & Communications Technology Law*, Vol. 21 No. 3, pp. 221–236.

Stolterman, E. and Fors, A.C. (2004), "Information Technology and the Good Life", in Kaplan, B., Truex, D.P., Wastell, D., Wood-Harper, A.T. and DeGross, J.I. (Eds.), Information Systems Research, *IFIP International Federation for Information Processing*, Vol. 143, Kluwer Academic Publishers, Boston, pp. 687–692.

Strassel, K.A. (1996), "Deutsche Bank to Test 'E-Cash' With DigiCash in Pilot Project", available at: http://www.wsj.com/articles/SB831416067295410500 (accessed 29 July 2016).

Sumanjeet, S. (2009), "Emergence of payment systems in the age of electronic commerce: The state of art", in *2009 First Asian Himalayas International Conference on Internet*, Kathmundu, Nepal, 3/11/2009 - 5/11/2009, I E E E, Piscataway, pp. 1–18.

Swanson, T. (2015), *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*.

Swift, H. (2015), "The Offshore Game of Online Betting", *New York Times,* 26 October, available at: http://www.nytimes.com/2015/10/26/us/pinnacle-sports-online-sports-betting.html?_r=0 (accessed 1 September 2016).

Swiss Federal Council (2014), *Factsheet: Bitcoins*.

Szabo, N. (1997), "The Idea of Smart Contracts", available at: http://szabo.best.vwh.net/smart_contracts_idea.html (accessed 8 September 2016).

Takao, M., Kajikawa, Y., Takeda, Y., Sakata, L. and Matsushima, K. (2012), "Diffusion of e-Money and Industrial Structure Change in Japan", in *2012 Portland International Conference on Management of Engineering and Technology*, IEEE, Piscataway, pp. 1085–1098.

Takats, E. (2011), "A Theory of "Crying Wolf". The Economics of Money Laundering Enforcement", *Journal of Law, Economics, and Organization*, Vol. 27 No. 1, pp. 32–78.

Taulli, T. (2013), "Lessons From The Fall Of BlackBerry", available at: http://www.forbes.com/sites/tomtaulli/2013/09/23/lessons-from-the-fall-of-blackberry/#2715e4857a0b6b681931175c (accessed 5 February 2016).

Taylor, S. (2015), "Blockchain: understanding the potential", available at: https://www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf (accessed 8 September 2016).

Tellis, G.J. and Gaeth, G.J. (1990), "Best Value, Price-Seeking, and Price Aversion: The Impact of Information and Learning on Consumer Choices", *Journal of Marketing*, Vol. 54 No. 2, p. 34.

The Economist (2016), "The DAO of accrue", available at: http://www.economist.com/news/finance-and-economics/21699159-new-automated-investment-fund-has-attracted-stacks-digital-money-dao (accessed 8 September 2016).

The Law Library of Congress (2014a), *Canada Passes Law Regulating Virtual Currencies as "Money Service Businesses"*, available at: http://www.loc.gov/law/foreign-news/article/canada-canada-passes-law-regulating-virtual-currencies-as-money-service-businesses/ (accessed 9 September 2016).

The Law Library of Congress (2014b), *Regulation of Bitcoin in Selected Jurisdictions*, available at: https://www.loc.gov/law/help/bitcoin-survey/ (accessed 9 September 2016).

Thomas, L. and Pravin, C. (2013), *French central bank warns over bitcoin risks*, available at: http://www.reuters.com/article/us-france-bitcoin-idUSBRE9B40IF20131205 (accessed 9 September 2016).

TMF, G. (2014), *BITCOIN UK TAX REVIEW TO GIVE CURRENCY GLOBAL BOOST*, available at: http://www.tmf-group.com/en/media-centre/news-and-insights/january-2014/bitcoin-uk-tax-review-to-give-currency-global-boost (accessed 9 September 2016).

Trautman, L.J. (2014), "Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?", *Richmond Journal of Law and Technology*, Vol. 20 No. 4.

Tsiakis, T. and Sthephanides, G. (2005), "The concept of security and trust in electronic payments", *Computers & Security*, Vol. 24 No. 1, pp. 10–15.

Turing, A.M. (1937), "On Computable Numbers, with an Application to the Entscheidungsproblem", *Proceedings of the London Mathematical Society*, s2-42 No. 1, pp. 230–265.

UBS (2016), *Extreme automation and connectivity: The global, regional, and investment implications of the Fourth Industrial Revolution: UBS White Paper for the World Economic Forum Annual Meeting 2016*.

Uckelmann, D., Harrison, M. and Michahelles, F. (2011), "An Architectural Approach Towards the Future Internet of Things", in Uckelmann, D., Harrison, M. and Michahelles, F. (Eds.), *Architecting the Internet of Things*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–24.

Une, M. (2001), "The security evaluation of time stamping schemes: The present situation and studies", *IMES Institute for Monetary and Economic Studies*, No. No. 2001-E-18.

Unger, B. (2009), "Money Laundering - A Newly Emerging Topic on the International Agenda", *Review of Law & Economics*, Vol. 5 No. 2.

United Nations Office on Drugs and Crime (1988), *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*.

United Nations Office on Drugs and Crime (2005), *Model legislation Model legislation on money laundering and financing of terrorism*.

United Nations Office on Drugs and Crime (2011), *Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crimes*.

United Nations Office on Drugs and Crime (2013), *Risk of Money Laundering through Financial and Commercial Instruments*, Bogota, D.C.

United Nations Office on Drugs and Crime (2014), *Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, United Nations Office on Drugs and Crime.

US Conference of State Bank Supervisors (2015), *STATE REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES CSBS MODEL REGULATORY FRAMEWORK*.

Valenta, L. and Rowan, B. (2015), "Blindcoin: Blinded, Accountable Mixes for Bitcoin", in Brenner, M., Christin, N., Johnson, B. and Rohloff, K. (Eds.), *Financial Cryptography and Data Security*, *Lecture Notes in Computer Science*, Vol. 8976, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 112–126.

van Lamsweerde, A. (2001), "Goal-oriented requirements engineering: a guided tour", 27-31 Aug. 2001, Toronto, Ont., Canada.

Vargo, S.L. and Lusch, R.F. (2004), "Evolving to a New Dominant Logic for Marketing", *Journal of Marketing*, Vol. 68 No. 1, pp. 1–17.

Varian, H.R. (2010), *Intermediate microeconomics: A modern approach,* 8th ed., W.W. Norton & Co, New York.

Velde, F. (2013), "Bitcoin: A primer", *Federal Reserve Bank of Chicago Essays on Issues*, No. 317.

Verified by Visa (2011), *Acquirer and Merchand Implementation Guide: U.S. Region*.

Vigna, P. and Casey, M. (2015), *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order,* First edition.

Villasenor, J., Monk, C. and Bronk, C. (2011), *Shadow Figures: Tracking Illicit Financial Transactions in the Murky Word of Digital Correncies, Peer-to-Peer Networks, and Mobile Device Payments*, available at: http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf.

Virtualpolicy.net (2012), *RuneScape Theft – Dutch Supreme Court Decision*, available at: http://www.virtualpolicy.net/runescape-theft-dutch-supreme-court-decision.html (accessed 9 September 2016).

Vockathaler, B. (2015), *The Bitcoin Boom: An In Depth Analysis Of The Price Of Bitcoins*, uO Research, University of Ottawa.

Wagstaff, J. (2015), *Stakes are high in hunt for bitcoin's 'messiah'*, Reuters, Singapore.

Walker, J. and Unger, B. (2009), "Measuring Global Money Laundering: "The Walker Gravity Model"", *Review of Law & Economics*, Vol. 5 No. 2.

Walley, K. (2007), "Coopetition. An Introduction to the Subject and an Agenda for Research", *International Studies of Management and Organization*, Vol. 37 No. 2, pp. 11–31.

Walsh, K. and Murphy, J. (2013), “ATO targets Bitcoin users”, available at: http://www.afr.com/news/policy/tax/ato-targets-bitcoin-users-20130623-jhj8r (accessed 9 September 2016).

Weir, C.S., Douglas, G., Carruthers, M. and Jack, M. (2009), “User perceptions of security, convenience and usability for ebanking authentication tokens”, *Computers & Security*, Vol. 28 No. 1-2, pp. 47–62.

West, J. and Gallagher, S. (2006), “Challenges of open innovation: the paradox of firm investment in open-source software”, *R and D Management*, Vol. 36 No. 3, pp. 319–331.

Western Union (2016), “Fees for Western Union Services”, available at: https://www.westernunion.com/us/en/price-estimator/start.html (accessed 31 August 2016).

Whynes, D.K. and Bowles, R.A. (1981), *The economic theory of the state*, St. Martin’s Press, New York.

Williams, E., Eyo, B. and Akpan, S. (2011), “Linden Labs Second Life: Understanding the Business Model and Sources of Commercial and Social Success or Decline of Second Life”, *Computer and Information Science*, Vol. 4 No. 2.

Williams, R. (2016), “Apple Pay launches in China: will it catch on?”, available at: http://www.telegraph.co.uk/technology/2016/02/18/apple-pay-launches-in-china-will-it-catch-on/ (accessed 25 July 2016).

Winkler, M. and Dosoudil, V. (2011), “On Formalization of the Concept of Value Proposition”, *Service Science*, Vol. 3 No. 3, pp. 194–205.

Wong, J.I. (2014), *UK Treasury Committee MP: Bitcoin Doesn’t Need New Laws*, available at: http://www.coindesk.com/uk-treasury-committee-mp-bitcoin-doesnt-need-new-laws/ (accessed 9 September 2016).

World Economic Forum (2015), *Deep Shift Technology Tipping Points and Societal Impact: Survey Report, September 2015.*

World Economic Forum (2016), *The future of financial inftrastructure: An ambitious look at how blockchain can reshape financial services*.

Wright, D. (2002), “Comparative Evaluation Of Electronic Payment Systems”, *INFOR: Information Systems and Operational Research*, Vol. 40 No. 1, pp. 71–85.

Yermack, D. (2013), *Is Bitcoin a Real Currency? An economic appraisal*, NBER Working Paper No. 19747.

Yu, E. (1997), “Towards modelling and reasoning support for early-phase requirements engineering”, 6-10 Jan. 1997, Annapolis, MD, USA.

Yu, E.S. (2009), “Social Modeling and i*”, in Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Borgida, A.T., Chaudhri, V.K., Giorgini, P. and Yu, E.S. (Eds.), *Conceptual Modeling: Foundations and Applications*, *Lecture Notes in Computer Science*, Vol. 5600, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 99–121.

Zagaris, B. and MacDonald, S.B. (1992), “Money laundering, financial fraud, and technology the perils of an instantaneous economy”, *The George Washington journal of international law and economics*, Vol. 26 No. 1, pp. 61–107.

Zohar, A. (2015), “Bitcoin: Under the Hood”, *Communications of the ACM*, Vol. 58 No. 9, pp. 104–113.

Zott, C., Amit, R. and Massa, L. (2011), “The Business Model: Recent Developments and Future Research”, *Journal of Management*, Vol. 37 No. 4, pp. 1019–1042.