Distributed Ledgers for the
Prevention of Accounting Fraud

Blockchains Between Expectations and Reality

Inaugural-Dissertation
zur
Erlangung der Doktorwürde
der Wirtschafts- und Verhaltenswissenschaftlichen Fakultät
der Albert-Ludwigs-Universität Freiburg i. Br.

vorgelegt von
Nadine Rückeshäuser
aus Bad Soden am Taunus

Sommersemester 2017
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: 19.05.2017
Datum des Promotionsbeschlusses: 03.07.2017
Acknowledgments

I am deeply grateful to several people, who guided and supported me throughout the journey of writing this dissertation and contributed in many different ways to it. I want to express my sincere gratitude to them.

I want to express my deepest gratitude to my doctoral supervisor Professor Dr. Dr. h.c. Günter Müller for his excellent guidance and caring over the past 2 years, proving me with an excellent atmosphere for doing research. I also want to emphasize his role for my personal development, for which I am truly indebted and thankful. What I have learned goes far beyond specialized knowledge and technical competences. Overall, I found my time as doctoral student at the Institute of Computer Science and Social Studies as especially pleasant, very productive and creative. Thank you for all the encouragement!

I want to show my gratitude to Professor Dr. Dieter K. Tscheulin, who was the second reviewer of my dissertation as well as an examiner at my Rigorosum. Thank you for your contribution and support during the last weeks of my doctorate. I further want to thank Professor Dr. Günter Knieps, who was an examiner at my Rigorosum as well.

It is a great pleasure for me to thank all my current and former colleagues, who made the process of writing my thesis a valuable and great experience. Especially, I want to thank Dr. Christian Brenig, who encouraged me to do my doctorate and with which I worked together several times in terms of teaching and researching. I want to thank Adrian Lange, Claus-Georg Nolte, Julius Holderer as well as Richard Zahoransky and Anja Jülch for the great time at the institute as well as for the help and guidance throughout the process of writing my thesis and everything associated with it. I want to thank Dr. Christian Zimmermann, who left the institute shortly after my start of work; nevertheless, it was a truly enriching encounter on a technical as well as personal level.

I am especially grateful to my family, my parents Ariane and Robert, my grandparents Inge and Wolfgang and my brother Florian, who have supported me unconditionally with emotional as well as any other kind of support not only during the time of writing this thesis but already my whole life. I am also grateful to all other family members and friends, which I cannot mention here individually. I am convinced that this thesis would not have been possible without your support.

I am truly thankful to Markus, my future husband and love of my life, who was at my side during the whole process of researching and writing this thesis and supported me at any time in any possible way. Your contribution to this thesis was especially important, since you were expecting nothing but excellence from me, you boosted me morally and provided me constantly with great emotional support.
Acknowledgments

Nadine Rückeshäuser
# Table of Contents

1 Improving Accounting Fraud Prevention Through Distributed Ledger Technology .......................................................... 1

    1.1 Definitions: Bitcoin, Blockchains and Distributed Ledgers ................................................................. 3

    1.2 State of the Art and Identified Research Gap .......................................................... 6

    1.3 Research Questions and Objectives .......................................................... 9

    1.4 Outline, Related Publications and Contributions .......................................................... 14

2 Economics of Distributed Ledgers: Value Generation and Business Strategies .......................................................... 19

    2.1 Why Bitcoin Failed: An Analysis of User Acceptance .......................................................... 21

        2.1.1 The Trust Model of Bitcoin .......................................................... 22

        2.1.2 Determinants of Trust .......................................................... 23

        2.1.3 Explanation and Prediction of Trust in Bitcoin .......................................................... 25

        2.1.4 Research Method .......................................................... 28

        2.1.5 Data Analysis and Interpretation .......................................................... 29

        2.1.6 Implications and Discussion of the Results .......................................................... 33

    2.2 Distributed Ledger Business Model Transformation .......................................................... 34

        2.2.1 The Concept of the Business Model .......................................................... 35

        2.2.2 Case Studies and Selected Business Model Cases .......................................................... 38

        2.2.3 Methodology and Morphological Box .......................................................... 40

        2.2.4 Typology of Distributed Ledger Based Business Models .......................................................... 43

        2.2.5 Implications of the Typology and Discussion of the Results .......................................................... 48

    2.3 Interim Conclusion .......................................................... 49

    2.4 Contextualization: Distributed Ledgers, Digital Business Ecosystem and User Sides .......................................................... 50

    2.5 Evaluation Framework for Distributed Ledgers .......................................................... 53

        2.5.1 On the Notion of Value and Value Generation .......................................................... 53

        2.5.2 Framework: Evaluation of the Value of Distributed Ledgers .......................................................... 54

        2.5.3 Exemplification of Business Strategies and Value Creation .......................................................... 56

    2.6 Concluding Remarks .......................................................... 59
3 Accounting Fraud Prevention: A Requirements Analysis.......................... 61

3.1 Definition of Accounting Fraud and General Prerequisites ...................... 62
3.2 Existing Deterrence and Detection Techniques...................................... 65
3.3 Case Studies: How to Conduct Accounting Fraud? .................................. 68
   3.3.1 The Enron Scandal (Case Study 1).................................................. 68
   3.3.2 The Comroad Scandal (Case Study 2).............................................. 71
   3.3.3 The Parmalat Scandal (Case Study 3).............................................. 73
   3.3.4 Further Accounting Scandals.......................................................... 76
3.4 Generalization of Accounting Fraud Patterns......................................... 81
   3.4.1 Business Entities Dependencies and Mutual Control Functions .......... 82
   3.4.2 Requirements for the Prevention of Accounting Fraud....................... 84
3.5 Concluding Remarks ................................................................. 85

4 Distributed Ledger Design for Applications in Fraud Prevention............... 87

4.1 The Four-Layer Architecture of Distributed Ledgers and System Design
   Decisions.............................................................................................. 88
   4.1.1 Network Layer.................................................................................. 89
      4.1.1.1 Distributed Ledger Access Control ............................................ 90
      4.1.1.2 Node Authentication and Message Encryption ......................... 92
   4.1.2 Proccession Layer: Authorization and Validation............................. 94
      4.1.2.1 Distributed Consensus Mechanisms ......................................... 95
      4.1.2.2 Smart Contracts......................................................................... 99
      4.1.2.3 Peer-to-Peer-Network Free Riding............................................. 102
   4.1.3 Representation Layer.......................................................................... 108
   4.1.4 Storage Layer.................................................................................... 109
   4.1.5 Overview: Layer and Design Decisions for Accounting Applications .... 114
4.2 Interim Conclusion .................................................................................. 116
4.3 Paradigm Changes in Management Factors ............................................ 117
   4.3.1 Strategic Alignment Options ............................................................ 117
      4.3.1.1 Alignment Strategy 1: Distributed Ledger as Digital
        Infrastructure...................................................................................... 118
      4.3.1.2 Alignment Strategy 2: Distributed Ledger as Shared Platform.... 120
      4.3.1.3 Alignment Strategy 3: Distributed Ledgers as External
        Application .......................................................................................... 122
   4.3.2 Paradigm Changes and Relation to Alignment Strategies.................... 123
      4.3.2.1 Resilience versus Redundancy .................................................... 124
      4.3.2.2 CAP Goals Maximization versus Trade-Off ................................. 126
      4.3.2.3 Data Transparency versus Confidentiality.................................. 128
      4.3.2.4 Process Integrity versus Discretionary Decision-Making .......... 129
      4.3.2.5 (Pseudo-) Anonymity versus Undesired Behavior .................... 131
   4.3.3 Relationship Between Alignment Strategies and Paradigm Changes ...... 132
4.4 Distributed Ledger Customization Model for Fraud Prevention................ 135
# Table of Contents

4.4.1 Infrastructure Development .......................................................... 136
4.4.2 Deployment Mode Decisions ......................................................... 137
4.4.3 Application Foundation and Integration ........................................ 137
4.4.4 Application and Application Security ........................................... 138

4.5 Concluding Remarks ........................................................................... 139

5 Blockchain-Based Accounting: Scenario Development and Evaluation .......... 141

5.1 Scenario Definition ........................................................................... 142
5.2 Scenario Construction ........................................................................ 144
5.3 Scenario Specification ....................................................................... 147
  5.3.1 Automated Compliance Realization Through Distributed Ledgers ........ 147
  5.3.2 Compliance-by-Design in Blockchain-Based Accounting .................. 149

5.4 Interim Conclusion ............................................................................ 152

5.5 Evaluation: Does Decentralized Consensus Prevent Accounting Fraud? .... 153
  5.5.1 Game Theoretic Analysis Framework ............................................ 154
    5.5.1.1 Setting 1: Internal Control System versus a Selfish Management ... 154
    5.5.1.2 Setting 2: Selfish Internal Auditor versus Selfish Management .. 156
  5.5.2 Does Incentives Set by Distributed Ledgers Prevent the Commitment of Accounting Fraud? ................................................................. 157
    5.5.2.1 Proof-of-Work ................................................................. 158
    5.5.2.2 Effect of Proof-of-Work on the Incentive to Conduct Fraud ....... 159
  5.5.3 Analysis of Further Decentralized Consensus Mechanisms ............... 162
    5.5.3.1 Proof-of-Stake ............................................................... 163
    5.5.3.2 Delegated Proof-of-Stake ............................................... 165
    5.5.3.3 Proof-of-Activity ........................................................... 166
    5.5.3.4 Further Proof-of-Work Based Derivatives ......................... 167
    5.5.3.5 Federated Byzantines Agreement ...................................... 168
  5.5.4 Discussion: Transferability of the Results and Other Solutions ........... 169

5.6 Concluding Remarks ........................................................................... 171

6 Conclusion and Outlook ......................................................................... 173

6.1 Main Findings and Discussion of the Results ...................................... 173
6.2 Limitations ......................................................................................... 177
6.3 Implications for Further Research: Towards Process-Centered Research on Distributed Ledger Technology ....................................................... 179

Appendix ................................................................................................. 181

References ............................................................................................. 200
List of Figures

Figure 1. Graphical representation of the terminology ......................................................... 5
Figure 2. Approach: Analysis of distributed ledger applications for fraud prevention .......... 9
Figure 3. Modified technology acceptance model ................................................................. 27
Figure 4. Participants' assessment of perceived security and perceived privacy ................. 29
Figure 5. Participants' assessment of perceived ease of use and perceived usefulness .... 31
Figure 6. Contextualization of distributed ledgers and business strategies ...................... 51
Figure 7. Occupational fraud tree (ACFE, 2017) .................................................................... 63
Figure 8. The new fraud triangle model (Kassem and Higson, 2012) ................................. 65
Figure 9. Security extended enterprise metamodel (Müller und Accorsi, 2013) .......... 66
Figure 10. Generalization of identified fraud patterns ............................................................. 82
Figure 11. The four-layer architecture of distributed ledgers ................................................. 89
Figure 12. Rule types and specifications ................................................................................... 95
Figure 13. Simplified representation of the hash structure 'linked list' ............................... 111
Figure 14. Simplified representation of the hash structure 'Merkle tree' ......................... 112
Figure 15. Simplified representation of the blockchain ......................................................... 113
Figure 16. Alignment strategy 1: Distributed ledger as digital infrastructure ............... 119
Figure 17. Alignment strategy 2: Distributed ledgers as shared platform ......................... 121
Figure 18. Alignment Strategy 3 – Distributed ledgers as external application .......... 123
Figure 19. Distributed ledger implementation and customization model ....................... 136
Figure 20. Scenario of blockchain-based accounting ............................................................ 145
Figure 21. Process of compliance realization through distributed ledgers .................... 149
Figure 22. Information-processing view on blockchain-based accounting .................... 150
List of Tables

Table 1. Overview of chapters and related publications ........................................... 15
Table 2. Technology- and user-related characteristics ............................................... 24
Table 3. Cognitive responses and associated user-related characteristics ................. 26
Table 4. Overall assessment of the fulfillment of user-related characteristics ............ 32
Table 5. List of business model features ....................................................................... 37
Table 6. Overview of companies disclosing information about their business model.... 38
Table 7. Short form business model description UniquID ............................................ 39
Table 8. Short form business model description DXMarkets ...................................... 40
Table 9. Morphological box for distributed ledger based business models ............... 42
Table 10. Business model type I.: Data infrastructure provider ................................. 44
Table 11. Business model type II.: Development facilitator ......................................... 45
Table 12. Business model type III.: Integration enabler ................................................. 46
Table 13. Business model type IV.: Application provider ............................................. 47
Table 14. Business model type V.: Supporting or supplementary services ............... 48
Table 15. Value framework for distributed ledgers ....................................................... 55
Table 16. Overview of further accounting scandals and explanatory factors .......... 80
Table 17. Classification of peer-to-peer networks ....................................................... 90
Table 18. Overview of Distributed Ledger Layer and Design Decisions .................... 115
Table 19. Paradigm Changes Implied by Distributed Ledger Technology ............... 124
Table 20. Paradigm Changes and Relation to Alignment Strategies ............................. 133
Table 21. Scenario set for blockchain-based accounting ............................................ 143
Table 22. Payoff matrix first setting: audit vs. selfish management ............................ 155
Table 23. Payoff matrix second setting: selfish auditor vs. selfish management ....... 157
Table 24. Payoff matrix second setting with high costs ............................................. 160
Table 25. Overview of distributed consensus mechanisms ....................................... 162
### List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>Accounting Information System</td>
</tr>
<tr>
<td>BPM</td>
<td>Business Process Management</td>
</tr>
<tr>
<td>BTC</td>
<td>Bitcoin (native coin in the Bitcoin system, denoted with lower case b)</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-Peer</td>
</tr>
<tr>
<td>PoW</td>
<td>Proof-of-Work</td>
</tr>
<tr>
<td>PoS</td>
<td>Proof-of-Stake</td>
</tr>
<tr>
<td>PoA</td>
<td>Proof-of-Activity</td>
</tr>
<tr>
<td>SEC</td>
<td>U.S. Securities and Exchange Commission</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture</td>
</tr>
<tr>
<td>TAM</td>
<td>Technology Acceptance Model</td>
</tr>
<tr>
<td>T-TAM</td>
<td>Trust-extended Technology Acceptance Model</td>
</tr>
<tr>
<td>TTL</td>
<td>Time-to-Live</td>
</tr>
<tr>
<td>2P-PoW</td>
<td>Two-Phases Proof-of-Work</td>
</tr>
</tbody>
</table>
1 Improving Accounting Fraud Prevention Through Distributed Ledger Technology

Accounting fraud is a worldwide phenomenon that affects and happens in corporations on every continent and in all sectors of the economy (Bhasin, 2013). The negative consequences of accounting fraud impact not only the company itself, for instance, through significant economic losses that sometimes even lead to bankruptcy; The unveiling of illicit accounting practices also frequently results in a loss of shareholder’s confidence and undermines investor’s trust, thereby, inducing negative effects on financial and investment markets, which manifest itself in overpriced securities and over-borrowing of firms (Gerety and Lehn, 1997; Sadka, 2006). Accordingly, the Enron scandal (2001), the WorldCom scandal (2002) as well as the Freddie Mac (2003) and Fannie Mae scandal (2004) are only a few examples of accounting fraud incidents, whose negative economic effects elevated the awareness and responsibilities for the deterrence, prevention and detection of accounting fraud (Hogan et al., 2008). Thus, following these events, several methods for securing accounting processes were developed, reaching from the refinement of legal regulations and standards, tools for the detection of policy violations, the specification of processes using Petri nets, monitoring approaches to trace process execution and responsibilities as well as a posteriori analysis mechanisms, such as auditing methods for the screening of event logs (Müller and Accorsi, 2013). Nevertheless, given reoccurring accounting fraud attempts, until today, there seems to be no appropriate technical as well as organization or legal mechanism that is capable of preventing the emergence of fraud or whose detection probability is sufficiently high to deter potential perpetrators from the commitment of accounting fraud (AICPA, 2005; ACFE, 2016).

This could change given distributed ledger technology, which is frequently proposed as a possible mechanism for the prevention of accounting fraud (e.g. Yermack, 2015; Fanning and Centers, 2016; Iansiti and Lakhani, 2017). In particular, distributed ledgers are shared, distributed databases that are maintained by a peer-to-peer network and secured through distributed consensus and cryptographic mechanisms. Distributed consensus is a method to reach consensus between distributed peers with different incentives within the network, through which, principally, the automated execution and enforcement of nearly any set of rules, that is pre-specified in the protocol, can be supported. Given this digital infrastructure, distributed ledgers are expected to enable so-called real time accounting, which facilitates the maintenance of permanent and timely records of financial transactions as well as automated and decentralized authentication
and validation of transactional data on the ledger (Yermack, 2015; Pinna and Ruttenberg, 2016; Seibold and Samman, 2016). The benefit of the decentralized nature of distributed ledgers is, thereby, that no central instance is necessary to guarantees the correctness of transactions, which probably reduces time and costs. However, despite the characteristic of decentralization, distributed ledgers, furthermore, introduce transparency of ledger entries, which together with cryptographic securing implies potential immutability. In particular, immutability of distributed ledger entries means that financial records cannot be altered ex post and, if so, the probability of detection will be very high (Andersen, 2016). Given these features, accounting processes facilitated through distributed ledger could possibly rule out the conduction and concealment of improper accounting methods, illicit structuring of transactions and financial database manipulations through the features decentralization, transparency and potential immutability (Feng et al., 2011; Yermack, 2015; Andersen, 2016).

In view of the potentials enabled by the features of the technology, the term distributed ledger became a dictum, not only in the scientific context. Notably, there is hardly any major industry that does not try to exploit the opportunities opened up by the technology and potential use cases, in order to decrease costs and to smooth value chains. Examples of further application areas include, among others, the application of distributed ledgers in the realm of logistics, health care or biotechnology (Rückeshäuser, 2017c). However, while the opportunities opened up by the technology sound promising, problems arise, if current implementation- as well as technology-related challenges are neglected and not considered sufficiently. For instance, one of the major barriers for the implementation of distributed ledgers in the financial sector is immaturity of the technology as well as a lack of a clear concept, how to increase return on investments through appropriate implementation, incentivizing and usage of distributed ledger technology (IBM, 2016a). Notably, the need for a suited implementation mode and associated incentivizing is especially important, if undesired and even illicit behavior of network participants should be avoided. Related to this problem is the existence of numerous misleading assumptions about the technology’s characteristics and associated abilities. One example of such a misjudgment is the assumptions that data on distributed ledgers are always immutable. In fact, however, immutability of data is determined by a variety of factors, among others, by network size and the applied distributed consensus mechanism, with which data are incorporated into the ledger. Presupposing such assumptions without reflecting determinants, led to the present state of ‘distributed-ledger-hype’, resulting in inflated expectations about the technologies capabilities. In the worst case, wrong expectations result in non-economically investments that are caused by research and development efforts, ultimately leading to unexpected and undesired results. One recent example thereof is the research and development project R3
CEV, which started to explore the potentials of distributed ledgers for the financial industry that, now, ended up with the development of an inter-bank network that is inspired by, but generally does not need distributed ledger architecture after investments amounting to $59 million (Brown, 2016; Suberg, 2017).

To avoid economic losses as a result of misperceptions about the technology’s capabilities, a more careful assessment of the technological features and its interactions with the respective environment is necessary. The following thesis will, therefore, be developed within the described field of tension and investigates the application of distributed ledger technology in accounting. In particular, the overarching research question of this thesis is: (RQ.) Do distributed ledgers, applied as foundational technology in accounting information systems, prevent accounting fraud through its characteristics decentrality, transparency and potential immutability? Thus, it will be investigated whether, and if so, how distributed ledger technology prevents the emergence of accounting fraud. Thus, simultaneously, this thesis is an appeal to reject the seemingly existing normative premise to apply distributed ledger technology, without a critical review of its actual capabilities. Consequently, in the following, not a mere technological or economic perspective on distributed ledgers is provided: A corporate perspective on the implementation of distributed ledger technology and associated adjustment processes to existing infrastructures is emphasized that links the technological to the economic domain, resulting in a more realistic view on the technology’s capabilities as well as implementation and incentivizing issues. However, before the application of distributed ledgers for accounting fraud prevention is discussed, first, a terminology is provided, not only for the term distributed ledger but also for the related concepts blockchain as well as Bitcoin.

1.1 Definitions: Bitcoin, Blockchains and Distributed Ledgers

In order to understand and assess the potentials and opportunities distributed ledgers deliver for accounting fraud prevention, first, a consistent approach concerning the terminology is needed, which especially holds with regard to the central terms Bitcoin, blockchain and distributed ledger as well as the associated concept of distributed consensus. Notably, the terms blockchain and distributed ledger are often used as synonyms, but actually lead to divergent implications once applied in a concrete application scenario, owing to the particularly related technological features. In order to receive clarity about the differences but also the relationships between the terms, a pragmatic approach for the description of the terminology is chosen, following the temporal, technological development and the associated notions.
Distributed ledgers evolved originally from the world of virtual currencies and decentralized payment systems, of whom Bitcoin is the most prominent as well as first use case (Pinna and Ruttenberg, 2016). The payment system Bitcoin is based on cryptographic proof and a peer-to-peer network, allowing any two willing parties to transact directly without the need for a trusted third party. By this, Bitcoin positions itself as an alternative to trust-based models that rely on financial intermediation, which increases transactions costs and cuts off the possibility for small casual transactions as well as so-called micro-transactions (Nakamoto, 2008). A bitcoin (denoted with lower case b), which is the native asset transferred by using the peer-to-peer payment network, is a fixed-value cryptographic object, represented as a chain of digital signatures over the transactions, in which the bitcoin was used. The validity of a bitcoin can be checked by simply examining the cryptographic validity of the signature that constitutes its history, whereas the history is recorded using a special type of a distributed ledger (Kroll, Davey and Felten, 2013).

The distributed ledger underlying Bitcoin is called blockchain, which ensures transactions to be aggregated chronologically in so called blocks and added to a chain of existing transactions applying cryptographic signatures (Fanning and Centers, 2016). New blocks are referenced to the preceding block by using hash values, meaning that blockchains represent a history of information stored on it and the chronological ordering of information constitutes an inherent feature of blockchains (Taylor, 2013). The integrity and security of data is provided by so-called ‘miners’ that exert effort to validate and store information on the blockchain, whereas, generally, every node in the Bitcoin network could be a miner, provided that the node has the right and capability to expense a sufficient amount of mining effort (Walport, 2015). Bitcoin mining and the maintenance of the blockchain requires global, i.e. network-wide, decentralized consensus that is achieved by solving proof-of-work (PoW), which is a mechanism specified in the decentralized consensus protocol. Particularly, proof-of-work consists in solving a challenging computational puzzle and was originally invented in the early 1990s to prevent, among others, various forms of denial-of-service attacks and abuse in anonymous networks (Bonneau et al., 2015). In the case of the blockchain, if the mathematical puzzle is solved correctly, a transaction is added to a block, which is subsequently affiliated to the blockchain (Nakamoto, 2008). Through this proceeding, the double-spending problem is solved, meaning that it is not possible to spend a single digital token twice (Nakamoto, 2008; Bonneau et al., 2015). Summarizing, Bitcoin can be defined as a special use case of a distributed ledger, whereas the distributed ledger applied in the case of Bitcoin is called blockchain that generally features decentralization, transparency as well as chronological ordering of blockchain entries. However, despite the usage of blockchains in the case of Bitcoin, blockchains can also be applied for other purposes,
which necessitate a chronological and potentially fully public storage for any kind of information. Contrarily, this does not imply that a chronological information record must necessarily back every distributed ledger. For instance, a contrary design of a distributed ledger compared to a blockchain, implies that ledger entries are stored in a non-chronological order and that there exist restricted transparency by limiting the network access to a particular group, e.g. individuals within a corporation (Rückeshäuser, 2017c).

Figure 1. Graphical representation of the terminology

The resulting relationships of the terminology are graphically represented in Figure 1. Summarizing, a distributed ledger is a distributed and shared database that is maintained through consensus in a distributed peer-to-peer networks and can, but must not necessarily feature chronological storage. A blockchain is defined as a sub-type of distributed ledgers, featuring chronological storage and most often complete transparency. In combination with the applied distributed consensus mechanisms blockchain potentially imply immutability of information stored on the ledger. For instance, certain consensus mechanisms enable counterfeit protection – at least to some degree – by enforcing the exertion of scare resources for data alteration or verification, which makes fraud or any other kind of data manipulations computational hard (Nakamoto, 2008; Becker et al., 2013). Bitcoin, for example, employs Proof-of-Work that requires peers in the network to solve a mathematical puzzle and to use their computer power to verify and alternate ledger entries. Thereby, changes of transactions incorporated into the blockchain are hard to conduct or possibly not feasible for a single peer (Nakamoto, 2008). However,
the concrete choice of a particular distributed consensus mechanisms depends also on further requirements, such as the desired ledger performance, scalability or security (Seibold and Samman, 2016). Nevertheless, every distributed ledger necessitates one kind of consensus mechanisms to find consensus between peers in the distributed system.

Given this fundamental description of the terminology the flexibility of the technology in regard to ledger design already gets apparent. Notably, this flexibility enables the application of distributed ledgers in various business activities such as accounting and as digital infrastructure within divergent environments, e.g. corporations. In the following a stronger focus is placed on the concrete implementation of the technology within a corporation for the facilitation of accounting fraud prevention as well as associated steps that will be discussed in the course of this doctoral thesis. In the following, the analysis will refer mainly to the term and construct of distributed ledgers instead of blockchain, even if automated chronological ordering is certainly a desirable feature in the context of accounting. However, this terminology is chosen purposefully as using the term distributed ledger implies the broadest range of possible ledger design decisions and, consequently, flexibility and adjustment possibilities that are needed for the subsequent investigations. However, before implementation possibilities are discussed in the following it should be further elaborated, which features and how distributed ledger are supposed to prevent accounting fraud according to the existing literature on this topic.

1.2 State of the Art and Identified Research Gap

Academic literature as well as industrial white paper frequently propose the application of distributed ledger for accounting and accounting fraud prevention. The rational behind this proposal is that the previously described characteristics of distributed ledgers are expected to enable real-time accounting, thereby, reducing accounting fraud incidents, owing to increased transparency as well as decentralized consensus that rules out arbitrary modifications of ledger entries through individual peers. In the following, six exemplary and widely recognized paper proposing the application of distributed ledger technology for accounting are presented, including their argumentation of expected effects on the accuracy of accounting data as well as potential overarching effects.

Yermack (2015) suggests the application of distributed ledger technology for real time accounting, while building his analysis concerning the potentials of the technology mainly on Lazanis (2015). In particular, both authors propose that a firm that uses a blockchain could voluntarily post all ordinary business transactions on the ledger, thereby imposing transparency for shareholders, since all transactions would be visible.
immediately. Moreover, entries on the blockchain can be prevented from being altered ex post through digital time stamps. Firms could use digital currencies to automate this proceeding or can apply other tokens or even conventional currencies, if the network is restricted to a particular amount of peers through permissions (Lazanis, 2015; Yermack, 2015). Yermack and Lazanis further emphasize that this form of real-time accounting would have positively effects for shareholder, since they are no more enforced to trust auditors and the integrity of managers, but are rather able to make their own judgment by creating their statements autonomously from the transparent ledger for whatever time period they wish. More importantly, in the context of this thesis however, is that distributed ledgers are expected to reduce financial statement fraud and earnings management, respectively, owing to the irreversibility of entries on the distributed ledger and time stamping, which decreases the opportunities to manipulate reports through particular fraud strategies or exploiting legal gray areas through, e.g. backdating of sales contracts prior to a reporting period (Yermack, 2015). Lastly, related party transactions and suspicious asset transfers may be prevented according to the authors, as transparency would impact managerial incentives. Thus, insiders would have less incentives to tunnel assets out of the firm, which permits creditors to engage in real-time surveillance against fraudulent conveyances by distressed firms (Lazanis, 2015; Yermack, 2015).

Similar to Yermack (2015) and Lazanis (2015), Byström (2016) emphasizes that real time accounting enabled through distributed ledgers could improve the quality of accounting data, by making ledger entries not only more trustworthy but also more timely. Despite that, the author predominantly focuses on the effects of real time accounting for credit risk modeling, where it is implicitly assumed that ambiguous and non-uniform accounting practices, creative accounting or financial reports that lag real events, can be ruled out by the application of distributed ledgers as foundational technology for accounting information systems (Byström, 2016).

Fanning and Centers (2016) stress the effects of distributed ledger enabled real time accounting for auditing and the accountant’s profession. In particular, by using blockchains, accounting entries between two trading partners could be easily compared without threatening data privacy. Thereby, the reliance on auditors for testing financial transactions could be significantly reduced (Fanning and Centers, 2016). Apparently, the argumentation of the authors is based on the assumption that data entries on the distributed ledger cannot be altered ex post, however, they did not take into account the problem that accounting information may be manipulated ex ante.

Andersen (2016) introduces distributed ledger technology as a ‘game changer’ in accounting, helping the industry to grow out of its infancy in terms of technology use. In contrast to the previous authors, Andersen proposes a joint register, where two or more corporations record their transaction history, thereby creating an interlocking system of
enduring accounting records (Andersen, 2016). Based on the assumption that records are immutable and firms exert mutual controls, corporations could benefit according to the author from distributed ledger based accounting in two ways: first, standardization, which allows auditors to verify large portions of data beyond mere financial data automatically, leading to cost and time reduction; Second, auditors could spend more time on activities that add more value, such as auditing very complex transactions or internal control systems (Andersen, 2016).

Most recently, Watson and Mishler (2017) highlighted that distributed ledgers not only enable real time accounting but also substitute the traditional double-entry general ledger system by triple-entry accounting, in which all accounting entries involving outside parties can be cryptographically sealed by a third entry, which is the chain of validated prior transactions. Notably, while the implied proceeding to place digital blocks side by side could solve many data integration issues, it could also help to prepare more accurate financial statements and business analytics through transparency and immutability of entries, thereby, even increasing productivity of business processes (Watson and Mishler, 2017).

Further examples of proposals to apply distributed ledgers in the realm of accounting include among others Swan (2015), Peters and Panayi (2015), Brandon (2016), as well as Tapscott and Tapscott (2016). Notably, not all authors discuss the application of distributed ledger technology in detail. However, most often they refer to the literature stated above and emphasize their argumentation by applying the already mentioned assumptions and, especially, the assumption of immutability of ledger entries.

Overall, the previously stated literature presents a very positive image of distributed ledger applications in accounting, whereas the technology seems to alleviate several of contemporary problems in accounting, i.e. timeliness and prevention of accounting fraud (Swanson, 2015; Yermack, 2015; Watson and Mishler, 2017). In contrast, this doctoral thesis asserts that this assessment might be a misperception given significant deficiencies with respect to the analyses of distributed ledger applications for fraud prevention that underlie the above cited works. In particular, two shortcomings shared by all of the cited papers can be identified: First, assumptions about the technological features of distributed ledgers are taken as given, without applying any critical questioning or review. This holds, as already mentioned, especially for the feature immutability of distributed ledger entries, which has been shown to be an untenable assumption given small network sizes (Becker et al., 2013). Literature that proposes the application of distributed ledgers for fraud prevention neither accounts for the possibility that ledger entries are mutable nor discuss the opportunity to alter entries already before they are entered into the system. Thus, severe misperceptions about the ledgers capabilities could arise at this point already. Second, these assumptions concerning the features aris-
ing from the technological design of distributed ledgers are directly transferred to the economic domain, as indicated by the shaded areas in Figure 2. The main problem, thereby, is that considerations about corporate specific implementations, i.e. the implementation of the distributed ledger within existing corporate infrastructures as well as business models that mediate between the technological domain and the economic domain are neglected, leading to a mere theoretical discussion about the application of distributed ledger in accounting that lack any practical approach and considerations. Moreover, works highlighting the opportunity of fraud prevention through distributed ledgers exclude existing and potential future system-human-interactions from their analyses, resulting in the ignorance of actual problems in corporate accounting, such as the emergence of accounting fraud despite existing technical and organizational precautions as well as legal prosecution.

Figure 2. Approach: Analysis of distributed ledger applications for fraud prevention

To tackle the overarching research question and the identified shortcomings, a comprehensive analysis of distributed ledger applications for accounting fraud prevention is proposed, while taking into account the interdependencies presented in Figure 2. Especially, this implies bridging theoretical consideration and concrete application scenarios by taking a firm-centered perspective and focusing on the alignment of distributed ledger technology with existing business processes as well as infrastructures (Rückeshäuser, 2017a).

1.3 Research Questions and Objectives

Research questions that constitute the necessary steps to answer the overarching research question (RQ.) of this thesis are presented in the following and their objectives are discussed.
(RQ.1): What is the business value of distributed ledger technology and how does value emerge?

The proposal to apply distributed ledgers for accounting fraud prevention is initially based on the expected effect on accounting processes implied by the already mentioned characteristics of distributed ledgers. However, so far, it is not clear, how exactly the business value from distributed ledger emerges and how the induced effects are exploited for accounting fraud prevention. The question, how value though distributed ledger emerges is particularly important, since the business value of IT is expected to be not a mere technological issue but a joint technological-organizational development (Mooney, Gurbaxani and Kraemer, 1996). Consequently, the first research question investigates how business value emerges by analyzing actual use cases on the one hand, and conducting a theoretical evaluation of the economic effects of distributed ledgers on the other hand. In particular, RQ.1, which is subdivided into two related research questions, provides insights on the technical and organizational changes induced by distributed ledger that lead to value creation and capture, thereby, providing a framework for firms, how to exploit the characteristics and induced effects of the technology for the support of accounting processes.

(RQ.1a) Which distributed ledger based business models are currently applied and how can these business models be characterized?

The discussion about the potentials of distributed ledgers underlies the assumption that distributed ledger technology potentially disrupts existing business models and shapes business alignment. Questionable, however, is how exactly distributed ledger based business models look like as well as how and to which degree they shape the contemporary way of doing business and interactions with the surrounding ecosystem. One such example of a new business model is the above noted distributed payment system Bitcoin, which is expected to disrupt traditional business models and modes of interactions within the financial market. Despite an investigation of the concrete application case of Bitcoin, answering RQ.1a requires an extended approach that is capable of investigating the effects of distributed ledgers on business models and on a more general level. Consequently, an investigation of currently existing business models is necessary, through which a characterization of different distributed ledger based business models should be achieved based on pre-specified parameters. These business models are subsequently compared to each other as well as to other contemporary, IT-enabled business models. Overall, answering RQ.1a is expected to deliver insights on, how at to which degree distributed ledger shape existing business models, thereby, providing first indications on the business value generation through the technology.
(RQ.1b) Which business strategies underlie the identified distributed ledger based business models and how can value creation through the technology be captured and measured?

Identifying business models underlying actual distributed ledger applications, possibly does not fully reveal the induced organizational as well as social changes that imply value generation for the respective business. Consequently, by answering RQ.1b, business strategy is linked to business models, whereas the first describes, how individuals should interact and make decisions throughout a company in order to create value for the corporation and to achieve key objectives defined in the business model (Watkins, 2007). A related questions that are necessary to answer RQ.1b is, therefore, why distributed ledgers are used in a particular application case, meaning that the expected economic effects that underlie the decision to facilitate business models and associated processes by means of distributed ledgers must be investigated. Moreover, the general economic mechanisms that are accelerated by distributed ledgers and that facilitate value creation must be investigated by using an appropriate analysis framework. Finally, it must exemplified, how the emerging value can be measured that is created through the technology, by exemplifying business strategies that underlie the previously identified business models.

(RQ.2): What are the current fraud patterns in accounting that should be prevented through distributed ledger technology?

Today, various technical as well as organizational precautions exist that should prevent the emergence of accounting fraud or should lead to immediate detection of fraud patterns. Notwithstanding these precautions, accounting fraud frequently occurs and had its last peak at the beginning of the 21th century, including accounting scandals like Enron or Parmalat. More recent account scandals were, furthermore, characterized by not only drastic economical, but also social impacts that emphasize the urgency of more effective fraud prevention techniques. However, before distributed ledgers can be applied for accounting fraud prevention, first, recent accounting fraud incidents must be analyzed, the circumstance of their emergence as well as how the perpetrators concealed fraud. To this end, a definition as well as the circumstances that lead to the conduction of fraud must be discussed generally. Against this background, case studies are proposed to answer RQ.2 and to identify fraud patterns. Given the actual system-human-interactions, it must be discussed, how distributed ledger may change interactions and incentives in such a way that fraud is impeded. The successful application of distributed ledgers in accounting would require that current fraud patterns are prevented. Notably, from a corporate perspective, the costs and efforts associated with the implementation of distributed ledgers as well as organizational adjustment processes are only justified, if the prevention of accounting fraud can be expected.
(RQ.3): Does the technical architecture of distributed ledgers fit for the purpose of accounting and is it capable of preventing accounting fraud?

Given the characteristics of distributed ledgers as well as the induced effects on business models and strategies, the previously presented fraud patterns can potentially be prevented. However, the other side of the coin is that distributed ledger also imply significant technological, organizational as well as social paradigm changes, which corporations need to address properly in order to adjust distributed ledger technology to already existing technical infrastructures and business processes. Consequently, RQ.3 is concerned with the questions, how the technical infrastructure of distributed ledger is designed, which design opportunities are possible and, lastly, which technological, organizational and social impacts are implied. Notably, RQ.3 focuses on a process-oriented view and is, thus, expected to deliver insights on the alignment of accounting processes and distributed ledger technology, by which fraud patterns may be prevented. RQ.3 will be answered by analyzing the following related research questions.

(RQ.3a): How is the technical architecture of distributed ledgers designed and what are the associated ledger design decisions that enable its application for the prevention of accounting fraud?

So far, distributed ledgers were treated as a ‘black box’ and investigated with respect to their expected economic effects that are mainly induced by the feature decentralization, transparency and potential immutability. However, as already mentioned, the economic effects stem from and are determined by the technological features of distributed ledgers and the flexibility implied by possible design options. Thus, complementary to the economic justification for the variety of proposed application cases of the technology, now, the technical architecture of distributed ledgers must be analyzed. Especially, it must be discussed, how the technical architecture is designed and what particular technological features allow the obvious adaptability and flexibility of distributed ledger technology for various business purposes. Related to this issue is the discussion of distributed ledger design decisions that support accounting processes.

(RQ.3b): Which technical, organizational as well as social paradigm changes are implied by distributed ledger technology and how can firm approach these changes in order to prevent accounting fraud?

Distributed ledgers are expected to imply significant technological, organizational as well as social paradigm changes that challenge common business processes and necessitate adjustments of existing digital infrastructures. RQ.3b investigates these paradigm changes that result from the technical infrastructure of distributed ledgers and evaluates possible alignment strategies that mitigate these changes. Notably, the quality of mitiga-
tion is assumed to depend on the degree of technology and business process adjustments. Thus, in the focus of this investigation is the question, which alignment strategies may be suited, if the technology is applied in the context of accounting and what paradigm changes are implied by the particular distributed ledger design, depending on the chosen alignment strategy. Based on these investigation the results of this and previous analyses are compiled, leading to the question, how the components can be combined to a coherent model of distributed ledger implementation. In particular, the implementation of distributed ledgers into a corporation and the associated adjustment processes to already existing organizational structures as well as technical infrastructures must be taken into account. By answering RQ.3b and through its combination with the previous findings, a comprehensive foundation is expected to be developed that is helpful for practitioners as well as necessary, whenever a concrete application scenario should be investigated.

(RQ.4): Does distributed ledger technology prevent the emergence of accounting fraud?

After having discussed, how corporations can use the paradigm changes implied by distributed ledgers for supporting accounting processes and for the prevention of accounting fraud, now a concrete scenario for an intra-corporate, distributed ledger based accounting information system will be developed. In particular, it will be evaluated, whether or not distributed ledgers are a able to prevent accounting fraud, given the provided scenario.

(RQ.4a): How does a scenario of distributed ledger based accounting look like and through which mechanisms is accounting fraud prevented?

The first question related to RQ.4 is concerned with the technical design decisions necessary to achieve the desired organizational and behavioral changes that affects human-system-interactions, i.e. impedes the identified fraud patterns. Moreover, given decentrality of decision making implied by the technology, it must be discussed whether or not, and if so, how responsibilities are newly defined within the organization as well as how to design the structure of the company in such a way that fraud is impeded. Notably, the development of this scenario is equal to the development of an optimal scenario, which prerequisites making assumptions about distributed ledger features as well as network peer behavior. Consequently, this scenario deploys the reference scenarios for the subsequent analysis, in which the initial assumptions are successively relaxed.

(RQ.4b): Does the distributed ledger based accounting system and associated distributed consensus mechanism prevent the emergence of accounting fraud in the proposed scenario?
Given the reference scenario, the question whether or not distributed ledger based accounting systems are able to prevent fraud is reduced to the probability of, how likely it is that consensus participants behave according to the pre-specified rules in the protocol, i.e. do not conduct illicit actions. Answering RQ.4b, therefore, first requires the development of an appropriate analysis framework that can be adjusted to the proposed scenario as well as changing scenario assumptions. Based on the analysis framework, subsequently, different consensus mechanisms need to be explained and analyzed in order to investigate whether or not the applied consensus mechanism prevents the conduction of accounting fraud. Given the possibility that the emergence of accounting fraud is not prevented completely, it must be discussed whether the distributed ledger based accounting system enables opportunities for improved detection mechanisms or automated fraud detection. Consequently, overall it is investigated whether or not distributed ledgers enable both, a change in incentives that alters human-system-interaction in such a way that fraud is prevented or a change in the detection likelihood, meaning that the possibility of getting away with fraud possibly decreases.

1.4 Outline, Related Publications and Contributions

Table 1 provides an overview over the publications related to the respective chapters and an outline of the following dissertation. Moreover, the contribution of the respective chapters to this dissertation as well as to the state-of-the art in distributed ledger research is discussed.

<table>
<thead>
<tr>
<th>Chapter &amp; Research Question</th>
<th>Related Publications</th>
</tr>
</thead>
</table>
Table 1. Overview of chapters and related publications

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Chapter 6 Conclusion and Outlook</td>
</tr>
</tbody>
</table>
Putting aside the concrete application case of Bitcoin, further business models based on distributed ledgers are investigated in Chapter 2, in order to assess the impact of the technology on businesses. Based on an empirical analysis, a typology of distributed ledger based business models is developed, using six parameters that define a business model. Given the identified business models, their similarities and differences with other contemporary and IT-driven business models are discussed. Based on this analysis, the disruptive forces of distributed ledgers could not be attested. Notably, business models did not change significantly since the emergence of the technology in 2008. Consequently, either the disruptive forces of distributed ledger did not unleash so far or the technology changes businesses in a much more subtle way than by disruption. Eventually, a contextualization of businesses and the ecosystem, surrounding distributed ledger technology is provided, which links the previously analyzed business models to business strategy. Thus, whereas business models seem not to be influenced by the technology so far, business strategy may be influenced that affects the business model subsequently. Having identified different business strategies and the associated actors, an evaluation framework is developed that captures these strategies and translates them into value for businesses as well as customers. Thereby, a method to capture and quantify the value generated by distributed ledgers is provided, which delivers additional insights to the previously conducted business model investigation.

Overall, Chapter 2 provides insights on, how the business value of distributed ledger technology emerges and how the value manifests itself within a company through, e.g., organizational transformation. This provides not only a rational for using distributed ledger technology in accounting, but also shows how the technology will probably affect accounting processes as well as related business activities.

**Contribution Chapter 3:** Accounting fraud incidents are investigated in Chapter 3, which requires a definition of the term accounting fraud as well as circumstance that lead to the emergence of fraud. Moreover, currently applied fraud prevention and detection techniques are discussed, assuming that distributed ledger must at least provide the same level of security and fraud prevention as existing mechanisms. Most importantly, chapter 3 analyzes contemporary accounting fraud incidents to identify the circumstance that ultimately led to the emergence of accounting fraud. Thereby, the basic problem in accounting is defined, which distributed ledger technology must solve in order to prevent the emergence of accounting fraud.

**Contribution Chapter 4:** Chapter 4 presents a four-layer model of the distributed ledger architecture and discusses the technical foundations and associated technical design decisions for each layer. Thereby, the justification for the observed business models is provided from a technical perspective, by acknowledging that flexibility with respect to the technical design of distributed ledgers allows various business applications and the
application for fraud prevention. Moreover, technological, organizational and social paradigm changes that are implied by the technical architecture of distributed ledgers and associated design decisions are emphasized. In particular, these paradigm changes determine to which degree existing business infrastructures and business processes must be adjusted to the technology. Moreover, alignment strategies are presented that mitigate these changes through the adjustment of business processes and distributed ledger technology. Ultimately, this leads to an assessment, which strategy might be suited, if a distributed ledger should be applied for the prevention of accounting fraud. Moreover, chapter 4 discusses, how distributed ledgers can be customized to a particular corporation, business activity as well as processes, by providing a distributed ledger customization model, which combines all previous results of this thesis. By this, a framework for distributed ledger implementation is developed that delivers an orientation for corporations, which infrastructures, processes and further factors need to be considered and adjusted, if a distributed ledger is applied for fraud prevention.

**Contribution Chapter 5:** Chapter 5 evaluates the ability of distributed ledger applications to prevent accounting fraud. To this end, first, a scenario is defined and constructed according to Mahmoud et al. (2009), which implies the identification of relevant actors as well as their mode of interaction and associated relationships within the proposed scenario of a intra-corporate, distributed ledger based accounting system. After defining this general scenario, the scenario is specified by interpreting distributed ledger technology as an instrument for the realization of compliance, thereby shifting the focus rather on business processes than on organizational structures and relationships. The scenario specification is exemplified by describing the chronological sequence of a concrete transaction that is processed by an accounting information system based on distributed ledger technology.

Different decentralized consensus mechanisms are applied to the scenario and evaluated in order to assess, whether the respectively applied consensus mechanism is capable of preventing the emergence of accounting fraud, given the predefined fraud patterns. To conduct this assessment, first a game theoretic analysis framework is applied, through which the identified fraud patterns can be explained and that allows for changing payoffs in accordance to the applied decentralized consensus mechanism (note that this method can be applied, since the usage of scarce resources to validate or change information on a distributed ledger implies an economic calculus, meaning that the resource exertion can be approximated by the costs that are implied by applying, for instance, computer power in the case of proof-of-work). Beside the consensus mechanism proof-of-work, further decentralized consensus mechanisms are applied and evaluated, after a discussion of their general functioning. Furthermore, a discussion is provided that takes
up issues concerning the transferability and generality of the proposed scenario and, consequently, of the results of the scenario assessment.

**Contribution Chapter 6:** Chapter 6 summarizes the main results of this thesis and discusses its limitations. Moreover, an outlook on further research questions and a proposed orientation of future distributed ledger technology research is provided that follows this thesis.
2 Economics of Distributed Ledgers: Value Generation and Business Strategies

Since the emergence of Bitcoin, academics as well as practitioners expect significant economic benefits to arise from the application of distributed ledger technology, which can be reduced to the technological features of the shared database, i.e. decentrality, transparency, and potential immutability. In particular, distributed ledgers are typically referred to as disruptive technology, meaning that economic benefits will result from the opening of new markets as well as the displacement of contemporary business models, which typically rely on third party intermediation, thereby, inducing a significant amount of transaction costs (Christensen, 1997; Christensen and Overdorf, 2000; Böhme et al., 2015). In contrast, by enabling direct peer-to-peer interactions without the need for third-party verification, distributed ledgers pave the way for an open and scalable digital economy (Probst et al., 2016). However, despite the economic beneficence induced by the technological features of distributed ledgers, the discourse about the potentials and future applications of distributed ledger technology typically neglects that applying a disruptive technology always implies risks for a company; risks arise, especially, from the necessity for business process adjustments, organizational restructuring and associated investments in the technology as well as in change management (Johnson, Christensen and Kagermann, 2008; Tallon, 2008; Rückeshäuser, 2017a). Consequently, for companies, implementing and using distributed ledger technology is a trade-off, which also counts for the application of distributed ledger technology in accounting. One of the most important questions in this context, which is also the first research question of this thesis, is therefore (RQ.1): What is the business value of distributed ledger technology and how does it emerge? Notably, the emergence of the business value of distributed ledgers is important, since companies need to understand wherein the value of distributed ledger lies as well as how the business value emerges exactly within the desired application area and what are the interrelated organizational and economic consequences of technology use that may be positive as well as negative. In particular, only if companies can expect that value arises from the application of distributed ledger in accounting, i.e. that distributed ledger affect existing accounting processes and associated infrastructures in such a way that fraud is possibly prevented, a discussion about the challenges implied by technology implementation is necessary. Consequently, answering RQ.1 is expected to deliver, at first, the economic rational for applying distributed ledgers for fraud prevention.
In the following, RQ.1 is subdivided into two further research questions. The first question is: *(RQ.1a) Which distributed ledger based business models are currently applied and how can these business models be characterized?* Thus, to answer the question, how business value emerges through distributed ledger, firstly, an analysis of existing business models based on distributed ledger technology will be provided. In particular, this research questions delivers insights on how distributed ledgers shape existing business models and what are the organizational and economic effects that companies need to expect. To this end, first the case Bitcoin is investigated, as the current most prominent decentralized payment system and as an example of a particular business model based on distributed ledger technology. Thereby, Bitcoin constitutes one of the most interesting use cases, given the divergence between actual and intended usage of the payment system (Glaser and Bezzenberger, 2015). In fact, participants of Bitcoin use the native coins, called bitcoins, rather as speculative asset than as currency. Looking at Bitcoin, thus, delivers insights on how the technology defines the design of a business model and which design features lead to user behavior that is against expectations, i.e. shows possible system deficiencies and associated user reactions that should be avoided, when applying distributed ledgers for fraud prevention.

Despite the analysis of the concrete business model of Bitcoin, further distributed ledger based business models are analyzed in order to answer RQ.1a. In particular, business models are now investigated on a rather abstract level in order to provide a characterization and differentiation of distributed ledger based business models as well as from contemporary IT-based business models. To this end, an empirical study is conducted, which allows a typological differentiation and characterization. Ultimately, the purpose of answering RQ.1a is to identify the unique characteristics of distributed ledger technology as well as potential strength and weaknesses of ledger designs that are currently applied. This filters out the value of technology, i.e. the technological features and its impact on business models as well as the economic and organizational consequences, which helps firms to decide whether or not to apply distributed ledger for the business activity of accounting, and if so, how it could facilitate accounting information systems more specifically.

The second research question of this chapter and second step necessary for answering RQ.1 is: *(RQ.1b) Which business strategies underlie the identified distributed ledger based business models and how can value creation through the technology be captured and measured?* Consequently, after having identified the value of distributed ledger, now, the emergence of the business value of the technology is investigated by placing a stronger focus on business strategy that mainly determines organizational structures, business relationships, and especially competitive advantages (Al-Debei and Avison, 2010). The first step in answering RQ.1b is to classify businesses and their po-
tential customers in the wider context of an ecosystem that surrounds a distributed ledger. Thereby, the relationships and interdependencies between the technology, different types of business provider and the remaining ecosystem are defined. Particularly, the hereby-developed classification provides the basic framework for capturing value generation through distributed ledgers and can be interpreted within the broader context of business strategies. Apparently, there are intersections between business models and business strategy that frequently lead to confusions about the terminologies as well as interchangeable usage of the terms. However, following Al-Debei and Avison (2010), business models are assumed to deliver different information about a company than business strategy and that strategy determines and delivers the business model (Morris, Schindehutte and Allen, 2005; Al-Debei and Avison, 2010). Consequently, business value generation through distributed ledgers will be exemplified by providing an evaluation framework for distributed ledgers that includes the ecosystem and end-users, on which basis business strategies can be discussed. Notably, these two distinct steps deliver the economic foundation and justification for distributed ledger usage that facilitates business strategy and business models, respectively. Summarizing, based on these analyses, insights on the technological features and economic rational should be delivered that justify and make the application of distributed ledgers in accounting economically meaningful.

2.1 Why Bitcoin Failed: An Analysis of User Acceptance

Bitcoin is a decentralized payment system with no central trusted party and a variety of unknown participants in charge for the validity and correctness of payments (Nakamoto, 2008). Notably, the central trusted party is replaced by so called ‘sociality of code’, meaning that trust is technology-based and embedded within the system (Maurer, Nelms and Swartz, 2013). However, given the fact that user role, level of engagements as well as types of intervention in the system differ, discontinuities emerge that require that peers (also called nodes) trust each other, meaning that each node expects that the majority of other nodes behaves honest (Mallard, Méadel and Musiani, 2014). However, node behavior is significantly determined by the divergent interest of nodes as well as ledger design. Thus, in the following the trust model of Bitcoin is investigated, provided that trust is assumed as the main factor responsible for the actual usage of Bitcoin that is influenced by ledger design. Notably, design decisions should be identified that led to the unexpected user behavior in Bitcoin, thereby, providing indications, which system-user interactions must be considered for an application in accounting, which potentially can be reduced to a particular ledger design and its influence on a business model.
2.1.1 The Trust Model of Bitcoin

The decentralized payment system Bitcoin has the potential to disrupt existing payment mechanisms due to network features that allow for financial disintermediation (Böhme et al., 2015). Thereby, Bitcoin separates itself from conventional payment mechanisms, such as debit or credit cards, because it does not require central institutions to implement trust (Nakamoto, 2008). Through the omission of central institutions, significant transaction cost reductions can be achieved, which yields particular benefits for customers, such as the possibility to conduct micro-transactions, i.e. the transfer of very small transaction sums in an economically viable way (Jaag and Bach, 2014; Böhme et al., 2015). The decentralized and distributed architecture of Bitcoin, thereby, stands in stark contrast to the concept of a central entity in charge of regulating the actions of the network user. This function is delegated to the network itself, and the verification of transactions as well as creation of coins is implemented by the distributed network. Collectively, these features enable a system that is understood to be less expensive, more flexible, more private, and less amenable to regulatory oversight than other forms of payment (Böhme et al., 2015). Despite these advantages provided by the Bitcoin system, there exist a divergence between the intended and actual use of Bitcoin, whereas the effective use of the electronic payment system does not indicate widespread acceptance for retail payments. For instance, in 2014 transfers of over USD 100 represent a stable portion of Bitcoin activity, whereby these transfers are less likely to involve payments for retail goods and services (Badev and Chen, 2014). Still today, Bitcoin is seldom offered as means of payment for retail payments, which indicates that there may be some serious drawback preventing customers from using the decentralized payment system.

Former research has shown that there exist a strong relationship between the usage of a payment system and user’s trust (Pavlou, 2001; Gefen, Karahanna and Straub, 2003; Gefen and Straub, 2004). Consequently, it is important to identify the characteristics that lead to trust in Bitcoin as well as the lack thereof. Moreover, given the lack of a single trusted party, assumptions are necessary to define, how trust is spread across the network (e.g. whether everyone is trusted or particular network participants). Generally, trust is a central aspect of human behavior as well as in the focus of every economic transaction (Gefen, Karahanna and Straub, 2003; Gefen and Straub, 2004). The need to control and predict, or, at least to understand the social environment led to the development of rules and customs that provide some measure of social complexity reduction by regulating particular aspects of individual behavior. However, individual behavior is never fully controllable, leading to the fact that people rely on the expectation that individuals will behave, at least, in a socially acceptable manner, which is the essence of trust (Gefen and Straub, 2004). According to Mallard, Méadel and Musiani (2014), the
decentralized architecture of Bitcoin allows to speak of the implementation of distributed trust: Every user that joins the network contributes a brick to the collective building of trust that no longer needs to be incarnated in a specific institutional authority. Trust in decentralized networks can be established through higher confidence in Bitcoin’s algorithm and in the algorithm’s authority in particular (Maurer, Nelms and Swartz, 2013; Lustig and Nardi, 2015). Since algorithms are a set of abstract instructions and possibilities for actions, they can cause human actors to respond accordingly. As a consequence, human judgment acts as a supplement to algorithm authority to take precautions to prevent theft or falling victim to scams (Lustig and Nardi, 2015). Trust in Bitcoin is, therefore, built upon both Bitcoin algorithm authority and sociality of trust, encouraged by experience system’s characteristics, respectively (Maurer, Nelms and Swartz, 2013).

Certainly, there are more factors that are responsible for the acceptance and usage of Bitcoin, such as lock-in effects and associated switching costs, however, in the following trust is defined as the main factor responsible for the initial use of the electronic payment system, whereas the latter is more responsible for continuous usage. Thus, in the following, an empirically study is conducted examining, why Bitcoin does not achieve a sufficient level of trust in order to gain user acceptance as a payment network. In particular, three issues will be discussed that are related to the following questions: what are the determinants of trust in Bitcoin; how can these determinants be translated into a model that allows for their empirically investigation; and how do consumers evaluate the fulfillment of these determinants by Bitcoin?

### 2.1.2 Determinants of Trust

In order to evaluate these questions a user-centered perspective was taken in order to evaluate the factors promoting the formation of trust and subsequent user acceptance of Bitcoin. In a first step, the relevant literature was reviewed for identifying the crucial determinants of trust that are presented in Table 2. The determinants are clustered referring to a differentiation provided by Yu et al. (2002), separating the determinants into technological, economic, social as well as legal factors. It is assumed that any cashless payment mechanism irrespective of its type, needs to fulfill at least some of those requirements in order to generate a positive attitude towards its usage and trust (Yu, Hsi and Kuo, 2002). Moreover, especially in the field of technological aspects, it is important to distinguish between determinants that can be directly perceived by users, e.g. through experience (user-related characteristics) and those, which are only indirect perceivable (technological-related characteristics). For instance, users’ perceptions of encrypted connections might be secure, but they might be hardly able to verify the actual security of the applied encryption method (Abrazhevich, 2001).
<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Technology-Related Characteristics</th>
<th>User-Related Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aspects</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Technological Aspects** | - Validity (Yu, Hsi and Kuo, 2002)  
- Integrity (Yu, Hsi and Kuo, 2002; Tsiakis and Sthephanides, 2005; Kim et al., 2010)  
- Authorization Type (Abrazhevich, 2001)  
- Anonymity (Abrazhevich, 2001)  
- Scalability (Abrazhevich, 2001) | - Security (Yu, Hsi and Kuo, 2002)  
- Reliability (Kim et al., 2010) |
| **Economic Aspects** | - Efficiency (Yu, Hsi and Kuo, 2002)  
- Atomic Exchange (Yu, Hsi and Kuo, 2002)  
- Interoperability (Abrazhevich, 2001)  
- Acceptability (Yu, Hsi and Kuo, 2002)  
- Convertibility (Abrazhevich, 2001) | |
| **Social Aspects** | - Traceability (Abrazhevich, 2001; Tsiakis and Sthephanides, 2005)  
- Privacy (Yu, Hsi and Kuo, 2002; Kim et al., 2010)  
- Usability (Abrazhevich, Markopoulos and Rauterberg, 2009) | |
| **Legal Aspects** | - Compliance with existing policies and rules (Abrazhevich, 2001; Abrazhevich, Markopoulos and Rauterberg, 2009) | |

Table 2. Technology- and user-related characteristics
Designing a payment system that should be widely accepted by customers necessitates the considerations of those requirements as well as of the trade-offs associated with particular design aspects that may be mutually exclusive. For instance, providing full security may prohibits full anonymity. Nevertheless, taking into account most of those aspects should enhance consumers’ trust in the respective payment system and, consequently, should lead to a higher consumer acceptance (Abrazhevich, 2001; Abrazhevich, Markopoulos and Rauterberg, 2009).

2.1.3 Explanation and Prediction of Trust in Bitcoin

In order to explain and predict the user acceptance of Bitcoin, a theoretical model is needed that displays the formation of trust and, which is, subsequently, empirically testable. In the following the Technology Acceptance Model (TAM) is used and extended by the factor trust to analyze the effects of the Bitcoin system characteristics and design features on users’ acceptance of the decentralized payment system (Gefen, Karahanna and Straub, 2003; Davis, 2014).

The technology acceptance model refers to the Theory of Reasoned Actions as proposed by Fishbein and Ajzen (1975), in which system design features (i.e. external stimuli) lead to a motivational process that mediates between a system’s characteristics and user behavior, by having a direct affect on the respective cognitive user responses. Cognitive responses are hypothesized to be the fundamental determinants of a user’s attitude towards using a technology that exhibit interdependencies. Consequently, external factors determine the degree to which individuals are motivated to use the system and impact the actual system usage decision (Davis, 1985, 2014). Resting upon this basic model, various extensions and modifications of the technology acceptance model have been applied by scientists, giving a hint on the complex structure, which stands behind the acceptance of certain technologies as emphasized, among others, by Pavlou (2001). In addition, empirical tests have shown that the technology acceptance model is a robust model for the prediction of behavior and, especially, technology acceptance for a variety of applications and settings (Venkatesh et al., 2003). Successful applications of the technology acceptance model can also be found in e-commerce literature, emphasizing trust as the central element of user acceptance (Pavlou, 2001; Gefen, Karahanna and Straub, 2003).

To combine the previously identified determinants of trust with the basic technology acceptance model, determinants are assigned to four major areas of cognitive responses according to, among others, Pavlou (2001) and Gefen and Straub (2004), while a placing a special focus on user-related characteristics. This focus is reasonable, since trust and the associated concept of consumer acceptance is highly subjective. Moreover, by taking a user-centered approach, it is taken into account that not all determinants of trust
and related payment system design features are directly perceivable and transparent to the consumer. Table 3 depicts the cognitive responses, i.e. perceived security, perceived privacy, perceived usefulness and perceived ease of use, as well as the associated trust determinants. Since the determinants security and reliability are the only directly perceivable technology related but consumer perceivable characteristics, both determinants are considered within the wider context of financial and performance risk. Financial risks include the risk of financial losses resulting from the use of a digital currency that is not secured by a government or central institution, whereas performance risks covers risks that result from the possibility that transactions cannot be processed in a timely manner. An analysis of the legal framework surrounding Bitcoin is purposefully omitted as this is out of the scope of the analysis.

<table>
<thead>
<tr>
<th>Cognitive Response</th>
<th>Aspects</th>
<th>User-related characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Security</td>
<td>Technological</td>
<td>• Security&lt;br&gt;→ Financial Risk&lt;br&gt;• Reliability&lt;br&gt;→ Performance Risk</td>
</tr>
<tr>
<td>Perceived Privacy</td>
<td>Social</td>
<td>• Traceability&lt;br&gt;• Privacy</td>
</tr>
<tr>
<td>Perceived Usefulness</td>
<td>Economical</td>
<td>• Efficiency&lt;br&gt;• Atomic Exchange&lt;br&gt;• Liability &amp; Financial Risk&lt;br&gt;• Interoperability&lt;br&gt;• Convertibility&lt;br&gt;• Acceptability</td>
</tr>
<tr>
<td>Perceived Ease of Use</td>
<td>Social</td>
<td>• Usability</td>
</tr>
</tbody>
</table>

Table 3. Cognitive responses and associated user-related characteristics

Based on cognitive responses, the associated user-related characteristics as well as the basic version of the technology acceptance model, now, a modified version of the acceptance model is constructed, in which trust constitutes the main determinant of the intention to use a technology. The trust-extended technology acceptance model (T-TAM), thereby, defines trust as the key factor for consumer acceptance of the electronic payment system Bitcoin. Based on the above-indicated multi-dimensional definition of trust, the fulfillment of user-related characteristics through network design features of Bitcoin is responsible for the emergence of user acceptance, because of the direct effects on the four cognitive responses (Figure 3). Moreover, interdependencies between the cognitive responses perceived ease of use and perceived usefulness, as well as be-
between perceived security and perceived privacy are expected. However, whereas in the first case it is expected that perceived ease of use and perceived usefulness are positively correlated, no prediction about the relationship between expected security and privacy can be made, meaning that they can affect each other positively as well as negatively.

Figure 3. Modified technology acceptance model

The identification of determinants of trust in the trust-extended technology acceptance model allows for an empirical evaluation of users’ trust in Bitcoin. In the following, two hypotheses will be stated that are expected to explain reluctant user acceptance of Bitcoin and that must be empirically evaluated afterwards. Notably, the hypotheses also imply different predictions about the future development of Bitcoin usage.

**H1: Insufficient use of Bitcoin as a payment network results from an inadequate fulfillment of user-related characteristics and, thus, a lack of trust.**

The lack of trust in Bitcoin is expected to emerge due to the relative importance of the fulfillment of certain user-related characteristics that have a direct effect on user’s cognitive responses and, consequently, trust. If H1 holds, Bitcoin at its current state has probably little chance to exceed a critical mass in order to become a dominant payment network, since it does not fulfill users’ requirements for commonly used cashless payment systems. Fostering users’ acceptance, therefore, requires changes of certain system design features to take account of user’s perceptions. However, given the trust formation process, implying interactions as well as experience, it is also possible that the reluctant acceptance of Bitcoin results from a lack of user experience and interaction as well as knowledge about the decentralized payment system, leading to the second hypothesis:

**H2: Insufficient use of Bitcoin as payment network results from a lack of experience with and knowledge of Bitcoin.**

If insufficient usage of Bitcoin as common payment network results from a lacking interaction as well as knowledge as implied by H2, Bitcoin may exceeds the critical mass
to become the dominant or at least a frequently used payment network, when experience within the group of users grows and interaction increases. Thus, the underlying assumption is that the perception of users is biased due to a lack of knowledge and interaction, leading to a wrong assessment of the design features and associated fulfillment of user-related characteristics.

2.1.4 Research Method

In order to tackle the research question, how consumers evaluate the fulfillment of the trust determinants by Bitcoin, the cognitive responses of users to the perceived network design features of the decentralized payment system are evaluated by means of an online survey (Appendix A). The questions refer to user-related characteristics and participants are required to give their assessment concerning the fulfillment of each characteristic, resulting in an overall assessment of cognitive responses. Furthermore, participants are asked to indicate their experience with Bitcoin, which is approximated by the frequency of use and their knowledge concerning the general functioning of a Bitcoin transaction. The survey closes with general questions regarding gender, age, and education, as well as the intention to gain experience with the decentralized payment network. The same procedure is done for the online payment system PayPal, which is chosen as benchmark case, as it is currently the uncontested market leader (Deutsche Bundesbank, 2015). Assessment of the user-related characteristics takes place through the participants’ agreement or refusal of prescribed statements. In particular, participants of the survey could refuse or agree to statement by choosing a value between one and six, indicating full agreement up to full disagreement. For the evaluation, the arithmetic mean of all answers is calculated for each cognitive response. Summing up those mean values leads to the identification of the overall influence of cognitive responses on the formation of trust. In order to test H2, the findings of the subjective assessment of user-related characteristics are compared to theoretical considerations on the potential beneficence of Bitcoin use.

Participants of the survey were recruited with the help of Facebook, assuming that people using this social platform represent a section of the population, holding a certain degree of affinity to technology and, thus, are able to give a realistic evaluation of both Bitcoin and PayPal. Furthermore, members of the forums Bitcointalk and Reddit were asked to participate on the survey, representing a group, which is more familiar with the concepts and functionality of Bitcoin. In total, 120 people participated on the survey. Thirty people cancelled the survey prematurely, which would cause inconsistencies within the data. Thus, their answers were omitted from the subsequent analysis, leaving a data set of 90 complete responses of the participants, whereas 63% were male, 30%
female and 7% did not provide information on the gender. All participants graduated from school, whereof 34% attained a bachelor’s degree and 19% a master’s degree.

### 2.1.5 Data Analysis and Interpretation

Figure 4 shows the graphically representation of the evaluation of cognitive responses based on the conducted survey, and refers to the participant’s perception of security as well as privacy within the Bitcoin and PayPal payment system. Concentrating first on perceived security, it seems to be obvious that there exist vast divergences between subjective evaluations of several security aspects of PayPal and Bitcoin, especially, when referring to payment reversal and availability. In particular, it seems unequivocal that participants are aware of the fact that payments conducted with Bitcoin are not reversible. Besides that, differences between the overall assessment of perceived security of PayPal and Bitcoin are not significantly high.

**Figure 4. Participants’ assessment of perceived security and perceived privacy**

**Assessment H1 (perceived security):** Based on the evaluation presented in Figure 4, Bitcoin seems to lack the fulfillment of certain user-related characteristics associated with the user perceived security of transactions conducted by the system. Particularly, in the case of perceived financial risks, owing to the inability to reverse payments using Bitcoin, a huge gap exists between the assessments of perceived security of Bitcoin compared to the assessment of PayPal. Whereas in the categories likelihood of unapproved access and withdrawal, Bitcoin is perceived slightly more secure than PayPal, it is not clear, whether these positive perceptions towards Bitcoin outweigh the negative assessment of security with respect to payment irreversibility. However, overall there seem to be an insufficient fulfillment of user-related characteristics that leads to a more negative perception of the security of Bitcoin than of PayPal.

**Assessment H2 (perceived security):** According to the subjective assessments, participants have indicated to have a considerably better knowledge about PayPal than about
Bitcoin. The majority of participants declared to have good or very good knowledge of PayPal. In contrast, over half of participants claimed to have bad or very bad knowledge about Bitcoin; the poor assessment of Bitcoin relative to PayPal in terms of security can, consequently, be partially traced back to a lack of knowledge as well as a lack of prior interaction. Thus, overall, both hypotheses seem to hold in the case of perceived security of Bitcoin.

The right-hand illustration depicted in Figure 4 shows the perception of privacy in Bitcoin and PayPal, respectively. Notably, privacy in the Bitcoin payment system is constantly perceived higher than the privacy of PayPal with a magnitude of about one point on the scale.

**Assessment H1 (perceived privacy):** Given the public available ledger of Bitcoin, researchers have shown that payments can be easily traced back and personal information can be acquired by using appropriate clustering techniques (Böhme et al., 2015). From a theoretical point of view, Bitcoin fails to offer the degree of privacy conventional payment systems provide. Given the positive evaluation of privacy characteristics from the participants’ side, trust in the distributed ledger system is emphasized by wrong perceptions. Consequently, the first hypothesis seems not to hold, when focusing on perceived privacy, which fosters trust in Bitcoin, however, based on wrong expectations about the systems capabilities.

**Assessment H2 (perceived privacy):** It seems obvious that participants are not sufficiently informed about the drawbacks of Bitcoin with regard to privacy. Possibly, participants anticipate the effects of services that enhance privacy in the network such as mixing services or Bitcoin anonymizers. Given a share of roughly 40% of participants who claimed to have bad knowledge about Bitcoin this assumption seems unrealistic. In this case, participants’ assessment of privacy rather fosters than impedes the acceptance of Bitcoin. Consequently, the second hypothesis seems to hold.

Figure 5 depicts the evaluation of participants’ perceived ease of use for Bitcoin and PayPal on the left side as well as perceived usefulness one the right. Perceived ease of use of PayPal clearly exceeds the perceived ease of use of Bitcoin, which holds for all three statements. Probably, participants based their assessment on the anticipation of switching costs, which makes Bitcoin much less favorable than PayPal (Farell and Klemperer, 2007).

**Assessment H1 (perceived ease of use):** Intermediaries like payment processors provide ready to use interfaces as well as a clear representation of payment and product details within Bitcoin. In terms of ease of use, the assessment of Bitcoin should be relatively comparable to PayPal. However, participants assessed the usage of Bitcoin less intuitive and easy than that of PayPal. Given this discrepancy, negative evaluation of
user-related characteristics relies on rather wrong expectations than realistic assessment of user-related characteristics, leading to the conclusion that the first hypothesis does not hold with respect to perceived ease of use.

**Assessment H2 (perceived ease of use):** Given the discrepancy between negative evaluation of Bitcoin and actual ease of use, lacking acceptance builds upon bad knowledge and missing interaction of participants with Bitcoin resulting in wrong expectations concerning the ease of use of Bitcoin. The low share of participants, who already used Bitcoin emphasizes this assumption. Consequently, the second hypothesis holds.

![Graph](image)

*Figure 5. Participants’ assessment of perceived ease of use and perceived usefulness*

Usefulness of PayPal is overall perceived higher than usefulness of Bitcoin with a difference equaling to roughly one point on the scale.

**H1 (perceived usefulness):** Bitcoin falls clearly behind PayPal in terms of usefulness, with one exception that is the ability to transact micropayments. By the majority, however, lacking consumer acceptance of Bitcoin seems to result from insufficient fulfillment of user-related characteristics, especially concerning the offering to conduct payments via Bitcoin from the merchants’ side. Data on the intention to use Bitcoin indicate that there is probably less demand for Bitcoin. 52% of participants stated that they do not want to use Bitcoin in the future. Moreover consumers seem to be aware about the fact that Bitcoin does not include different payment options like PayPal (e.g., credit or debit card).

**H2 (perceived usefulness):** The relative neutral assessment of Bitcoin’s usefulness in terms of consumer protection shows that participants are not sufficiently informed. Usefulness of Bitcoin is significantly limited by its inability to declare a responsible authority in case of fraud or bitcoin losses. However, realistic assessment of participants of user-related characteristics of Bitcoin concerning usefulness outweighs this misperception, leading to the conclusion that rather the first than the second hypothesis holds.
The comparison of overall cognitive responses of both PayPal and Bitcoin shows that, beside in the area of privacy, PayPal achieved better results in terms of user perception than Bitcoin (Table 4). According to the trust-extended technology acceptance model, these assessments have an effect on users’ trust towards the respective payment mechanism. By calculating the mean value of the arithmetic means, one can define the average score of trust for PayPal and Bitcoin. PayPal achieved a score of 4.32, while Bitcoin receives a score of 3.93. Notably, it is surprising that the scores are not more divergent. The reason for this, is probably the good perception of participants with respect to the privacy of Bitcoin, which outweighs the relatively lower assessment of the other characteristics. Excluding privacy values from the analysis, because there is a clear divergence of subjective assessment and real privacy patterns of Bitcoin, the results get clearer. PayPal then reaches an average score of 4.60, while Bitcoin only reaches a score of 3.80. Consequently, participants overall clearly agreed on the statement that trust in Bitcoin lies below the level of trust in PayPal.

<table>
<thead>
<tr>
<th>Overall Assessment</th>
<th>Bitcoin μ</th>
<th>PayPal μ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Security</td>
<td>3.93</td>
<td>4.06</td>
</tr>
<tr>
<td>Perceived Privacy</td>
<td>4.32</td>
<td>3.47</td>
</tr>
<tr>
<td>Perceived Usefulness</td>
<td>3.93</td>
<td>4.87</td>
</tr>
<tr>
<td>Perceived Ease of Use</td>
<td>3.55</td>
<td>4.88</td>
</tr>
<tr>
<td><strong>Average Score Trust</strong></td>
<td><strong>3.93</strong></td>
<td><strong>4.32</strong></td>
</tr>
</tbody>
</table>

Table 4. Overall assessment of the fulfillment of user-related characteristics

A number of methodological issues are, furthermore, worth discussing: System and network design features that are tested include a variety of user-related characteristics, which are mentioned as highly important for the success of both PayPal and Bitcoin. Certainly, there are other factors that may influence the acceptance of Bitcoin, but cannot be implemented into the model to maintain explanatory power. One factor that should clearly not be underestimated is individuality and disposition to trust or trust propensity. The external validity of this preliminary study is restricted due to two factors, which are sample size and the representativeness of the sample. Firstly, with a sample size of 90 participants, statistical significance is not achieved and serves, therefore, as a pre-test. Secondly, within the sample, participants with an academic background are overrepresented. This empirical analysis clearly constitutes only a first indication, why the acceptance of Bitcoin is low compared to established payment systems like PayPal. For future work larger sample size is proposed as well as controls for additional factors that possibly influence the acceptance of decentralized payment network.
2.1.6 Implications and Discussion of the Results

The empirical investigation of trust in the payment system Bitcoin shows that there is a large divergence between expectations regarding the electronic payment network and its actual usage, which is reducible not only to a lack of users’ trust due to an insufficient fulfillment of user-related characteristics, but also to missing interaction with the system. Though, providing information about its characteristics and functioning can enhance acceptance of Bitcoin as means of payment. However, one should be aware of the fact that better-informed individuals may refrain from using Bitcoin as they realize that it fails to offer at least a minimum degree of privacy. Moreover, there exist a range of weaknesses of Bitcoin, which should not be underestimated. Missing consumer protection and reliability in case of fraud, for instance, may be a huge obstacle to the acceptance of Bitcoin as users gain additional information. Most importantly, however, might be that the lack of customer acceptance in Bitcoin is the first example of a business case and model that was highly promoted in the beginning, but seemed to fail so far, which is in line with the opinion of critics, which assert that too much hype is create around distributed ledger technology, that possibly will not lead to the expected disruption of whole business models and industries. Thus, despite the fact that the underlying business model of Bitcoin may be highly disruptive, due to the associated disintermediation and induced transparency of all transactions on the ledger, disruption does not come into effect without the actual usage of the payment system. Consequently, only minor economic and social changes can be expected from Bitcoin given its current state of usage.

Given these results it is questionable what remains from Bitcoin in general as well as for the further analyses in the course of this thesis. Notably, this is the technical infrastructure underlying the distributed payment system, which is the blockchain, characterized by transparency, automated chronological storage and potential immutability. Thus, based on the previous analysis, it get apparent that, if the technology should be applied in the context of accounting, companies must be very clear about the technological features implied by the respective blockchain design as well as the intended effects on the user side. Certainly, in contrast to the Bitcoin system, the use of a distributed ledger or blockchain application in a company can be enforced and does not depend on the employees’ evaluation of trust in the ledger. However, companies must consider two challenges when applying distributed ledgers for accounting, that get apparent from the assessment of user perceptions and the associated hypothesis that are related to the usefulness as well as ease of use of the technology. The first insight for companies with respect to the usefulness of a distributed ledger is that, if cryptocurrency is transferred within the system, the exchange of this currency in a fiat currency may be difficult and prone to exchange rate volatilities. Moreover, the time to validate a transaction in
Bitcoin seems to be too long for small-scale transactions at brick-and-mortar shops. Thus, if the technology is applied in a corporate context, companies must be aware about the fact that the time to validate transactions and information within a distributed ledger backed accounting system may critically depends on the choice of an appropriate consensus mechanisms. The second implications for firms that stems from the analysis of the Bitcoin business model and user acceptance relates to the ease of use. Users of Bitcoin that do not posses a technical affinity or posses education in the relevant areas may have problems to use the system without a provider that delivers appropriate interfaces. Similar, if a distributed ledger should be applied for a business activity, corporations must take care about learning curves of their employees. Thus, if learning processes and the associated adaption of business processes should not exceed an acceptable time, companies must learn the lessons from the failure of Bitcoin and must take care of ease of use as well as usability of distributed ledgers application in accounting, in order to prevent economic losses from technical- or user-related problems or even temporal exposure of a particular business activity.

2.2 Distributed Ledger Business Model Transformation

Given the reluctant use of Bitcoin as a payment system, in more recent times, the academic as well as industrial focus of interest shifted away from the decentralized payment system to the underlying infrastructure as well as to the second generation of distributed ledger applications, using so called smart contracts that are self-enforcing sets of rules, executed through the distributed ledgers. More precisely, the applicability of distributed ledger technology for various business cases is increasingly discussed leading to controversial discourses on the capabilities and potentials of the technology. What is most conspicuous is that there seem to exist only two predominant opinions on the disruptive potentials of distributed ledgers. On the one hand, advocates of the technology emphasize the economic benefits of decentralization and transparency, which is expected to lead to the alleviation of several of today’s economic and technological problems (e.g. Yermack, 2015; IBM, 2016); On the other hand, critics assert that the potential of distributed ledgers, especially for the finance industry, might be overhyped, possibly leading to the next tech bubble (e.g. Evans-Greenwood et al., 2016; Rückeshäuser, 2017b).

In the context of this controversial debate, in the following it is asserted that the application of distributed ledger technology may be justified by its possible economic benefits; however, in order to quantify its potential a more differentiated discussion is necessary. Notably, the potential of distributed ledger technology may manifest itself in different ways and strengths, among others, depending on the industry and the value proposition provided by businesses. Before the potentials of distributed ledgers are discussed, it is
therefore necessary, to identify the emerging business models based on this technology. To this end a typology of business models based on distributed ledgers is provided, using previously identified parameters, for a subsequent characterization and comparison of distributed ledger based business models. Consequently, the possible changes of business models identified in this study are expected to be transferable to the realm of accounting, where the induced effects can be exploited for the support of accounting processes and the prevention of fraud.

2.2.1 The Concept of the Business Model

Although the concept of business models has been extensively discussed in the literature, there is still a lack of consensus on what comprises a business model (Hedman and Kalling, 2003; Morris, Schindehutte and Allen, 2005; Kujala et al., 2010). This is mainly because the concept of business models aims to combine a variety of different views, such as the perspective of industrial organization (Porter, 1980), a resource-based view (Peteraf, 1993) or the perspective of strategic process (Chakravarthy and Doz, 1992). Consequently, before a typology of business models based on distributed ledger technology can be developed, first, a definition as well as associated concepts must be identified for the purpose of this paper. Moreover, the hereby-derived definition is used in the questionnaire, to capture the following case studies and business models in a most comprehensive way.

On a most basic level a business model can be defined as a method of doing business by which a company sustains itself and positions itself in the value chain (Chesbrough and Rosenbloom, 2002; Baden-Fuller and Morgan, 2010). This generic description can be proliferated by specifying features of a business model. In this paper, the selected features are based on the comprehensive overviews provided by Morris, Schindehutte and Allen (2005), Chesbrough and Rosenbloom (2002), Kujala et al. (2010) as well as its comparison to the practical approach of business model generation proposed by Osterwalder and Pigneur (2010). The remaining six features of business models are presented and described Table 5.
### Customer Value Proposition

A business model should solve an important problem or fulfill an important need for a target customer, by offering an appropriate product or service (Johnson, Christensen and Kagermann, 2008). If technology is the foundation of that offering, the value of a technology will be mirrored by the willingness to pay for the offered product or service (Chesbrough and Rosenbloom, 2002). The inclusion of the value proposition as feature of a business model is supported, among others, by Afuah and Tucci (2001), Alt and Zimmermann (2001), and Chesbrough and Rosenbloom (2002).

### Identification of a Market Segment

The market segment includes users to whom the offered product or services is useful and defines the purpose. On this basis revenue generation mechanisms are specified that also rely on the customer types, geographic dispersion, and their interaction requirements (Chesbrough and Rosenbloom, 2002; Morris, Schindehutte and Allen, 2005). This feature of the business model is emphasized by, among others, Markides (1999), Gordijn and Akkermans (2001), and Chesbrough and Rosenbloom (2002).

### Estimation of the Cost Structure and Profit Potential

A business model must provide a consistent logic for earning profit (Morris, Schindehutte and Allen, 2005). In particular, this implies questions such as, how will the customer pay and how much to charge. Especially if the business acts within the Internet, payment models are numerous, reaching from charging by transactions, licensing, or selling after-sales supports as well as services. At the same time the pricing strategy must consider the cost structure of a business (Chesbrough and Rosenbloom, 2002). The inclusion of costs and revenue structures is proposed by, among others (Markides, 1999; Alt and Zimmermann, 2001).

### Positioning within the Value Network

The positioning within the value network involves third parties within the vertical value chain as well as from the value network. As part of the positioning, a business must establish relationships with suppliers, partners, and customers through which is can achieve complementary goods, increase network effects, and a leveraging effect on the value of the technology. Moreover, the positioning in the value network involves thinking about the point on the value chain, at which value is created for the customer (Chesbrough and Rosenbloom, 2002; Morris, Schindehutte and Allen, 2005). Positioning in the value network is a
Definition of the Structure of the Value Chain

To define the structure of the value chain, offerings must be created and distributed. This also includes the determination of complementary assets needed to support the businesses position in the value chain (Chesbrough and Rosenbloom, 2002). Notably, a superior structure of the value chain could lead to competitive advantage through the successful management of the interface between the business and others in the value network (Morris, Schindehutte and Allen, 2005). This feature is proposed among others, by Afuah and Tucci (2001) and Chesbrough and Rosenbloom (2002).

Formulation of a Competitive Strategy

A business model includes the formulation of an appropriate competitive strategy, delineating how the company intends to achieve advantages over competitors by identifying differences that can be maintained and mitigate on-going development. This requires thinking about the core competency, helping a business to perform relatively better than others (Morris, Schindehutte and Allen, 2005). This feature is proposed by, among others, Weill and Vitale (2001), and Chesbrough and Rosenbloom (2002).

Table 5. List of business model features

Based on these features, a case study of business models is conducted that are premised on or deal with distributed ledger technology. The elucidated business model features indicate that the two axes of a business model were considered in this paper that are related to the concept of value creation as well as value capture, following among others Oliva, R. and Kallenberg (1991) and Antonopoulou, Nandhakumar and Panourgias (2014). This takes into account that business models must not only consider the value creation, which is the value proposition for the customer, but also value capture, dealing with the revenue generation and cost structures of a business. Notably, the financial domain of business models is oftentimes left out (Chesbrough and Rosenbloom, 2002). However, assuming that a business is financed from external capital, e.g. through venture capital, which is a reasonable assumption looking at the huge influx of venture capital in distributed ledger related business as well as into the related ecosystem over the past years (Chester, 2016), the incorporation of business model features related to value capture is an important part of the construct of a business model offered here.
Case Studies and Selected Business Model Cases

In order to create a dataset for the following empirically grounded typification, a case study focusing on corporations, deploying business models based or focusing on distributed ledger technology is conducted. Using the information from the databases Blockchain Technologies, Crunchbase and AngelList, in total, 150 corporations were contacted and asked for information using a questionnaire (Appendix B). This questionnaire captures the previously identified six features of a business model. There was not pre-selection of companies in regard to business lifecycle positioning, geographical aspects or industry affiliation. However, companies were contacted in accordance to the degree of attention they receive, which gets obvious from the number of followers, indicated on AngelList. Descriptive statistics on the company’s geographical location, industry affiliations as well as the questionnaire feedback is accessible in Appendix C.

Out of 150 contacted companies, 6% answered the questionnaire, 1% provided additional information on the company and 4% rejected to give any answers in a time period of 3 months, starting in August 2016. Deducted from the justifications received from the companies that reject to answer the questionnaire, it is assumed that companies that did not react are either not willing to disclose information of their business model, e.g. if they not yet launched their products or services, or due to time constraints. Moreover, it must be considered that start-up markets are typically volatile and some companies and, especially, companies that were in their early stages at the time they were contacted, may no longer exist. Table 6 provides an overview of the companies that answer the questionnaire (small companies: up to 10 employees, middle-sized companies: up to 50 employees).

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Industry</th>
<th>Company Size</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>MultiChain</td>
<td>Infrastructure</td>
<td>n/a</td>
<td>UK</td>
</tr>
<tr>
<td>Singular</td>
<td>Property Rights</td>
<td>Middle</td>
<td>USA</td>
</tr>
<tr>
<td>Uniquid</td>
<td>Identity Management</td>
<td>Small</td>
<td>USA</td>
</tr>
<tr>
<td>SETL</td>
<td>Finance</td>
<td>Small</td>
<td>UK</td>
</tr>
<tr>
<td>DXMarkets</td>
<td>Finance</td>
<td>Middle</td>
<td>Singapore</td>
</tr>
<tr>
<td>Symbiont</td>
<td>Smart Contracts</td>
<td>Middle</td>
<td>USA</td>
</tr>
<tr>
<td>Factom</td>
<td>Infrastructure</td>
<td>Middle</td>
<td>USA</td>
</tr>
<tr>
<td>Fuzo</td>
<td>Payment</td>
<td>Middle</td>
<td>China</td>
</tr>
<tr>
<td>VARcrypt</td>
<td>Property Rights</td>
<td>n/a</td>
<td>USA</td>
</tr>
<tr>
<td>Provenance</td>
<td>Business Applications</td>
<td>Middle</td>
<td>UK</td>
</tr>
<tr>
<td>StingLabs</td>
<td>Infrastructure</td>
<td>Small</td>
<td>UK</td>
</tr>
</tbody>
</table>

Table 6. Overview of companies disclosing information about their business model
Some of the companies indicated in Table 6 did not reveal certain types of information on their business model. In particular, 4 companies did not reveal their strategically business relationships, 3 did not want to disclose information on the network positioning and two companies reveal no information on both costs structure and/or competitive strategy. Despite business models seem to differ significantly at a first glance, during the review process similarities as well as differences become visible depending on particular business model features. In the following two business models will be exemplary presented focussing on features with the greatest identified differences. This limited representation is mainly done because of space restrictions. An overview over the complete information on business models provided by the companies is available in the Appendix (Appendix D).

CASE STUDY 1: UNIQUID

UniquID is a software provider trying to solve the increasing challenges on the Internet of Things and growing interconnectedness of smart devices. UniquID provides device-centric solutions that recognized users through personal connected objectives, thereby removing the risk of user-generated passwords. Moreover, UniquID offers appliances that serve lightweight trusted node services, built to run on virtual machines and workstations inside a company’s infrastructure. By hosting a proprietary blockchain infrastructure, smart contracts are kept decentralized, confidential and redundant (UniquID, 2016). By this the company claims to reduce infrastructure complexity and eases the management of and interaction with devices and remote cloud services for big companies. UniquID generates profits by using Software-as-a-Service pricing strategy, licensing and from consulting services (Rückeshäuser, 2017c).

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Customer Value Proposition | - Software Provider removing the need of passwords to access digital systems  
- Eases the management of devices and remote cloud services  
- Reduction in infrastructure complexity  
- Higher pricing flexibility for customer tailored sales models due to blockchain |
| Market Segment | - Companies that need to manage hundreds or thousands of customers and/or need to connect things e.g. sensors, meters, vehicles, etc. |
| Revenue Stream | - Software-as-a-Service (SaaS) and Licensing  
- Minor revenue flow from consulting services |
- Service offered to system integrators or businesses |

Table 7. Short form business model description UniquID
CASE STUDY 2: DXMARKETS

DXMarkets is a proprietary professional-grade exchange platform that provides liquidity for digital assets in high-grade secure and scalable environments. By integrating blockchain technology into enterprise-based financial processes, DXMarkets expects to increase efficiency and to reduce costs by growing operating margins and the generation of new revenue streams. DXMarkets also offers strategic consulting as well as smart contracts for customer-based modeling of digital instruments for, e.g. self-executing trades or automated coupon payments (DXMarkets, 2016). By this, DXMarkets addresses both private and institutional investors as well as businesses and positions itself as connector of demand and supply within the market.

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Customer Value Proposition | - Grade trading platform for digital currencies  
- Low latency trading, real-time charting, profit and loss sharing, bulletproof security  
- Increased efficiency and reduced costs by integrating blockchain technology into enterprise based financial processes |
| Market Segment | - Private/Institutional Investors  
- Businesses |
| Revenue Stream | - Commissions, based on the transacted volume  
- 6% on sell-side, 2% on buy-side |
| Value Network Positioning | - Platform as connector of supply and demand side  
- Value capture at the point of transaction |

Table 8. Short form business model description DXMarkets

2.2.3 Methodology and Morphological Box

In the following a typology of business models based on distributed ledger technology will be constructed based on the answers on the questionnaire and exemplified by selected businesses cases. Typologies are regularly used in management science and, especially, in the context of business models for example in Pugh, Hickson and Hinings (1969) as well as by Kujala et al. (2010).

A typology is a method for delineating types of things or events, where types are created conceptually, using a top-down approach as well as facts from experience and observation (Baden-Fuller and Morgan, 2010). By this, every typology is a result of a grouping process, where an object field is divided into some subgroups (types) with the help of dimensions and attributes (Doty and Glick, 1994; Kluge, 2000). In social sciences, these types are sometimes also referred to as ‘ideal types’ following Max Weber’s notion of ideal types as generalisations mediating between ideas and theories. To this end, the method of empirically grounded type building is applied in this paper, following
Kluge (2000) and Charmaz (2006), taking advantage of the method’s flexibility compared to other approaches for type building, e.g. Kuckartz (2010). Notably, empirically grounded type building allows for various analysing methods to reach the sub-goals, depending on the research question and quality of data (Kluge, 2000). Moreover, a four-step process for type building was applied according to Kluge (2000).

The first step of the empirically grounded type conduction process consists in defining relevant dimensions and attributes, which form the basis of the typology. Notably, dimensions and attributes are required to adequately grasp the similarities and differences between the identified business models and are finally needed to describe the resulting types (Kluge, 2000). Within qualitative studies, Keller and Kluge (1999) noticed that the definition of dimensions and attributes happens during the process of analysis of collected data and with the additional help of theoretical knowledge. Accordingly, the case study provides the dimensions, which are the business features as well as the associated attributes, which get apparent from the questionnaire answers. Afterwards, business models must be grouped and analysed in regard to empirical regularities by means of the defined dimensions and attributes. In this paper a morphological box (Zwicky and Wilson, 1976) represents all possible combinations, on which basis the distribution of the business models to these combinations must be proofed for internal and external heterogeneity. Notably, the morphological box is suited for this study as it is typically used for the structuring of a set of relationship containing multi-dimensional, non-quantifiable problem complexes (Ritchey, 1998). This analysis builds the foundation for type building and constitutes the second step of the typology building process (Kluge, 2000). Step three, consists in identifying meaningful relationships and building types through the combination of attributes. Notably, this also requires the building of new attributes and the repetition of step one to three for an empirically grounded type construction. After type building, a characterization of types must be conducted, using the types attributes or by using other criteria such assignments as ideal type or extreme type, etc. (Kluge, 2000).

In the following, a morphological box according to Zwicky and Wilson (1967) is developed and used as instrument to graphically represent the combinations of dimensions and options of business models (Table 9). The morphological box comprises step one and two of the type generation process. In a first step, all identified business model features were assumed as dimensions for the subsequent typology building process, assuming that the features identified in the previous section describe business models in comprehensive way, leading to an in-depth understanding of the detailed characteristics of the subsequently analysed business cases. Based on these dimensions the information provided in the context of the questionnaires were analysed first individually and, afterwards, through the comparison of relevant keywords as well as associated and similar
expressions. Examples for such keywords in the dimension customer value proposition are, among others, ‘Platform’, ‘Infrastructure’, ‘Service’, ‘Distribution’, which provided a first differentiation of the analysed business cases. Particularly, the hereby achieved conceptual elaboration of similarities and differences of the provided information related to the different dimensions, enabled the derivation of options for the particular business model features. The identified options are expected to fulfil the requirement of great external heterogeneity, meaning that the identified options must differ significantly. Dimensions, in which no significant divergences of options could be identified based on the answers provided by the companies, were excluded from the morphological box. Moreover, one additional option is added as a result of the general screening of the contacted companies’ homepages. In particular, one characteristic was observed, which referred to the keyword infrastructure. Questionnaires, which contained this keyword were platforms that allow for further development. However, during the screening it was observed that business that can be assigned to be infrastructure provider also supply databases or other infrastructures that do not offer additional functionalities for development efforts. In this paper, this observation was taken into account by adding one additional option called infrastructure provision to the dimension core value proposition. At the end, this leaves 4 dimensions and 18 options, which describe business models premised on distributed ledger technology (Rückeshäuser, 2017c).

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core Value Proposition</strong></td>
<td>Infrastructure Provision, Platform-Based Development, Application-Based Integration, Service/Application Provision, Supporting/Supplementary Services</td>
</tr>
<tr>
<td><strong>Market Segment</strong></td>
<td>Software Developers, Big Businesses, Small- &amp; Medium-sized Businesses, Business End-Consumer, Private End-Consumer, Government</td>
</tr>
<tr>
<td><strong>Value Network Positioning</strong></td>
<td>Before Transaction, During Transaction, After Transaction</td>
</tr>
<tr>
<td><strong>Revenue Stream</strong></td>
<td>Transaction-Based, Revenue Sharing, Licensing &amp; Consulting, Subscription/Account-Based</td>
</tr>
</tbody>
</table>

Table 9. Morphological box for distributed ledger based business models

The dimension core value proposition is divided into five options. The option infrastructure provider refers to businesses that provide distributed ledgers as mere data infrastructure, e.g. as a database. Businesses that provide platform-based development also provide a general infrastructure, but additionally allow for the development of, for instance, applications on top of their infrastructure. Application-based integration com-
prises services based on a proprietary infrastructure, to develop and integrate various applications and solutions suited to the organizational structure and demands of a particular business. The next option is service or application providers that offer ‘ready to use’ applications, for example, for compliance, accounting or for property rights management that can be either based on a proprietary or open blockchain but without the opportunity for customization. Lastly, businesses may offer supporting or supplementary services, for example consulting or information services. The dimension market segment comprises six options. Software developers are customers that use a given infrastructure, e.g. databases or platforms, to develop their own software. Thus, developers are typically no end-users, but are encouraged to sell their products afterwards. Big businesses are expected to be rather no end-users as the potentially posses the ability to develop and integrate applications based on existing infrastructures using their internal human resources. However, in principal they can be both, developers as well as end-users. Middle-sized to small-sized businesses are also expected to have development and integration capacities, at least to some extend. Business- or private end-users are characterized as passive users, meaning that they are not able or not willing to take on development or integration efforts. The government is also assumed to be a passive end-user. The option value network positioning comprises three options, whereas the value is created either ex ante, ex post or during the transaction, whereas a transaction is defined as a transfer of products or services across a technologically separable interface that links a consumer with a producer or service provider (Williamson, 1981). However, there may also be business models that comprise two or more options, e.g. if the value is created throughout the whole supply chain of a product. The dimension revenue stream can be divided into four options, where revenue is generated either on a transactional basis, by revenue sharing with strategically business partners, by the offering of licensing and consulting services or by charging of customers on the basis of a subscription to a network or per account. Based on this morphological box, a typology is developed to illustrate different types of business models and by exemplifying theses types by the use of distributed ledger based businesses (Rückeshäuser, 2017c).

2.2.4 Typology of Distributed Ledger Based Business Models

By comparing all possible paths through the morphological box, types of business models are generated in the following, which is equivalent to step three and four of the typology building process.

BUSINESS MODEL 1: DATA INFRASTRUCTURE PROVIDER

The first type of business model derived from the morphological box is the data infrastructure provider (Table 10). One example of a business based on this type of business model is the German start-up BigchainDB. Typically these businesses provide a distrib-
uted ledger as mere database and decentralized storage without allowing any further applications build on top of it and developed by external entities. By this, these business models build on the increasing need in storage technology of high throughputs up to millions of transaction per seconds or higher, low latency as well as capacity of petabytes or more (Mcconaghy et al., 2016). Consequently, the customers of data infrastructure providers comprise all kind of end-users, including the government as well as big businesses and small- to medium-sized business using the database either with permissioned or permission-less access. In particular, the latter allows industry specific database solutions (Mcconaghy et al., 2016). Moreover, this type of business model is described by value creation ex post of a transaction, by, for example, secure and transparent storage of transactional data. The value captured by businesses is generated via subscription to an account, which is equivalent to renting space on the distributed data infrastructure and may depend on the storage capacity.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core Value Proposition</strong></td>
<td>Infrastructure Provision</td>
</tr>
<tr>
<td><strong>Market Segment</strong></td>
<td>Software Developers</td>
</tr>
<tr>
<td><strong>Value Network Positioning</strong></td>
<td>Before Transaction</td>
</tr>
<tr>
<td><strong>Revenue Stream</strong></td>
<td>Transaction-Based</td>
</tr>
</tbody>
</table>

Table 10. Business model type 1.: Data infrastructure provider

**BUSINESS MODEL 2: DEVELOPMENT FACILITATOR**

The second type of a business model based on distributed ledger technology is called development facilitator, mainly responsible for platform-based development (Table 11). Examples of development facilitators are, for instance, MultiChain, which is a software platform for the deployment of blockchain-based applications by offering special niche database architecture, as well as Symbiont, which is a smart contract platform. According to the information provided by MultiChain, customers are enabled to treat the blockchain and its technical functioning as a black box by using a platform (in the case of MultiChain a separate ‘fork-chain’ and a MultiChain-node), leading to reduced development times for blockchain applications. As the platform-based approach allows for the development of applications on top of the existing infrastructure, customers of de-
Development facilitators are software developers as well as big businesses that want to build blockchain or distributed ledger solutions internally. Notably, the ability to build applications on top of the infrastructure divides development facilitators from data infrastructure providers. Moreover, customers may also be small- to medium-sized companies or start-ups that want to build blockchain applications as well as consulting companies that want to advise other companies with the development of blockchain based applications. Value creation typically happens before the actual transaction by providing the critical infrastructure and building the fundament for the realization of the transaction or ex post transaction documentation. Revenue generation is obtained by licensing as well as by subscription or based on an account, e.g. by ‘renting’ a fork chain as infrastructure for own development efforts. However, also consulting services are conceivable. MultiChain, for example, offers according to their own information, small-scale but high-priced consulting and wants to price service level agreements for live deployment in the future as well as premium versions with regular licensed software.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Value Proposition</td>
<td>Infrastructure Provision</td>
</tr>
<tr>
<td>Market Segment</td>
<td>Software Developers</td>
</tr>
<tr>
<td>Value Network Positioning</td>
<td>Before Transaction</td>
</tr>
<tr>
<td>Revenue Stream</td>
<td>Transaction-Based</td>
</tr>
</tbody>
</table>

Table 11. Business model type II.: Development facilitator

BUSINESS MODEL 3: INTEGRATION ENABLER

Integration enabler is the third type of business model, whereas their core value proposition mainly consists in services concentrated on application-based integration (Table 12). In contrast to the former business model development facilitator, there is no flexibility in regard to the offered product or service. Integration enablers rather offer particular applications located in a specialized application field and provide integration services of these applications suited to the needs and organizational aspects of a particular business. An example of an integration enabler is Factom, offering blockchain-enabled tools and services build on top of an open source blockchain network. By this customers do not need to implement tools on their own and benefit from cost and time
reductions due to reduced development and integration efforts. Moreover, Factom states that the implementation of applications also leads to a reduction of the learning curve of using the blockchain for their customers. Customers of integration enabler are all kind of businesses as well as end-consumers including the government or other public companies such as public infrastructure providers. Value for customers is typically generated ex ante, as the service provided by these businesses provides the basis for the operational activities of their customers, the associated transactions and the reporting of transactional data. The revenue stream for integration enablers results from licensing activities, as, for example in the case of Factom, tools are offered as Software-as-a-Service, leading to lower implementation barriers. Moreover revenue is generated from consulting services as well as from subscription or account-based pricing, if customers need to become a part of the network, e.g. in form of a node.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Value Proposition</td>
<td>Infrastructural Provision</td>
</tr>
<tr>
<td>Market Segment</td>
<td>Software Developers</td>
</tr>
<tr>
<td>Value Network Positioning</td>
<td>Before Transaction</td>
</tr>
<tr>
<td>Revenue Stream</td>
<td>Transaction-Based</td>
</tr>
</tbody>
</table>

Table 12. Business model type III.: Integration enabler

BUSINESS MODEL 4: APPLICATION PROVIDER

The fourth type of business model is the application provider (Table 13). These businesses typically offer fixed applications without the possibility for customization. Examples of this type of business model are Fuzo, offering among others mobile phone remittance services, SETL, responsible for market transaction settlement as well as payment, and DXMarkets, which provides a trading platform for digital currencies. According to their core value proposition, the customers of application providers are mostly business and private end-users as well as the government. Typically, these customers can be described as passive users, as they are not interested in the integration of the distributed ledger technology within their own organizational structure as well as in independent development efforts. Pursuant to the variety of applications that can be realized
on the basis of distributed ledger technology the value creation can happen ex ante or ex post as well as during the transaction, e.g. by offering a payment system. Lastly, the revenue stream for application providers can be based on a numberous pricing models and revenue streams including transaction-based pricing, revenue sharing with strategic business partners, licensing and consulting as well as via subscription and account-based.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Value Proposition</td>
<td>Infrastructure Provision</td>
</tr>
<tr>
<td></td>
<td>Platform-Based Development</td>
</tr>
<tr>
<td></td>
<td>Application-Based Integration</td>
</tr>
<tr>
<td></td>
<td>Service/Application Provision</td>
</tr>
<tr>
<td></td>
<td>Supporting/Supplementary Services</td>
</tr>
<tr>
<td>Market Segment</td>
<td>Software Developers</td>
</tr>
<tr>
<td></td>
<td>Big Businesses</td>
</tr>
<tr>
<td></td>
<td>Small and Medium-sized Businesses</td>
</tr>
<tr>
<td></td>
<td>Business End-Consumer</td>
</tr>
<tr>
<td></td>
<td>Private End-Consumer</td>
</tr>
<tr>
<td></td>
<td>Government</td>
</tr>
<tr>
<td>Value Network Positioning</td>
<td>Before Transaction</td>
</tr>
<tr>
<td></td>
<td>During Transaction</td>
</tr>
<tr>
<td></td>
<td>After Transaction</td>
</tr>
<tr>
<td>Revenue Stream</td>
<td>Transaction-Based</td>
</tr>
<tr>
<td></td>
<td>Revenue Sharing</td>
</tr>
<tr>
<td></td>
<td>Licensing &amp; Consulting</td>
</tr>
<tr>
<td></td>
<td>Subscription/Account-Based</td>
</tr>
</tbody>
</table>

Table 13. Business model type IV.: Application provider

BUSINESS MODEL 5: SUPPORTING OR SUPPLEMENTARY SERVICE PROVIDER

The fifth and last type of business model identified in this paper is the supporting or supplementary service provider (Table 14). An example of this kind of business model is the incubator and investor StringLabs, specialized on advanced decentralized protocols and applications. According to StringLabs, customers benefit from the professional experience and capital to build open protocol ventures for the realization of projects, e.g. such as decentralized commercial banking. Thus, costumers of String Labs might be entrepreneurs, such as individual or several software developers as well as small- to middle sized start-ups. Other supplementary services identified in this paper are organizations, striving for the provision of information and that want to push forward the public recognition of the technology (e.g. Blockchain University (2016)). Therefore, also businesses and private-end user are potential costumers of supporting or supplementary services. Given the variety of services that can be offered based on this type of business model, the value creation can happen before, after as well as during transactions. Except for non-profit organizations, supporting or supplementary service providers are able to generate revenue via revenue sharing as well as by offering consulting services.
## 2.2.5 Implications of the Typology and Discussion of the Results

Given the five divergent business models and subsequent characterization it gets apparent that the emerged business models as such, are not new and already observed in other contexts, such as in the context of platform-based cloud solutions (Giessmann and Legner, 2016) or applications offered as a part of a software-as-a-service strategy (Weinhardt et al., 2009). However, two important implications can be derived that must be discussed in the context of prior research, concerned with business models in general and IT-enabled business models, specifically (e.g. Hedman and Kalling (2003), Al-Debei and Avison (2010) and Ojala (2016)). The first implication is that, so far, distributed ledger technology seems not to lead to an apparent disruption of existing business models. However, it must be considered that distributed ledger may shape business models in a more inconspicuous way, as existing business practices must be aligned to the technology leading to more varieties and rearrangement of existing social orders including the dynamic interplay between different corporate actors (Kuk and Janssen, 2013). Consequently, while business models might stay the same on the surface, actually they might get more explicit and flexible, owing to a increasing insecurities implied by the use of distributed ledgers as infrastructure facilitating digital interactions (Al-Debei and Avison, 2010; Ojala, 2016).

Related to this issue is the fact that technologies can take different roles according to Adomavicius et al. (2007), whereas roles may change depending on the component of the business model that is affected by the technology (e.g. organizational activities and structures, resources, offering) (Hedman and Kalling, 2003). For instance, looking at the identified business models the role of the distributed ledger differs between platform-based solutions and applications. Whereas in the latter case, distributed ledger take on a

### Table 14. Business model type V.: Supporting or supplementary services

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Value Proposition</td>
<td>Infrastructure Provision</td>
</tr>
<tr>
<td>Market Segment</td>
<td>Software Developers</td>
</tr>
<tr>
<td>Value Network Positioning</td>
<td>Before Transaction</td>
</tr>
<tr>
<td>Revenue Stream</td>
<td>Transaction-Based</td>
</tr>
</tbody>
</table>
product or application role, meaning that distributed ledger technology is the focal point and in direct competition with other, alternative technologies (e.g. other payment or remittance services in the case of Fuzo), applied as platform-based solution, distributed ledgers rather function as enabler for further component or application development. Consequently, the second implication is that depending on the role of the technology, a particular business model is shaped to varying degrees by the technology and with respect to the organizational structure and activities. For instance, distributed ledgers that are applied as digital infrastructure for the realization of an corporate-owned application, e.g. for supporting business activities such as accounting, may lead to a deconstruction of commonly applied roles within organizations, leading to the necessity to define new roles and responsibilities that differ from traditional hierarchical structures. More precisely, if distributed consensus is applied for decision-making in the context of accounting, every validating node is then responsible for the correctness of a transaction and, thus, also liable. The implied decentralization of responsibilities is in stark contrast to contemporary and predominantly applied management practices. The resulting third implication that eventually leads back to the first implication is, therefore, that given a product role of a distributed ledger’s, the consequences for business models may be significant and change the understanding of current business models and relationships, for instance, given incompatibilities with existing business routines (Kuk and Janssen, 2013). The fact that these effects are not captured by the business model typification and characterization may reflects that the majority of analysed firms are still in the founding or product development phase, meaning that the effects of distributed ledger technology could not unfold so far, or unfold rather on an organizational or social level that is not captured by the identified business model key-features.

2.3 Interim Conclusion

The previous two sub-chapters were concerned with answering RQ.1a that is: Which distributed ledger based business models are currently applied and how can these business models be characterized? To answer this question an investigation of the trust model of Bitcoin and analysis of the reasons, why user acceptance lacks expectations was conducted on the one hand, and a typology of distributed ledger based business models was provided and discussed on the other hand. The first emphasized the role of the blockchain as well as the importance of technological features and ledger design, if distributed ledgers should be applied in the context of accounting. The latter analysis placed a focus on the characterization of the variety of business models that are based on distributed ledger technology and showed that the disruptive forces that are expected to have an impact on business models are yet not present. Another possible explanation for this observation is that distributed ledgers do impact less business models, but rather
influence other parts of businesses, meaning that the capabilities of the technology do not lie in the radical disruption of existing business models. This would imply that the application of distributed ledgers in accounting will not change the whole accounting process as well as related practices, but will impact accounting in a more subtle way. Thus, in order to identify, how distributed ledger impact businesses and, consequently, how business value emerges through the application of distributed ledgers in accounting, in the following, RQ.2b will be answered: What business strategies underlie the identified distributed ledger based business models and how can value creation through the technology be captured and measured? Thus, assuming that there must be some value for corporations that use the technology or at least for those who operate in the market for some years already (e.g. MultiChain), the economic effects of distributed ledgers once applied in a corporate context must be discussed. Notably, it is assumed that the particular economic effects are already in place, but to varying degrees, depending on the role of the technology within the respective business model. Business models might undergo minor, but important changes that are not captured by the analysis of business models and the respective parameters. This holds, especially, for organizational aspects as well as business interactions, which is strongly determined by business strategy.

2.4 **Contextualization: Distributed Ledgers, Digital Business Ecosystem and User Sides**

Distributed ledgers are digital infrastructures that support heterogeneous types of business models (Glaser and Bezzenberger, 2015; Brenig, Schwarz and Rückeshäuser, 2016). By further analyzing the identified business models and, especially, by focusing on business strategy, the key factor market segmentation and, subsequently, summarizing the respective intended value propositions, a contextualization of distributed ledgers can be provided, which is depicted in Figure 6. From a non-technical view, it can be distinguished between the layer of the distributed ledger, the ecosystem and end-users as well as the respective interactions between the layers. Notably, the distributed ledger is here still treated as black box and business strategies are defined as the interaction patterns between business providers and the technology, including customer approaches and the respective value proposition. The layers as well as interactions and interdependencies are explained in the following.
Distributed ledger system

According to the contextualization, on the top-layer, management and maintenance of a distributed ledger can be differentiate, whereas governance is either conducted by a non-profit and for-profit organization (Chesbrough, 2006). Whilst non-profit organizations are predominantly foundations, e.g. Bitcoin Foundation or the Ethereum Foundation, for-profit organizations are profit-seeking enterprises, such as Ripple Labs (Brenig, Schwarz and Rückeshäuser, 2016). Accordingly, value proposition as well as revenue generation differs significantly between these governance modes; however, the concrete design of the business model of firms using distributed ledger technology is strongly determined by the business strategy, i.e. interaction with the ecosystem and user side.

Ecosystem

The evolving ecosystem around the distributed ledger consists of organizations providing complementary applications or services for distributed ledgers. 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 (Basole and Karla, 2011; Hennigsson and Hedman, 2014). Usually end-users are treated as an entity of the ecosystem. Nevertheless, in this contextualization they are examined independently owing to the complexity of distributed ledgers and their application variety. Although prevailing distributed ledgers follow an open approach to encourage the par-
ticipation of a community of developers providing applications and services, closed implementations without an ecosystem are also conceivable.

Applications are implemented on top of a given distributed ledger system to provide additional functionalities that are not initially available. They are related by a technical link to a specific distributed ledger. For instance, 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 distributed ledger by providing a blockchain with a built-in Turing-complete programming language (Buterin, 2014). Contrary to applications, services do not require a technical link to the distributed ledger. Instead, a distributed ledger determines their legitimacy. They render the use of already existing functionalities of distributed ledgers or applications more convenient, but do not add new functionalities. Consequently, the functionalities are in the center of the business strategy that determined the business model of a service provider. For example, BitPay offers payment processing as a service for enterprises that 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, 2017). Another service for distributed ledger systems are, for instance, exchanges, converting the respective exchange medium into fiat currencies (e.g. Bitstamp, Bitcoin.de or BTC China). Furthermore, 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

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

After having identified the core actors related to distributed ledgers, the expected economic impact of the technology must be discussed, including a general discussion on the notion of value and value generation. In particular, it will be explained, how value is generated on the different layers presented in the conceptualization. Eventually, an evaluation framework is developed that enables the quantification of the value added through the use of distributed ledgers. For exemplification particular business strategies are emphasized.

2.5.1 On the Notion of Value and Value Generation

The notion of value describes a complex and abstract concept, which causes confusion around economists about its meaning and how it can be operationalized (Adrian Payne and Holt, 2001; Farber, Costanza and Wilson, 2002). A variety of economic research is focused on how concepts like value, utility, quality and costs are related, such as, among others, Giddings (1891) and Grönroos (2011). This results in a large number of differing definitions and uses of the value concept amongst academics (e.g. Salem Khalifa (2004) and Zott, Amit and Massa (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, Nandhakumar and Panourgias, 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 (Brenig, Schwarz and Rückeshäuser, 2016).

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 (Tellis and Gaeth, 1990; Afuah, 2002). This understanding is particular suited to study the economics of distributed ledgers, because it implies an interaction between single end-users and applications and/or services (Payne and Holt, 2001). For instance, an exchange that offers 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; Wang, Lo and Yang, 2004). The current paper follows a uni-dimensional approach by using economic reasoning, operationalized as utility, to assess the benefits and costs associated with distributed ledgers (Agarwal and Teas, 2002). 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 or service and the disutility represented by the price consumers need to pay (Sanchez-Fernandez and Iniesta-Bonillo, 2007).

2.5.2 Framework: Evaluation of the Value of Distributed Ledgers

Although all distributed ledger share the same fundamentals, the concrete technical design can be diverse and will be discussed in the following chapters. However, referring only on the organizational structure and associated business strategy, some distributed ledgers encourage third parties to provide complementary applications and services via open interfaces, while also proprietary systems are conceivable. Additionally, distributed ledgers also differ in regard to their provided functionalities. Thus, the potential value of every concrete distributed ledger needs to be assessed independently and in combination with the underlying business strategy. Table 15 illustrates the proposed framework to evaluate the value of distributed ledger applications.

In evaluation framework, a distinction is drawn between two layers, on which value is provided. The ecosystem (layer 1) consists of organizations providing complementary applications and services for a distributed ledger. End-users (layer 2) are individuals and organizations that demand the functionalities offered by a distributed ledger or corresponding applications and services. Layer 1 and layer 2 are interconnected, because value is not only provided out of the use of the distributed ledger, but also by applications and services. Thereby, the emerging value is not only depending on the distributed ledger as a digital infrastructure, but also on the whole spectrum of applications and services that support a successful use of the distributed ledger (Vargo and Lusch, 2015). Thereby, distributed ledgers can be defined as a platform 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 multi-sided platforms (Armstrong, 2006; Evans and Schmalensee, 2013). This is represented through interactions between the ecosystem and the end-users.
## Digital Infrastructure: Distributed Ledger
Governed by Non-Profit/For-Profit Organization

### Open Systems
- Open Strategy: Business models based on invention and coordination with community (Chesbrough and Appleyard, 2007)
- Publicly available source code
- Promote the development of applications

### Closed Systems
- Closed Strategy: Business models based on ownership and control (Chesbrough and Appleyard, 2007)
- Privately kept source code
- Prevent external applications

<table>
<thead>
<tr>
<th>Layer</th>
<th>Value Proposition</th>
<th>Measurements</th>
<th>Perceived Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ECOSYSTEM</td>
<td>Higher return on business activities (Chesbrough and Rosenberg, 2002)</td>
<td>Profit</td>
<td>$U_E = \sum_{i=1}^{n} u_i$</td>
</tr>
<tr>
<td>END-USERS</td>
<td>Higher return on innovation activities &amp; intellectual property (West and Gallagher, 2006)</td>
<td>Market share</td>
<td>$U_D(U_E, U_U)$</td>
</tr>
<tr>
<td>INTERACTION</td>
<td>Network effects (Armstrong, 2006; Evans, 2014)</td>
<td>Decreasing costs for information and processing (Brynjolfsson and Hitt, 2000)</td>
<td>$U_U = \sum_{j=1}^{m} u_j$</td>
</tr>
</tbody>
</table>

### Value Capture
- Organizations offering complementary applications & services

### Value Creation & Value Capture
- Individuals and Organizations (in)directly using distributed ledger

Table 15. Value framework for distributed ledgers
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 distributed ledger, 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). This is because customers perceive value differently depending on their needs (Hassan, 2012; Rückeshäuser, 2015). 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 utility functions) to model the preferences of different individuals.

### 2.5.3 Exemplification of Business Strategies and Value Creation

Regardless of the organizational structure, i.e. a non-profit or for-profit organization governing a distributed ledger system, 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 (2003) as well as Chesbrough and Appleyard (2007), 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 strategies, 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 distributed ledgers, irrespective of whether they are governed by a non-profit organization or for-profit organization. This aims at promoting the development of corresponding applications on layer 1. But also closed systems are conceivable, where organizations governing a distributed ledger pursue a closed strategy. The associated business strategies 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 business strategy seems more appealing for distributed ledgers governed by for-profit organiza-
tions, as innovation from outside sources is the most beneficial choice for non-profit organizations (Hull and Lio, 2006). Moreover, through restricting source code as well as network access the interference on potential sensible data and data transferring processing, such as accounting data processing and storage, is avoided. How value is concretely captured by organizations governing a distributed ledger requires the examination of concrete application cases, which is done in the following. 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 usage of distributed ledgers as well as the development of applications. Irrespective of organizational aspects referring to the distributed ledger as such, business strategy choices on the ecosystem layer are explained in the following as well as value creation and capture by end-users.

The ecosystem consists of application and service providers, who capture value by extending the scope of distributed ledgers provided as mere digital infrastructure or by offering intermediary services. The former provides direct access to distributed ledgers via executing complementary applications on top of digital infrastructure. Smart contracts, for instance, are able to automatically verify the interactions between parties and, thus, add additional functionality to the existing distributed ledgers (Peters and Panayi, 2015). By offering additional functionalities, application providers generate profits, which increase proportionally to the amount of end-users that demand them. The latter supports services by intermediation that renders the direct or indirect use of a distributed ledger system 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 and Kauffman, 1999).

End-users create value by the use of the distributed ledger systems, 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 potential irreversibility of transactions, distributed ledgers are potentially able to decrease the costs during the respective phase of a transaction, given that sufficient amount of network participants is not faulty (Becker et al., 2013). For instance, 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 innovations, which enables complementary organizational investments as well as productivity increases. For instance, NASDAQ, which makes use of a distributed ledger 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 (Orcutt, 2015).

A comprehensive approach to assess the value of a distributed ledger system 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 distributed ledger system requires the distinction of two scenarios. The first scenario is described by a distributed ledger, 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 distributed ledger system, 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 distributed ledger system by entities on the second layer.

Notably, only the latter case comes into question given the sensible nature of financial data and the attempt to prevent unlawful interference and modification of accounting data. Consequently a closed system strategy is assumed in the following. The effects implied by distributed ledger technology application for accounting fraud prevention, therefore, will probably express themselves through the support of transactions phases and accounting processes, more specifically, the reduction of information asymmetries as well as organizational transformation and/or improvement. Overall, this is expected to increase profits, in particular, through the decrease of costs of accounting information processing. Moreover, accounting processes and the prevention of fraud could be further supported through the use of complementary applications and services. In particular, thereby the challenges identified in the case of Bitcoin could be tackled, by providing ease of use and enhanced usability through additional features and services.
2.6 Concluding Remarks

In consideration of the growing propagation of distributed ledgers, enabling various types of applications ranging from cryptocurrencies up to smart property, it is important to be able to predict and evaluate the economic valued distributed ledger may deliver for business. This issue is exacerbated owing to short development cycles and a flexible environment, where novel systems, applications and services emerge regularly. Therefore, an approach is needed that is general enough to take these dynamics into account, but at the same time sufficiently specific to capture the particular technology-related features. This chapter addressed this challenge by presenting, first, an analysis of the Bitcoin trust model as well as insights on the technical design and associated user side effects. What can be learned from Bitcoin is that corporations that want to apply distributed ledgers for accounting cannot only rely on the fact the usage of the ledger is enforced within a company. If the technology is applied as supporting infrastructure for accounting processes, employees will experience learning processes and must adjust old business practices to new ones, determined by the usefulness as well as ease of use of the ledger design. Despite that, further investigations of distributed ledger based business models did not reveal substantial changes of key factors associated with business models such as, for instance, the value proposition offered to costumers or the structuring of the value network. Potentially, the disruptive forces of distributed ledgers are, therefore, not as significant as expected, leading to the presupposition that applications of distributed ledgers will affect businesses and accounting processes in more subtle way than predicted.

Thus, to investigate, how distributed ledgers create value aside of business model disruption, an evaluation framework for distributed ledgers is developed. After setting the context, the concept of economic value is described, which is subdivided into value proposition and perceived value, which was necessary due to the complexity and abstractness of the term value. In particular, the value concepts constituted the theoretical foundation for the construction of the evaluation framework. As main players within the context of a distributed ledger used as a digital infrastructure, the ecosystem (i.e. organizations offering complementary applications and services) and end-users (i.e. individuals/organizations (in)directly using a distributed ledger) were identified as layers, on which value is created and captured trough, among others, the reduction of information asymmetries, higher return on intellectual property or associated network effects. Consequently, firms that use a distributed ledger as digital infrastructure and as end-user for the facilitation of accounting processes, should not expect a disruption of existing business activities, but instead increased efficiency of information processing stemming from the support of transaction phases, a reduction of information asymmetries as well as organizational transformation, owing to the technological design and the associated
characteristics of distributed ledgers.

<table>
<thead>
<tr>
<th>Key Points Chapter 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Bitcoin’s business model seems to have failed: What remains is the general technical architecture – the <strong>distributed ledger</strong> – inducing <strong>decentralization</strong>, <strong>transparency</strong> as well as <strong>potential immutability</strong>.</td>
</tr>
<tr>
<td>• Firms that want to apply the technology for the facilitation of business activities and, especially, accounting, must learn from Bitcoin and consider the technically induced <strong>user-side effects</strong>.</td>
</tr>
<tr>
<td>• Distributed ledgers may affect business model in a more subtle way than by disruption, e.g. by <strong>organizational transformation</strong> and <strong>increased efficiency of information processing</strong>.</td>
</tr>
<tr>
<td>• Companies that apply distributed ledgers must exploit these changes to <strong>improve accounting processes</strong> through increased information transparency and potential immutability of ledger entries.</td>
</tr>
</tbody>
</table>
3 Accounting Fraud Prevention: A Requirements Analysis

Prominent examples of accounting fraud incidents include, among others, the Enron accounting scandal (2001), the WorldCom scandal (2002), the Freddie Mac (2003) and Fannie Mae scandal (2004) as well as more recently, the Lehman Brothers (2008) as well as the Toshiba accounting scandal (2015). The associated violations of corporate disclosure rules and directives take on various forms, from failure to file appropriate financial statements to internal fraud, such as the intentional misrepresentation of corporate financial health (Gerety and Lehn, 1997). The concealment of true corporate performance most often serves to maintain personal status and control as well as helps to increase personal income and wealth (Gerety and Lehn, 1997). For firms, accounting fraud has several negative effects, reaching from inefficient pricing of debt and equity to further impacts on financial markets, whereas false financial reporting results in overpriced securities and over-borrowing of firms (Sadka, 2006).

In order to prevent accounting fraud, distributed ledger technology is frequently proposed as a possible technical solution, among others, by Yermack (2015), Andersen (2016), and Fanning and Centers (2016). The economic rational behind this proposal was exemplified in the previous chapter and can be reduced to increased efficiency in information processing, the decrease of information asymmetries as well as organizational transformation that result from the technical design of the ledger. In particular, it is argued that transparency and potential immutability of ledger entries and the associated actions of network participants deters users from committing accounting fraud (Andersen, 2016) However, present papers that propose the application lack a concrete analysis, how fraud is actually conducted within corporations and which behavioral patterns distributed ledger technology must deter in order to prevent the emergence of fraud. Thus, if distributed ledger technology should be applied in the context of accounting, currently existing fraud patterns must be identified that result from organizational as well as technical vulnerabilities. The distributed ledger must consequently, prevent these fraud patterns, without introducing significant new security threats. This chapter, therefore, discusses the following research questions (RQ.2): **What are the current fraud patterns in accounting that must be considered, if distributed ledger are used as foundational technology in the context of an accounting information system?** Answering this research question first implies an analysis of the preconditions that are necessary for the emergence of fraud. Second, existing prevention and detection methods will be discussed. Subsequently, fifteen exemplary case studies will be conducted, on which basis it will be investigated, how accounting fraud was actually conducted, despite the existence of organizational and technical prevention as well as ap-
appropriate detection methods. As an essence of these investigations, the main challenge of today’s accounting practices, methods and supporting systems will be identified that must be considered and addressed by the subsequent endeavor to build a scenario for the assessment of distributed ledger based accounting and its ability to prevent or deter accounting fraud.

3.1 Definition of Accounting Fraud and General Prerequisites

Occupational fraud is a typical white-collar crime, related to economics and business activities (Holtfreter, 2005; Dorminey et al., 2012). More precisely, occupational fraud is defined as the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets (ACFE, 2016). Most often, this type of fraud is conducted either by individuals in order to achieve personal gains, or by individuals on behalf of an organization (Holtfreter, 2005; Jones, 2011). Occupational fraud occurs in the form of three major types of fraud, depicted in Figure 7, that are corruption, asset misappropriation, and fraudulent financial statements. Corruption includes among others the preparation of purchasing or sales schemes as well as invoicing kickbacks. Asset misappropriation involves methods such as skimming or cash larceny, when referring to the theft of cash receipts as well as the development of billing, payroll or expense reimbursing schemes. Lastly, financial statement fraud is either conducted by net worth or net income under- as well as over-statement, which are practices typically defined as accounting fraud. Methods to conduct accounting fraud include among others the creation of fictitious revenues, the concealment or overstating of liabilities and expenses, improper asset valuation or improper disclosure (ACFE, 2016, 2017).

Generally, accounting fraud can be defined as the intentional misrepresentation of financial statements, punishable criminally or civilly, in order to wrongfully obtain an advantage, retain a benefit, or avoid a detriment (Shapiro, 2011). A uniform, legal definition of fraud, however, is elusive since the definition of fraud varies in each country. However, in essence it evolves breaking the law and/or violating the regulatory framework (Jones, 2011). What kind of occupational fraud is conducted typically differs according to the position of an individual within an organization. Most often, the management conducts accounting fraud by preparing false financial statement to deceive users. In contrast lower level employees seem to tend to other kinds of fraud, i.e. asset misappropriation, which involves the theft of, for example inventory or cash (Rezaee, 2002; Holtfreter, 2005; Jones, 2011).
The definition of the three major types of occupational fraud and accounting fraud as one particular subset of occupational fraud, does not say much about the preconditions and reasons, leading to the conduction of fraud. The first study, which examined why people commit fraud and, thereby, violate trust, was conducted in 1950 by the criminologist Donald Cressey, who interviewed in total 250 criminals over a period of five months (Kassem and Higson, 2012). Cressey found out that three particular preconditions must be met, that is pressure, opportunity and rationalization – also called fraud triangle – which in turn most likely lead to the commitment of fraud (Hogan et al., 2008). In particular, pressure means that an individually perceived, non-shareable financial problem creates a motive for crime that is associated with social stigmata, preventing the individual from sharing his or her problem or seeking help. In addition, the impression that a problem is non-shareable might be reinforced by a strong sense of ego or pride. Opportunity means that there exist the individual perception of control weakness and that the likelihood of being caught is, therefore, remote (Dorminey et al., 2012). Thus, perceived opportunity requires the ability to commit the act of crime without being detected (Hogan et al., 2008). Lastly, rationalization requires the individual to reduce the cognitive dissonance within itself in order to remain in their moral comfort zone. This means that the perpetrator of fraud does not want to be consider as trust violator and, therefore, justifies his or her dilemma as a special exception (Dorminey et al., 2012).

However, looking at actual accounting fraud incidents, some of the aspects of the fraud triangle seem missing, leading to the conclusion that the preconditions and reasons to conduct fraud may be more complex. For instance, a prominent example of accounting fraud is the Tyco accounting scandal, in which context the former CEO Dennis Kozlowski and the CFO Mark Swartz stole $170 million from Tyco by loan program abuse and personal enrichment through unauthorized bonuses. Moreover, they took $430 mil-
lion by artificially inflating the company stocks by creating financial misstatements. However, besides the extend of criminal activity, the company also paid for rare art, parties as well as sport activities unrelated to Tyco’s business activities, which, among others, financed the excessive lifestyle of the Kozlowski (Dorminey et al., 2012). Obviously, the factor of the non-shareable financial need is not present in this case, which necessitates an extension of the fraud triangle in order to explain, why wealthy, influential and/or prominent members of the society risk to be involved in and be convicted for conducting white-collar crime (Dorminey et al., 2012).

One of the most recent and comprehensive model explaining the occurrence of fraud is the so-called new fraud triangle model by Kassem and Higson (2012), which relates several existing fraud models to Cassey’s fraud triangle. In particular, the new fraud triangle includes motivation, opportunity, integrity as well as the fraudster’s capabilities to commit fraud as shown in Figure 8. For the fact that not every fraud involves a non-shareable financial need is taken care, by including the factor motivation and by referring to the MICE model, which modifies the pressure side of the traditional fraud triangle (Dorminey et al., 2012). In particular, according to MICE, motivational factors to conduct fraud might be money, ideology, coercion as well as entitlement or ego. Whereas the motivational factors money and ego are self-explanatory, ideology means that a person acts according to the motto ‘the end justifies the means’, e.g. if money is stolen to achieve some perceived greater good. Actually, this justification can be frequently observed in association with taxpayer evasion schemes. Coercion occurs, if a person is victimized and unwillingly made part of a fraud scheme (Kranacher, Riley and Wells, 2011; Dorminey et al., 2012). The fraudster’s capabilities, however, refer to the so-called fraud diamond, developed by Wolfe and Hermanson (2004), who stated that many fraud incidents would not have happened, without the right person with the right capabilities implementing the details of fraud (Dorminey et al., 2012). Thus, the fraud diamond extents the fraud triangle by the factor capability. According to the authors, a person with the right capabilities to conduct fraud can be described as follows: first, the person is in the right position or function within an organization that furnish the ability to create or exploit an opportunity for fraud that is not available for others; second, the person must be smart enough to understand and exploit the control weaknesses that exist and use its position or functions for his or her own benefit; third, the person has a strong ego that creates strong confidence that he or she will not be detected or could easily get out of trouble if caught; fourth, the person is able to coerce others to commit or conceal fraud; fifth, the person is able to lie effectively and consistently and; lastly, the person deals very well with stress (Wolfe and Hermanson, 2004).

Rather an alteration than an extension of the fraud triangle is the factor integrity, which initially replaces rationalization as a part of the so-called fraud scale (Albrecht et al.,
The fraud scale states that the risk that fraud occurs is a function of opportunity and financial pressure as well as personal integrity. For example, when there is situational pressure and highly perceived opportunities, a low personal integrity may lead to the occurrence of fraud (Dorminey et al., 2012).

![Image of the new fraud triangle model](attachment:image.png)

**Figure 8. The new fraud triangle model (Kassem and Higson, 2012)**

Given the knowledge about the emergence of fraud provided by the new fraud triangle model, the assessment of the risk that fraud occurs should be better evaluable. Simultaneously, prevention and detection mechanism must take account of these factors, if they should lead to deterrence. Thus, based on this theoretical foundation, several existing prevention and detection methods will be explained and subsequently discussed, placing a special focus on the question, why perpetrators of fraud are obviously able to circumvent those safety precautions.

### 3.2 Existing Deterrence and Detection Techniques

Rezaee (2002) describes the procedure of accounting fraud prevention and detection in a five-step process, whereas the steps reach from the act of releasing a financial statement on behalf of a company and the deterrence and prevention of fraud by implementing an effective corporate governance system, to external controls, either by a purposefully chosen external auditor or through imposed investigations by national or international regulatory bodies. Alternatively, the process of fraud detection can be separated into three different phases that is the design time, run time as well as audit time phase, which are depicted in Figure 9. In particular, Figure 9 illustrates the process of fraud prevention and detection, extended over three indicated layers that describe the support
of information security in modern companies. The business layer is related to business processes, -object-, and –targets and defines the assets as well as organizational structures of a company. In contrast, the application layer contains services and data schemes for the execution of processes and the infrastructure level provides the software and hardware needed to automate the execution of services (Müller and Accorsi, 2013). Besides these different layers, fraud prevention typically takes place during design time and run time, whereas fraud detection happens predominantly in the audit time as well as in the run time. The associated mechanisms for the prevention and detection of fraud are described in the following that are, more generally, the state of the art (Müller and Accorsi, 2013).

Deterrence of fraud refers to the act of creating an environment, in which people are discouraged to commit fraud. The design time phase, thereby, describes the time prior to the actual process of execution and is related to the design of processes as well as to business process management (BPM) lifecycles. Mechanisms to prevent illicit behavior include focusing on policies and, specifically, on the optimal assignment of roles and activities within an accounting information system. Moreover, mechanisms must be implemented that ensure that no structural process vulnerabilities exist. To this end, the specification of processes can be translated into Petri nets, whereas a subsequent Petri net analysis allows the verification of processes (Accorsi, Wonnemann and Dochow, 2011; Müller and Accorsi, 2013). Furthermore, legislation and accounting standard compliant business process design is a further approach to prevent illicit activities that should minimize the problems of run time compliance checking and consequent violations and penalties (Sadiq, Governatori and Namiri, 2007). During run time, monitoring activities can be conducted that are, as already mentioned, preventive or detective. Preventive monitoring activities stop processes, whenever its continuation violates a policy (Müller and Accorsi, 2013). Despite these technical aspects, an appropriate control environment consisting of, among others, a robust ethical culture, a perpetrator punishment protocol and a proactive internal fraud auditing can enhance the prevention of accounting fraud. However, today, the transfer of information always involves some form
of information and communication technology and modern accounting draws heavily on those technologies (Vaassen, Meuwissen and Schelleman, 2011). Consequently, to prevent the opportunity to produce fraudulent financial statements, modern accounting information systems implement access controls, that prevent unauthorized persons from gaining access to a system as well as authentication methods, that guarantee that a user, who communicates with another user, actually communicate with the person he or she claims to be. Moreover, data and time stamps as well as confirmation methods and/or digital signature schemes can be applied in order to decrease the probability that financial data can be altered, without being detected in the aftermath. However, the application of such technical methods requires internal audit but also external auditors to have at least some knowledge about the used information technology (Vaassen, Meuwissen and Schelleman, 2011).

Detective mechanisms during the run time are monitoring activities, whereas in contrast to preventative monitoring, these mechanisms merely signal a violations without interference (Müller and Accorsi, 2013). The run time detection phase, moreover, typically requires the establishment of an audit plan. However, detecting accounting fraud is a difficult task using traditional auditing techniques, especially, when conduced by the management, owing to their increased options for concealment compared to lower-level employees (Kirkos, Spathis and Manolopoulos, 2007). To this end, various data mining techniques can be applied in the audit phase in order to increase the probability of financial statement fraud detection. Thereby, the identification of fraudulent statements is regarded as a classification problem, which is solved by methods derived from the fields of statistics and artificial intelligence. In particular, classification means that a learning model is used to predict the categorical labels of unknown objects to distinguish between objects of different classes. Three methods enjoy good reputation for their classification capabilities that are decision trees, neutral networks as well as Bayesian belief networks (Kirkos, Spathis and Manolopoulos, 2007; Ngai et al., 2011). However, other data mining applications can be also used that are supported by a set of algorithmic approaches. For instance, clustering can be applied to divide objects into conceptually meaningful groups, with objects in a group being similar to another, but very dissimilar to the objects in other group, such as in case of the K-nearest neighbor as well as self-organizing map techniques. Moreover, regressions or outlier detection methods can be used, whereas the latter measures the distance between data objects to detect those objects that are grossly different from or inconsistent with the remaining data set (Ngai et al., 2011). Thereby, the described methods are all based on event logs generated during business process execution (Accorsi, 2009, 2011; Müller and Accorsi, 2013).
3.3 Case Studies: How to Conduct Accounting Fraud?

Despite the variety of methods to prevent and detect fraud, obviously, accounting fraud still occurs, which is especially apparent, when considering the already mentioned examples, including the Enron or Parmalat accounting scandal. Consequently, there must exist some factors or actions that allow the circumvention of technological and organizational safety precautions as well as of the associated prevention and detection methods. In order to identify these factors, in the following, case studies will be conducted to analyze the proceedings and concealment techniques of perpetrators of accounting fraud.

3.3.1 The Enron Scandal (Case Study 1)

Enron was founded 1985, in the aftermath of the federal deregulation of natural gas pipelines, as a merger between the companies Houston Natural Gas and InterNorth (Thomas, 2002). Market deregulation meant challenges to Enron, owing to a loss of exclusive rights to its pipelines on the one hand. However, on the other hand, deregulation opened up new market opportunities. In particular, deregulations led to flexible prices and arrangements, whereas former, most contracts between natural gas producers and pipelines where ‘take-or-leave’-contracts, based on which pipelines agreed either to purchase a predetermined quantity at given price or were liable to pay the equivalent amount in case of failure to honor that contract. In turn, pipelines had similar long-term contracts with fixed prices with local gas distribution companies or electric utilities to purchase gas from them at fixed prices over the contract term or increasing with inflation (Healy and Wahlen, 1999; Thomas, 2002).

Facing these market changes, Enron created a new product and a new paradigm for the industry, the energy derivative, which was a result of the increased use of spot market transactions. Accordingly, in 1990, 75 percent of gas sales were transacted at spot prices rather than through long-term contracts and Enron, who owned the largest interstate network of pipelines, profited from increased gas supply on spot markets (Thomas, 2002; Healy and Palepu, 2003). Despite these achievements, Enron strived for further diversification and growth and reached beyond its pipeline business. In 2001, Enron had become a conglomerate that owned and operated gas pipelines, electricity plants, pulp and paper plants, broadband assets and water plants internationally and traded extensively in financial markets for the same products and services (Healy and Palepu, 2003). The development of Enron was also honored by the stock market. Already in 2000, Enron’s stock prices hit the all-time high of $90.56 per share and the company was touted as one of the most admired and innovative companies (Thomas, 2002).
Enron’s extensive business model stretched the limits of accounting practices, owing to two characteristics of particular business activities and the associated financial transactions: first, Enron’s trading business required complex long-term contracts. At this time, accounting rules used present value frameworks to record transactions, which requires the management to make forecasts of future earnings that is the so-called market-to-market accounting practice. This practice was central to Enron’s income recognition (Healy and Palepu, 2003). Second, Enron relied extensively on hedge risks. These transactions involved shared ownership of specific cash flows and risks with outside investors and lenders (Healy and Palepu, 2003). In addition, Enron’s use of special purpose entities under CFO Andrew Fastow took new heights of complexity, capitalizing them with not only a variety of hard assets and liability, but also extremely complex derivatives, its own restricted stock, rights to acquire its stock, and related liabilities (Thomas, 2002). Traditional accounting practices, which focused on arms-length accounting between independent entities, faces problems in dealing with such transactions. However, while accounting rule-makers discussed about appropriate accounting rules, mechanical conventions have been used to record these transactions, what already created divergences between the economic reality and the accounting numbers of Enron (Healy and Palepu, 2003).

Despite these general accounting issues, in 2001, Enron experienced problems with some investments, leading to a series of asset write-downs as well as after tax charges accounting to $287 million for Azurix, a water business, in which Enron invested in 1998. Additionally, the company was forced to sell Portland General Corp., which was an electric power plant, after a loss of $1.1 billion over the acquisition price (Healy and Palepu, 2003). These developments eventually result in a loss of more than $600 million in the third quarter report of 2001. In particular, Enron announced the restatement of its financial statements back to 1997 in order to reflect consolidation of the special purpose entities it has omitted as well as to book recommended adjustments from these years, which the company had previously deemed immaterial (Thomas, 2002). Together with a massive fall in stock prices, this led to a crisis of confidence in Enron. Six weeks after the third-quarter report, Enron collapsed and was filed for bankruptcy (Gordon, 2002). The collapse triggered investigations of Enron’s board special committee by the SEC, the Justice Department, and nearly a dozen congressional committees as well as various shareholder plaintiffs’ attorneys. The investigations revealed that a substantial fraction of the companies reported profits over a four-year period had been a result of accounting manipulations. Moreover, despite the fact that Enron apparently field false and misleading disclosures, insiders allegedly sold stocks and exercised options, while publicly restating their faith in the company. By contrast, rank-and-file employees were unable to sell their stocks, as they were locked into Enron’s 401(k) retirement plan. Thus, privi-
leged insiders were able to earn hundreds of millions in stock related profits, while normal employees were loosing a substantial part of their life savings (Gordon, 2002).

**Manipulation and Concealment Techniques**

As previously indicated, Enron’s accounting manipulations were not detected over a period of four years – questionably is, therefore, how Enron concealed the illicit practices and why nobody noticed substantial misstatements for such a long period? One concrete example of an illicit practice is the use of the special purpose entity Chewco that was controlled by an Enron executive, which raised debt that was guaranteed by Enron and acquired a joint venture stake for $383 million. Thereby, accounting standards were violated according to which at least 3 percent of assets must be owned by independent equity investors. However, Enron ignored this requirement and was, therefore, able to avoid the consolidation of the special purpose entity, thereby understating its balance sheet’s liabilities and overstating its equity and earnings (Gordon, 2002; Powers, Troubh and Winokur, 2002).

Remedy for such kind of practices should, theoretically, be the board of directors, which major features are independent directors to perform crucial monitoring functions and a clear charter of board authority. In the case of Enron, the board seemed to be splendid, consisting of fourteen members, of whom only two members were independent. Most of the board member had accounting backgrounds, some were prior senior managers and held board positions as well as senior regulatory posts (Gordon, 2002). However, despite stock based compensation is argued to align the interest of board directors with those of the shareholders, it can be assumed that the fact that director’s owned significant amounts of Enron’s stocks as well as stock options or phantom stocks as a part of the director compensation package, led to a lack of skepticism. For instance, the audit committee, did no challenge several important transactions that were primary motivated by accounting goals, nor did they asked for full disclosure of transactions with related parties and the associated potential conflicts (Powers, Troubh and Winokur, 2002; Healy and Palepu, 2003). In fact, investigations in the aftermath of Enron’s collapse revealed that virtually every board member, including the audit committee members, were dependent, meaning that the independence of the board was undermined by side payments of various kinds. Moreover, the board was blamed for bonds of long services and familiarity, which further compromised independence (Gordon, 2002). However, besides stock compensation and other side payments for directors, leading to the overlooking of grievances in accounting, top management compensation was as well heavily relying on short-term stock prices, which set the incentive to pump up short-term stock performance without creating medium or long-term value (Healy and Palepu, 2003).
A second explanatory factor for the long period of undetected illicit practices of Enron was external audit conducted by Arthur Andersen, who was accused of applying lax accounting standards as well as of partiality, because of the significant consulting fees generated through his work with Enron. Whether Andersen had a conflict of interest, because he wanted to hold Enron as a client, or whether he lacked expertise in auditing a big client like Enron is hard to determine ex post. However, Andersen failed to exercise sound business judgment in reviewing transactions that were obviously designed for financial reporting rather than business activities (Healy and Palepu, 2003). Though, looking at the reports attested by Andersen the first, i.e. a conflict of interest, seems to be the case: for example, when the credit risk related to the special purpose entities became clear, the auditors succumbed the pressure of Enron’s management and permitted the company to defer recognizing charges (Powers, Troubh and Winokur, 2002; Healy and Palepu, 2003).

Eventually, also fund managers, which were in late 2000 and early 2001 about 60 percent of institutional investors, contribute at least to some extend, to the concealment of the accounting problems of Enron. For instance, despite the magazine Fortune published an article in late 2000, asking whether Enron’s stocks are overprices, based on a hint from a hedge fund manager, major institutional investors were not reacting. Particularly, the article pointed out to insider trading as well as related party transactions involving Enron’s senior officers. One explanation for such a behavior is certainly, that investors had only modest incentives to demand long-term company analyses. In fact, it is more likely that the majority of fund managers were following the crowd, focusing on the identification of what and when other fund managers are likely to buy or sell stocks, without making an own fundamental analysis (Healy and Palepu, 2003). Overall, the behavior of various internal and external control instances, which should actual be able to detect accounting manipulations and illicit insider trading, may be explained according to Gordon (2002), by a state of cognitive dissonance. Precisely, Enron may have appeared to be going so well and profitable and the management told such convincing stories that the apparent signs of trouble did not stir skepticism and healthy scrutiny (Gordon, 2002).

3.3.2 The Comroad Scandal (Case Study 2)

Comroad was a German telematics service provider, who developed worldwide applicable, server-based traffic systems. These systems were sold to trading partners, whereas retailers offered the systems as well as complementary services to end-costumers (Dorin, 2006). Comroad entered the international trading floor in the beginning of 1999, whereas it sales quadrupled at the end of this year, compared to its prior year’s level of DM4.6 million. Afterwards, the company exhibited exorbitant growth perspectives,
despite overall negative trends in the industry. In particular, Comroad forecasted an increase of sales to DM250 million in 2002 (Dorin, 2006).

Comroad’s success story, however, turned out to be one of the major accounting scandals of publicly traded firms in Germany. In 2001, first voices were raised, which were skeptical about the business model and reported figures of Comroad. In particular, planned sales volumes released by Comroad were contradictory to the numbers reported by its British client Skynet (Jones, 2011). After these inconsistencies became public, investigations actually showed that sales developments were the result of numerous fictitious transactions, for which Comroad invented commercial relationships with non-existing trading partners, amounting to €19.9 million as declared in Comroad’s financial annual report (Daum, 2011). One of those trading partners was a company named VT Electronics, which was allegedly in charge of the production and delivery of board computers on behalf of Comroad. However, VT Electronics was only collecting money from likewise fictitious end-customers. For the purpose of concealment, payment from end-customers was cleared with the production costs of equipment of VT Electronics and by down payment for further hardware and possible retained surpluses. The only task of Comroad was to prepare invoices and to pretend that invoices were send to end-customers. Comroad stated additional transactions with various other Asian trading partners following a similar fraud pattern (Dorin, 2006). Surprisingly, the illicit practices of Comroad were not detected over a period of three years and despite of various controls in accordance to national and international legal requirements (e.g. the Germany Stock Corporation Act (AktG), Euro-Bilanzgesetz (EuroBilG)) as well as standards for accounting (e.g. IFRS). Thus, in the following the manipulation and concealment techniques of Comroad will be discussed.

**Manipulation and Concealment Techniques**

According to German regulations, the publicly traded company Comroad was managed by a two-tier board structure consisting of the management, responsible for the oversight of day-to-day business operations, and the board of directors, responsible for oversight of the management and acting as final authority with respect to decision making (Adams and Ferreira, 2007). Despite this top-down approach of control, additional internal controls are legally required, for example, according to the AktG (Deutschland, 2015), the Act for Control and Transparency in the Corporate Sector (KonTraG) (Bungartz, 2012), as well as auditing standards such as IDW PS 261 (IDW, 2012). Internal controls are measures and methods adapted to safeguard assets of a company as well as to check the accuracy of bookkeeping (Bungartz, 2012). However, there exist no specified requirements for the corporate-specific design of internal control systems in the German legislation. In general, the board of directors is under legal obligation to
monitor the implementation and development of an adequate internal control system, which may include internal auditors and/or an audit committee (Bungartz, 2012).

In the case of Comroad, it seems obvious that neither the board of directors nor the internal control system was sufficient to prevent the deduction of accounting fraud. Particularly, the CEO of Comroad was able to bypass and suspend the internal control system – a practice called management override of internal controls (Caplan, 1999) – by staffing the board of directors with his wife, who was involved in the fraudulent activities, thereby undermining the board’s independence. As a consequence, the board tolerated the illicit practices (Dorin, 2006) as well as the internal auditor, who received monetary remuneration for the maintained silence (Daum, 2003). Despite the arrangements within the company, the establishment of a close relationship to the external auditor KPMG, by which both parties received mutual advantages, offset external controls. Lastly, financial statement users such as investors, the stock market as well as supervisory authorities, were misled and deceived, as they relied to a great extend on the audited and certified financial statements attested by KPMG (Dorin, 2006; Daum, 2011).

3.3.3 The Parmalat Scandal (Case Study 3)

Parmalat was founded 1961 by Calisto Tanzi, who was the head of family-owned food trader company, entering the milk market by taking advantage of continuous packing process developed by Tetra Pak as well as a Swedish pasteurizing invention called ultra-high temperature (Buchanan and Yang, 2005; Ferrarini and Giudici, 2005). By late 1980s, Parmalat had already become one of the eight largest food companies in Italy, owing to new opportunities, which were opened up after the consolidation of the Italian milk market through changes in the Italian legislature. In particular, these developments enabled a variety of aggressive acquisitions, which made Parmalat an international conglomerate (Buchanan and Yang, 2005). Particularly, Parmalat consolidated its position as a world leader in the dairy market and extended into other food markets, such as bakery products, tomato sauces or fruit juices (Ferrarini and Giudici, 2005).

However, because of the rapid expansion in late 1980s, Parmalat was also in a financial crisis. For financing, Parmalat relied solely on bank loans, leading to chronic undercapitalization, which eroded profits and burdened the company with high debt. Notably, at the end of 1989, liabilities amounted to approximately L520 billion, which equals roughly $400 million, of which $169 million was short-term debt. Consequently, takeover threats emerged and offerings were made to buy all or just some parts of Parmalat, for instance, by Kraft Food Inc. (Buchanan and Yang, 2005). However, Tanzi found a solution to those problems by starting an unique capital raising campaign in the 1990s, in the course of which Tanzi also subscribed to 50 percent of the capital raised, thereby, becoming the major shareholder of Parmalat (Buchanan and Yang, 2005; Ferrarini and
Giudici, 2005). At this time Parmalat opened the door for external financing and, especially to tap on international bond markets. As a result, over the next decade Parmalat started to visit the bond market more than 40 times, providing the firm with fresh capital and funding for a new global acquisition drive (Buchanan and Yang, 2005). This trend continued until the beginning of the new millennium. Despite a BBB-rating from Standard and Poor’s in late 2000, owing to increased costs of capital, due to problems with businesses in Latin American economies, Parmalat continued its strategy of holding huge amount of cash to be used in mergers and acquisitions, whilst financing its cash needs through bonds (Ferrarini and Giudici, 2005). At the end of 2002, Parmalat was the listed holding of a multinational food group made up of more than 200 companies spread around 50 countries. In addition, Parmalat’s last quarterly report shows €3.35 billion in cash and equivalents, whereas its assets amounted to €10 billion with €7.17 billion liabilities, of which 1.5€ were bond debt. At the beginning of 2003, Parmalat was included in the Mib30 index, which is an index of the 30 largest Italian companies in terms of market capitalization (Ferrarini and Giudici, 2005).

The collapse of Parmalat at the end of 2003 was swift, however, first doubts about Parmalat’s desire for issuing bonds, while simultaneously having cash surplus, were raised already in 1999. Nevertheless, first at the end of 2003, the Bank of America announced a document, purportedly certifying that a Cayman island-based unit of Parmalat stated to have €3.9 billion in cash at the end of 2002, was a fake. Additionally, in January 2004, PricewaterhouseCoopers LLP reported that Parmalat had a net debt of €14 billion on September 30, 2003, including nearly €13 billion that were not disclosed before. The new CEO, appointed by the government after Parmalat was filed for bankruptcy protection, further revealed that the company was technically insolvent as far back as 1998 and Parmalat’s former CFO stated that financial statement manipulations may have began already in 1984 (Buchanan and Yang, 2005; Coffee, 2005).

Manipulation and Concealment Techniques

Parmalat’s fraud scheme essentially involved manipulations in the balance sheet, rather than in the income statement such as in the case of the Enron scandal, which is frequently compared to the Parmalat scandal (Coffee, 2005). To this end, perpetrators applied very basic technical means, when it comes to the conduction of fraud and simply hide losses, overstated or recorded non-existent assets, understated debt and diverted company cash to Tanzi’s family members. For instance, to hide losses, Parmalat used various wholly owned entities, whereas uncollectible receivables were transferred from the operating companies to these nominee entities, where their real value was hidden. Fictitious trades and financial transactions were subsequently organized to offset losses of operating subsidiaries and to inflate assets and income. Understatement of debt, on the other hand, was generated through the record of non-existent repurchases of bonds or by
simply selling receivables falsely described as non-recourse. Eventually, funds were
diverted to family members, for example, by channeling of repayments of business
partners into bank accounts held by a company that was fully controlled by the family
(Ferrarini and Giudici, 2005).

Given these techniques, investigations in the aftermath of the scandal focused on auditors and especially the external auditor Grant Thornton, who has been Parmalat’s auditor since the 1980s. In particular, Italian law actually mandated the rotation of audit firms, however, Thornton found an easy solution to this problem. Thornton gave up the role as auditor of the main company in the Parmalat group and continued auditing its subsidiaries, such as the Cayman island based subsidiary Bonlat (Coffee, 2005). In 1999, Parmalat started putting more falsified transactions to Bonlat’s books and, thereby, assigned more assets and revenue to be audited by Thornton. Between 1999 and 2002 Thornton’s share of auditing process increased from 22 to 49 percent, even though only 17 out of 137 units were actually audited through Thornton and despite Deloitte & Touche was the lead auditor at this time. However, Deloitte certified the group accounts of Parmalat as fair between 1999 and 2002, without checking Thornton’s work and without independent verifications. As late as 2003, Deloitte was the first time legally required to prove the findings of the second auditor Thornton, leading to several and severe concerns about the correctness of reports (Buchanan and Yang, 2005).

Despite partiality and missing objectivity of Thornton, it is questionable, if in the case of Parmalat further diligent auditors would have monitor earnestly, given the threat of being dismissed at the point, where they report illicit activities. In particular, maybe auditors can do little to stop squeeze-out mergers, coercive tender offers or unfair related-party-transactions without protection. In this case, shareholder should receive protection from large banks that typically monitor corporations, with whom they work (Coffee, 2005). In the case of Parmalat, however, creditor banks did not play an active role in monitoring. Consequently, banks also received criticism, because they continued giving loans to Parmalat that was already in financial difficulties. Nevertheless, banks made good profits with the placement of bonds, which were often sold to their own clients. Major criticism, however, applied to the Deutsche Bank, who first increased their shares in Parmalat from 2.3 to 5.2 percent, in order to reduce their shares shortly after the purchase to 0.8 percent. This raises the question, whether the Deutsche Bank had significant information advantage about the actual financial situation of Parmalat as well as knowledge about accounting manipulations. Furthermore, the Deutsche Bank was accused for helping Parmalat to falsely report the actual liquidity situation of the company to Standard & Poor’s (Dorin, 2006).

Parmalat’s board of directors was to a large part not independent. More precisely, only 15 percent of all directors were independent, whereas the remaining directors were four
family members of Tanzi, four company executives, two of Tanzi’s school friends, one long term business associate, one lawyer as well as one accountant (Buchanan and Yang, 2005). Similar, the audit committee seemed to be entangled as it consisted as well of two former school friends and a former CFO, who served Parmalat for more than 15 years. In addition, Tanzi visited the meeting of the audit committee six times in 2002, leading as well to increased partiality (Buchanan and Yang, 2005). Obviously, in the case of Parmalat no effective board as well as internal audit committee was in place to prevent the illicit practices. Eventually, Tanzi mentality played a major role in the concealment of fraud. Buchanan and Yang (2002) concluded that Tanzi’s willingness to scarify the firm’s economic wellbeing for independence and control, transformed him from an entrepreneur to a rent-seeker (Buchanan and Yang, 2005). Additionally, Tanzi did everything to control shareholders. For instance, in the aftermath of the scandal it was revealed that at least €2.3 billion were paid to affiliate persons and shareholders through related-party transactions (Coffee, 2005).

### 3.3.4 Further Accounting Scandals

Table 16 provides an overview over further accounting scandals between the years 1998 and 2015. Notably, this list is by no means complete, however comprises some of the most important and severe accounting scandals that raised worldwide attention. This list is not restricted to any particular country, which is often done in scientific analyses concerned with accounting fraud. Especially, this applies to analysis of accounting fraud incidents in the USA, which was the epicenter of a whole new wave of accounting scandals at the beginning of the 21th century (Ball, 2009). In contrast, the approach which is taken here should lead to the identification and emphasize of fraud patterns, irrespective of a particular legal regulation or corporate system and, thus, to the elaboration of more general, universal fraud patterns. Accordingly, the following table includes accounting fraud incidents that happened, among others, in Germany, Italy, in the USA as well as in Japan or India.
<table>
<thead>
<tr>
<th>Scandal/Case Study (CS) No.</th>
<th>Year</th>
<th>Estimated Economic Damage</th>
<th>Explanatory Factors</th>
<th>Sources</th>
</tr>
</thead>
</table>
| Waste Management Scandal (CS4) | 1998 | Estimated shareholder value loss due to 33 percent stock drop: approx. $6 billion | • Involvement of external auditor in manipulation concealment  
• Conflicts of interest between Waste Management CFO and external auditor  
• Absence of oversight function through audit committee  
• Ineffective internal control structure | (Razaee and Riley, 2002; SEC, 2002; Mintz, 2014) |
| Flowtex Scandal CS5) | 2000 | -                         | • Insufficient controls through external auditor  
• Partial cooperation with politicians and tax author-ity  
• Cooperation of management and control organs | (Dorin, 2006; Schönmann, 2006; Boecker, 2010) |
| Enron Scandal | 2001 | Estimated total shareholder value loss approx. $63 billion | • Lack of board independence  
• Stock-based compensation of top-management  
• Partiality of external auditor  
• Lack of investors’ skepticism | (Gordon, 2002; Powers, Troubh and Winokur, 2002; Thomas, 2002; Healy and Palepu, 2003; Petrick and Scherer, 2003) |
| World-Com Scandal (CS6) | 2002 | Estimated total shareholder value loss approx. $175 billion | • Lack of board independence due to compensation schemes  
• Enforcement of employee loyalty through bonus schemes  
• Failure of internal and | (Zekany, Braun and Warder, 2004; Kuhn and Sutton, 2006; Sadka, 2006; Singh and Busen, |
<table>
<thead>
<tr>
<th>Scandal (CS7)</th>
<th>Year</th>
<th>Description</th>
<th>Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tyco Scandal</strong></td>
<td>2002</td>
<td>80% stock drop after exposure of accounting manipulations</td>
<td>- Bribery of employees to hide fraudulent schemes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Override of internal controls (especially of the board)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Lax corporate governance procedures (poor documentation etc.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Sorking and Berenson, 2002; Center, 2006; Neal, 2014)</td>
</tr>
<tr>
<td><strong>Comroad Scandal</strong></td>
<td>2002</td>
<td>-</td>
<td>- Lack of board independence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Great proximity of external auditors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Daum, 2003, 2011; Peemöller and Hofmann, 2005; Dorin, 2006; Jones, 2011)</td>
</tr>
<tr>
<td><strong>Health-South Scandal (CS9)</strong></td>
<td>2003</td>
<td>-</td>
<td>- Executives pressure to inflate earnings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Deliberate deception of external auditors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Lax internal controls (board and audit panel)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Weld, Bergevin and Magrath, 2004; Albrecht et al., 2012; Smith, 2013)</td>
</tr>
<tr>
<td><strong>Parmalat Scandal</strong></td>
<td>2003</td>
<td>40% stock drop after Parmalat bonds received junk status</td>
<td>- Ownership structure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additional 60% drop after revelation of manipulations</td>
<td>- Lack of board and internal audit committee independence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Lax Italian accounting and corporate governance standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Lack of objectivity of external auditor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Missing sense of responsibility of creditor banks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Buchanan and Yang, 2005; Coffee, 2005; Ferrarini and Giudici, 2005; Melis, 2005; Dorin, 2006)</td>
</tr>
<tr>
<td><strong>American International Group Scandal (CS10)</strong></td>
<td>2005</td>
<td>-</td>
<td>- Executive compensation as incentive to increase engagement in accounting misappropriations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Lax internal controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Bhagat and Romano, 2008; Thomas, 2009; Vasudev,)</td>
</tr>
<tr>
<td>Company/Scandal</td>
<td>Year</td>
<td>Description</td>
<td>Key Factors</td>
</tr>
<tr>
<td>------------------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lehman Brothers Scandal (CS11)</td>
<td>2008</td>
<td>$46 billion of market value lost after bankruptcy</td>
<td>• Missing transparency in operations and finance</td>
</tr>
<tr>
<td>Satyam Scandal (CS12)</td>
<td>2009</td>
<td>Stock price decrease of nearly 70% after fraud disclosure</td>
<td>• Collective fraud and concealment by CEO, board, and internal audit</td>
</tr>
<tr>
<td>Olympus (CS13)</td>
<td>2011</td>
<td>Shareholder value loss of approx. 80% after fraud revelation</td>
<td>• Lack of board independence</td>
</tr>
<tr>
<td>Tesco (CS14)</td>
<td>2014</td>
<td>Tesco group value declined after fraud discovery by £2 billion</td>
<td>• Ineffective internal audit committee and board of directors</td>
</tr>
<tr>
<td>Toshiba (CS15)</td>
<td>2015</td>
<td>Shares of Toshiba</td>
<td>• Corporate culture implying strong loyalty to exec-</td>
</tr>
</tbody>
</table>
Table 16. Overview of further accounting scandals and explanatory factors

As apparent from the table, explanatory factors or circumstances, which led to the emergence of accounting fraud, resemble each other in regard to the 15 analyzed accounting fraud incidents. According to this analysis, the most often existing circumstance, if accounting fraud occurred, is an inefficient internal control system, which applies to 93 percent of the investigated accounting fraud incidents. This implies that internal controls, such as the board of directors and an internal audit committee, are indeed present, however, are ineffective either in detecting fraud or are not willing to do so. The second most common present factor is the existence of extraordinary and partially exorbitant compensation and bonus schemes for executives, employees but also for the members of control bodies, which sometimes rather commemorate to bribery than fair compensation. In fact, this factor is also mentioned by other academic literature as a frequently observed cause and means for the concealment of accounting fraud, which serves as a method to obtain silence over the applied illicit practices (Demerens, Paréa and Redis, 2013). The third most common factor and present in roughly 33 percent of the analyzed fraud incidents, is inability of external auditors to detect fraud, direct involvement of external auditors in conducting fraudulent activities as well as the inability of the market (e.g. shareholder or potential shareholders) and supervising, regulatory bodies to detect accounting fraud. Differentiation between inability to detect fraud and involvement in fraudulent activities is based on, whether or not involvement is actually proofed. For instance, in many cases, in which external auditors or regulatory bodies claim that they have not discovered accounting fraud, there is an accusation of involvement or at least toleration of illicit practices through the control bodies. However, in this study, if there is no final evidence, inability is assumed.

An additional influencing factor is pressure from top management or executives, which is present in 20 percent of the investigated fraud incidents. Pressure means that employees or other individuals related to the company are enforced to conduct fraud. Otherwise, loyalty to the company may be imposed, meaning that employees must tolerate fraud in order to not being fired or to receive other ramifications, such as disciplinary transfer or salary reductions. Notably, this factor is highly linked to the corporate and country specific culture. For example Japanese culture often implies high corporate loy-
ality, such as in the case of Olympus as well as censorship of outspoken employees (Tabuchi, 2013). Direct involvement of regulatory bodies or market participants is only observed in 2 out of the 15 accounting fraud incidents. However, most often fraudulent patterns, which include the toleration or involvement of regulatory bodies, are of considerable dimension. For instance, in the case of Flowtex, it was revealed that fraud could only be concealed, because a taxman and the prosecution covered the illicit practices (Dorin, 2006). Eventually, the lack of parts of an internal control system or absence of the whole internal control system was only present in one scandal, which is Satyam, an Indian telecommunication company (Kumar, Paul and Sapkota, 2012).

Based on these case studies and the subsequent evaluation, two conclusions can be drawn, which also coincide with other existing, empirical studies. First, perpetrators of fraud are most often top executives as well as the founders of the company itself that act as inciting force. This applies to all 15 analyzed accounting fraud incidents and is underpinned, by looking at existing empirical studies, such as Razaei and Riley (2002), Albrecht et al. (2012) as well as ACFE (2016). Second, in roughly 93 percent of the analyzed fraud incidents, internal and external controls are in place, thus, the problem is not a lack thereof, but the obvious inefficiency of these systems to prevent and detect fraud. However, so far, the case studies did no deliver insights on, why internal control systems are seemingly inefficient. Consequently, in the following, the circumstances that lead to the inefficiency of internal as well as external controls will be investigated.

### 3.4 Generalization of Accounting Fraud Patterns

Dorin (2006) describes several incidents of accounting fraud, among others, the previously presented case studies of Comroad and Parmalat, by using the so-called swiss cheese model. In particular, the model shows, how systems may breakdown due to human intended or unintended as well as technical failures (Reason, 1990). Most importantly, a single weakness often do not lead to a breakdown, or in the case of accounting, to fraud. Thus a single factor, e.g. lax internal audit or technical weaknesses within the accounting information system may be insignificant and not relevant, if everyone behaves honest; however, if there exist, for instance a manager, who is willing to conduct fraud in order to increase his own benefit, together with a technical or organizational weakness, this may builds up to a problem, waiting to result in accounting fraud (Sadgrove, 2016). Thus, the swiss cheese model implies that fraud can be conducted despite the existence of several legally required and/or voluntarily implemented firewalls, i.e. internal and external control systems as well as technical precautions. Perpetrators of fraud are able to circumvent those controls and security measures by using the system’s deficiencies (loopholes) for their own benefit (Dorin, 2006).
In the following the approach of Dorin (2006) is followed, by applying the swiss cheese model as underlying construct and explanatory factor for the emergence of fraud. However, since the identified fraud patterns in the case studies indicate that the emergence of fraud is predominantly an organizational problem, leading to the inefficiency of internal control systems, an organizational view on the relationship within a company and, especially, between the management and the respective control bodies is taken. In particular, a generalization of the previously identified fraud patterns is provided in Figure 10. The figure depicts entities within an organization and the theoretically indented as well as unintended relationships. Theoretically intended, i.e. desired relationships between entities are derived from related literature and indicated in the figure by using solid lines. The relationships and interferences observed in the case studies are described and indicated using dashed lines. The relationships depicted in Figure 10 and the associated implications are discussed in the following sub-chapters.

Figure 10. Generalization of identified fraud patterns

### 3.4.1 Business Entities Dependencies and Mutual Control Functions

In the context of corporate governance, several mechanisms exist that should prevent corporate executives from exploiting information asymmetries, resulting from the agency relationship between shareholders and the management of a corporation. One example of a control entity responsible for so called ‘good governance’ is the board of direc-
tors that is responsible for solving contractual problems between shareholders and the corporate executives. In Figure 10, a two-tier board system is assumed, meaning that the management of the corporation and overarching controls are separated. From an organizational viewpoint, this separation is realized by the distinction between of a board of directors and an executive board that is responsible for corporate management and the oversight of employees. In turn, the board of directors is responsible for the monitoring of the managerial and corporate performance and is in charge of the ratification of managerial decisions on behalf of the shareholders (Bushman et al., 2004). Additionally, the board of directors has the right to intervene in cases, where corporation’s interests are seriously affected by actions taken by the executive board (Jungmann, 2006). A proper control of risks, moreover, requires the board of directors to develop and implement an internal control system that may includes control committees that partially overlap with the responsibilities of the board of directors. Most importantly, the internal control system should enhance the functioning of the board of directors by providing additional controls and increased insights in management activities as well as financial transactions (Kendrick, 2000). An example for an additional control body, which is a part of the internal control system, is an internal audit committee, which serves to increase the accuracy of financial statements and the quality of work performed by internal and external auditors (Sarens, De Beelde and Everaert, 2009).

Despite control entities that should enhance the ability to control and reduce risks resulting from managerial decisions, it must be noticed that risks can only be minimized rather than fully eliminated through internal controls, leading to the necessity of additional external controls i.e. an external and independent auditor (Kendrick, 2000). The external auditor performs tests and controls in gathering sufficient evidence in providing reasonable assurance that the financial statement is free from material misstatements. If an auditor detects a material misstatement, a company must correct it, in order to conform to the generally accepted accounting principles as well as further national laws. Only if the financial statement is correct, it will contribute to rational investment decisions and efficient capital markets, when it is use by investors, creditors and the public. Eventually, a company is potentially subject to an examination by an exchange supervisory authority (e.g. SEC) and will be forced to restate and correct misstated financial reports (Razae and Riley, 2002; Hogan et al., 2008). Lastly, an indirect control function may be assumed for stock market participants and especially, the shareholders of a corporation. Notably, if a stock develops in an exceptional way, this probably could raise skepticism about the correctness of transactions among shareholders (Dorin, 2006).
3.4.2 Requirements for the Prevention of Accounting Fraud

With the analysis of Figure 10, the existence of circular references between the management, the board of directors and the internal control system get apparent that are, especially opposed to the intended and previously described mutual control system. In particular, if the board of directors depends partly or completely on the management and if the internal control system is determined by the management, than there exist no internal mechanism that might prevents the management from conducting accounting fraud by the exposure of effective controls. This observation is supported by the findings of Caplan (1999) as well as Sawyer et al. (2012), noticing that the management will always be able to override internal controls, especially, because it is in a position to choose the strength of these systems through its influence on the board. Moreover, if management override of internal controls happens, there is no obvious reason for external auditors to revise their evaluation of management integrity (Caplan, 1999; Lennox and Pittman, 2010), leading to additional negative effects for the effectiveness of controls. Despite the effects of external auditors are controversial discussed, the observations of Caplan (1999) and Lennox and Pittman (2010) coincide with the interferences identified in the case studies, where the assurance service of external auditors seem to have deteriorated after the override of internal controls and, therefore, external auditors were not able to deter accounting fraud (Dorin, 2006). Lastly, these inefficiencies are expected to exert further negative effects on the remaining direct and indirect external controls, that are, for instance, regulatory bodies as well as stock markets, which typically trust (at least to a great extend) third-party financial audit and verifications (Lennox and Pittman, 2010).

Overall, Figure 10 leads to the conclusion that the core problem of fraud prevention and the inefficiency of internal as well as external controls is a powerful, highly centralized management that is able to offset controls or is capable of building coalitions and alliances with control entities. Consequently, the inefficiency of control systems can be defined as a problem of organizational structures and responsibilities that lead to undesired interferences between the management and control bodies. Against this background, distributed ledgers may be a solution to the problem of inefficient controls as they imply organizational transformation, owing to their decentralized nature and associated collective consensus finding. This is in contrast to the typical hierarchical structure of firms and, probably, enables independence of control entities due to changed responsibilities and intra-organizational relationships. Despite that, distributed ledger may increase the security of data on a technical level, due to potential immutability and increased transparency of data on the ledger incorporated by distributed consensus.
3.5 Concluding Remarks

The main part of this chapter is concerned with the investigation of fifteen accounting fraud incidents in order to identify regular occurring fraud patterns and circumstance that lead to the emergence of accounting fraud in the discussed case studies. Most apparently, fraud was most often conducted on behalf of or by the management in mutual cooperation with internal control systems that actually (or at least in theory) should prevent the emergence of fraud. Transferring this pattern as well as further results on a more abstract level, undesired relationships between control entities within and outside a corporation get obvious. Based on this generalization, management override of controls is identified as one main factor that enables the conduction of accounting fraud, whereas the ability to override internal controls is highly determined by the organizational structure of an organization and, thereby, is less a concern of the technical design of an accounting information system. Eventually, the generalization of fraud patterns provides a framework, on which basis scenarios of distributed ledger based accounting systems should be built and oriented, assuming that the identified fraud patterns should be prevented by such systems. In particular, one possible scenario of distributed ledger based accounting will be developed in the course of this dissertation, while taking into account the identified fraud patterns.

Thereby, the present chapter provides the starting point for subsequent considerations related to the question, how distributed ledger technology can be applied exactly to prevent the emergence of accounting fraud. In particular, answering of RQ.2 delivers the basic problem in today’s accounting that is the ability of a powerful management to offset existing internal controls and, consequently, also external controls. From this, requirements for an effective distributed ledger design can be derived that are organizational restructuring and the dissolution of hierarchical decision structures within organizations. Moreover, on a technological level, immutability of ledger entries and full transparency are desirable characteristics of a distributed ledger based accounting system, providing full insights and control over accounting data to internal and external control entities, thereby, facilitating their monitoring function. Distributed ledger technology should fulfill these requirements in order to be successfully applied for accounting fraud prevention.
Key Points Chapter 3:

- **Existing fraud prevention and detection techniques** are not capable of deterring illicit behavior and the emergence of accounting fraud.
- Distributed ledger technology has the potential to affect and facilitate fraud prevention and detection in the design time, run time as well as audit phase through the specification of protocol rules, consensus mechanisms as well as increased transparency of ledger entries.
- Distributed ledgers that should prevent accounting fraud must, especially, prevent management override of internal controls.
- **Requirements** on distributed ledgers for the prevention of management override of internal controls are organizational restructuring, the dissolution of hierarchical decisions making in combination with the already mentioned technical precautions implied by distributed ledgers.
4 Distributed Ledger Design for Applications in Fraud Prevention

So far, distributed ledger technology was treated as a ‘black box’. This means that the technical features of distributed ledgers and consequences were mainly derived from real case observations and the thereby induced implications that are decentralization, transparency and potential immutability. However, the architecture and concrete functioning of distributed ledger technology are particularly important, given the fact that the already discussed value generation for corporations as well as for customers and all kind of end-users is only enabled by technology’s characteristics. Thus, together with the results derived from the previous chapter, in the following the distributed ledger architecture is explained and design decision are discussed that are desirable if the technology is applied for corporate accounting. Consequently, the third research question of this thesis is (RQ.3): Does the technical architecture of distributed ledgers fit for the purpose of accounting and is it capable of preventing accounting fraud? This overarching research question is answered through the investigation of two related research questions. In the following, first the technical architecture, its features as well as the associated technical design decision are described by using a four-layer architecture model of distributed ledgers. Based on the model, characteristics of distributed ledgers and design decision will be discussed on each level. Moreover, a range of definitions is provided that is important for the following thesis and understanding of distributed ledger technology. Eventually, design decisions that are desirable, if distributed ledgers are applied in the context of accounting, are emphasized. The associated research question (RQ.3a) is, therefore: How is the technical architecture of distributed ledgers designed and what are the associated ledger design decisions that enable its application for the prevention of accounting fraud?

The second research question necessary to answer RQ.3 is (RQ.3b): Which technical, organizational as well as social paradigm changes are implied by distributed ledger technology and how can firms approach these changes in order to prevent accounting fraud? Answering this question implies an investigation of the paradigm changes induced through distributed ledgers and their relation to ledger design. This is especially important given the fact that the paradigm changes induced by distributed ledgers must be expected to change common ways of doing business and possibly even our present-day economy (Iansiti and Lakhani, 2017). Thus, implementing distributed ledger technology within existing business infrastructures also implies that ledger implementation comes at costs and that firms face significant adjustment processes on all organizational
levels, i.e. resources, processes as well as values of firms (Lucas and Goh, 2009). Consequently, it is discussed how companies can deal with these changes by proposing strategies for the alignment of business processes and distributed ledger technology and describing the imposed impacts on management and operational processes. Notably, thereby, it is assumed that the business value of distributed ledgers can only emerge, if business processes and the technology are aligned (Barua, Kriebel and Mukhopadhyay, 1995; Rao, Angelov and Nov, 2006). Eventually, it is shown how firms customize distributed ledger technology for their desired purpose. Notably, this delivers a framework for companies, giving insights on how to implement the technology, while respecting and/or adjusting existing infrastructures and accounting processes.

4.1 The Four-Layer Architecture of Distributed Ledgers and System Design Decisions

A four-layer architecture of distributed ledgers is presented in Figure 11, consisting of a network layer, a procession layer, a representation layer and a storage layer. In the following, the respective layers will be explained individually, starting from the bottom layer. Thereby, the architecture is explained by emulating the course of an arbitrary chosen transaction, which starts with its initiation through a network participant and ends with the storage on the distributed ledger. The separation of the distributed ledger architecture into single layers allows the identification of layer dependent technological features and associated design decisions, which eventually influence the characteristics of the distributed ledger and how information as well as data is processed and stored on the ledger. The double-sided arrows between the layers indicate that it is possible to analyze the layers independently, however, in reality the layers are interrelated and overarching effects must be considered. The following explanations on the four-layer architecture and the related concepts are held on an abstract level. To provide clarification regarding some technological concepts and to highlight notable features of distributed ledgers, examples are used occasionally. Mostly, these examples refer to Bitcoin, which is chosen, since it constitutes the prominent example of an application case of distributed ledgers and was, furthermore, discussed at the beginning of this thesis.
4 Distributed Ledger Design for Applications in Fraud Prevention

Figure 11. The four-layer architecture of distributed ledgers

4.1.1 Network Layer

The first layer of the distributed ledger architecture is the peer-to-peer network, which relies on the voluntary and mutual contribution of resources from individual network participants (Feldman et al., 2006). Thereby, the concept of peer-to-peer networks is in stark contrast to the client-server concept, assuming the existence of a service provider and a service user, including the determination of certain hierarchy levels regulating their interaction. In contrast, the peer-to-peer network consist of homogenous and equal nodes, offering themselves services through the exertion of own resources, such as processing power, storage capacity or network link capacity (Schollmeier, 2001; Müller, Eymann and Kreutzer, 2003). The participants of the network are, therefore both, resource provider and requester, whereas the offered resources must be crucial to the network service or content (Schollmeier, 2001). Summarizing, a peer-to-peer network can be defined as follows (Schollmeier, 2001):

Definition 1 (Peer-to-Peer Network): A network architecture is called peer-to-peer (P2P), if (i.) the participants of the network share a part of their own hardware resources, and (ii.) mutual resource sharing is a necessary condition for the provision of network services or content.

The concept of a peer-to-peer network can be refined and divided into two subsets, as shown in Table 17. Depending on the subset, the peer-to-peer network either allows the existence of a central entity or is managed completely decentralized. Centralization means that one entity may be substantial for providing some parts of the offered network services and provides directory services for regions of the network (Fox, 2001; Schollmeier, 2001; Lu and Callan, 2003). Particularly, a directory contains information, such as descriptions or locations about data items in the database (Özsu and Valduriez,
If a central entity exists in the peer-to-peer network, it is called hybrid peer-to-peer network as there is no complete decentralization (Lv et al., 2002). Contrarily, a network that forbids the existence of any central entity is called pure peer-to-peer network and is characterized by the ability to provide network services without suffering any loss, if any arbitrary, single node is removed, also called partition tolerance (Schollmeier, 2001; Bitfury and Garzik, 2015). Consequently, pure peer-to-peer networks are fully decentralized, however, they can either feature a structured or unstructured approach in regard to the set of connections between network participants (Lv et al., 2002). Structured approaches imply according to Lv et al. (2002) that the network topology is tightly controlled and that files are placed not at random nodes but at specified locations that will make subsequent queries easier. Loosely structured peer-to-peer architectures are, therefore, networks, in which the placement of files is based on hints, whereas in highly structured networks the network topology as well as the placement of files is precisely determined (Lv et al., 2002). Unstructured peer-to-peer architectures posses neither a centralized directory nor a file placement and participants join the network according to some loose rules, specified in the underlying protocol (Karakaya, Korpeoglu and Ulusoy, 2009).

<table>
<thead>
<tr>
<th>Architecture/Characteristic</th>
<th>P2P Network Type</th>
<th>Decentralized</th>
<th>Partially Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structured</td>
<td>Pure Peer-to-Peer</td>
<td></td>
<td>Hybrid Peer-to-Peer</td>
</tr>
<tr>
<td></td>
<td>Loosely</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unstructured</td>
<td>Loose rules</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 17. Classification of peer-to-peer networks

4.1.1.1 Distributed Ledger Access Control

Distributed ledger leverage the flexibility of peer-to-peer networks concerning the particular network type and structure, in order to share information between all participants and apply either pure or hybrid forms of peer-to-peer networks, depending on the requirements on the network’s capabilities, such as scalability or applicability of a particular query method (Lv et al., 2002). For instance, blockchains, as applied in the case of Bitcoin, draw on a pure, decentralized peer-to-peer network, in which participants can join without any prior authorization. Moreover, there is no restriction concerning the ability to read data on the blockchain (which may be still encrypted) or to submit information for the inclusion into the blockchain (Bitfury and Garzik, 2015; Peters and Panayi, 2015). Given the openness of the Bitcoin blockchain, residing on a pure peer-to-peer network, this type of distribute blockchain is also called permissionless distributed
ledger. A permissionless distributed ledger can be defined as follows (Peters and Panayi, 2015; Rückeshäuser, 2017c):

Definition 2 (Permissionless Distributed Ledger): Permissionless distributed ledgers are characterized by (i.) free access to the underlying peer-to-peer network, and (ii.) unrestricted readability of information on the ledger. Permissionless distributed ledgers are typically featured by unstructured network architectures.

However, given fact that an unstructured network architecture is used – which implies that the typology has certain properties, but the placement of files is not based on any knowledge of the typology – permissionless distributed ledger require a special query method called flooding. Flooding is a method to find a file in unstructured networks, by querying all neighbor by propagating the query through the network (Lv et al., 2002). In particular, flooding or information propagation in an unstructured peer-to-peer network works as follows: After a node has entered a permissioned peer-to-peer network through initiating at least one connection with another node in the network, it can search the network by sending a request (query message) to its neighbors. Each neighbor then forwards this message to all its neighbors and so on, until the message is forwarded by a pre-determined number of so-called hops from the sender (Karakaya, Körpeoğlu and Ulusoy, 2008). Similar to this approach, Bitcoin uses a special flooding algorithm also called gossip protocol, to relay messages across the network. Thus, whenever a node creates a transaction, it sends it directly to its connected nodes, which decides whether or not the transaction is valid (which will be discussed in the following). If the transaction is valid, connected nodes relay the messages to their related peers and the message gets propagated through the network (Koshy, Koshy and McDaniel, 2014). However, it might not be reasonable to send this message to all nodes of the network, depending on the network size. Thus, forwarding of messages can be restricted to a certain number of nodes by using the Time-To-Live (TTL) field of the request message in order to control the number of hops (Karakaya, Körpeoğlu and Ulusoy, 2008).

Contrarily, other distributed ledger may apply a hybrid peer-to-peer approach, in which the access to information and the ability to submit transactions is limited to predefined number of nodes (Bitfury and Garzik, 2015; Peters and Panayi, 2015). To this end, nodes may be white- or blacklisted, using some type of gatekeeping mechanism, such as Know-Your-Customer procedures. Consequently, the distributed ledger can be characterized as permissioned ledger (Peters and Panayi, 2015; Swanson, 2015). A permissioned distributed ledger can be defined as follows (Peters and Panayi, 2015):

Definition 3 (Permissioned Distributed Ledger): A permissioned distributed ledger is characterized by (i.) a pre-specified set of nodes that is capable of par-
participating on the peer-to-peer, and (ii.) restrictions regarding the ability of
nodes to read information on the distributed ledger. Permissioned ledgers typically
feature hybrid peer-to-peer network structures.

4.1.1.2 Node Authentication and Message Encryption

Associated with the degree of structuring and knowledge about the network typology
and its properties is the circumstance whether nodes are known in the network, or
whether they are partially or completely anonym, whereas partial anonymity means that
nodes are only known as pseudonyms. Obviously, anonymity of nodes is of less concern
in permissioned distributed ledgers compared to permissionless distributed ledgers such
as Bitcoin. Whereas both types of ledgers apply digital signature schemes, they can be
used for different purposed, such as for the proof of ownership or for the assignment of
identities. Generally, digital signatures can be defined according to Narayanan et al.
(2016) as follows:

Definition 4 (Digital Signature): A digital signature is the digital analogue to a
handwritten signature to proof the authenticity of a digital message or doc-
ument as well as ownership.

More precisely a digital signature consist of the following three algorithms and the asso-
ciated methods:

- \((sk, pk) : = \text{generateKeys(keysize)}\): The generateKeys method takes a key size
  and generates a key pair consisting of a private (secret) key \((sk)\) and a public key
  \((pk)\) corresponding to a security parameter \(k\). The private key is used to sign a
  message or document whereas the public key is used as verification key, with
  which everyone is able to verify the respective signature (Fromknecht and
  Velicanu, 2014; Narayanan et al., 2016).

- \(\text{sig} : = \text{sign}(sk, message)\): The sign method takes a message and the private key
  \(sk\) as inputs. Then, it outputs a signature for a message under the private key \(sk\)
  (Narayanan et al., 2016).

- \(\text{isValid} : = \text{verify}(pk, message, sig)\): The verify method takes a message, a si-
gnature, and the public key as input and returns a boolean value, isValid, which is
a value that can only take two values. The value will be true if sig is a valid sig-
nature for message under the public key \(pk\), and false otherwise (Narayanan et al.,
2016).

Moreover, digital signatures must have two properties that require, first, valid signatures
to verify and, second, that digital signatures are existentially unforgettable. More pre-
cisely, valid signatures must verify, such that \(\text{verify}(pk, message, \text{sign}(sk, message)) =
true\). The requirement of existentially unforgettable digital signatures means that
without knowledge of a the private key corresponding to the public key, no probabilistic, polynomial-time adversary $A$ should be able to produce a signature-message pair $(\text{sig}, \text{message})$, such that $\text{verify}(\text{sig}, \text{message}) = 1$, with probability non-negligible in the security parameter $k$. Consequently, the adversary $A$ should fail, if he or she has already seen a polynomial number of valid signatures on messages of his or her choice not equal to message (Fromknecht and Velicanu, 2014; Narayanan et al., 2016).

---

**Digression: Use of digital signatures in Bitcoin**

Bitcoin uses digital signatures to create key pairs to control the access to bitcoins in the network, which are stored on a wallet that is, basically, a private file or database. Generally, digital keys are independent of the Bitcoin (consensus) protocol and can be created without referencing it on the blockchain as well as without access to the Internet. In contrast, keys are needed to conduct transactions in Bitcoin, as every bitcoin transaction requires a valid signature to be included in the blockchain, which can only be generate by applying a valid digital key. Thereby, Bitcoin uses signatures to spend coins and to proof the ownership of funds used in a transaction (Antonopoulos, Nandhakumar and Panourgias, 2014; Narayanan et al., 2016).

Bitcoin uses a particular digital key scheme called Elliptic Curve Signature Algorithm (ECDSA), which is an U.S. government standard and generally believed to be secure (Narayanan et al., 2016). More precisely, ECDSA is a based on the discrete logarithm problem as expressed by addition and multiplication on the points of an elliptic curve. Bitcoin uses a specific elliptic curve and a set of mathematical constants, defined in the standard called secp256k1, estimated to provide 128 bits of security (Antonopoulos, 2014; Narayanan et al., 2016). However, the elliptic curve is difficult to visualize, as it is defined over a finite field of prime order instead of over real numbers, which makes it look like a pattern of dots scattered in two dimensions. The function, which produces the elliptic curve looks as follows:

$$y^2 \mod p = (x^3 + 7) \mod p,$$

whereas $\mod p$ (modulo prime number $p$) indicates that the curve is over a finite field of primer order $p$, also written as $\mathbb{F}_p$, with $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, which is a very large prime number. By using ECDSA, a secure source of entropy or randomness is guaranteed, which ensures that the key number is not predictable or repeatable (Antonopoulos, Nandhakumar and Panourgias, 2014).

Despite the use of signatures for the proof of ownership, digital signatures can also be applied to identify nodes or identities within a network, by equating the public key with...
the respective node. Thereby, the public key $pk$ can be thought of as being like a node in the network, which can send a message or make a statement by simply signing a message or statement. From this viewpoint, $pk$ is like an identity, however, this also requires the respective node to know the corresponding private key $sk$. In permissioned systems, the threat of hiding identities by using multiple public keys as identities is indeed small, owing to the implied network access control. In permissionless distributed ledgers, nodes may randomly create new key pairs by using the `generateKeys` operation in the digital signature scheme, given a (intended) lack of network access control. This enables single nodes to cover the real world identities and prevents others of identifying a special node by examining the respective private key (Narayanan *et al.*, 2016).

### 4.1.2 Procession Layer: Authorization and Validation

After information was propagated through the peer-to-peer network underlying either a permissioned or permissionless distributed ledger, consensus must be found about the validity of information submitted by the respective nodes. Thereby, consensus whether information is valid or not does not only refer to the fact, whether or not information is qualified to be included into the ledger, but also which nodes are eligible to validate transactions as well as how the validation process is actually carried out. Thus, in order to find consensus, a set of rules must be specified within the distributed ledger protocol beforehand, such that information will only be automatically included into the ledger, if they conform to the pre-specified set of rules. Generally, protocol rules can be classified into general and contextual rules (Figure 12). Specifically, the two set of rules differ according to their scope: While general rules describe the provisions applying to every information processed throughout a peer-to-peer network and distributed ledger, respectively, contextual rules are binding only to a specific set of information, such as a special type of transaction or even only to a single transaction.

General rules are embedded into the protocol of a decentralized ledger and determine the fundamental characteristics and features of the decentralized ledger. On the highest level, general rules define the degree of openness of a ledger by setting the terms of participations. This decision is basically already taken on the network layer. However, despite the decision, whether a permissionless or permissioned distributed ledger is employed, including the decisions for either a pure or hybrid peer-to-peer network, general rules also imply, among others, rules with regard to the node’s capability for validation, how information is tied to nodes as well as which kinds of signatures are used to prove ownership, etc. Contrarily, contextual rules provide a set of rules that is limited to specify a minimum of requirements on the structure and operation of correct transactions. Thereby, they describe provisions, to which not all information that are intended to be
incorporated are obliged to conform to. Therefore, contextual rules constitute the foundation for new functionalities of the distributed ledger.

![Diagram showing General Rules and Contextual Rules]

Having specified the rules information have to comply with, contextual and general rules must be implemented into the distributed ledger in order to enforce them. One major innovation of distributed ledger technology is that the consensus process is carried out in a decentralized fashion. Instead of trusting a third party checking the conformance of transactions, the distributed peer-to-peer network consisting of consensus participants agrees upon the validity of information that will be incorporated into the ledger using a particular distributed consensus mechanisms. Thus, in the following distributed consensus mechanisms will be discussed as enforcement mechanism of a set of general rules that is applied within the context of a distributed ledger. In contrast, smart contracts and their functioning are discussed as an example of the automated enforcement and execution of contextual rules. Moreover, a common threat to peer-to-peer networks is discussed as well as how peer free riding can be avoided by appropriated incentivizing.

### 4.1.2.1 Distributed Consensus Mechanisms

Distributed consensus is a method for the authentication and validation of information, without the need of any third party or central authority within distributed networks (Olfati-Saber, Fax and Murray, 2007; Seibold and Samman, 2016). Generally, consensus is found through the process of goal revelation and information exchange, that can be loosely categorized under the label negotiation (Ephrati and Rosenschein, 1993; Durfee, 1999). One way to handle negations is to have agents that converge to a single choice in a so-called negotiation set, which is the group of all agreements that exhibit the properties of positive utility for all agents. This implies Pareto optimality (Ephrati and Rosenschein, 1993). Distributed consensus can, consequently, be defined as follows (Olfati-Saber, Fax and Murray, 2007):
Definition 5 (Distributed Consensus): Distributed consensus is a method to reach an agreement regarding a certain quantity of interests, depending on the state of all agents.

When referring to distributed ledgers, consensus must be found about the information that needs to be validated and that is, subsequently, incorporated into the ledger. This problem is technically solved, by the ability of each player to read the actual state of the ledger, i.e. the information that is already incorporated. In order to validate information, thereby achieving a consistent state of the ledger across all nodes, consensus must be found, despite the possibility that some players may deviate from the pre-specified rules in the distributed ledger (Kroll, Davey and Felten, 2013). To achieve this, distributed consensus algorithms are employed that are defined as follows (Olfati-Saber, Fax and Murray, 2007):

Definition 6 (Consensus Algorithm): The consensus algorithm or mechanism contains all interaction rules (general and contextual) that specify the information exchange between a node and all his neighbors in a network, the validity of information, and the rights of network nodes.

Whereas in theory, reaching distributed consensus through consensus algorithms may seems straightforward, this only holds, if related processes and the network are completely reliable, i.e. processes and networks must handle malfunctioning components that may give conflicting information to different parts of a network (Lamport, Shostak and Pease, 1982). In practice, however, processes and networks may be subject to a number of faults, such as process crashes, network partitioning as well as lost, distorted or duplicated messages (Fischer, Lynch and Paterson, 1985). For instance, one classical problem and disruptive type of failure, typically occurring within distributed networks, is the so-called Bytazzines failure (Fischer, 1983; Tannenbaum and Van Steen, 2002). In particular, if a Byzantines failure occur, messages may be send, when they are not supposed to, conflicting claims may occur to other processes, and processes may act dead for a while and then revive itself (Fischer, 1983).

Digression: Byzantine Generals Problem

The Byzantine Generals Problem is the abstract expression for problems coping with a special type of behavior within distributed networks, where nodes may send conflicting information to different nodes (Lamport, Shostak and Pease, 1982). This computing problem can be illustrated by using a thought experiment, in which a group of generals, each commanding a part of a Byzantines army, surround an enemy city. The generals can only communicate via a messenger, but in order to conquer the city, they must agree on a battle plan (Seibold and Samman, 2016). The problem in this scenario consists of
the threat that some of the generals may be traitors that want to prevent loyal generals from reaching agreement. Therefore, the question is how many traitorous generals can the army have and still come to agreement for one battle plan?

Formally, the generals must have an algorithm that guarantees:

I. that all loyal generals decide upon the same plan of action, and
II. that a small number of traitors cannot cause the loyal generals to adopt a bad plan (Lamport, Shostak and Pease, 1982).

Given that \( v(i) \) is the information communicated by the \( i \)th general and each general has a method to combine the values \( v(1), \ldots, v(n) \), then condition i. is fulfilled, if all generals use the same method of combination. For the \( i \)th general the obvious method is to send \( v(i) \) by messenger to each other general. However, condition i. requires that each loyal general receives same values \( v(1), \ldots, v(n) \) and a traitorous general may send different values to different generals. Thus, the possibility that the generals use a value of \( v(i) \), different from the value send by the \( i \)th general - even if the \( i \)th general is loyal – must be introduced (Lamport, Shostak and Pease, 1982).

Moreover, this must not be allowed to happen if condition ii. is to be met (Lamport, Shostak and Pease, 1982). A few traitors cannot be deterred from causing loyal generals to base their decision on intentional deflected values. Thus, in order to meet ii., it must be assumed that if the \( i \)th general is loyal, then the value that he sends must be used by every loyal general as the value of \( v(i) \). Given these specification, the Byzantine Generals Problem can be summarized as follows: A commanding general must send an order to his \( n-1 \) generals such that (a.) All generals obey the same order and (b.), if the commanding general is loyal, every loyal general obeys the order he sends. For this scenario it is possible to develop an algorithm, such that the Bytzantines army is reliable, if at least two-thirds of the generals are loyal (Lamport, Shostak and Pease, 1982; Seibold and Samman, 2016).

Given the knowledge about Byzantines failure and associated node behavior, an important goal of every distributed ledger design is to construct a system that is able to automatically recover from partial failures, i.e. one component fails without seriously affecting the overall performance (Tannenbaum and Van Steen, 2002). Distributed consensus mechanisms are, therefore, not only responsible for the enforcement and execution of rules within the distributed ledger network, but are also responsible for enabling nodes to connect and work together, while tolerating partial failures, which is a feature called partition tolerance (Seibold and Samman, 2016). To this end, various decentralized consensus algorithms can be applied, depending on general network and ledger requirements, such as performance and security as well as further desired features, for
instance, special governance types or the capability to process and store high data capacities. Moreover, the decision for one particular distributed consensus mechanism must be taken in accordance to the decisions made on the network layer. Notably, private ledgers that feature hybrid peer-to-peer networks may require different kinds of consensus mechanisms than public distributed ledgers that rely on pure peer-to-peer networks and, consequently, necessitate different governance modes. Choosing a consensus mechanism for a particular distributed ledger application is, therefore, always a trade-off, determined by the desired characteristics as well as other design decision. For instance, the consensus mechanism Paxos makes certain compromises with respect to protocol failure. However, it never produces inconsistent results (Lamport, 2001; Narayanan et al., 2016). In contrast, the decentralized consensus mechanism proof-of-work works very well in case of node failure, but shows limitations with respect to consensus finality (Bonneau et al., 2015).

Notably, there exist a variety of hitherto known decentralized consensus mechanisms that can be classified according to their applicability, depending on the network layer design decision (Rückeshäuser, 2017b). However, a description of every single distributed consensus mechanism goes too far at this point and will be discussed later. Instead the distributed consensus mechanism of Bitcoin, which is proof-of-work, is exemplarily explained, since it deploys one of the most frequently analyzed mechanism to overcome Byzantines failure and to reach a consistent global view of the Bitcoin distributed ledger across all participating nodes (Narayanan et al., 2016).

**Digression: Bitcoin’s consensus mechanism Proof-of-Work**

The concept of proof-of-work (PoW) was originally proposed by Dwork and Naor (1993) as mechanism to combat junk mails and, more generally, to ration access to services, which would be abuse otherwise (Becker et al., 2013). In Bitcoin, proof-of-work is used to approximate the selection of a random node by selecting nodes in proportions to a resource that, hopefully, nobody can monopolize. In particular, this resource is computer power. Consequently, nodes are allowed to compete with another by using their computing power, which will result in nodes automatically being picked in proportion to that capacity (Narayanan et al., 2016).

Bitcoin achieves consensus by using a hash puzzle. In order to create a block, which contains bitcoin transactions, a node that proposes a block is required to find a number called nonce. Nonces must be chosen by the creator in such a way that, when hashing the block, the hash starts with a certain number of zeros. Notably, this can only be done by randomly trying many different values. Consequently, the probability of finding a block depends on the number of trials (Becker et al., 2013). Trials can be characterized
as Bernoulli trial, which is an experiment with two possible outcomes. The probability of each outcome to occur is fixed between successive trials. In the case of Bitcoin, the two outcomes are (i) the hash falls in the target, and (ii) it does not. Assuming that the hash functions behave like random functions and nodes try infinitely many nonces, however, the Bernoulli trial, which is a discrete probability process, can be approximated by a Poisson process. By this it is assumed that events occur independently at a constant average rate, also known as exponential distribution (Narayanan et al., 2016).

Without going into detail about the concrete functionalities of hashes (since this will be discussed later), the hash puzzle used in Bitcoin must fulfill three properties. First, it must be moderately difficult to compute, which is a factor that basically varies with time. Second, costs for finding a nonce are parameterizable rather than fixed for all times. This property is fulfilled by regular adjustments, meaning that the peer-to-peer network regularly recalculates the target every 2,016 blocks. This translates into an average time of 10 minutes between successive blocks created in the network (Becker et al., 2013; Narayanan et al., 2016). The last and third property of the hash puzzle is that it is trivial to verify that a node has computed the proof-of-work correctly. If the goal of a node that wants to create a block is to find a nonce that makes the block hash fall below a target, then the nonce must be published as a part of the block. Thus, it is trivial for another node to look at the blocks contents, hash them together, and verify that the output is less than the target. Notable, this is an important property for enabling decentralization. If any node can instantly verify that another node done the proof-of-work correctly, no central verifying authority is necessary (Narayanan et al., 2016).

4.1.2.2 Smart Contracts

A legal definition of the term contract states that a contract is an agreement with specific terms between two or more persons or entities, including a promise to do something in return for a valuable benefit known as consideration. Furthermore, a contract must be enforceable by law (Thorpe and Thorpe, 2008). Smart contracts feature the same kind of agreement, but remove the need for legal enforcement and trust in form of human judgment, involved between the contracting parties (Melanie Swan, 2015). Szabo (1997) firstly defined smart contracts as a method to combine protocols with user interfaces to formalize and secure relationships over computer networks. Thereby, it was expected that the hitherto high mental and computational transaction costs could be reduced that are imposed by principals, third parties, or additional applied tools. At the end, the contractual phases of search, negotiation, commitment, performance and adjudication may be collected under the realm of the smart contract (Szabo, 1997).

Nowadays, smart contracts are increasingly realized on the basis of distributed ledgers that can be classified as contextual rules, which are enforced by decentralized consensus
mechanisms. Thereby a contract can encode any set of rules, which can be represented by a programming language (Luu et al., 2016). According to Peters and Panayi (2015), smart contracts residing on distributed ledgers can, consequently, be defined as follows:

Definition 7 (Smart Contract): Smart contracts encode rules of a contract into a computer code, which is replicated across peer-to-peer network participants. Smart contracts are self-enforcing, monitor external inputs from trusted sources, and provide settlement according to the contract’s stipulations.

In particular, smart contracts realized on distributed ledgers can be characterized by the following three properties that are autonomy, self-sufficiency, and decentralism. More precisely, autonomy means that after a contract has been launched and is running, a contract and the initiating persons or entities do not need to be in further contact. Self-sufficiency implies that smart contracts possess the ability to raise funds by providing services and spending them on needed resources, such as processing power or storage. Lastly, smart contracts based on distributed ledgers cannot be executed by a single server, but are self-executed across nodes in the network (Melanie Swan, 2015). Additionally, some smart contracts are permanent, if desired: When Touring-complete programming languages are used, the built-in contract as well as the fact that the computation is executed on every node, allows for infinitive loops, leading to the fact that a contract never terminates (Peters and Panayi, 2015).

Given the flexibility of rules that can be encoded by using appropriate programming languages for smart contracts, various contracts are conceivable. For instance, a contract could execute transfers of money whenever a certain event happens, such as payments of securities in an escrow system. In the Bitcoin network, for instance, a smart contract resides on the blockchain and is identified using an address and a 160-bit identifier. After a transaction is initiated, and the network accepts the transaction, the contract code with the current state of the blockchain and the transaction payloads as inputs are executed and confirmed. Subsequently, the network agrees on the output and, thereby, on the next state of the contract (Luu et al., 2016). Despite smart contracts deployed in Bitcoin, other platforms emerged, such as Ethereum, using Turing-complete programming languages, supporting contracts in which values can persist on the blockchain to be used in multiple invocations (Luu et al., 2016). However, despite the differences concerning the most suitable programming language as well as smart contract properties, recently issues arose concerning the implementation of smart contracts. For instance, Norta (2016) noted that smart contracts that equip the protocol layer on top of blockchains using Turing-complete language might not be suited and lead to false claims. In contrast, a currently missing application layer should be implemented (Norta, 2016). However, despite these implementation issues are important for the concrete application of smart contracts, for a basic description of their functioning this discussion
should not be deepened in the following. Instead a practical example is delivered, on how the smart contracts platform Ethereum implements and uses smart contracts for the automatically enforcement of rules.

**Digression: Smart contracts in Ethereum**

In Ethereum, a smart contract is defined as an autonomous smart agent stored in the blockchain and encoded as a part of a ‘creation’ transaction that includes a contract into the blockchain (Luu *et al.*, 2016). Once implemented, a contract is identified via an address and holds some amount of the cryptocurrency natural to Ethereum, called Ether. Moreover, the smart contract employed in Ethereum possesses an own private storage and is associated with a predefined executable code (Buterin, 2014; Luu *et al.*, 2016). The code of an Ethereum smart contract is in a low-level, stack based byte-code language referred to Ethereum virtual machine code. Users define contracts by using high-level programming languages such as JavaScript-like languages, subsequently compiled to the Ethereum virtual machine code (Luu *et al.*, 2016).

In principal, three basic categories of smart contracts can be realized on Ethereum. The first category is financial applications, providing users with a new way of managing and entering into contracts, which includes the management of sub-currencies, financial derivatives as well as hedging contracts. Ultimately, even some classes of full-scale employment contracts are conceivable on top of Ethereum. The second category are semi-financial applications, where money is involved, but their non-monetary side is also implied, for instance in self-enforcing bounties for solutions to computational problems. Lastly, applications for online voting or decentralized governance are conceivable that are programmed as a smart contract on top of the Ethereum platform (Buterin, 2014).

Despite the economic advantages of smart contracts including the reduction of transaction costs (Szabo, 1997), security threats as well other insecurities exist that must be solved or at least alleviated, when deployed in distributed ledgers. However, so far, the security of smart contracts has not received much attention and only several incidents of malfunctions have been reported, including incidents, where contracts do not execute as expected or values were locked (Luu *et al.*, 2016). Security issues and other threats to smart contracts that must be considered, include among others:

- Code correctness: Reasoning about the correctness of a code before deploying it into a distributed ledger is a necessary task, since there is no way to patch a buggy smart contract without reversing a distributed ledger and associated entries. Therefore, both developers as well as users of smart contracts have to be confi-
dent about the correctness and performance of a smart contract in accordance to its intended use. Moreover, the execution should not entail excessive fees to avoid computational burden or other excessive resource input (Melanie Swan, 2015; Luu et al., 2016).

- Scalability: Smart contract platforms are presently considered as unproven in terms of scalability (Ream, Chu and Schatsky, 2016). In particular, it seems not feasible that transactions and the execution of smart contracts are processed and confirmed by every node, when the number of participants and smart contracts steadily grows (Peters and Panayi, 2015).

- Legal issues: To date the relationship between smart contracts as a new body of regulations and its legal counterpart that are courts or other legal institutions, is unclear. Especially, problems might arise given the divergence between contracts that are based on mere technically and strictly binding codes and traditional contracts that are potentially more flexible and allow for different interpretations (Melanie Swan, 2015; Peters and Panayi, 2015). So far, smart contracts are not legally enforceable, although there have been efforts in this directions. However, several companies work on solutions in order to remove the ambiguity, by accurately reflecting written legal contracts (Peters and Panayi, 2015).

4.1.2.3 Peer-to-Peer-Network Free Riding

In general, distributed ledger performance often depends on the effort of many individuals. In systems that are based on purely voluntary provision of efforts, it is well known that individuals may tend to shirk, resulting in an inefficient level of reliability (Varian, 2004). In fact, this rather general statement also holds true for peer-to-peer networks and systems based on distributed network structures. Despite nodes in peer-to-peer networks are expected to contribute to the network’s performance by sharing their resources in return for using the network and other’s peers resources, in many peer-to-peer networks a considerable portion of peers are reluctant to share resources (Karakaya, Korpeoglu and Ulusoy, 2009). As a result individual nodes may interact with one another with varying degrees of collaboration and competition, resulting in a possible negative impact on the peer-to-peer network’s performance (Feldman and Chuang, 2005). According to Karakaya, Korpeoglu and Ulusoy (2009) as well as Feldman and Chuang (2005) free riding in peer-to-peer networks can, consequently, be defined as follows:

Definition 8 (Free riding): In peer-to-peer networks, free riding is the exploitation of peer-to-peer resources through searching, downloading or using services without the contribution to the network with own resources.
One of the earliest studies analyzing the behavior of nodes within peer-to-peer networks and identifying the problem of free riding originates from Adar and Huberman (2000), analyzing individual node behavior and traffic on the peer-to-peer file sharing network Gnutella (Karakaya, Körpeoğlu and Ulusoy, 2008). In particular, they found that nearly 70% of Gnutella users share no files and nearly 50% of all responses in a network are returned by the top 1% of sharing nodes (Adar and Huberman, 2000). Similar, but more recent studies received comparable results, however, indicating an even higher degree of free riding in peer-to-peer networks. For instance, Hughes, Coulson and Walkerdine (2005) emphasize that 85% of nodes share no files in the Gnutella network, leading to the presumption that free riding in this network is even more evident since 2000 (Hughes, Coulson and Walkerdine, 2005). Handurukande et al. (2006) analyzed other file sharing systems, concluding that free riding might be a phenomenon that exist and is common in the majority of peer-to-peer networks (Handurukande et al., 2006; Karakaya, Körpeoğlu and Ulusoy, 2008).

The consequences of free riding in peer-to-peer networks are well known, impinge the efficiency of network operations and cause several negative side effects. For instance, if free riding occurs regularly, small number of nodes must serve larger number of nodes in the network, which leads to scalability problems, for instance, if many download requests are directed towards a few serving nodes. Moreover, peer-to-peer network free riding may results in increasing ‘client-server-like’ network tendencies, thereby, diminishing the advantages resulting from homogenous peer-to-peer relationships such as fault tolerance (Karakaya, Körpeoğlu and Ulusoy, 2008). The quality and the speed of information provided by the network may also sorrow from peer-to-peer free riding problems as the renewal and presentation of content may decreases in time and speed. Moreover, the quality of the search process may degrade. For example, if a large number of free riding nodes makes queries, a lot of peer-to-peer traffic is generated, which potentially leads to the degradation of peer-to-peer services. Lastly, the underlying available network capacity and resources will be occupied by free-riders, resulting in extra delay and congestion for non peer-to-peer traffic (Karakaya, Körpeoğlu and Ulusoy, 2008).

The observation of frequent appearances of free riding in peer-to-peer networks and the associated consequences led to a rethinking in the realm of system design, which traditionally assumed obedient users. Particularly, obedient users are expected to act in accordance to a pre-specified protocol. However, in response to the free riding problem, researchers turned to a model of rational users, trying to maximize their own utility, thereby, assuming a conflict between individual rationality and social welfare, i.e. overall network performance (Feldman and Chuang, 2005). Thus, in addition to the consensus protocol specifying general as well as contextual rules in the distributed ledger, ad-
ditional mechanisms might be employed in order to prevent individual nodes to exploit the protocol for their own benefit and at the cost of the overall network performance. Consequently, the success of distributed network as well as peer-to-peer network underly-
ing distributed ledger does not only emerge form the obedience of traditional tech-
nical considerations such as performance, robustness and scalability, but are also deter-
mined by economic trade-offs and considerations such as the provision of incentive-
compatibility (Feldman and Chuang, 2005). In this context, researchers proposed vari-
ous mechanisms, with which free riding in peer-to-peer networks can be prevented or, at
least, diminished. Generally, they can be divided into three classes of approaches that
are explained in the following (Lai et al., 2003; Feldman and Chuang, 2005; Feldman et
al., 2006; Karakaya, Körpeoğlu and Ulusoy, 2008).

Reciprocity-Based Approaches

In order to prevent free riding, reciprocity-based approaches expect nodes to monitor
other nodes in the network to assess individual nodes’ contribution levels (Karakaya,
Körpeoğlu and Ulusoy, 2009). Based on this assessment, a node decides how to serve
another node either by using a direct or indirect reciprocity scheme (Feldman and
Chuang, 2005). Direct reciprocity, also called mutual reciprocity, means that node A
makes a decision how to serve user B solely based on its previous interaction experi-
ence with this node, which is a strategy comparable to tit-for-tat, an often used concept
in game theory. Moreover, nodes often keep this history of interaction private and is,
therefore, useful when nodes are interacting repetitive (Lai et al., 2003; Feldman and
Chuang, 2005). Direct reciprocity schemes are suitable for applications with long ses-
sion durations as well as for different flavors of peer-to-peer multicast streaming appli-
cations. For instance, in the first case, direct reciprocity allows for ample opportuni-
ties for reciprocation between pairs of users (Feldman and Chuang, 2005).

In contrast, indirect reciprocity schemes allow peers to consider the overall contribution
of other peers to the network when providing services. Karakaya et al. (2009) proposed
a method, in which each peer monitors his neighbor and the associated contribution to
the network. Depending on the contribution level a node subsequently apply actions to
each neighbor (Karakaya, Körpeoğlu and Ulusoy, 2009). Schemes based on indirect
reciprocity exhibit certain advantages compared to direct reciprocity-based schemes. In
particular, they are more scalable, especially, in large peer-to-peer networks with dy-
namic memberships and infrequent repeat of transactions. This is because the interac-
tion history of a node is shared with others, however, thereby exhibiting the threat of
collusion, i.e. the opportunity that free riding nodes claim that other free riders cooper-
ate with them, subverting the decision of a nodes reputation in a network. Moreover,
while the implementation of private histories in decentralized systems is straightfor-
ward, the implementation of a shared history requires, among others, the implementa-
tion of a peer-to-peer storage system or the dissemination of information to other players similar to routing protocols (Dabek et al., 2001; Lai et al., 2003).

**Reputation-Based Approaches**

Reputation based approaches construct and maintain reputation information about nodes based on feedbacks they receive from other nodes. After a node interacted with other nodes, feedback can be positive or negative or both and is used to build up a good reputation for contributing nodes and a bad reputation of free riding nodes. Nodes with a good reputation get offered better services (Karakaya, Korpeoglu and Ulusoy, 2009). Reputation-based approaches differ from reciprocity-based approach mainly in terms of the computation of reputation or reciprocity scores as well as in regard to the mapping of scores to strategies (Lai et al., 2003).

A peer’s reputation corresponds to its long-term behavior, such that reputation-based approaches necessitate the storage and management of long-term node histories (Karakaya, Korpeoglu and Ulusoy, 2009). However, to some extend the tracking of peer reputation requires a certain degree of centralization in order to realize a reputation system, which implies that reputation-based mechanisms are not suitable for unstructured peer-to-peer networks (Karakaya, Körpeoğlu and Ulusoy, 2008). This especially applies when implementing a global reputation approach, where reputational information about a note is obtained from several nodes and shared with all nodes. This approach typically implies the storage of consolidated reputation information in either a central storage location or with a set of nodes in the network (Karakaya, Korpeoglu and Ulusoy, 2009). Consequently, in the context of distributed ledgers, reputation based approaches for node incentivizing are so far only proposed for permissioned ledgers, where nodes are known and hold real-life reputation (Swanson, 2015). Despite issues concerned with the openness of networks, reputation based systems are often shown to be vulnerable to whitewashing attacks, which are attacks, where free riders repeatedly rejoin the network under new identities or pseudonyms to avoid possible penalties or even exclusion (Feldman et al., 2006). However, global reputation approaches are expected to speed up the identification process of free riders especially if the network is large, such that repeated interactions with same nodes are unlikely (Karakaya, Korpeoglu and Ulusoy, 2009).

**Incentive-Based Approaches**

Incentive-based approaches typically rely on monetary payment schemes in order to prevent the emergence of free riding. Notably, these schemes specify that the service recipients pay the service provider for resources they consume. However, since these services are still very low cost, micro-payment based solutions are typically applied (Karakaya, Korpeoglu and Ulusoy, 2009). Any monetary based scheme must rely on
two key mechanisms that is an accounting module for secure storage and a settlement module for fair exchange. In practice, however, monetary-based solutions do not guarantee totally fair exchange of goods and payment, as dealing with small payments only justifies lightweight security measures. Consequently, while monetary approaches allow for flexible economic mechanisms, they are expected to suffer from impracticability (Feldman and Chuang, 2005; Karakaya, Korpeoglu and Ulusoy, 2009).

**Digression: Incentive compatibility in Bitcoin**

One special type of an incentive-based approach can be found in the distributed payment network Bitcoin, which employs the concept of reward mining and is a build-in incentive that encourages useful behavior, i.e. engagement in mining activities (Böhme et al., 2015). According to Kroll, Davey and Felten (2013) reward mining can be defined as follows:

Definition 9 (**Reward Mining**): Reward mining is the procedure, by which a node, also called miner, adds a special transaction to a prospective block, thereby creating a number of reward bitcoins.

Notably, given reward mining, the proof-of-work protocol employed in the case of Bitcoin is expected to be incentive-compatible and secure against colluding minority groups (Eyal and Sirer, 2014). The amount of bitcoins, which are received by miners, are adjusted to a predetermined schedule, according to which the reward is halved each time 210,000 more blocks have been mined (Kroll, Davey and Felten, 2013). Eventually, the reward received by miner will drop to zero in 2140, leaving the further incentivizing of mining activities unclear (Meiklejohn et al., 2013). However, since mining is expensive to operate, mining activities will probably no longer pay off before rewards drop to zero. This is because a miner only makes profits, if the mining reward is higher than the costs of mining, whereas the mining reward is the block reward plus (currently voluntary) transaction fees. Mining costs consists of hardware costs plus operating costs, which result from electricity usage or the cooling of equipment. However, this simple equation is distorted given three influencing factors: Fixed and variable costs, the block finding rate as well as exchange rate dependency. The first factor refers to the fact that hardware costs are fixed costs that can be calculated beforehand, whereas electricity cost are variable, meaning that they may fluctuate over time and are, therefore, hard to anticipate. Second, rewards that are obtained by miners depends on the block finding rate, which depends on the power of the respective hardware, but also on the ratio of the individual hash rate to the total global hash rate. Lastly, costs incurred by miners are typically denominated by in fiat currency, whereas the reward is denominated in Bitcoin and, thus, the above equation partly depends on the Bitcoin exchange rate.
Given the described drawbacks of the reward mining approach, some scholars already propose further incentivizing possibilities in order to avoid a network collapse, when mining is no longer economically. For example, Böhme et al. (2015) suggested that in the future, all transactions may include a transaction fee that is paid to miners as a kind of bonus. Notably, in 2014 already 97% of the transactions conducted with Bitcoin included a fee, however, so far these fees were below 0.1% of the actual transaction value (Böhme et al., 2015).

Despite pure monetary payment schemes as in the case of Bitcoin, incentive-based approaches can also be based on utility values, for instance, as proposed by Ramaswamy and Liu (2003) or Vishnumurthy, Chandrakumar and Emin (2003). Ramaswamy and Liu proposed the calculation of utility functions for each node in order to assess its usefulness to the network. Subsequently, nodes cannot request a service, if the effort for a service-providing node is higher than the other node’s utility level. Similar, Vishnumurthy, Chandrakumar and Emin (2003), are using a single scalar value to evaluate a node’s utility to a network. However, each of these mechanisms has severe limitations, when applied to peer-to-peer structures due the required accounting infrastructure necessary for rewarding individual nodes (Karakaya, Körpeoğlu and Ulusoy, 2008). Consequently, incentivizing of node behavior in distributed ledger seems to be not feasible using these utility-based approaches, especially, when referring to permissionless networks.

Overall, however, it might be questionable at which point and to which degree such kind of interventional mechanisms, i.e. incentivizing, are necessary. In particular, several works showed that up to a certain degree, networks are able to tolerate free riding. Furthermore, free riding may be even sustainable in an equilibrium and can be part of an social optimum outcome (Krishnan et al., 2002, 2004). Thus, it is necessary to identify the circumstance, in which intervention is necessary in order to avoid the degrading of network performance, a loss of quality of peer-to-per service provision or even a system collapse (Feldman et al., 2006). In order to identify these circumstances, the node’s decision to contribute by exerting a certain level of information must be further examined. Particularly, the effort each node will exert depends on his own benefits and costs, the efforts exerted by other nodes as well as the technology that relates the individual effort to outcomes (Varian, 2004). To calculate the point at which intervention in form on incentivizing is necessary, different methods exist, for example, as proposed by Feldman et al. (2006). Here, the intervention point always depends on the concrete type of system, the characteristics of its participants, participant type distribution, as well as the system benefits and costs (Feldman et al., 2006). However, the decision whether or
not incentivizing is necessary, depends on the concrete application of a distributed ledger and the design of the underlying peer-to-peer network.

### 4.1.3 Representation Layer

The third layer of the distributed ledger architecture is the representation layer, including the decision whether the exchange and subsequent storage of information is tied to monetary values (such as dollars or euros) as well as to other kinds of tokens, or if the information is referenced directly on the distributed ledger. For example, tokens can be coins, such as bitcoins within the Bitcoin cryptocurrency system that are digital representation of assets and can also serve as container. In order to transfer an asset using a container, a transaction of bitcoins can be initiated involving a trivial amount of coins such as 0.00001 bitcoin, whereas attached to this transaction is a share of stocks or similar assets (Evans, 2014; Yermack, 2015). However, generally, tokenization is not an inherent feature of the blockchain. In fact, assets or all kind of monetary values can be directly referenced on the blockchain without using tokens. Though, if tokens are used, the third layer necessitates a second form of consensus, which refers to willingness of participants to agree on the fact that the used tokens have value. Notably, this form of consensus is also necessary for any fiat currency and also hold for the transfer of any kind of information on the distributed ledger (Kroll, Davey and Felten, 2013).

---

**Digression: Consensus that Bitcoins are Valuable**

Consensus that bitcoins have value is not self-evident and depends on the interplay between two particular assumptions. The first assumption is that the blockchain is secure, whereas the second assumption states that the mining ecosystem is healthy. A high and stable value of the bitcoins is, according to Narayanan et al. (2016), only possible if nodes generally trust in the security of the blockchain, meaning that the network could not be overwhelmed by an attacker by acquiring the majority of computer power in the network. A prerequisite for a healthy mining system is that the majority of nodes is honest and follows the underlying protocol. Obviously, these assumptions interlock with the provision of mining rewards and the actions, that might be taken when the maximal quantity of money of coins in Bitcoin is reached (Bonneau *et al.*, 2015; Narayanan *et al.*, 2016).

The emergence of any of these properties is not straightforward, however, media attention is potentially one part of it: As the media coverage increased after the launch of Bitcoin in 2008, more and more individuals became interested in participating on the network and in mining bitcoins. The more people are interested and participate, the more secure the network became, since the difficulty of acquiring the majority of com-
4.1.4 Storage Layer

The top layer of the distributed ledger architecture is the shared and distributed database, where transactional information is stored permanently (Harrison, 2016). According to Özsu and Valduriez (2011), a distributed database can be defined as follows:

Definition 10 (Distributed Database): A distributed database is a collection of multiple interrelated databases, distributed over a computer network.

To maintain a distributed database, there exist a number of autonomous, not necessarily homogenous nodes (e.g. computers may vary with respect to the processor type, memory size, or I/O bandwidth), processing elements that are interconnected by the distributed peer-to-peer network and that cooperate in performing an assigned task. Consequently, on the storage layer, the term distribution refers to information and data, respectively, and must be distinguished from the other modes of distribution, either on the network layer, where distribution refers to the processing elements (nodes) as well as on the procession layer, where distribution refers to control (Özsu and Valduriez, 2011). The physical distribution of information is an important feature of the distributed database and distinguishes it from related databases that reside in the same computer system. Physical distribution, however, does not imply that nodes must be geographically far apart, but communication must be done over a network, which is the only shared resource, instead of communicating through shared memory or shared disks (Tannenbaum and Van Steen, 2002; Özsu and Valduriez, 2011).

Related to the top layer and the distributed database are decisions concerning the characteristics of storage. In particular, storage of information can be done in a chronological order or not. Distributed ledgers that feature a chronological ordering are called blockchain, which consist of single blocks, linked by using hash functions and hash pointers, respectively (Antonopoulos, 2014). A generic definition of hash functions reads as follows (Bakhtiari, Pieprzyk and Safavi-Naini, 1995):

Definition 11 (Hash Function): A hash function is mathematical function that maps a large collection of messages into a small set of message digest and can be used for error detection, by appending the digests to the message (parity bits) during the transmission.

Besides this very general definition, the advent of digital signature schemes as well as public key cryptography led to the increasing prominence of cryptographic hash func-
tions. Cryptographic hash functions are expected to be secure, even if it is not completely clear, what the notion secure means for a cryptographic hash function. However, the notion of security is often tied to digital signature schemes, which is the most important application of cryptographic hash functions (Bakhtiari, Pieprzyk and Safavi-Naini, 1995; Stinson, 2006).

More precisely, according to Tannenbaum and Van Steen (2002), a hash function $H$ takes a message $m$ of arbitrary length as input and produces a bit string $h$ having a fixed length as output:

$$h = H(m).$$

The bit string $h$ is comparable to the extra bits that are added to a message in a communication system, in order to allow for error detection, such as a cyclic-redundancy check (Tannenbaum and Van Steen, 2002). Hash functions used in cryptographic systems have a number of properties, however, perhaps the most important one is that they are one-way functions, meaning that it is computationally infeasible to find the input $m$ that corresponds to a known output $h$ (Tannenbaum and Van Steen, 2002). Moreover, hash functions possess the property of weak collision resistance as well as strong collision resistance. The first means that given an input $m$ and its associated output $h = H(m)$, it is computationally infeasible to find another, different input $m' \neq m$, such that $H(m) = H(m')$. The property of strong collision resistance, means that given only $H$, it is computationally infeasible to find any two different input values $m$ and $m'$, such that $H(m) = H(m')$.

---

**Digression: Bitcoin’s SHA-256 Hash Procedure**

SHA-256 is a particular type of a secure hash algorithm (SHA), which is called SHA-2 that is used in Bitcoin. According to SHA-256, a hash function is built from a deterministic algorithm called block cipher. The underlying block cipher has 64 rounds and thus a 2048-bit expanded internal key (64x32 bits). This key is obtained from the message block to be compressed, which has 512 bits at the input and is expanded four times to form a 2048-bit internal key for the respective block cipher (Courtois, Grajek and Naik, 2014). In particular, the SHA-256 algorithm is at the core of the mining process, since the task of miner is to solve this function as quickly as possible. Actually, Bitcoin requires double computation, since SHA-256 has to be applied twice to a block to get the hash used by the nodes. SHA-256 was the strongest cryptographic hash function at the time of the emergence of Bitcoin, but is now possibly less secure compared to other SHAs, given the development of next generation SHA-3 functions (Narayanan et al., 2016).
A related concept to hash functions is the hash pointer, which is basically a pointer to a location, where some information is stored together with a cryptographic hash of the information at a fixed point in time that allows verifying whether information has been changed. Hash pointers can be used to build various data structures, however, familiar data structures that use hash pointers are linked lists and binary search trees (Narayanan et al., 2016). Using a regular linked list implies that there is a series of blocks, where each block has data and as well as a pointer to the previous block in the list. Contrarily, Figure 13 shows a linked list, where single blocks form a hash chain, meaning that each new block contains the cryptographic hash of its predecessor, thereby, creating backward link that constitute a unique path from the last block to the beginning of the hash chain (Kroll, Davey and Felten, 2013). Notably, this data structure constitutes the blockchain. Each block of the blockchain contains information about both, the value of the previous block as well as the digest of that value, which allows verifying whether data on the block has been modified (Narayanan et al., 2016). Blocks are, consequently, the basic element of a blockchain and consist of two parts that is the body, containing information about the actual transaction, and a header, which contains a sequence number, a timestamp, the cryptographic hash of the previous block, the Merkle root, a nonce and some metadata (Kroll, Davey and Felten, 2013; Antonopoulos, 2014).

![Figure 13. Simplified representation of the hash structure 'linked list'](image)

Similar to the concept of digital signatures or the usage of a peer-to-peer network typology, security features included in the block body are not completely new, which holds, especially, for timestamps. Hence, by applying hash functions for linking individual blocks, the blockchain falls back to a paper of Haber and Stornetta (1991), who identified the need to certify a digital document, when it is created or at least modified by using timestamps. Particularly, they propose a method, where digital documents are linked individually as well as linearly by a server that receives a document, signs the document together with the current time and a pointer to the previous document and, finally, issues a certificate with these information (Haber and Stornetta, 1991; Narayanan et al., 2016). The major efficiency improvement in comparison to Haber and
Stornetta (1991), however, is the idea of, instead of linking documents individually to collect them into blocks.

An alternative data structure that can be generated by using hash pointer is the so-called Merkle tree, which also uses blocks, but links them together into a tree structure. In particular, a Merkle tree arranges data blocks in pairs and the hash of each of these blocks is stored in a parent node. Parent nodes are in turn grouped into pairs and their hash value is stored one level up the tree as shown in Figure 14. This pattern continues until the root node is reached. Similar to the linked list, using hash pointer allows to traverse to any point in the tree. The rationale to use Merkle trees is that the data structure reduces the amount of checking that is needed to verify a particular document, which appears at a particular point in time (Narayanan et al., 2016). Generally, distributed ledger can either utilize linked lists to store information or can apply Merkle trees. In some cases, however, both hash structures can be combined, which can be exemplarily observed in the case of the Bitcoin blockchain.

![Figure 14. Simplified representation of the hash structure ‘Merkle tree’](image)

**Digression: The Bitcoin Blockchain**

The Bitcoin blockchain contains two different hash structures, whereas the first is a hash chain of blocks that links different blocks to one another and where blocks are rooted in Bitcoin’s genesis block (first block of the Bitcoin blockchain, whose hash is hardcoded in the software). The second hash structure is internal to each block and is a Merkle tree of transactions in the respective block. To prove that a transaction is included in a specific block, a path through the Merkle tree, whose length is logarithmic in the number of transactions in the block, is provided (Barber et al., 2012; Narayanan et al.,
The combination of both structures to the Bitcoin blockchain is illustrated, according to Narayanan et al. (2016), in Figure 15.

Figure 15. Simplified representation of the blockchain

Associated with the decision to use a particular hash structure is the decision for certain storage characteristics, meaning that data stored on the distributed ledger can potentially be changed ex post or not, i.e. data on the distributed ledger are immutable. Linked lists and Merkle trees are expected to provide a sufficient degree of immutability of stored information. For instance, give the structure of the blockchain, an adversary that wants to change any block without being detected, must change the hash pointers of all blocks up to the block he actually wants to change. In an extreme case, an adversary must tamper with all hash pointers up to the end of a hash chain, which is, in the case of the Bitcoin blockchain, the genesis block (Narayanan et al., 2016). The effort, which is needed to change hash chains or Merkle-trees can be enormous, depending on the mechanism applied to include and store information on the hash structure. In particular, the more difficult and expensive it is to change hash chains or the equivalent in Merkle trees, i.e. Merkle-roots, the more likely it is that data cannot be changed once incorporate in the respective hash structure. However, in the case of a distributed ledger, difficulty to change data depends on the particular distributed consensus mechanism, which is applied. Thus immutability of data cannot be assumed without looking at a concrete application case of distributed ledger and all associated ledger design decisions, including the choice of a particular distributed consensus mechanism.
Digression: Immutability of data on the Bitcoin blockchain

Bitcoin blockchains are expected to provide immutable data storage through the interplay of linking blocks by hash functions and hash pointers as well as by applying the distributed consensus mechanism proof-of-work. This assumption is based on the fact that the proof-of-work mechanism implies that an entity that wants to change data, has to afford the majority of computer power in the network (51% attack). More precisely, the malicious entity would have to create a new transaction that conflicts with the original transaction and include it into a block. The malicious entity would subsequently continue to create blocks on top of this block, until this new chain overtakes the original blockchain, i.e. is the longest chain (Decker and Wattenhofer, 2013). However, the assumption that it is hard acquire the majority of network power is threatened by so called mining pools or professional mining centers, which already achieved the majority of power in the past. For instance, the mining pool GHash.IO, was able to acquire the majority of computer power in the Bitcoin network in June 2014. Whilst, today, mining power is less concentrated, the possibility that a mining pool or mining center is able to reach the majority of network power is still a concern in the Bitcoin community (Narayanan et al., 2016).

4.1.5 Overview: Layer and Design Decisions for Accounting Applications

The previous chapter emphasizes the different and partially interrelated system design decisions, which exist within the context of any distributed ledger. However, when designing a distributed ledger for a special use case, the system design decisions must be made, while taking into consideration not only computer system goals, but also further objective such as corporate goals or existing digital infrastructures, to which the distributed ledger is applied simultaneously. Table 18 summarizes the general distributed ledger functionalities in relation to the respective layers as well as the associated design decisions. Especially, the table shows, how design decisions and, in particular, the decisions towards network access and openness, determines subsequent design decisions.

The first decision, which needs to be considered, is access to the network, which is linked to the decision to deploy either a permissionless or permissioned distributed ledger. Notably, this first decision lays the foundation for a range of subsequent decisions and limits, for instance, the ability to read data on the distributed ledger only to actual network participants. In the case of accounting, so far, existing literature proposed permissioned ledgers, owing to the sensible nature of financial data of firms (e.g. Yermack, 2015; Andersen, 2016, and Rückeshäuser, 2017b). Consequently, a permissioned network approach is also proposed in the course of this thesis. Notably, this re-
stricts ledger design to particular design choices and implies, for instance, restricted rights for reading and creating ledger entries. However, these trade-offs equally apply, if a permissionless peer-to-peer network would be chosen as foundation for a distributed ledger based accounting system. In particular, permissionless ledgers imply partition-resistance and the absence of a single point of failure as well as the, hereby, induced resilience towards the entering and leaving of nodes on the system. However, this comes at the cost of the performance of search mechanisms, their scalability and generates large loads on network participants (Lv et al., 2002). In contrast, the permissioned network, which is chosen as foundation for a distributed ledger based accounting system provides better scalability, while being prone to a single point of failure.

<table>
<thead>
<tr>
<th>Layer &amp; Functionalities</th>
<th>Distributed Ledger Design Decisions</th>
<th>Distributed Ledger Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Distributed Ledger Layers</strong></td>
<td><strong>Ledger Functionalities</strong></td>
<td><strong>Permissionless</strong></td>
</tr>
<tr>
<td>Network Layer</td>
<td>Access</td>
<td>Unrestricted</td>
</tr>
<tr>
<td></td>
<td>Read-Function</td>
<td>Unrestricted</td>
</tr>
<tr>
<td></td>
<td>Characteristics</td>
<td>(+) Partition resistance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-) Scalability limited</td>
</tr>
<tr>
<td>Consensus Layer</td>
<td>Create-Function</td>
<td>Unrestricted</td>
</tr>
<tr>
<td></td>
<td>Information Integration</td>
<td>Distributed consensus mechanism choice - restricted</td>
</tr>
<tr>
<td>Representation Layer</td>
<td>Tokenization / No Tokenization</td>
<td>Applicable</td>
</tr>
<tr>
<td></td>
<td>Delete-Function</td>
<td>(Im)mutable</td>
</tr>
</tbody>
</table>

Table 18. Overview of Distributed Ledger Layer and Design Decisions

On the second layer, a particular consensus mechanism must be found that supports the integration of information into the ledger. Moreover, distributed consensus mechanism must be found that respect the features of the underlying network. Thus, not all consensus mechanism allow for completely decentralized consensus finding without showing centralization tendencies and vice versa. Consequently, the previously made decisions also partly restrict the choice of a consensus mechanism. Simultaneously, this implies
that the ability of nodes to create information that are subsequently incorporate into the distributed ledger is restricted by the decision concerning network access.

The third decision determines how information is referenced on the blockchain. However, this is only of minor importance, as it does not restrict or affects subsequent design decision-making. Eventually, on the storage layer data on the distributed ledger are either mutable or immutable. In particular, permissionless distributed ledgers are typically expected to feature immutable data storage, whereas permissioned ledgers are rather expected to feature mutability. However, as already mentioned, the ability to feature immutability depends heavily on the chosen distributed consensus mechanisms, so that, theoretically, the two ledger types can be designed to feature both, mutable as well as immutable storage. In the case of accounting, the feature of immutability is clearly preferable in order to prevent ex post data manipulations in addition to the prevention of internal override of controls. However, ultimately whether or not the feature immutability is feasible, will only be elucidated, when a concrete scenario and associated design decisions are developed and assessed.

4.2 Interim Conclusion

The present chapter presents a four-layer architecture of distributed ledgers and describes the functionalities as well as design decisions on the respective layers. To exemplify the partially abstract concepts, the functioning of Bitcoin is sometimes used for illustration. In the context of this chapter, basic definitions are derived that build the foundation for the subsequent discussion. The last part of this chapter emphasized the interconnectedness of particular design decisions starting with the lowest layer. In particular, a commonly required design feature of distributed ledgers that are applied in the context of accounting is a permissioned network access. This approach is followed in this thesis, taking into account that financial data of corporations are sensitive data and typically not public, unless an official report is disclosed. Moreover, immutability of ledger entries would be a desired feature of a distributed ledger based accounting system, which could prevent ex post data manipulation, additionally to the prevention of management override of internal controls. However, whether immutability is technically feasible is mainly determined by design decisions on the procession layer, which necessitates a concrete scenario. The provided layer architecture, therefore, delivers a starting point for the design of concrete applications of distributed ledgers in accounting, as it strengthens the focus on each component the technology.

However, despite the fact that rather superficial assumptions about favorable ledger designs can be made at this point, it gets obvious that distributed ledger potentially provide significant improvements with regard to the deterrence of management override of
control, which results from decentralization and the associated mechanisms of distributed consensus as well as transparency. In particular, the ability to restrict the possibilities of single entities to read and create ledger entries in a permissioned ledger implies that a management is possibly not able to acquire insights and influence on ledger entries. Thereby, direct interference on a ledger through the management is prevented. Moreover, given decentralization and the inclusion of multiple parties in the consensus process, several parties are directly involved in the consensus process and do not merely act as supervising entity, e.g. as in the case of the internal control system and associated entities as described in the previous chapter. Thereby, the responsibility for the correctness of transaction within an accounting information system for entities participating in the consensus process is increased. Potentially, the excessive influence of the management on internal control entities can ultimately be reduced through an appropriate distributed ledger protocol design.

4.3 Paradigm Changes in Management Factors

The description of the technical architecture, the design decisions and resulting characteristics of distributed ledgers indicated that technological and, thus, also organizational as well as social paradigm changes arise from distributed ledger use that necessitates adjustments of organizational structures and business processes (Rückeshäuser, 2017a). However, as already mentioned, the concrete design of ledgers may varies according to the application and purpose of the implementation that also affects the kind and significance of paradigm changes. Thus, first, general alignment strategies must be discussed that adjust business processes and distributed ledgers. Based on these strategies, the significance of paradigm changes and the associated consequences for corporations that want to apply distributed ledgers for accounting purposes can be assessed (Rückeshäuser, 2017a).

4.3.1 Strategic Alignment Options

The alignment of information technology and businesses strategy, denoted by the term strategic alignment, is an enduring challenge for businesses worldwide, which determines how and to which degree business value through IT is generated (Rao, Angelov and Nov, 2006; Tallon, 2008). The occurrence of innovative technologies, however, poses a challenge to alignment since, typically, disruptive innovation occurs intermittently, such that companies have barely any routine processes for handling them (Christensen and Overdorf, 2000). Consequently, if companies want to exploit the technological features offered by distributed ledgers, they must find a strategy, how to adjust their processes to deal with paradigm change and to seek new forms of competitive advantage (Christensen and Overdorf, 2000; Lucas and Goh, 2009). Thus, in the follow-
ing, three distinct alignment strategies that are based on the previously described architecture are presented and the expected impacts on operational and management processes will be discussed (Mooney, Gurbaxani and Kraemer, 1996).

4.3.1.1 Alignment Strategy 1: Distributed Ledger as Digital Infrastructure

The first strategy to align distributed ledger technology with business processes is the use of distributed ledgers as digital infrastructure that underlies a particular or several business activities (e.g. accounting, purchase or supply chain management). Thereby, the distributed ledger can be defined as a basic information technology and organizational structure, along with the related services and facilities necessary for an enterprise function (Tilson, Lyytinen and Sørensen, 2010). The use of a distributed ledger as digital infrastructure requires a closed network approach as indicated in Figure 16, meaning that the participants of the peer-to-peer network are entities of a single firm that can be, among others, individual employees or departments. More precisely, only entities within the firm have the right to read information that is stored on the distributed ledger as well as the right to propose and validate information that should be included. The choice of an appropriate distributed consensus mechanism is determined by network and consensus design decisions. For instance, not all distributed ledger mechanisms allow validation in a permissioned network, while simultaneously providing centralized or decentralized validation or hybrid forms (Rückeshäuser, 2017b). Assuming that a corporation wants to employ pure decentralized consensus finding, for instance, only particular consensus mechanisms are applicable, i.e. Proof-of-Work, or the Proof-of-Work based derivatives such as Proof-of-Stake or Delegated Proof-of-Stake, whereas the latter are mechanisms that build on the network node’s capabilities to acquire stakes in the system. Based on this choice, storage is either chronologically or not, whereas in Figure 16 a chronological order is indicated by depicting a blockchain, assuming that chronological ordering of information is of benefit in accounting.

More important than the actual design choices, however, is the question, which and how the use of distributed ledgers affects business processes depending on the chosen alignment strategy. To this end, a differentiation between operational and management processes is provided, based on Mooney, Gurbaxani and Kraemer (1996). It is assumed that operational processes are primary concerned with business operations, while management processes focus on associated information handling, coordination and control processes that are required to ensure the efficiency and effectiveness of the primary business operations (Mooney, Gurbaxani and Kraemer, 1996). To identify the impact of distributed ledger technology on these processes, a closer look on the interaction patterns of entities within a company must be placed, that are related to business activities and, thereby, affect business processes (Aguilar-Savén, 2004). Particularly, the interac-
tions between two entities within a company (company A) will be described, indicated by entity 1 (E1) and entity 2 (E2). Apparently, E1 and E2 are both part of the peer-to-peer network consisting of company-affiliated nodes. E1 and E2 communicate directly with each other over the network. It is assumed that E1 and E2 are eligible to validation information flooded through the network and that they can retrieve information directly from the ledger. Consequently, this type of interaction is, in the following, denoted as direct communication and coordination through the ledger, owing to the fact that the ledger is maintained by the company-affiliated nodes activities and that the network simultaneously delivers information to all participating nodes.

Figure 16. Alignment strategy 1: Distributed ledger as digital infrastructure

Given the direct interaction and coordination of E1 and E2 through the ledger, an impact on management processes is expected. In particular, given the decentralized approach, hierarchical decision-making is unnecessary and substituted through decentralized consensus finding, which renders communication and coordination processes significantly. To this end, information must also be transparent, leading to a divergent approach concerning the protection objective confidentiality and thereby confidential information handling that is typically pursued in contemporary corporate database solutions (Müller, Eymann and Kreutzer, 2003). An accounting information system based on a distributed ledger would consequently not only require that consensus over the validity of a transaction is taken in real-time, but also that all transactional information must be transparent to the consensus participants (Yermack, 2015; Rückeshäuser, 2017b). Additionally, operational processes will probably be affected. Mooney, Gurbaxani and Kraemer (1996) define operational processes as marketing and intelligence processes as well as design and development, procurement, logistics, production and product or service delivery processes. Generally, information technology is expected to affect operational processes through automation as well as by enhancement of their effectiveness and reli-
ability by linking them together (Mooney, Gurbaxani and Kraemer, 1996). Accordingly, smart contracts and consensus rules in general, imply automation of rule enforcement specified in the protocol, such that it can be assumed that distributed ledger have an impact on operational processes through business process automation. Thus it can be expected that transaction settlement and storage are no longer separated processes that potentially must be initiated separately, but are executed automatically through a consensus mechanism executed by the network. Given the overarching effects on organizational as well as management processes, overall, the change implied by distributed ledgers and the associated strategy to use the technology as digital infrastructure, can be described as organizational transformation, which is defined as an intangible organizational investment in business process and organizational restructuring that potentially leads to complementary innovation or efficiency increases in intangible aspects of products or services, such as quality, time, convenience or variety (Brynjolfsson and Hitt, 2000). Consequently, using distributed ledgers implies entrepreneurial rethinking as it challenges hierarchical forms of decision-making as well as common organizational structures and processes (Rückeshäuser, 2017a).

4.3.1.2 Alignment Strategy 2: Distributed Ledger as Shared Platform

The second strategy to align distributed ledgers and business processes consists of employing the strategy of using distributed ledgers as shared platform that is deployed by two or more companies, whereas the first case is depicted in Figure 17. The design choices are similar as in the first alignment strategy, i.e. a closed network approach is chosen, whereas the network can be extended to several companies. Again, the decision for a consensus mechanism and general rules concerning nodes’ ability to participate in the validation process is determined by the concrete application scenario as well as further design decisions, such that no concrete prediction about these design features can be made at this point. The same holds for the features of automated chronologically ordering and immutability. However, given the fact that immutability only holds if 51% of the network behaves according to the protocol rules (Becker et al., 2013), the probability that entries on the ledger are altered after they are included on the shared databases decreases if the platform is shared. The reasons therefore are two-folded: First, it might be the case that two firms build a greater network than one firm, such that the alteration of ledger entries, e.g. through the acquisition of the majority of network capacity in the case of Proof-of-Work is harder than in the case of alignment strategy 1, which probably implies a smaller network. However, this must not necessarily hold, if the firm that deploys a distributed ledger as digital infrastructure is sufficiently large. The second reason, why the probability of immutability of ledger entries is probably higher in the platform solution, however, is that, potentially the two different firms have divergent interests and, therefore, control each other more intensively (Andersen, 2016).
Nevertheless, this must not necessarily be the case as indicated by (Rückeshäuser, 2017b).

Despite considerations concerning design decisions and ledger features, the interaction of entities within and between firms is, again, used as an indicator for the changes induced through distributed ledger technology and their effect on business processes. E1 and E2 are again used as exemplary entities, e.g. individuals or departments within one company (company A). Entity 3 (E3) is an entity of a different firm (company B) that is part of the peer-to-peer network and thereby maintains the distributed ledger together with the entities of company A. As depicted in the Figure 17, deploying a shared platform necessitates not all entities to be part of the underlying network, whereas non-participating nodes (E1) can still use the information stored on the distributed ledger. Thus, in the following the interaction pattern of E1 is denoted as interaction with the ledger, owing to the fact that E1 can retrieve information from the ledger that is shared by the two companies, but can neither propose nor validate information for the incorporation into the ledger. Consequently, management processes that relate to information, knowledge, control or communication are not affected with respect to the interaction patterns identified for E1, since the entity retrieves information comparable to the retrieval of information from a central database and is not involved in consensus finding. Contrarily, interaction patterns of E2 and E3 can be characterized comparable to the interaction of E1 and E2 in the first setting (alignment strategy 1), where entities communicate and coordinate actions through the ledger and over the peer-to-peer network that is dispersed over the two companies. Consequently, management processes are affected. Overall, alignment strategy 2 implies a partial impact on management processes, but probably not to the extent, which can be observed if the distributed ledger is applied as digital infrastructure (Rückeshäuser, 2017a).

More likely, the ledger used as a shared platform affects operational processes. As an
example, again the usage of distributed ledgers as foundational technology in accounting can be assumed, whereas the ledger is now organized as a platform, in which transactional information is stored transparently for all network participants and for those who are eligible to read information on the ledger. The impact on the organizational process for E2 and E3 are comparable to the first setting, and manifest itself by the automation of processes, whereas the only difference is that the efforts for the validation process of information may a collaboration of nodes of company A and the collaborating company B. With respect to E1, organizational processes are only partially and probably only little affected. However, it can be assumed, if E1 is excluded from the network that is responsible for a particular business activity, E1 might not be important to the execution of a particular business activity and, therefore, negligible. Summarizing, the strategy used to handle change implied by the application of distributed ledgers as shared platform can be characterized by organizational process restructuring, given the fact that management processes are only partially affected and changes predominantly affect management processes through altered interaction patterns.

4.3.1.3 Alignment Strategy 3: Distributed Ledgers as External Application

The last strategy that firms may employ dealing with distributed ledgers consists in exploiting the features offered by the technology through the use of an external application that is based on a distributed ledger and offered through another, trusted company. Thus, a company that wants to benefit from decentralized storage, transparency and potential immutability of distributed ledgers, does neither maintain nor participate on the peer-to-peer network. As illustrated in Figure 18, thus, E1 and E2, which can be both, single entities or different departments of company A, are not part of the network. Consequently, company A does not need to decide for any distributed ledger design decisions that are only made by company B, which maintains the ledger. An example for the use of a distributed ledger as an external application is the use of a distributed ledger as a mere storage capacity, where the technology as such is treated as a ‘black box’ by company A. Thereby, company A can expected that data stored on the ledger are immutable, at least for the company affiliated entities E1 and E2 that are not part of the network. Notably, this presuppose that company A trusts nodes of company B, meaning that nodes in the peer-to-peer network are not expected to change information stored on behalf of company A. The rational for company A to use the service offered by company B is that the company might want to benefit from the features implied by distributed ledgers, but does not want to invest and pay for organizational restructuring, which mainly result from adjustment as well as learning processes.

The resulting interaction patterns of E1 and E2 can, consequently, be described as interaction with the distributed ledger, since information can be retrieved, given their right to
read information on the ledger, but nodes of company A can neither propose nor validate information that should be incorporated. Thus, information retrieval is comparable of having a trusted third party that is responsible for the security of information shared on an off-premise storage location. As a result, it is expected that management processes are not affected by the use of the distributed ledgers as external application. Moreover, it is expected that operational processes are not affected as well, as E1 and E2 are not involved in decentralized consensus processes, meaning that basic operational processes and business activities will not change. Therefore, it can be assumed, that paradigm changes is not present or only minor, if distributed ledgers are used as an external application maintained and managed by another company. Consequently, one can classify the third alignment strategy as information management outsourcing strategy, whereas only increased security features are exploited by company A that expects the stored information to be immutable, at least from its own viewpoint.

Figure 18. Alignment Strategy 3 – Distributed ledgers as external application

4.3.2 Paradigm Changes and Relation to Alignment Strategies

In the following, technological, organizational and social paradigms changes will be discussed that are implied by distributed ledger usage as well as how the proposed alignment strategies mitigate those changes. In particular, it is expected that depending on the strategy, paradigm changes will manifest itself with different significance. Thereby, paradigm changes are defined as changes that necessitate considerable efforts regarding change management, which is the process of passing from old ways of doing business to new ways (Issa-Salwe et al., 2010). Table 19 provides an overview over the paradigm changes that will be discussed in the following.
## Paradigm Changes Implied by Distributed Ledger Technology

<table>
<thead>
<tr>
<th>Distributed Ledger Feature</th>
<th>Common Paradigm</th>
<th>Paradigm Change</th>
<th>Characteristic of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Ledger Copies</td>
<td>Resilience</td>
<td>Data Redundancy</td>
<td>Technological</td>
</tr>
<tr>
<td>Peer-to-Peer Network Connectivity</td>
<td>Availability &amp; Partition Resistance</td>
<td>CAP Goals Maximization</td>
<td>Technological</td>
</tr>
<tr>
<td>Read-Function</td>
<td>Confidentiality</td>
<td>Information Transparency</td>
<td>Technological</td>
</tr>
<tr>
<td>Consensus Protocol/Rules</td>
<td>Discretionary Decision Making</td>
<td>Process Integrity</td>
<td>Organizational</td>
</tr>
<tr>
<td>Digital Signature Schemes</td>
<td>Authentication</td>
<td>(Pseudo-) Anonymity</td>
<td>Technological/Social</td>
</tr>
</tbody>
</table>

Table 19. Paradigm Changes Implied by Distributed Ledger Technology

### 4.3.2.1 Resilience versus Redundancy

Resilience can be defined as the ability of a system to withstand major disruptions within acceptable degradation parameters and to recover within acceptable time and composite costs and risks (Haimes, 2009). In the context of databases and data management, resilience can be defined as a core component of high availability of data, which implies the protection of companies from lost revenue, when access to data resources is disrupted, for instance, due to unplanned outages or in the event of a disaster (IBM, 2017).

Methods to obtain resilience in database systems are manifold and include for example replication, the usage of switchable devices or cross-side mirroring. One possible approach for receiving node failure resilience through replication is, among others, data centric storage as proposed by Ratnasamy et al. (2002, 2003). Data centric storage implies that data of a particular type are stored at one of several replica nodes in a distributed network, and storage of control and summary information pertain to this type at geographically distributed monitor nodes in the network (Ghose, Grossklags and Chuang, 2003). In contrast, resilience of data on distributed ledgers is achieved by the inherent data structure, meaning that every participating node in the network stores a copy of the entire ledger on his or her computer, secured through the respective decentralized consensus mechanism (Morabito, 2017). While this holds true for the usage of distributed ledgers as mere digital infrastructure, the development of distributed application based on distributed ledger technology often implies database-replication protocols and particularly, classical state-machine replication protocols as, for instance, in the
case of the smart contract platform Ethereum (Vukolic, 2016). However, staying with the application of distributed ledger technology as digital infrastructure, resilience against network attacks and data loss is enabled by copies of the distributed ledger on nodes, whereas at the same time, this approach induces costs, due to efforts associated with the avoidance of data inconsistencies, and limitations regarding storage capacity.

Efficient data management solutions imply awareness about the amount of redundant data in diverse data sets and locations and assess whether saving space can be used more sensibly (Policroniades and Pratt, 2004). To this end, data cleansing or scrubbing techniques are typically applied in order to avoid data quality problems due to, for example, the existence of sheer data volumes as well as limitations of storage capacity and excessive costs (Rahm and Do, 2000). Three different methods are typically used to eliminate redundant files that are whole file content hashing, fixed size blocking, and chunking strategies that use Rabin fingerprints to delimit content-defined portions of data (Policroniades and Pratt, 2004). Whereas these methods might be possibly applied using state-machine replication protocol, replication of data cannot be avoided if distributed ledger is used as infrastructure, owing to the fact that replication is necessary for data validation.

Given the apparent inevitability of data redundancies using distributed ledgers, some proposals suggest to change or supplement existing hash structures. Enigma, for instance, is a decentralized computation platform, which uses secure multi-party computation, guaranteed by a verifiable secret sharing scheme, while storage is provided by applying distributed hash-tables for holding secret-shared data. An external blockchain is simultaneously used as a controller of the network that manages access controls, identities and servers as a tamper-proof log of events. The off-chain distributed hash-table is accessible through the blockchain, which stores references to the data but not the data themselves. Thus, private data must be encrypted on the client-side before stored on the distributed ledger. Since data is thereby not replicated on every node, redundancies are decreased compared to original distributed ledgers and blockchain solutions, which enables more demanding computing (Zyskind, Nathan and Pentland, 2015).

Given these considerations, corporations need to be aware of the trade-off resulting from the data redundancy and resilience in accounting systems. The implied redundancy of data may be costly due to the needed storage capacity and storage limitations may occur. Obviously, the distributed ledger back-up system is thereby the clear opposite of the attempt to cleanse corporate databases. However, it is worth mentioning that data redundancy can also be useful, for example, to exploit data duplications in order to optimize the use of storage space and bandwidth. Moreover, file systems may obtain improved caching performance if they are aware of contents shared between files, thereby provide better hit ratios for a given cache size (Policroniades and Pratt, 2004). Eventual-
ly, replication can be used to increase the durability and availability of data as well as to enable fault tolerance and low latencies for distributed clients using a distributed ledger (Bermbach and Kuhlenkamp, 2013).

### 4.3.2.2 CAP Goals Maximization versus Trade-Off

The fact that multiple redundant copies of the distributed ledger reside on participating nodes implies not only redundancy, but also and at least in theory, consistency. Consistency means that all replicas of the ledger are identical and that the ordering guarantees of the specific consistency model are not violated (Bermbach and Kuhlenkamp, 2013). Applied distributed ledger applications such as Bitcoin, however, typically imply only eventual consistency (Decker, Seidel and Wattenhofer, 2016). Eventual consistency informally provides the guarantee that, if no additional updates are made to a given data item, all reads to that item will eventually return the same value. Thus, at no given time, the user can rule out the possibility that inconsistent behavior is observed, meaning that the system can return any data and still be consistent, as it might converge at a later point, which must be ensured by conflict resolution and reconciliation (Anderson, Lehnardt and Slater, 2009; Bailis and Ghodsi, 2013). More formally, eventual consistency can be defined according to Anderson, Lehnardt and Slater (2009) by the following conditions that must hold all times at any node $n$ with a replica of $x$.

**Definition 12 (Weak Consistency):** A replicated object $x$ is eventual consistent if all replicas have the same initial state. There is, furthermore, a prefix of the schedule $S_n^x$ that contains the same operations and is state equivalent to a prefix of the schedule $S_{n'}^x$ of any other node $n'$ holding a replica of $x$, whereas the schedule describes the sequence of update operations that node $n$ performs on this replica of object $x$. This prefix is called committed prefix of $S_n^x$. The committed prefix then (i.) grows monotonically over time, (ii.) must assure that for every operations $w_i$ or $w_j$ eventually appears in the committed prefix of $S_n^x$ but not both, and (iii.) an operation of the form $w_i$ in the committed prefix satisfies all its preconditions.

As already mentioned, an example of eventual consistency is Bitcoin and the associated block confirmation time, which accounts for approximately 10 minutes until a transaction is confirmed. Thus, eventual the Bitcoin network has a consistent view of all transactions, but one can never be sure, and it may always happen that a blockchain fork will destroy a substantial amount of transactions, sometimes even multiple hours later (Decker, Seidel and Wattenhofer, 2016). The fact that Proof-of-Work consensus remains eventual is also referred to as the absence of consensus finality (Vulkolic, 2016). Based on this observation, attempts have been conducted to introduce strong consistency in the distributed ledger systems to enable stronger safety guarantees and faster con-
firmation, which is certainly one of the major problems, when implementing eventual consistency (Bailis and Ghodsi, 2013; Decker, Seidel and Wattenhofer, 2016). According to Kemme et al. (2013) strong consistency can be informally defined as follows:

**Definition 13 (Strong Consistency):** Strong consistency implies that shared states behave like on a centralized system, and programs or users cannot observe any anomalies caused by concurrent execution, distribution or failures.

Achieving strong consistency, however, may be especially challenging when referring to distributed ledgers, since typically applied agreement protocols seem not to work in peer-to-peer environments. This is because of the openness of the network, especially, when considering the Bitcoin payment network as well as the possibility of Sybil attacks as well as Churn attacks (Decker, Seidel and Wattenhofer, 2016). Despite that, introducing strong consistency always comes at costs and, thus, its introduction must be weighted in the context of the CAP theorem (Vogels, 2008; Brewer, 2012). In particular, the CAP theorem states that given three desired properties of shared data systems, namely data consistency, system availability and tolerance of the network for partition, only two can be achieved at any given time. Thus, making consistency a high property means that under certain conditions the system will not be available, whereas relaxing the requirement of strong consistency means that the system will probably remain highly available under the partition-able conditions (Vogels, 2008; Bailis and Ghodsi, 2013; Kemme et al., 2013). Moreover, scaling distributed databases typically requires idioms, i.e. among others replications and partitioning, for which strongly consistent protocols, such as 2-Phase Commit, are expensive and hard to scale (Kemme et al., 2013).

Generally, availability is a common protection objective in distributed systems (Müller, Eymann and Kreutzer, 2003) and can be defined according to Gilbert and Lynch (2012) as follows:

**Definition 13 (Availability):** Availability means that each request eventually receives a response, whereas a fast response is better than slow response.

Thereby the desired property of availability is a classical liveness property that states that ‘eventually something good happens’. However, this property says nothing about the state at any instant time, but requires that if an execution continuous long enough, something desirable will happen (Gilbert and Lynch, 2012). Distributed ledgers also provide availability. In particular, each node receives an answer about its success or failure, since the network accepts new transactions at any time (Bitfury and Garzik, 2015). Consequently, distributed ledgers are initially designed to support eventual consistency, while guaranteeing high availability and partition resistance. However, as shown above different weightings of the distributed ledger properties are conceivable, however, require a careful trade-off between benefits and costs for the whole network.
and in the context of a concrete application case. In the case of accounting, consistency and partition resistance are certainly important features of the distributed ledger, which ensures that not only all nodes have the same information, but also that the accounting system does not break down, if a particular peer or several peers fails. Notably, the exposure of whole business activities such as accounting through network failure could imply severe economic losses as well as legal sanctions that must be avoided under any circumstances. Availability of nodes is, thereby, closely linked to this feature, however, principally minor time delays of transactional information updates are acceptable, whereas a strong focus should be placed on the issue that these delays should not exceed an acceptable time frame, which, otherwise, possibly results in severe data inconsistencies. Thus, overall a distributed ledger based accounting system would benefit from the maximization of CAP goal, which is principally feasible, given distributed ledger design. Moreover, today it is assumed that designers, despite they still need to choose between consistency and availability, have a range of flexibility for handling partitions and to recover from them. Therefore, modern CAP goals should maximize combinations of consistency and availability that make sense of the specific applications. Particularly, the three properties promoted by the CAP theorem are more continuous that binary variables, meaning that there exist many levels of consistency and availability and also partition may have different nuances, such that the choice between them must no longer seen as a mere ‘either-or-decision’, which especially holds for distributed ledgers (Brewer, 2012).

4.3.2.3 Data Transparency versus Confidentiality

Given the fact that a copy of the distributed ledger is stored on all participating nodes in the peer-to-peer network, everyone is able to read the current and past consensus state with regard to the flow and the amount of all validated transactions, which means there is complete transparency over all data incorporated on the ledger (Ober, Katzenbeisser and Hamacher, 2013). In the context of a distributed database, however, transparency can take on different forms, among others, network (or distribution) transparency, replication transparency as well as fragmentation transparency and full transparency, whereas full transparency is not a universally accepted objective, as it makes distributed database management very difficult and introduces poor message performance (Ozsu and Valduriez, 1991). According to this differentiation, also distributed ledgers are not initially designed to provide limitless or full transparency. For instance, permissionless distributed ledgers are designed to follow a ‘parties-unknown/transactions-known’ model, which implies that transactional data or other information is publicly available, but not identities of individual nodes (in the following referred to as full data transparency). Full data transparency as provided by some distributed ledgers, however, may be in
contrast to the security goal of confidentiality, whereas the protection objective can be defined as follows (Müller, Eymann and Kreutzer, 2003; Peters and Panayi, 2015):

Definition 14 (Confidentiality): Confidentiality implies that an unauthorized person cannot disclose data, either by direct retrieval or through indirect logical interference.

Considering distributed ledgers, design decisions taken on the network layer are responsible for the degree of confidentiality of data. In particular, the decisions for a permissioned or permissionless ledger decides, whether or not data are accessible by the public (Peters and Panayi, 2015). Thus the ‘parties-unknown/transactions known’ model can generally be altered, if a permissioned distributed ledger is applied, and restricted to a set of pre-specified nodes. However, the restriction of transparency in distributed ledger must be thoughtful, since the ability of nodes to validate accounting data correctly depends on the degree to which they are able to generate insights from past data on the ledger. Thus, restrictions of transparency in favor of the security goal confidentiality may come at costs of the distributed ledger performance and correctness of transactional information. Moreover, transparency in peer-to-peer networks is typically applied as a prerequisite for coordination. This holds especially, if the behavior of single nodes in such networks is hard to monitor and regulate and, if users must interact directly, without the approval of any intermediary operator. Thus, in order to achieve some form of coordination in a distributed fashion, specific data or metadata must be disclosed to all nodes on the network in order to collectively verify the legitimacy of accounting data that should be integrated into the distributed ledger (De Fillippi, 2016).

4.3.2.4 Process Integrity versus Discretionary Decision-Making

Despite the trade-off between classical security and privacy goals, distributed ledger imply further trade-offs concerning consensus finding as well as network control, which is defined and enforced through the underlying protocol rather than by law. Particularly, distributed ledgers are ruled by a technical code, which implies both benefits in regard to process automation and trust, but also sever drawbacks in regard to discretionary decision making (Walport, 2015).

As already exemplified in this chapter, every node is following the same protocol, in which the general and contextual rules are specified. By this, the distributed ledger protocol is a part of business process automation and a method to check process integrity, which implies among others responsibilities in regard to system maintenance, workflow as well as automated task execution (Giaglis, 2001). In permissionless distributed ledgers, individual behavior gets predictable, by following the technical code, which implies integrity through economic incentivizing. This is expected to decrease uncertainty about the behavior of single node, whereas at the same time, there is no trust in
individual nodes, which necessitates the public character of all ledger entries (Swanson, 2015; Walport, 2015). Notably, the Bitcoin system is an example of this form of uncertainty reduction, as it is based on the single node’s trust into the majority of nodes, which will behave honest, i.e. pursuant with the protocol (Nakamoto, 2008). The benefits of such systems are straightforward: if participants can rely on the protocol to exclude the possibility of dishonest behavior, then compliance costs are low. Moreover, it might seem that enforcement costs are lower too, given the functionalities and automated enforcement mechanisms of smart contracts. However, at the end, this depends on the applied consensus mechanism. For instance, Proof-of-Work has proven to be very costly in terms of energy consumption, which eventually must be borne by network nodes, making the enforcement of rules costly again (Dwyert and Malone, 2013; Walport, 2015).

Whereas on the one hand, decreased uncertainty with respect to individual behavior that is completely determined by a protocol, seems to be beneficial, permissionless systems often facilitate open codes that remain available for adopters for modification or improvement (Lessig, 1999, 2000). For instance, if an open source code carries a government-mandated encryption routine, that routine will be apparent to open source coders, who can chose whether or not to adopt that portion of an open code project (Lessig, 1999). Thus, the assumption that distributed ledger system and the behavior of participant nodes is merely determined by algorithms and the protocol rules is a misconception, since the technical code needs to be produced and maintained by humans, who define the rules that the code embodies. Consequently, it is important, who exactly writes the code and is, therefore, able to implement changes to a predefined set of rules (Walport, 2015).

Using closed codes, as typically applied in permissioned distributed ledgers, the problem of decentralized conducted changes and modifications of codes is of less concern, as changes are easier to monitor and access is harder compared to open codes. However, using permissioned distributed ledgers, on the other hand a centralized validation entity can easily regulate user behavior and is responsible for decisions concerning transaction validity. Thus, in closed systems there is less uncertainty compared to permissionless distributed ledgers, as integrity is more often assured through conventional means, such as legal contracts (Walport, 2015). On the other hand, ad hoc rule making, which may be able in permissionless distributed ledger systems, is not possible. For instance, bug fixes in Bitcoin can be easily done by a handful of informational institutions and power holders, such as mining pools. Permissioned systems are probably not able to conduct such forms of unconventional problem solving and require a more formal progress, including decisions concerning the prioritizing of stakeholder interests (Walport, 2015). Thus, protocol rules that are implemented for a distributed ledger based accounting sys-
tems must be thoughtful and tested beforehand, since changes on the closed code approach are hard to conduct and may cause significant problems to running accounting processes.

4.3.2.5 (Pseudo-) Anonymity versus Undesired Behavior

Distributed ledgers are often assumed to imply full anonymity of participants and their transactions. In computer science, anonymity refers to pseudonymity together with un-linkability. Pseudonymity means that real identities are not used for system interaction; instead a pseudo-identity is used that is not the real name of the person. Unlinkability means that if a user interacts with the system repeatedly, these different interactions should not be able to be tied to another by an adversary (Narayanan et al., 2016). More generally, anonymity is also the state of being not identifiable within a set of subjects, which is defined as anonymity set (Pfitzmann and Köhntopp, 2001). Given, for example, a payment system such as Bitcoin, the anonymity set of transactions of node A is the set of transactions that a particular adversary cannot distinguish from node’s A transactions. Thus, even if the adversary knows that node A made a transaction, he or she cannot identify the transaction within the set. Staying with the concrete example of Bitcoin, however, it gets obvious that Bitcoin does not imply anonymity given the implied ‘parties-unknown – transactions-known’ model (Luu and Imwinkelried, 2015). In particular, in order to conduct a Bitcoin transaction a node does not use its real name but its public key hash as an identity. While the node is referenced on the ledger as pseudo-identity, the transaction is publicly available meaning that the system only implies pseudo-anonymity as long as the separation between identities exists. Contrarily, if anyone is able to link a node’s address its real world identity that all past and present transaction will have been linked back to the particular identity and pseudo-anonymity is threatened (Luu and Imwinkelried, 2015; Narayanan et al., 2016). Notably, this holds for all permissionless ledgers that are based on the assumption that participating nodes use pseudonyms.

Pseudo-anonymity is, especially important in a financial context as the disclosure of all transactional information together with node information and identities would threaten the privacy of nodes and makes individual nodes traceable (Narayanan et al., 2016). On the other hand, pseudo-anonymity also implies severe downsides, which manifest itself in undesired behavior of individual nodes in a network, provided that nodes expected to be not identifiable. This can be observed in various cases, for instance, when looking at money laundering incidents or trade with illicit items like weapons or drugs that is conducted using a distributed ledger (Taylor, 2013). Individuals, who try to exploit distributed ledger protocols that imply pseudo-anonymity expect that transactions cannot be linked to their identity, especially, as there exist several methods to increase this possi-
bility, among others, the use of multiple pseudo-identities or, in the case of Bitcoin, through the use of mixing services. Notably, the ability to conceal real identities in distributed networks imposes challenges to digital forensic, which needs to identify individuals in order convict someone of fraud (Luu and Imwinkelried, 2015). This also holds for accounting fraud, meaning that the feature of pseudo-anonymity certainly must be dropped in a distributed ledger based accounting system, in order to avoid undesired behavior such as accounting fraud.

However, generally, Swanson (2015) noticed that there is an inherent trade-off between having a pseudo-anonymous system, where no one is trusted and all information must remain public, and a (partly) centralized system with trusted nodes that are verified by true underlying identities. Thus, the question whether or not a system is pseudo-anonym and, thereby, implies certain incentives for unintended or even fraudulent behavior, is primarily a question of distributed ledger design. In permissioned ledgers, the identification of nodes is most often necessary, which implies that the probability of being convicted, if a node conducts illicit activities, is higher compared to permissionless systems. Notably, this feature is expected to decrease incentives and the opportunity to conduct accounting fraud in a distributed ledger based accounting system compared to the case, where pseudo-identities are used for authentication. Corporations that want to apply distributed ledgers for accounting, thus, need to balance the benefits and challenges of pseudo-anonymity. The benefits of pseudo-anonymity could be in the social realm, where it allows nodes to communicate without the fear to be sanctioned (Melanie Swan, 2015). However, in corporate settings and especially in accounting, this feature is not necessary and also not desirable. Consequently, a distributed ledger based accounting system will most likely deploy a permissioned system that allows for identification of each participating corporate node, which reduces the probability of undesired node behavior and the conduction of accounting fraud.

4.3.3 Relationship Between Alignment Strategies and Paradigm Changes

Table 20 summarizes and combines the described paradigm changes and the alignment strategies. Starting with the paradigm change data redundancy, initially it seems that this feature is inherent to every distributed ledger and, thereby, a general issue with respect to ledger design decisions. However, the relevance and severity of the costs and risks implied by data redundancy differ and are determined by the chosen alignment strategy as indicated by Table 20. Most apparently, using distributed ledgers as digital infrastructure implies data redundancy involving all participating nodes in the intra-corporate peer-to-peer network. Consequently, besides the risks that evolve from possible data inconsistencies (e.g. if a node is not online and, thus, was not able to receive new information from the network to updated the copy of its ledger immediately), sig-
nificant costs may evolve, because each entity that is part of the network needs a computer that is capable of storing the entire ledger. It must be noticed that partitioning is a possible solution to that problem; however, partition of the ledger requires a central storage of the detached part of the ledger, what is here assumed to be not desirable, if the initial attempt was to employ a decentralized accounting infrastructure. The same issues applies to the application of distributed ledgers as shared platform, whereas the need to hold a copy of the ledger possibly can be restricted to some nodes of a particular company, as validation responsibilities are shared with a second or more companies. Thus, data redundancy can, but must not necessarily be a relevant paradigm change, when using the ledger as shared platform. Lastly, applying the third alignment strategy, i.e. the external platform that is based on a distributed ledger, the company that make use of the application does not experience any paradigm change with respect to data redundancies as it is not part of the network. Notably, the same holds for the second paradigm that is CAP fulfillment, which as well only applies, if a firm fully or partially maintains a distributed ledger (Rückeshäuser, 2017a). In contrast, transparency, which is a direct consequence of data redundancy, affects companies equally, independent of the applied alignment strategy. In particular, this holds since, despite the fact that the degree of transparency depends on the openness of peer-to-peer network design, transparency of information between validating parties is a necessary feature and inextricable linked to distributed consensus.

<table>
<thead>
<tr>
<th>Alignment Strategy</th>
<th>Data Redundancy</th>
<th>Cap Fulfillment</th>
<th>Data Transparency</th>
<th>Process Integrity</th>
<th>(Pseudo-) Anonymity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Infrastructure</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared Platform</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>(√)</td>
</tr>
<tr>
<td>External Application</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>(√)</td>
</tr>
</tbody>
</table>

Table 20. Paradigm Changes and Relation to Alignment Strategies

The organizational paradigm change process integrity, especially, applies, if the third alignment strategy, i.e. the use of the distributed ledgers as external application, is chosen. This is because a firm that is not part of the network, cannot individually decide to implement protocol changes, and is, therefore, required to ask the other firm to implement the desired changes, which provides the ledger and is therefore in charge for the protocol. Thus, if a distributed ledger is offered as application, then there is a paradigm change for the company that uses the service, since node behavior is determined by code without any option to intervene directly. This rules out the possibility of ad hoc
rule making and changing (Walport 2015). In the case of the shared platform, the paradigm change only partially applies. In particular, process integrity is implied in the sense that a firm cannot individually decide to change the protocol, but probably can find consensus about the desired rule changes with the second company. In this case dictionary decision-making in terms of ad hoc rule changes may be possible, but not as easy as in the case of the first alignment strategy, which allow complete control over the ledger in possession of the respective company (Rückeshäuser, 2017a). Lastly, pseudo-anonymity is commonly expected to be a feature and paradigm change implied by distributed ledgers. However, several studies showed that nodes can be identified using heuristics and observing node’s past and present behavior (Ober, Katzenbeisser and Hamacher, 2013; Reid and Harrigan, 2013; Böhme et al., 2015). Notably, if a permissionless distributed ledger cannot provide pseudo-anonymity for its participants, the probability of possible smaller, permissioned distributed ledger to provide this feature is even lower (Becker et al. 2013). More importantly, however, is the fact that for companies, there exist an inherent trade-off between having a pseudo-anonymous system, where no one is trusted and all information must remain public, or a partly centralized system with trusted nodes that verify information by using true identities. Given the proposed alignment strategies and the closed network approaches, pseudo-anonymity may not be important and makes undesired node behavior (i.e. violating protocol rules) less likely, given the fact that nodes can be identified. Thus, looking at the first two alignment strategies, the feature of pseudo-anonymity is possible not given as well as not desired. Using distributed ledger as external application, the trusted firm possibly does not know the identities of nodes that submit information to be incorporated in the ledger. Thus, theoretically, distributed ledger can induce a paradigm change in terms of anonymity of network participants applying the third alignment strategy. However, in reality and, especially, in a corporate setting and by referring to the first two alignment strategies, network participants are typically identifiable or use their real world identity as key, since anonymity is certainly not a priority in networks with already pre-selected participants and closed network approaches.

Summarizing, paradigm changes that are relevant for applying alignment strategy 1, are predominantly of technological nature, while organizational and social changes through process integrity or (pseudo-)anonymity are only of minor importance. Applying distributed ledgers as shared platform has probably the greatest effect on firms, by inducing technological, organizational as well as social paradigm changes. In particular, organizational paradigm changes are induced through process integrity and the underlying decentralized consensus mechanisms, which diminish the necessity for hierarchical decision-making. Social changes are induces through partial pseudo-anonymity, which possibly has an effect on node behavior and incentives, since nodes are potentially not
easily identifiable. Lastly, aligning distributed ledger technology and business processes through the use of an external application, the no technological paradigm changes are implied for firms that use the services offered by a third party. Instead, organizational and social paradigm changes are induced, however, they are probably less significant as in the case of alignment strategy 1 or 2, since entities within the firm are not involved in maintaining the ledger. Given these results, a distributed ledger based accounting system is expected to exploit the paradigm changes offered by alignment strategy 1. In particular, using applying the distributed ledger as digital infrastructure implies decentralization and data transparency that was previously identified as a requirement for the prevention of accounting fraud. Moreover, the CAP goal maximization ensures the effectiveness of the accounting system, which is especially important in order to prevent economic losses due to the exposure of the central nosiness activity. Notably, also shared platforms are conceivable as a solution to accounting fraud prevention, given the similar paradigm changes implied. However, since the scenario developed in this thesis is one of the first attempts to provide an in-depth analysis of the ability of distributed ledger to prevent accounting fraud, first the simpler case is investigated, which can be of course, extended to alignment strategy 2 in subsequent analyses.

4.4 Distributed Ledger Customization Model for Fraud Prevention

In the following, a model for distributed ledger implementation and business customization is provided and depicted in Figure 19, which combines not only the results of the present chapter, but comprises the analysis results of all previous sections. The illustrated layers are assumed to overlap and to be partially interconnected. The layer model, moreover, provides an overview on, how distributed ledgers fit in and support a company, by providing deployment choices and enabling flexibility in regard to application possibilities. Thereby, not only the previously presented architecture and alignment strategies are taken up, but also further issues that must be considered, if the technology is applied for accounting fraud prevention. Figure 19 shows, how distributed ledgers can be implemented and adjusted to a particular business activity or application, by following three divergent steps and making associated design decisions, as indicated by the layers. The first alignment strategy is applied by using the distributed ledger as digital infrastructure for an accounting information system (Rückeshäuser, 2017b).

The first step in order to implement the distributed ledger within a corporate context is to build the distributed ledger as such, which implies the decisions towards the technical design choices discussed in the previous sub-section. The second step implies the choice for a particular deployment mode, which implies decisions concerning the network
openness and governance modes. Notably, these decisions are made simultaneously with the first step decisions, as they are partially interdependent. Subsequently, the particular use case must be defined, including the adjustment of the distributed ledger features and functioning to potentially already existing business infrastructures as well as building the concrete applications. Eventually, this step also implies the employment of further security mechanisms to account for emerged security gaps or threats resulting from organizational restructuring. The model as well as the respective steps for distributed ledger implementation and customization are now discussed successively.

Figure 19. Distributed ledger implementation and customization model

### 4.4.1 Infrastructure Development

At the lowest layer of the distributed ledger implementation and customization model, the distributed ledger constitutes a mere digital infrastructure. This basic infrastructure consists of three major elements that are already discussed in the context of the technical architecture of ledgers. The representation layer is here purposefully omitted as it does not significantly affect other design decisions and can be grouped under the realm of protocol rules. Consequently, the digital infrastructure consists of the peer-to-peer network, characterized by the ability to exist without a central node, the decentralized
consensus mechanism that executed protocol rules, and the shared storage, which is here denoted as logging as well as the associated design decisions, which can be made with respect to the single distributed ledger features (Rückeshäuser, 2017b). A discussion of the particular design decisions and the associated functionalities is omitted as this point, as this was already generally discussed in the previous chapter and will be specified in the following.

### 4.4.2 Deployment Mode Decisions

The second layer is characterized by the choice of different deployment modes that depend on the desired openness of the peer-to-peer network and the type of data validation. Notably this step is also important for the design of the infrastructure, as both layers exhibit strong interdependencies. Distributed ledger can either feature permissionless access or permissioned access, however, irrespective of the access type, the validation of the blockchain can be either performed in a decentralized way or by one particular or several nodes, i.e. centralized validation (Peters and Panayi, 2015). Despite this sounds counterintuitive applying distributed consensus mechanisms for decision making, centralization may stems from the fact that the validation is transmitted to a set of changing nodes (e.g. delegated proof-of-work) that are responsible for the validation. Contrarily, decentralized validation is characterized by the fact that all nodes in the network are able to validate data that should be incorporated into the blockchain. Typically, permissionless decentralized ledgers are featured by decentralized validation (e.g. Bitcoin) whereas permissioned ledgers use centralized validation. However, every other combination or hybrid form are conceivable (Swanson, 2015). This definition excludes unintended centralization, for instance, through the undesired accumulation of the majority of computer power in the case of proof-of-work (Rückeshäuser, 2017b). For a detailed discussion of the deployment choices it is again referred to the previous subchapter that discusses the technical architecture of distributed ledgers.

### 4.4.3 Application Foundation and Integration

Based on the design of the distributed ledger, for its implementation, now, adjustments in regard to existing business infrastructures, e.g. currently applied information systems as well as to existing business processes must be performed. Thereby, the foundations are laid for the subsequent integration of the envisaged application in accounting. Among others, this step includes that rules within the application (contextual rules in the distributed ledger protocol) must be designed in accordance to the particular business process as well as particular compliance requirements. For example, business activities, which imply financial transaction, must respect a variety of national and international legislations that must be appropriately represented by the protocol. Moreover,
the correct execution of these rules must be assured in order to guarantee compliance, provided that the rules are technically feasible. Moreover, a service-oriented architecture (SOA) must potentially taken into account, if a distributed ledger application must be integrated within an existing enterprise systems in order to provide the same or even enhance service quality (Tsai et al., 2015). However, most likely not only the interaction of the distributed ledger and decentralized consensus with other business information systems must be considered, but also user interactions with the system, which was emphasized as a result of the investigation of Bitcoin user behavior. Consequently, user interfaces must be carefully designed in order to assure that the distributed ledger features are properly used within a corporate context. For instance, if it is not clear, how to read data on the distributed ledger, e.g. because the overview provided is confusing or unclear, then the expected benefits implied by increased transparency and decentrality will probably not unfold. However, the attributes presented on the third layer are only exemplary and customization may include numerous other aspects that are not listed in the model and evolve depending on the concrete application and the existing corporate infrastructure (Rückeshäuser, 2017b).

4.4.4 Application and Application Security

Lastly, on the top layer of the distributed ledger implementation and customization model, particular applications are built on the basis of the preceding layer decisions and efforts conducted in order to build a foundation for distributed ledger applications. For example, despite an application in accounting, smart contracts can be implemented for insurance services or digital rights management. However, as indicated in Figure 19, application areas of distributed ledgers are diverse and relate to various business sectors, whereas the examples provided in the model are again not exhaustive (Rückeshäuser, 2017b).

Apart from the fact that the blockchain itself offers particular security features through cryptography and the respective distributed consensus mechanism, additional security mechanisms might be implemented on the upper layer. Depending on the concrete application, these mechanisms may range from additional data securing mechanism and fraud detection or ex post auditing techniques, whereas, again, this list is not exhaustive. Moreover, these features are supported by the insights distributed ledgers deliver, depending on the degree of transparency that is enabled through the distributed ledger design (Rückeshäuser, 2017b).


4.5 Concluding Remarks

Chapter 4 provides a discussion on the, in a broader sense, trade-offs that arise if distributed ledger technology is applied in accounting. Notably, the usage of the technology does not only imply the emergence of business value; organizational changes as well as adjustments of business processes to the new technology are required. In order to take account for the downsides of distributed ledger applications in accounting, first the possible ledger design decisions were discussed that are a result of the technical architecture of distributed ledger technology. Afterwards, possible design decisions were emphasized that may facilitate accounting processes. However, it is acknowledged that without a concrete scenario, design decisions for distributed ledgers and an application for accounting fraud prevention only remain on the surface. Nevertheless, based on the previous investigations and the shown flexibility, it get obvious that distributed ledger probably provide significant improvements with regard to the deterrence of management override of internal controls, which is expected to arise mainly because of the distributed ledger features decentralization and transparency as well as from the associated mechanism for distributed consensus. Thereby, potentially, the excessive influence of the management on internal control entities can be prevented, through an appropriate protocol design. However, as already mentioned challenges simultaneously arise from the use of distributed ledger technology, i.e. paradigm changes that can be mitigated and approached by using one of the proposed alignment strategies. Thereby, firms must be aware of the fact that using distributed ledgers as digital infrastructures within a corporation implies far reaching technological and organization paradigm changes, whereas using the distributed ledger as external application involves less paradigm changes and, therefore, only minor restructuring efforts.

Taking together the technical architecture, design possibilities as well as the need to deal with paradigm changes depending on the chosen alignment strategy (which is here the digital infrastructure), an implementation and customization model for distributed ledgers is developed. In particular, the implementation and customization model of the distributed ledger delivered insights on the steps that need to be considered successively, if the technology is applied for the facilitation of accounting processes. Despite the highlighting of different design choices and issues that must be taken into account, as an implication of the model, more importantly, it is emphasized that a distributed ledger is not a fixed construct, which can be simply applied to a business context, continuously delivering the desired and expected features of transparency, decentralization and potential immutability. Instead, distributed ledger technology must be understood as a flexible mechanism, which characteristics and associated outcomes significantly depend on the concrete design, the ultimate application as well as the environment, surrounding the technology. Thereby, the customization model constitutes a starting point for all possi-
ble distributed ledger implementation and application efforts. Moreover, it serves as a framework for the evaluation of possible outcomes of particular design choices, the hereby-induced effects on application foundations and integration as well as for the assessment of further effects, such as possible newly emerging security threats.

**Key Points Chapter 4:**

- Distributed ledger architecture offers a variety of design decisions that can be exploited for an application in accounting and the prevention of management override on internal controls; however a concrete scenario is needed for evaluation.
- The technological features do not only imply benefits – significant adjustment processes are implied by paradigm changes, induced through the technology and depending on the chosen alignment strategy.
- Companies that apply distributed ledgers as digital infrastructure and foundation for accounting must be aware of the mainly technological paradigm changes and can use the customization model as a framework for technology implementation and business process adjustments.
Blockchain-Based Accounting: Scenario Development and Evaluation

5

Existing papers proposing the application of distributed ledger technology in accounting have shown a great lack of scenario development techniques, subsequent scenario assessment as well as risk management analysis. However, the development of a concrete scenario representing, how distributed ledger technology is applied for accounting fraud prevention is necessary, which is especially important given the fact that individual behavior of entities in response to a newly applied information technology can be diverse and may imply positive as well as negative behavioral changes, for instance, if emerging technical vulnerability are systematically exploited (Francis and Bekera, 2014).

Thus, in the following, a technological scenario according to Mahmoud et al. (2009) is developed, showing how technological changes, i.e. the use of distributed ledger technology as a foundational technology in accounting affects individual behavior and the emergence of accounting fraud, respectively. The associated research question is, therefore, (RQ.4): Does distributed ledger technology prevent the emergence of accounting fraud? To develop a scenario, an expert-judgment-driven scenario model is chosen, which builds on scientific knowledge, decision rules, objectives and criteria established by science investigators and field experts (Mahmoud et al., 2009). Consequently, the previous parts of this thesis are combined in order to achieve a comprehensive scenario including, theoretical considerations in regard to the technological flexibility as well as expected economic effects. Moreover, behavior and decision analysis according to the investigation of accounting fraud incidences and the associated factors that may facilitate fraudulent behavior should be taken into account. To this end, RQ.4 is divided into two related research questions, whereas the first is (RQ.4a): How does a scenario of distributed ledger based accounting look like and through which mechanisms is accounting fraud prevented? Consequently, answering RQ.4a requires the development of a concrete scenario and the review of the previously stated assumption about distributed ledger technology and its ability to prevent accounting fraud. Thereby, the advantages of the expert-judgment-driven approach make an impact through the integration of current thinking regarding future change and the incorporation of a wide range of pertinent information. However, it must be noticed that at the same time disadvantages may arise from the approach, including the possibility that scenarios are biased by subjectivity of experts and may lack political plausibility (Mahmoud et al., 2009). However, the application of other conceivable approaches of the family of anticipatory scenarios, such as policy-responsive scenarios as well as stakeholder-defined scenarios, are at the moment not feasible, given the fact that the cited, currently existing literature...
constitute the first theoretical attempts and proposals for the concrete application of the technology in accounting. Consequently, other approaches than expert-judgment-driven scenario development are yet not feasible, given a lack of data and information provided by policy makers as well as possible stakeholder, e.g. firms that already use the technology.

Having defined the scenario and the expectations regarding the capability of distributed ledgers to prevent the emergence of accounting fraud, the second research question, related to RQ.4, must be answered that is **(RQ.4b): Does a distributed ledger based accounting system and the associated distributed consensus mechanisms prevent the emergence of accounting fraud in the proposed scenario?** Thereby, the question whether or not the optimal scenario and associated expectations about fraud prevention will hold, can be reduced to the question whether the applied consensus mechanism works as expected. Several decentralized consensus mechanisms are, consequently, analyzed as well as the resulting system-user-interactions in the specified scenario, in order to come to an assessment, whether or not distributed ledgers are capable of preventing accounting fraud through the override of internal controls.

### 5.1 Scenario Definition

The definition of a scenario typically involves the identification of characteristics of a particular scenario that are of interest for stakeholders as well as decisions concerning the facts, whether the thereby predicted future is considered to be merely a trend of the present or, whether the future implies a paradigmatic shift in system behavior. Moreover, the key variables that drive the system under study must be defined, which are those variables to which the system is responsive (Mahmoud et al., 2009). The previous chapter already discussed the core challenges that must be considered, if distributed ledgers are applied in accounting and main actors were identified that will be present in the following scenario. Shortly summarized, the interest of main stakeholders is here defined as the prevention of financial statement fraud within an accounting information system. This could possibly be achieved by the features decentrality, transparency as well as potential immutability of distributed ledgers. Decentrality, foremost implies a paradigm shift not only in organizational behavior but also of the organizational structure. The associated changes in responsibilities could, thereby, prevent the management from making own decisions and to alter financial statements for their own benefit, which is otherwise enabled by the hierarchical structure of a corporation and a highly centralized as well as typically powerful management. While taking the possibly downsides of decentralization into account, distributed ledgers could furthermore decrease the possibility of the emergence of fraud owing to increased transparency. More precisely, if all transactional data are transparent, the possibility that no one detects ex post
alteration of data, especially, if everyone has a copy of that data on his or her own computer, is lessened given the possibility for comparison. Eventually, immutability of data would rule out the opportunity of ex post data alteration and manipulation.

Table 21 summarizes the respective variables into a scenario set and assigns them according to their characteristics, i.e. whether they are state, influencing or responsive variables, whereas different combinations of these factors lead to different outcomes regarding the prevention of accounting fraud in the subsequently defined scenario. Whereas state variables are either present or not, technological factors are defined as binary variables with respect to its degree of unfolding within the defined scenario. This differentiation is done given the fact that technological factors may differ given the chosen deployment mode and technical design decisions. For convenience only, and because grading between different degrees of technical factors is hardly possible, the degree of transparency, decentrality and immutability is either low or high, whereas a definition of these states will be provided in the following. Individual behavior, which will be the responsive variable in the following scenario, will be either licit or fraudulent, meaning that financial statement fraud will be either conducted or not, irrespective from the fact whether the management, which is assumed to be the perpetrator of fraud, conducts fraud by himself or by convincing, bribing or extorting other parties.

<table>
<thead>
<tr>
<th>Variables</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actors (state variables)</td>
<td>• Management (A1)</td>
</tr>
<tr>
<td></td>
<td>• Employees (A2)</td>
</tr>
<tr>
<td></td>
<td>• Internal control bodies (A3)</td>
</tr>
<tr>
<td></td>
<td>• External control bodies (A4)</td>
</tr>
<tr>
<td></td>
<td>• Supervisory/regulatory bodies (A5)</td>
</tr>
<tr>
<td></td>
<td>• Stock Market Participants (A6)</td>
</tr>
<tr>
<td>Technological factors</td>
<td>• Degree of decentrality (low/high) (B1_l, B1_h)</td>
</tr>
<tr>
<td>(influencing variables)</td>
<td>• Degree of transparency (low/high) (B2_l, B2_h)</td>
</tr>
<tr>
<td></td>
<td>• Degree of immutability (low/high) (B3_l, B3_h)</td>
</tr>
<tr>
<td>Behavioral factors</td>
<td>• Individual Behavior (licit/fraudulent) (C1_l, C1_f)</td>
</tr>
<tr>
<td>(responsive variables)</td>
<td></td>
</tr>
</tbody>
</table>

Table 21. Scenario set for blockchain-based accounting

Given the scenario set, the construction of a concrete scenario requires the identification of critical information reflecting the ultimate outcome(s) of a scenario as well as scenario characteristics. Moreover, the causal relationships must be taken into account and need to be combined in a comprehensive scenario (Mahmoud et al., 2009). To this end,
the desired scenario, which is here denoted as optimal scenario \( (S_o) \), is firstly developed. The desired scenario implies that all state variables are in place, meaning that internal as well as all direct and indirect external control entities are present. Furthermore, the degree of decentrality, transparency as well as immutability is initially assumed to be high, given the particularly applied consensus mechanism, which is provisionally proof-of-work. More formally, the optimal scenario can be defined as follows:

\[
S_o = \{A_{1,6}, B_{1b}, B_{2b}, B_{3b}\},
\]

subject to the condition \{PoW\}.

The optimal scenario is then expected to lead to the desired outcome \( C_{1b} \), where everyone or at least the majority of consensus participants behaves according to the rules specified in the protocol. This should exclude opportunities for the management to override internal controls in order to conduct accounting fraud.

### 5.2 Scenario Construction

Graphically, the optimal scenario is depicted in Figure 20. The basic infrastructure of the proposed accounting system is a distributed ledger and a blockchain, more specifically. Blockchains are chosen because they inherently store data chronologically, which is of benefit in an accounting system, as it implies automated creation and sequencing of ledger entries. The underlying peer-to-peer network access is only possible with permission. In particular, an intra-corporate network is proposed, whereas only the defined stakeholders have access to the network. Nevertheless, stakeholders may have different rights concerning the ability to validate data, which will be explained in detail later. However, restrictions concerning the ability to access and to validate data on the intra-corporate blockchain are chosen, since full transparency of sensible financial data to particular companies or in an extreme scenario - to the general public, could lead to severe losses in competitive advantages for the transparency providing company. For example, lawfully discretionary accounting practices would be no longer feasible, which could be exploited by a competitor, whose financial data are not transparent or only partially transparent. Moreover, the decision to limit the access to the network and to provide only restricted transparency in the scenario is inspired by, among others, the obligation of German stock companies for publishing annual accounts (AktG) as well as other national regulations concerning financial disclosures, which typically do not imply or enforce full transparency and real-time observability of financial transactions.

Without defining and considering a concrete transaction that is conducted using distributed ledger technology, in the first instance, it is assumed that the set of rules specified in the protocol are chosen in such a way that they are in line with relevant legal re-
quirements and accounting standards. Moreover, it is assumed that transactions are conducted without using tokens, meaning that a fiat currency is referenced directly on the ledger instead of using any form of cryptocurrency, nor as monetary unit neither as container value.

Figure 20. Scenario of blockchain-based accounting

While all network participants have the right to read data on the ledger, the right to validate data is only granted to particular stakeholders. Thus, in the following it must be differentiated between direct participants, which are participants, who are allowed to validate information to be incorporated on the ledger, and indirect participants, that are participants that have only the right to read information on the blockchain. This limitation of rights of a particular group of network participants is done, because fully decentralized consensus finding might be counterproductive, given a potentially very time-consuming consensus finding process. Thus, a hybrid form for consensus finding is proposed, where particular employees that is, especially, the accounting department, the management as well as internal control entities that are assumed to be the board of directors and an optional internal auditor or an audit committee, build the pool of consensus participants. In the terminology of the scenario set, this consensus pool is still considered to constitute a highly decentralized consensus finding system.

Basic employees are likely to be enforced to participate on the consensus process as part of their work assignment. Participation of the management could also be part of their work assignment, however, it is assumed that the management is most likely intrinsically motivated to participate in consensus finding. According to the conducted case studies and the definition of the management as perpetrator of fraud, thereby, the management acts in its own interest and participates, because it wants to influence the consent-
sus protocol in a negative way, i.e. in order to conduct accounting fraud. Validation is conducted by means of a proof-of-work consensus mechanism, which is in line with the cited literature that all propose proof-of-work as basic consensus mechanism for this type of application of distributed ledger technology (e.g. Yermack (2015), Andersen (2016)). Thus, consensus will only be found, if transactions are in accordance to the pre-specified rules. Consensus participants will reject transactions that are not compliant. Valid transactions are subsequently logged and serve as publicly available source of information within the company and to particular outsiders that are the remaining stakeholders A4, A5 and A6. Simultaneously, consensus participants are the source of information by conducting transactions via the accounting system and broadcasting it to the rest of the network for validation. The right to read is granted to external control bodies such as an external auditor, shareholders and potential supervisory or regulatory bodies. Those stakeholders have full insights in the transactional data and are, therefore, able to exert direct and indirect control functions. Theoretically, transparency to all stock market participants might be granted. However, this would be in contrast to the intra-corporate approach, chosen because of the sensible nature of financial data.

The defined scenario implies two mechanisms that have a particular effect on the desired outcome of rule conformant behavior: First, the scenario implies increased accountability, since control bodies such as the internal audit and the board of directors are directly involved in decisions processes, which increases their accountability for verified transactions. As observed in many accounting fraud scandals, for instance, external board members invoke to have no or too little knowledge about actual transactions and could, therefore, not detect fraudulent as well as concealment schemes conducted through the management. Whether this is true or not, using blockchain-based accounting and decentralized consensus, directors and other control entities would be directly accountable for illicit transaction, which decreases the probability to get away with fraud, if they are actually involved. Increased accountability, therefore, raises the probability of conviction, which has direct negative effects on the incentives to conduct fraud (Kassem and Higson, 2012).

Second, data stored on the blockchain are not only transparent to the consensus participants, but also to further pre-specified entities, which changes the role and responsibilities of shareholders, supervisory bodies and external auditors, whereas, depending on the scenario, these entities may change. In particular, this means that ex post changes on the data stored on the blockchain potentially can be detected directly, through fast comparison with an own copy of the ledger. More importantly, however, external controls, such as external auditors, may have a better oversight over all conducted transactions, owing to the automated chronological storage, which is in accordance to Andersen (2016). Consequently, this should diminish the need for subsequent requests or investi-
gations for mismatched or missing data on the side of the external auditor, thereby, leading to a concentration on core competencies and investigations of special cases as well as, probably, better detection rates.

Summarizing, given this optimal scenario, ex post alteration and data manipulation should be hindered or at least reduced through decentralized consensus that specifies the rules and correctness of conducted transactions. Furthermore, the incentives to conduct fraud should be decreased given higher accountability and transparency. However, it must be noted that higher accountability depends significantly on the fact, whether decentralized consensus is able to provide immutable storage. Otherwise, traces of fraud could be concealed afterwards, which also makes transparency pointless. Consequently, the question whether or not the application of blockchains prevents accounting fraud, can be reduced to the question, whether the associated distributed consensus mechanism provides immutability of stored data.

5.3 Scenario Specification

In the following a closer look on the mechanisms and a concrete transaction processed and referenced on the intra-corporate blockchain is provided for the further specification of the scenario. Before that, distributed ledgers are interpreted as mechanism to provide automated compliance and compared to currently existing techniques for automated compliance realization. Notably, this interpretation allows a subsequent investigation, how exactly protocol rules are obeyed in the context of a blockchain based accounting system as well as how immutability is possibly achieved. In particular, in the distributed ledger based accounting system, general as well as contextual rules defined in the protocol are responsible for the correctness of the transactions included into the ledger. Thus, this mechanism provides the basis for compliance realization, whereas the compliance process is defined as an integral approach, which links laws, regulations (e.g. Sarbanes-Oxley Act or Basel II) and other rules, to which transactions need to conform, and that are technically realizable through IT (Sackmann et al., 2008).

5.3.1 Automated Compliance Realization Through Distributed Ledgers

Starting with a set of transactions, the execution of the consensus mechanism through consensus participants decides, which transactions are actually valid and included into the distributed ledger in accordance to the pre-specified rules and policies. In this way, only transactions that conform to the rules specified in the protocol and the application are processed. Without using a distributed ledger, compliance during the execution of a transaction is normally 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. adjusting inconsistent policies). Contrarily, the consensus mechanism of distributed ledgers automatically enforces policies, which is equivalent to a compliance-by-design approach and potentially substitutes retrospective compliance checking methods.

After a transaction was confirmed and processed, the transactions are stored in the distributed ledger. Typically, appropriate internal and external monitoring activities need to be implemented within business processes of a company to ensure that compliance requirements are met (Scholte and Kirda, 2010). The aim of compliance requirements is, thereby, to enhance transparency of business decision and to augment the accountability of responsibilities (Sackmann et al., 2008). Owing to the compliance-by-design approach facilitated through distributed ledgers, the necessity to implement such ex-post compliance measures should be reduced. Thus, consensus will only be achieved over transactions that are in compliance with the rules specified within the protocol of the distributed ledger, such that non-compliance is likely to be technically impossible. However, there might be transactions within the system that are validated and executed through 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, information, which is processed by distributed ledgers, is stored in the 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.

The process of compliance realization using a distributed ledger for any arbitrary chosen financial transaction \(i\) is depicted in Figure 21. 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 (Sadiq, Governatori and Namiri, 2007). The specification of rules requires the formal representation of existing compliance requirements in the protocol and applications of distributed ledgers. In particular, for the realization of compliance, the specification of rules must be done before the execution of transaction \(i\). The final realization of compliance is achieved after the execution of the transaction by means of appropriate detection methods and audit, which is enhanced by transparency provided by the distributed ledger. In the following, the three different phases of the compliance realization process will be further explained by exemplified automated compliance
achievement using the example of a particular set of transactions that is facilitated through and with a blockchain based accounting system.

![Diagram showing the process of compliance realization through distributed ledgers.](Figure 21. Process of compliance realization through distributed ledgers)

### 5.3.2 Compliance-by-Design in Blockchain-Based Accounting

Based on the previously defined scenario, Figure 22 presents an information-processing perspective on how financial data is processed, stored and analyzed following Julisch et al. (2011). In particular, Figure 22 exemplifies, on which steps and how the proposed blockchain-based accounting information system fosters compliance-by-design considering a particular set of transactions, also including further implications on associated business processes, such as financial audit and internal control.

Every transaction conducted in the accounting information system is considered to create a data record that is subsequently processed by the activities of a business process. The goal of this process is in accordance to the previously defined scenario set, that is the fair and accurate representation of financial data on the ledger. In existing non-blockchain-based accounting information systems, financial statements are produced by an accountant and a financial auditor audits the statements for correctness, for which he or she is directed by national or international regulations or accounting standards. The financial accountant uses financial information that is provided by a financial database, which stores all relevant transactional information, that are collected, processed and stored by a business process. It is assumed that the business process is partially automated by information systems. Automation is achieved by the help of enterprise applications that are a special form of software, which forms an integral part
of the information system (Julisch et al., 2011). More precisely, according to Zimmermann (2009), enterprise applications are large and complex, physically distributed software processes for the procession of data, such as payment processing, customer relationship management as well as for business intelligence.

In contrast, the blockchain-based accounting information system comprises three roles in the specified scenario and directly influences the respective relationships within Figure 22. Since business processes are increasingly realized through IT (Sackmann et al., 2008; Ramezani et al., 2012), the basic function of the blockchain-based accounting information system is its role as information system, supporting the subsequent business process, which processes and stores the transaction and associated information on the shared database. Potentially, the distributed ledger includes also further enterprise applications or is implemented within the broader context of an enterprise system. The business process is executed based on the information system and facilitated by distributed consensus. Notably, distributed consensus fosters automated compliance and, specifically, compliance-by-design, since consensus can only be found, if the business process is in accordance to the specified rules. To this end, top-level compliance requirements must be transferred into machine-readable form in order to formulate control objectives on a technical layer. 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 distributed ledgers and the decision criteria of
decentralized consensus. As a result, rules in the blockchain based accounting information system could be, for instance, SOX 404, which determines the segregation of duty constraint, meaning that one individual does not participate in more than one key trading or operational function (Klamm and Watson, 2009).

The ability of the blockchain based accounting system to foster compliance-by-design is remarkable since existing technical mechanisms for the realization of automated compliance feature either a retrospective perspective, using so-called automated detection mechanisms, or foster a preventative approach. Automated detection mechanisms are typically realized using compliance software that is often specialized in a certain class of checks with corresponding economic disadvantages (Sadiq, Governatori and Namiri, 2007). For instance, the integration of hard-coded checks into standard software makes the compliance process very rigid, thereby, excluding the opportunity for scaling or the consideration of organization-specific rules (Sackmann et al., 2008). In contrast, the preventative approach of compliance-by-design enforces the achievement of compliance through the prevention of undesirable, non-compliant behaviour, by capturing compliance requirements e.g. through a generic requirements modelling framework (Sadiq, Governatori and Namiri, 2007; Sackmann, 2008). The involved top-down oriented and analytical approach requires all mandatory legal regulations to be technically realizable throughout the whole system. To this end, all possible activities and states as well as all special (i.e. unregularly business processes) must be known and pre-specified in the system. Thus, while the enforcement of specific processes such as the segregation of duties can be achieved using a pure compliance-by-design approach (Sackmann et al., 2008), it is questionable how compliance can be guaranteed in the blockchain based accounting system, given observable as well as non-observable policy rules. Observable rules are rules that cannot be enforced but observed ex ante through auditing or at runtime, given the current technical solutions for automated compliance. Furthermore, non-observable policy rules are rules, which adherence cannot be checked, which typically happens in distributed systems, where events are invisible for the observer (Sackmann et al., 2008).

While blockchains cannot provide a significant improvement in the case of observable policies, where they can only offer real-time controls due to complete transparency within the network, they are potentially able to improve the policy oversight in distributed systems. In particular, given full transparency and distributed consensus, no entity in the distributed network is expected to be able to deduct and conceal certain transactions. Potentially, this eliminates the possibility of non-observable policy rule violation, which increases the probability of automated compliance achievement. Thus, assuming that blockchain-based accounting information systems could not only enforce policies but are also able to prevent compliance violations that were so far non-observable, the
Blockchain would furthermore alter the role of external accountants and financial auditors. More precisely, the audit process is typically defined as a process of “after-the-fact” detection of compliance violations, often conducted by traditional audit and manual checks by consultants (Sackmann, 2008). Given that a compliant state of transactions that is stored in the shared database can be guaranteed, financial statements could be produced automatically. In particular, this may lessens the need of accountants and changes the role of financial auditors that do not need to proof every transaction, but can focus on particular activities in the network or the adherence to observable policy rules. Consequently, the proposed blockchain-based accounting information system is not expected to completely eliminate the need of ex post controls for business process compliance in accounting information systems, but potentially improves the compliance process due to greater flexibility as well as the induced changes for external accountants and financial auditing, thereby, leading to greater efficiency of controls as well as increased cost-effectiveness.

5.4 Interim Conclusion

The previous sub-chapter developed a scenario of distributed ledger based accounting or, more precisely, a scenario of a blockchain based accounting system, which is built on the theoretical and practical considerations, thereby, linking the previous chapters together. In particular, the developed scenario depicts an optimal scenario, in the sense that it is expected to prevent accounting fraud, which is assumed to be conducted through the intentionally override of internal controls through the management. Having defined the scenario as well as relevant parameters, which mainly stem from the design decisions on the respective ledger layers, distributed ledgers are interpreted as an instrument for compliance realization. In particular, this step allows the specification of the scenario by looking at a concrete financial transaction as well as how it is processed and stored in the context of a blockchain based accounting system. The scenario further emphasizes that the ability of distributed ledgers to prevent the emergence of accounting fraud, eventually, depends on the functioning of the applied consensus mechanism, which determines whether or not and how likely it is that an individual or a group of individuals modify accounting ledger entries. This is particularly important, since the ability to alter ledger entries at will, would also imply that the further features of distributed ledgers, such as transparency, are pointless. Notably, staying with the example of transparency, if alterations of ledger entries are possible, modifications would not be comprehensible and perpetrators of fraud could easily conceal their traces by overwriting the whole transaction history. Given the relative importance of the distributed consensus mechanisms, thus, in the following, the ability to prevent accounting fraud by the initially assumed proof-of-work consensus mechanisms is investigated using the pro-
posed scenario as well as, in the interest of comparability, by applying alternative distributed consensus mechanisms that fit the scenario.

5.5 Evaluation: Does Decentralized Consensus Prevent Accounting Fraud?

The previous chapter described an optimal scenario, which raises the expectation that the application of distributed ledgers will lead to the desired outcome, i.e. the prevention of accounting fraud, enabled through the features decentralized consensus finding, transparency and potential immutability of ledger entries. Notably, this scenario is the formal equivalent to the existing literature that merely assumes that fraud prevention can be realized by distributed ledgers, thereby, constituting the reference case for the subsequent scenario assessment. However, the prevention of accounting fraud can only be expected, if every network participant acts according to the protocol and protocol assumptions, i.e. for instance, that the majority of participating nodes acts honest. Consequently, the emergence of accounting fraud is ultimately determined by the incentives that prevail within the intra-corporate network that defines the entities’ behavior. Moreover, these incentives must be weighted against the costs and benefits, which arise for network participants that do not behave according to the rules.

A comprehensive assessment of the previously described scenario requires an appropriate analytical framework. Game theoretic approaches are typically used to derive incentive-based strategies and to predict behavior of individuals within complex settings. Moreover, game theoretic approaches have been shown to be applicable and helpful for interaction analysis in distributed networks, such as for the prediction of cooperative or selfish behavior in autonomous and mobile ad hoc networks (e.g. Yu and Liu, 2008; Li and Shen, 2012). Given the robust results of, among others, Yu and Liu (2008) as well as Li and Shen (2012), a game theoretic approach is proposed for the developed scenario and the analysis of node behavior, given the respectively applied consensus mechanism. Despite this analysis of consensus mechanisms and the resulting network participant’s behavior that might or might not results in the conduction of accounting fraud, the general functioning of the decentralized consensus mechanisms is described in this chapter. Lastly, to answer RQ.4b it necessary to discuss, whether the analytical results found in the context of the proposed scenario are also robust to variations, such as hybrid or open peer-to-peer networks as well as to the extension of the scenario to a two or multiple firm setting that share a corporate ledger.
5.5.1 Game Theoretic Analysis Framework

A game theoretic setting is proposed for the analysis of the incentives and expected actions of the management and the internal controls system, whereas the latter is treated as one entity in the following. According to the case studies, the emergence of accounting fraud can be reduced to large parts to the interaction pattern between those two entities, which justifies the restriction of the following analysis to the responsive behavior of the management and the internal control system, respectively. Before the game theoretic analysis is conducted, first two general cases will be exemplified, showing, which dynamics between those two entities evolve that may explain the fraud patterns observed in the case studies. Subsequently, the set-up is used as an analysis framework for the later proposed distributed consensus mechanisms in order to investigate, whether the thereby induced incentives lead to the prevention of accounting fraud.

The following game theoretic approach includes the following three elements (Sieg, 2000):

- Amount N of players \{1, ..., N\}
- Amount Si of pure strategies \(s_1, ..., s_M\) for every player i, and
- Disbursement function \(u_i(s_i)\), which specify the payout of player i given a strategy combination \(s = (s_1, ..., s_M)\)

Given these elements and their possible combinations, in the following, it will be analyzed, which strategy combinations are most likely chosen by a player i (which is the management), whereas the solution may be explicit or may contains different combinations of strategies (Sieg, 2000).

5.5.1.1 Setting 1: Internal Control System versus a Selfish Management

The first setting consists of two players (N=2), whereas player 1 is the internal control system, which is taken as one entity and treated like acting solely on behalf of the company, excluding individual utility maximizing interests and behavior. Instead, the goal of the control system is profit maximization on behalf of the company. The second player is the management, which is assumed to be selfish, meaning that its goal is the maximization of its own pay-offs. Both players have two potential strategies: The internal control systems either conducts controls in order to guarantee the correctness of corporate transactions and financial statements or not. A lack of controls can be either intentional e.g. if the control entity receives a bonus provided by the management to convince the internal control system to assist in conducting fraud, as well as unintended, for instance, if the management exerts pressure on the internal control system, such that it does not report a detected fraud incident. The management can either behave according to the rules or it conducts accounting fraud.
The payoff matrix depicted in Table 22, is based on the following conditions. Costs arise from the conduction of controls for the company in terms of human capital costs amounting to 100 monetary units (MU). Thus, if controls are conducted and no fraud is detected, the company or the internal control system, respectively, experiences a loss of 100MU. Contrarily, if fraud is detected in the course of the controls the loss of MUs is less severe (50MU), since greater losses for the company could be prevented. Conducting no controls is costless as long as the manager behaves according to the rules, otherwise the company will experience a loss of 500MU, which is equal to the profit the management receives, when it conducts fraud without being detected. While the management is able to acquire 500MU, when fraud is not detected, detection of fraud will cost him 700MU. This accounts for the fact, that the loss of the management equals not only the 500MU he would get, if no controls where in place, but additionally the management will experience further penalties such as the loss of his job or the payment of fines, which is costly and amounts to further 200MU. If he does his job according to the rules he will get a salary of 100MU, irrespective of the fact whether or not the internal control systems monitors the correctness of corporate financial transactions and the resulting financial statements.

<table>
<thead>
<tr>
<th>Player 1</th>
<th>Controls (A₃_present)</th>
<th>No control (A₃_absent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud (C₁)</td>
<td>-700; -50</td>
<td>500; -500</td>
</tr>
<tr>
<td>Licit Behavior (C₁)</td>
<td>100; -100</td>
<td>100; 0</td>
</tr>
</tbody>
</table>

Table 22. Payoff matrix first setting: audit vs. selfish management

Based on the setting, no Nash equilibrium in pure strategies can be achieved. If player 1 exerts controls, the optimal decision for the second player is to behave according to the rules, whereas, when no controls are in place, it is optimal for the management to commit accounting fraud. In contrast, if the management conducts fraud, it would be optimal for the internal control system to control the correctness of transactions and financial statements, whereas otherwise not. Consequently, there can only be equilibrium in mixed strategies.

Mixed strategies $\sigma = (\sigma_1, ..., \sigma_M)$ are probability distributions over a amount of pure strategies $S_i = \{s_1, ..., s_M\}$ with $\Sigma_i$ displaying the space of all mixed strategies of player $i$. A mixed Nash equilibrium is the combination $\sigma^*$ of mixed strategies, if:
for all \( i \) and for all \( \sigma_i \in \Sigma_i \) (Sieg, 2000). In order to come to a solution, the features of this game will be exploited in the following, assuming that one player in a mixed Nash-equilibrium is always indifferent between his pure strategies, if the other player applies a mixed strategy.

For the proposed setting the solution to the mixed Nash equilibrium looks as follows: The manager is indifferent between the two pure strategies either to behave according to the rules or to conduct fraud. With probability \( y \), the internal control system will control the actions of the management as well as the correctness of financial transactions. Consequently, with probability \( y \) the management is not able to convince or to enforce the internal control system to assist in fraud as observed in the case studies. This will result either in a loss of 700 MU, when controls are conduct or a profit of 500 MU. Since \( 500 MU = 700 MU \times y \) holds always if \( y = 0,714 \), in the mixed Nash equilibrium roughly 72\% of all transactions must be controlled in order to provide no incentives for the management to conduct fraud. Similar, the internal control system is indifferent between exerting controls and conducting no controls, by relying on the correctness of transactions and financial statements, assuming that with probability \( x \) the management will behave according to the rules. If no controls are conducted the payoff for the internal control system will be \(-500 MU(1 - x)\), however, if controls are conducted, the payoff equals \(-50 MU \times x \). Thus the payoffs for the internal control system are equal, if \( x \) is roughly 91\%, meaning that 91\% of all transactions must be correct in order to create no incentives for the internal control entity to conduct controls.

### 5.5.1.2 Setting 2: Selfish Internal Auditor versus Selfish Management

Obviously, the previous setting sets limited incentives for managers to conduct fraud, which is in contrast to the observed case studies. Thus, in the following the internal control entity is dissolved and treated as an individual person (here exemplary as individual internal auditor) that might not want to maximize the firms profit but instead his own welfare. Notably, this is in line with the case studies, where typically single persons were responsible for the conduction of fraud. The payoffs in this setting depicted in Table 23, will be as follows. The individual auditor receives salary from his auditing activities in the amount of 50MUs, irrespective whether he detects fraud or not. If he does not control transactions and financial statements and there are no fraudulent activities he will as well receive his regular salary. However, in accordance to the case studies, it will be assumed that the individual auditor may be bribed in order to assist in accounting fraud, which results in a payoff of 100 MU, given that monetary remuneration is assumed. If the management behaves according to the rules, he or she will get his salary that is higher than those of the auditor amounting to 100 MU, irrespective whether his
actions and the associated corporate transactions are controlled or not. If the manage-
ment conducts fraud and accounting fraud is detected, it will experience a loss of
700MU, such as in the first setting. However his payoff in the case of non-detected
fraud will now be less, assuming that the management needs to bribe the individual au-
ditor to assist him in fraud in the amount of 100MU. Thus, it is assumed that conducting
fraud is costly.

<table>
<thead>
<tr>
<th>Player 1</th>
<th>Controls (A₃ₚرزєst)</th>
<th>No control (A₃ₜₜєnt)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud (C₁)</td>
<td>-700; 50</td>
<td>400; 150</td>
</tr>
<tr>
<td>Licit Behavior (C₁)</td>
<td>100; 50</td>
<td>100; 50</td>
</tr>
</tbody>
</table>

Table 23. Payoff matrix second setting: selfish auditor vs. selfish management

Given this payoff matrix two Nash equilibriums are observable, which are first, con-
ducting controls and behave according to the rules as well as, second, conduct fraud and
assist in fraud, i.e. conduct no controls. However, the Pareto-optimal Nash equilibrium
is the combination ‘conduct fraud’ and ‘assist in fraud’, given the fact that both players
are better of compared to the other equilibrium. Therefore, most likely accounting fraud
will be conducted by building coalitions or an alliance, which is in accordance to the
fraud patterns observed in the conducted case studies. Moreover, since the provided
analysis framework helps to explain the behavior observed in the case studies, in the
following distributed consensus mechanisms and their ability to prevent fraud in the
propose scenario of blockchain-based accounting, will be analyzed with the help of the
second game theoretic setting, by putting a special focus on the possibly changing in-
centives for the management as well as the internal control system.

5.5.2 Does Incentives Set by Distributed Ledgers Prevent the
Commitment of Accounting Fraud?

Given the proposed scenario and the game theoretic analysis framework, in the follow-
ing, the ability of proof-of-work as well as of alternative distributed consensus mecha-
nisms to prevent accounting fraud will be investigated. Therefore, first the functioning
of the respective consensus mechanism is explained and, subsequently, directly or indi-
rectly applied to the analysis framework in the context of the proposed optimal scenario.
5.5.2.1 Proof-of-Work

Proof-of-work is a mechanism that was originally proposed by Dwork and Naor (1993) to increase the costs of emailing, such that spamming is no longer economically feasible. The rational behind this approach was to require an email sender to compute some moderately hard, but not intractable function of the message and some additional information in order to gain access to the resource, thus preventing frivolous use (Dwork and Naor, 1993). Today, the mechanism is used for various other purposes and was most recently applied in the case of Bitcoin and other cryptocurrencies, to secure data entries on the underlying blockchain together with cryptographic techniques and other technical security features.

The use of proof-of-work in the context of blockchains or distributed ledgers was already described and was generally defined as a mechanism to rationing resource access in client-server relationships, consisting of solving a mathematical puzzle by using computer power (Becker et al., 2013). Particularly, Proof-of-Work consists in finding a byte string, called nonce that combined with the block header, results in a cryptographic hash with a given number of leading zero bits. More formally, proof-of-work can be described according to Decker, Seidel and Wattenhofer (2016) as follows:

The function $F(d, c, x) \rightarrow \{true, false\}$ is a proof-of-work function, whereas $d$ is a positive number and $c$ and $x$ are bit-strings. The following properties apply to this function:

1) $F(d, c, x)$ is fast to compute if $d$, $c$ and $x$ are given, and
2) for fixed parameters $d$ and $c$, finding $x$ so that $F(d, c, x) = true$ using a unit-resource is distributed with $exp\left(\frac{1}{d}\right)$, meaning that finding that value is computational hard but feasible.

In the following the parameter $d$, $c$ and $x$ are referred to as difficulty, challenge, and nonce, respectively. The proof-of-work mechanism works consequently, by first issuing a difficulty/challenge-pair $(d, c)$. A nonce, for which $F(d, c, x) = true$, is then called proof-of-work for $(d, c)$. However, finding the nonce requires computational power, which changes with difficulty$^2$ that is adjusted between consecutive $(d, c)$ pairs, such that the expected time for any resource to find PoW is some constant (Decker, Seidel and Wattenhofer, 2016). More precisely, the difficulty to find Proof-of-work that validates a block changes after every 2,016 blocks, while adjustments are made based on the peers efficiency to find proof-of-work according to the following formula (Narayanan et al., 2016):

$$next \, difficulty = \frac{previous \, difficulty \times 2016 \times 10 \, minutes}{time \, to \, mine \, last \, 2016 \, blocks}.$$
A block then has the form \( b = (h, d, p, x) \), where \( h \) is the hash value, \( d \) is again the difficulty, \( x \) is a bit-string and \( p \) is a peer, whereas \( p \in P \), and \( P \) is the set of peer that join the network (Decker, Seidel and Wattenhofer, 2016). A block contains all transactions, which have been committed on the previous block. Finding a nonce, can only be done by calculating the hash \( h \) of the block by using the hash function \( H \) for all possible nonces (Decker and Wattenhofer, 2013). In addition, each block references to the preceding block, which hash has to be known, meaning that blockchains represent consensus over the history of data stored on the blockchain. The history is considered as true, when it deploys the longest chains, conforming to the exertion of the most power exertion (Pilkington, 2016). More formally, the blockchain can be described by a sequence of \( C = (b_1, ..., b_n) \) of blocks, and a genesis block \( b_0 \) that is fixed in advance.

For each block \( i \geq 1 \), block \( b_i = (h, d, p, x) \) is said to be valid if

\[
    h = H(b_{i-1}), \text{and} \]

\[ F(d, (h, p), x) = \text{true}, \]

i.e. the hash in \( b_i \) is obtained from \( b_{i-1} \) and \( b_i \) is a Proof-of-Work. Thus, for a valid block \( b_i, b_{i-1} \) is the parent block. A blockchain is then valid and considered as truth, if every non-genesis block is valid (Decker, Seidel and Wattenhofer, 2016).

If someone wants to revert or alternate existing blocks of the blockchain, an alternative reality must be created (blockchain fork), which occurs if not all nodes agree on the same blockchain header (Decker and Wattenhofer, 2013). The blockchain fork will only be accepted, if it becomes longer than the already existing blockchain, which implies the exertion of a huge amount of computer power, starting from the point that should be altered. Thus, attackers can use their network power to change the entries stored on the blockchain (51% attack), which requires not only the majority of computational power but also faster data processing than the rest of the network (Narayanan et al., 2016; Pilkington, 2016). However, there may be circumstances, in which a fork is desirable, for instance, if protocol rules must be changed.

### 5.5.2.2 Effect of Proof-of-Work on the Incentive to Conduct Fraud

The rational behind using proof-of-work to prevent accounting fraud is that rewriting the history of transactional data is costly, since it requires the exertion of computer power. In terms of the game theoretic framework, to prevent accounting fraud incidents, the payoffs must consequently change, such that only one Nash-equilibrium remains that is conducting controls as well as behave according to the rules. However, this can only be achieved, if the costs of acquiring computer power would be prohibitively high, such that the profit in case of non-detection is lower than the expected payoff in case of behavior in conformance to the protocol rules. For instance, if the costs of acquiring the
majority of computer power in the proposed second setting would be set to the arbitrary amount of 350MU, while holding everything else constant, the payoffs would change as presented in Table 24. In particular, in case of detection of illicit behavior the loss of the management will increase up to -1050MU, whereas in case of no detection, its profit equals now only 50MU. In this setting the management has never an incentive to conduct fraud, while the control entity will never conduct controls, anticipating that the management has now an incentive to behave according to the protocol rules.

<table>
<thead>
<tr>
<th>Player 1</th>
<th>Controls ((A_3^{\text{present}}))</th>
<th>No control ((A_3^{\text{absent}}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud ((C_1))</td>
<td>-1050; 50</td>
<td>50; 150</td>
</tr>
<tr>
<td>Licit Behavior ((C_1))</td>
<td>100; 50</td>
<td>100; 100</td>
</tr>
</tbody>
</table>

Table 24. Payoff matrix second setting with high costs

Two implications can be derived from Table 24 that is, first, no entity, which is responsible for the validation and the maintenance of a intra-corporate blockchain is assumed to be able to acquire the majority of network power and, second, that any combination of entities that are responsible for validation and maintenance is assumed to be not able to acquire the majority of computer power. Consequently, the management is supposed to have neither the monetary capability nor the power to build coalitions to conduct accounting fraud in the proposed scenario and given the applied game theoretic framework. Unfortunately, already the first assumption (which also underlies the majority of considerations made in the mentioned literature that proposes blockchain-based accounting) is questionable, which holds, especially, when applying intra-corporate solutions.

The first objection refers to the fact that the smaller the peer-to-peer network is, the easier it gets for the management to conduct fraud by reaching the majority of computer power. Moreover, the increasing efficiency of computers indicates that obtaining a lot of computer power is not as expensive as assumed in the above stated setting. Additionally, other mechanisms than computer power mining can be used that may be cheaper. For instance, instead of validating and maintaining the blockchain through the exertion of computer power, graphic cards can be used to run many types of computation more quickly than relying solely on the computer power available on general-purpose computers (Narayanan et al., 2016). Given the remaining hierarchical basic structure of the corporation – since only decision-making in the realm of financial transactions is distributed across the defined entities - the management is, therefore, able to deliberately
reach the majority of computer power by just using a more powerful computer than everyone else in the network. Because of its predominant position in the corporation, the management can, consequently create a network, in which it has the most powerful vote within the consensus process and decides, which transactions are incorporated into the blockchain as well as which ledger entries may be altered or even deleted ex post (Rückeshäuser, 2017b). Overall, accounting fraud appears to be even easier as well as cheaper in the proposed scenario of blockchain-based accounting, as ex post alterations and illicit transactions can be conducted at the management’s will, without the need to convince, enforce or circumventing internal controls as well as technical barriers in any conceivable way.

If the management is able to acquire the majority of computer power in small networks by itself, of course the second implication is void. However, the second objection refers to the fact that, even if the management is not able to acquire the necessary computer power by itself, there is no comprehensible reason, why coalitions should be hindered by a blockchain-based accounting system. Especially, if a coalition of the management and internal audit is able to alter ledger entries ex post without leaving any traces in the system, the incentives to conduct fraud are higher in the scenario of blockchain-based accounting than in accounting system that do not rely on distributed ledger technology, as concealment of fraud is easily possible. Furthermore, if the perpetrators of fraud create an alternative history of transactions, this blockchain will be accepted as the correct one. Consequently, external auditors and all other direct and indirect control entities must rely on the falsified blockchain and have no chance to detect fraud. In this case, transparency of financial information is useless, as retrospective fraud detection mechanisms that are conducted through external auditors are ineffective and, subsequently, also the indirect control functions of investors or exchange market participants, which rely on disclosed and allegedly external audited financial information.

Using proof-of-work as decentralized consensus mechanism in the proposed scenario of blockchain-based accounting, will, therefore, not impede accounting fraud, neither from an organizational perspective, through the decentralization of consensus finding, nor through immutability of data or transparency, i.e. due to technical security measures. Notably, proof-of-work would even ease the override of internal controls, as the management does not need to convince others to support and conceal fraud, such as frequently observed in the analyzed case studies of accounting fraud incidents. This, especially, holds in the absence of direct monetary incentives that encourage honest behavior, such as in the case of Bitcoin. Some authors, therefore proposed that the risk of ex post blockchain alterations can be reduced using modified Proof-of-Work versions, such as two-phases Proof-of-Work (2P-PoW) (King and Nadal, 2012; Bastiaan, 2015; Bonneau et al., 2015). However, the ability of an entity to change data on the block-
chain is heavily determined by previous blockchain design decisions, leading to the fact that a change of the underlying consensus mechanism possibly has only minor effects on the security and correctness of financial data on the blockchain, if a intra-corporate setting is supposed.

5.5.3 Analysis of Further Decentralized Consensus Mechanisms

Table 25 provides an overview over further decentralized consensus mechanisms developed after the emergence of proof-of-work. For the sake of completeness proof-of-work-based consensus is also included in the table. A differentiation of the distributed consensus mechanisms is conducted according to their ability to allow for permissionless or permissioned access of nodes on the network as well as whether the mechanisms facilitate decentralized validation or not. This differentiation is done in accordance to the second layer of the blockchain customization model presented in the previous chapter of this thesis.

<table>
<thead>
<tr>
<th>Decentralized Validation</th>
<th>Public Distributed Ledger</th>
<th>Private Distributed Ledger</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Proof-of-Work (PoW)</td>
<td>• Proof-of-Work (PoW)</td>
</tr>
<tr>
<td></td>
<td>• Proof-of-Stake (PoS)</td>
<td>• Proof-of-Stake (PoS)</td>
</tr>
<tr>
<td></td>
<td>• Proof-of-Work Based Derivatives</td>
<td>• Delegated Proof-of-Stake</td>
</tr>
<tr>
<td></td>
<td>• Federated Byzantines Agreement</td>
<td>• Proof-of-Work Based Derivatives</td>
</tr>
<tr>
<td>Centralized Validation</td>
<td>• Delegated Proof-of-Stake</td>
<td>• Redundant Byzantines Fault Tolerance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RAFT Consensus and Derivatives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Paxos</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ripple Consensus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bilateral Node-to-Node Consensus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delegated Proof-of-Stake</td>
</tr>
</tbody>
</table>

Table 25. Overview of distributed consensus mechanisms

As apparent from the table, certain distributed consensus mechanisms enable both permissioned as well as permissionless access, although they were initially designed to be used in a permissionless system. Contrarily, it is assumed that a mechanism, by intention, will not feature decentralized validation and centralized validation at the same
time. However, it is acknowledged that in practice, decentralized validation may exhibit centrality tendencies as it can be observed for example in the case of Bitcoin, where powerful mining pools potentially could control the network. In the following, the ability of decentralized consensus mechanisms to prevent accounting fraud will be analyzed, if they feature permissioned access as well as decentralized validation and, therefore, fit to the proposed scenario of blockchain-based accounting.

5.5.3.1 Proof-of-Stake

Proof-of-stake (PoS) is proposed as a solution to the problem that proof-of-work’s dependence on energy consumption creates unnecessary cost overhead, which is mainly borne by network participants in form of inflation and transaction fees. The assumption behind proof-of-stake is that the security of a blockchain must not depend on energy consumption, but rather on a form of proof-of-ownership, which is equivalent to the coin age consumed by an transaction, whereas coin age is defined as currency amount times the holding period (King and Nadal, 2012). In order to apply proof-of-stake, however, the blockchain must be modified, meaning that blocks are separated into different types, which are proof-of-work blocks on the one hand, and proof-of-stake blocks on the other hand. The latter includes a special transaction, which is called ‘coinstake’, wherein a block owner pays himself, thereby, consuming his coin age, while gaining privilege of generating blocks for the network and the permission to mint for proof-of-stake. The first input of the coinstake is called ‘kernel’ and is required to meet a certain hash target protocol, which renders the generation of proof-of-stake blocks to a stochastic process. Moreover, the hash target that the stake kernel need to meet, is a target per unit of coin age (coin-day), meaning that in contrast to proof-of-work the target is not a fixed value applied to every node (King and Nadal, 2012). Thus, instead of using relative hash rates of miners for network stability, the protocol splits blocks and the according transactions proportionally to the current wealth of miners (Pilkington, 2016). As a consequence, the more coin age is consumed in the kernel, the easier it is to meet the hash target protocol and the blockchain, where the highest total consumed coin age is chosen as the main chain (King and Nadal, 2012).

The expected main advantage of proof-of-stake compared to proof-of-work is that the costs of acquiring the necessary amount of network stake might be higher than acquiring the majority of network power, whereby the system is expected to be more secure, at least in regard to 51%-attacks. Accordingly, attacks in a proof-of-stake based consensus system are assumed to be more expensive than using a proof-of-work powered blockchain. Nevertheless, the concrete design of such a system in the proposed closed scenario requires that stakes in the system are most likely stocks (Rückeshäuser, 2017b). Actually, this assumption is in accordance to the rational underlying proof-of-
stake empowered cryptocurrency systems, which are expected to be secure, since nodes possessing the most stakes in the system, i.e. possess the majority of coins, do not have an incentive to threat the network security, since a network breakdown could result in the total destruction of all monetary values. Similar, at a first glance, the management or other stock holder should not have an incentive to damage a corporation by conducting fraudulent activities, which will possibly lead to a sensitive stock drop in case of detection. Consequently, in the sense of the game theoretic approach, the costs of committing fraud would be prohibitively high and potentially lead to a loss of all monetary values through a network breakdown.

In the proposed scenario and in accordance to the case studies (e.g. in the case of Comroad (Dorin, 2006)) the management is assumed to have the majority of stocks. However, if this is the case in proof-of-stake based accounting systems, the management would be enabled to change financial transaction entries at will, without having to respect or circumvent any control systems. Thus, despite proof-of-stake is initially designed to promote decentralized validation, in practice, the validation of transactions using this mechanism will be centralized and most likely dominated by the management. Consequently, looking at the concrete application of proof-of-stake in the proposed scenario, significant similarities get obvious with respect to the scenario proposing a proof-of-work based accounting system. First of all, receiving a considerable amount of stake may be costly but not difficult for the management and may happen anyway, for instance, if stock-based incentive systems are used to align shareholder interests with management interests. However, even in the case that the management is not able to acquire the majority of stocks, again, no mechanism prevents coalition building in the proof-of-stake based accounting system.

Consequently, the same conclusion can be drawn from the proof-of-stake empowered accounting information systems as from the former analyzed proof-of-work based system: Given the proposed scenario, conducting fraud by overriding internal controls gets easier, while external controls as well as other control entities are getting ineffective, since they must rely on the blockchain, which constitutes the ‘correct’ history of transactions. Lastly, the proof-of-stake protocol exhibits other general security issues, such as the possibility for so-called “nothing at stake” attacks (King and Nadal, 2012). More precisely, this means that an attacker can simply save up enough coin age to become the node with the highest stake, which can be subsequently used to fork the blockchain and to create an alternative history. After the attacker performed this attack, a second attack would require saving up coin age again, as the stake resets as soon as the alternative block was generated. However, performing a ‘nothing-at-stake’ attack would probably devalue the whole system, which makes the incentive for such attacks unclear (Vasin, 2017).
5.5.3.2 Delegated Proof-of-Stake

Delegated proof-of-stake (D-PoS) is a modified form of the previous describes proof-of-stake protocol, where stakeholders can select any number of witnesses, i.e. nodes that validate signatures and timestamp transactions, to generate blocks. Despite this implies some form of centrality, it is assumed that the number of witnesses is defined in such a way that at least 50 percent of voting stakeholders believe there is a sufficient decentralization (Bitshares, 2017). Witnesses subsequently produce a block and receive a reward for their activities, which sets the incentive to provide services similar to a trusted third-party. So-called delegates, who decide, among others, about the amount of payments to witnesses but also about transaction fees, block sizes as well as block intervals, can change network parameters. Thereby, delegates become co-signers of a special account, known as the genesis account, and are privileged to propose changes to the protocol, after have been elected by shareholders in a similar manner as witnesses. The purpose of the design of delegated proof-of-stake is to ensure that delegates technically have no direct power to change the network parameters in the underlying protocol, since stakeholders ultimately approve these changes (Bitscan, 2016; Bitshares, 2017).

Given the analyses of the previous decentralized consensus mechanisms, it is obvious that such a system is by no means suited as consensus mechanism in the proposed scenario and is not able to prevent accounting fraud. Especially, if every stakeholder has influence that is directly proportional to their stake (Bitshares, 2017), it is very easy for a powerful management to chose a witness that will act in the management’s interest with very high probability. As this mechanism is a form of approval voting, of course, any type of strategic voting can be applied, which does not exclude the emergence of accounting fraud. In contrast, as the management is not able to validate transactions directly, at least, it cannot override the internal control systems without convincing or enforcing other network participants. Notably, this is an advantage compared to simple proof-of-stake as well as proof-of-work consensus, where the management can potentially, deliberately conduct fraud without the need to care about other network participants. However, at the end, the mechanism implied by delegated proof-of-stake resemble the distribution of responsibilities in a classical, hierarchical organizational structure, where the management is able to delegate certain business activities to particular business divisions and, thereby, potentially makes an impact on the division’s work.

Given the fact that delegated proof-of-stake seems not to imply any core advantage compared to a system without a blockchain based accounting system, the costs for implementation and learning, however, are certainly too high for a company, such that the implementation of an accounting system based on delegated proof-of-stake seems to be unlikely.
5.5.3.3 Proof-of-Activity

Proof-of-activity (PoA) is a combination of proof-of-work and proof-of-stake consensus, developed to mitigate the risks implied by both decentralized consensus mechanisms, i.e. 51% hash-rate attacks. The underlying rational of proof-of-activity is that proof-of-work does, obviously, not set the right economic incentives for nodes to be in charge of network security, whereas in the case of proof-of-stake consensus, other risks emerge from centralization tendencies, e.g. when stakeholders try to exhibit control over the system. To alleviate these risks, the proof-of-activity protocol is designed as an extension of the Bitcoin proof-of-work consensus mechanism, while introducing more complex verification compared to the original protocol and the requirement for increased communication between the respective nodes (Bentov et al., 2014).

Finding consensus by using proof-of-activity consists of the transformation of a pseudorandom value into a satoshi, which is the smallest unit of the cryptocurrency Bitcoin. According to Bentov et al. (2014), this is done by selecting a pseudorandom index between zero and the total number of satoshis in existence, up to the last block, inspecting the block in which this satoshi was minted and following each transaction that subsequently transferred this satoshi to an address, until reaching the address that currently controls this satoshi. In particular, using proof-of-activity consensus, each miner has the hash-power to try to generate an empty block header, whereas this header does not reference any concrete transaction. If a miner was able to generate an empty header, the block is broadcasted to the network. The remaining network nodes regard this block header as data that deterministically derives N pseudorandom stakeholders, by concatenating the block’s hash with previous blocks’ hashes and with N fixed suffix values. Afterwards each of those combinations are hashed and ‘follow-the-satoshi’ is invoked with each to the N hashes used as an input (Bentov et al., 2014). Every stakeholder that is online checks whether this empty block is valid. If the block is valid, stakeholder check also whether they are one of the N lucky stakeholders of this block, then sign the empty block header with the private key that controls their derived satoshi and broadcast the signature to the network. When the Nth stakeholder observes that the block derives him or her, a wrapped block is created that contains, among others, all transactions that the Nth node wants to include. The wrapped node is, subsequently, broadcasted to the network, where other nodes find consensus about whether the block is a legitimate extension to the existing blockchain. For incentivizing, nodes receive a fee from transactions that the Nth node collected and that is shared between the miner and the N lucky nodes, derived by the block. However, only active stakeholders, who maintain an online node, get rewarded in exchange for the services they provide for the network (Bentov et al., 2014).

Reward that is only granted to active nodes should prevent the problems present in the
proof-of-stake protocol, namely that offline stakes can accumulate weight in terms of coin age over time, which are, ultimately, able to utilize their hash-power to conduct a network attack. However, there exist also significant similarities to the proof-of-stake consensus that mainly refer to the process of stakeholder picking. Particularly, picking a pseudorandom stakeholder and giving stakeholders voting power relative to their accumulated weight, leads to similar problems as in the case of proof-of-stake and delegated proof-of-stake. For instance, as Bentov et al. (2014) emphasized, if the underlying protocol is proof-of-stake and there are two groups of stakeholders, whereas one group behaves honest and controls 80 percent of the stake and the other group behaves malicious and controls 20 percent of the stake, then picking a pseudorandom stakeholder by using proof-of-activity implies that the malicious group is picked 20 percent of the times, which is equivalent to possessing 20 percent of voting power.

Thus, despite the proof-of-activity protocol shows some advantages compared to proof-of-work as well as proof-of-stake consensus, i.e. incentives for maintaining full online nodes as well as more efficient energy usage, the basic problem of the threat of 51% attacks and the ability of powerful groups within the network to reach the majority of the hash-rate easily, is neither eliminated nor diminished. Moreover, general security issues remain as in the case of the proof-of-stake protocol, e.g. the threat of “nothing-at-stake”-attacks, where rational stakeholders can maximize their expected reward by signing every forked branch (Bentov et al., 2014). Therefore, it must be concluded that the proof-of-activity consensus protocol does not guarantee fraud resistance within an intra-corporate blockchain based accounting system.

5.5.3.4 Further Proof-of-Work Based Derivatives

For the sake of completeness it should be mentioned that there exist further decentralized consensus mechanisms, such as proof-of-capacity or proof-of-burn that are based on, or are related to proof-of-work consensus. For instance, proof-of-capacity is based on the idea that mining is only possible by allocating a sufficient amount of volume of hard drive space. In contrast, proof-of-burn builds on the rational to ‘burn’ coins instead of electricity, by sending coins to an address where they cannot be redeemed. By this, a node get the permission to mine for a lifetime, which is actually a lottery between the owners of burnt coins (Patterson, 2015). However, even if these approaches do not consume energy, they destroy other resources that are money as well as storage capacity, which, of course, can be hardly reconciled with general corporate objectives. Consequently, these consensus mechanisms are rarely discussed in a scientific context as well as an underlying consensus mechanism for concrete distributed ledger applications.
5.5.3.5 Federated Byzantines Agreement

Federated Byzantines Agreement allows each node to select a set of other trusted nodes, which induces so-called flexible trust, meaning that all users have the freedom to trust any combination of parties to find consensus. More precisely, nodes agree on slot contents, whereas a node \( v \) can apply an update \( x \) in slot \( i \), when it has safely applied updates in all slots upon which \( i \) depends and, additionally, believes that all correct functioning nodes will eventually agree on the update \( x \) for slot \( i \). Moreover, it is assumed that a node \( v \) externalizes the update, thus may react to \( x \) in an irreversible way, such that a node cannot change his vote later. Voting or the agreement on updates is reached through quorum slices, which accounts for the fact that traditional majority voting would open up the opportunity that malicious node join the network many times, thereby, out-numbering honest nodes. Thus quorums are determined in a decentralized way, since each node selects his own quorum slice, whereas quorums are defined as the set of nodes sufficient to reach agreement and quorums slices are the subset of the quorum, sufficient to convince one particular node of agreement. Nodes may select their quorum slice based on arbitrarily criteria such as reputation (Mazières, 2016).

To find consensus, a node waits for the vast majority of the quorum slice set to agree on a transaction before considering the transaction to be settled. In turn, those nodes do not agree to the transaction until the participants they consider as important agree to the transaction, and so on. Eventually, if enough network nodes accept a transaction, it becomes infeasible for an attacker to roll it back. However, safety, meaning that given a set of nodes, no two of them ever externalize different values for the same slot, can only be guaranteed, if nodes choose their quorum slices correctly. Nevertheless, even if it is assumed that the quorum slice is chosen correctly, safety alone does not rule out other security issues especially, those related to federate voting systems (Mazières, 2016). In particular, federated byzantine agreements shows similar vulnerabilities as every other federated voting system and, especially, if voting nodes are known to each other in a closed system. The major problem arising from the federated voting system is that strategic voting cannot be excluded. Thus, in the context of the proposed scenario of blockchain-based accounting, it may be easy for the management to couple votes of particular nodes and their influence on other nodes to career perspectives and/or monetary or non-monetary incentives, leading to a strong influence of the management on the voting outcome and data that will be incorporated on the blockchain. Moreover, the management may also be able to influence the majority of nodes to, subsequently, alter data on the blockchain, in order to cover up traces of possible accounting fraud attempts. Similar to proof-of-stake and delegate proof-of-stake consensus, the management is not able to outvote the remaining votes alone, however, the ability to influence others is still present and no mechanisms are in place that prevent accounting fraud through joint co-
5.5.4 Discussion: Transferability of the Results and Other Solutions

The proposed scenario led to very clear results concerning the ability of distributed ledger technology to prevent accounting fraud. Obviously, the features transparency and decentralization are not sufficient to avoid the emergence of ex ante as well as ex post accounting fraud, conducted by or on behalf of the management. More precisely, the management is expected to be able to offset the possible positive effects that result from decentralized decision making by either centralize the decision making process, i.e. if the management has the capability or majority of the resources necessary to receive the majority of voting rights, or by convincing or enforcing others to vote in the interest of the management. So far, however, these results are limited to the proposed scenario and given the assumption that the management is the perpetrator of fraud by overriding internal controls for conduction and concealment of illicit behavior. Given this limitation it is questionable, whether and if so, how these results are transferable to modified or other scenarios of distributed ledger based accounting, which implies the question, how much generality can be awarded to the findings. Given these issues, three modifications for the scenario should be discussed that may threatens the universality of the results.

First, modifications of the entities that constitute the consensus participants are conceivable. For instance, one can argue that the goal of the prevention of accounting fraud is shareholder value protection and, therefore, shareholders should be included in the consensus process as they are the actual owners of the firm. Notably, shareholder should have an interest in protecting their own money via participation on consensus finding and proofing the correctness of transactions. Especially, shareholder could have a greater incentive to protect the value of the firm compared to the control entity even though the internal control system is initially responsible for the prevention of fraud. This would imply that at least the majority of shareholders could be expected to behave honest and according to the rules, enforced by the respectively applied consensus mechanism.

While this is, again, the optimal or desired behavior, it must be assumed that rational acting individuals might not act as described previously, if short-term profits are achievable. Thus, accounting fraud might emerge, even though shareholders are included into the consensus processes. In particular, this opportunity must be taken into consideration given investigations of shareholder behavior, testing the trade-off between liquidity and monitoring functions conducted by shareholders, whereas liquidity means that the ability to speculate with stocks potentially decreases the incentives to intervene and improve a companies performance (e.g. Kahn and Winton (1998), Maug (1998), Almazan, Hartzell and Starks (2005) as well as Klein and Zur (2009)). In the case of the
distributed ledger based accounting systems, this means that shareholder involved in the consensus process might accept illicit transactions or ex post alteration, if this increases their own utility. Consequently, shareholder may try to benefit form short-term stock increases resulting from accounting data manipulations, to unload their stock on the market shortly after. Certainly, such a behavior is related to liability in the sense that exploitation of short term stock increases may depends on whether or not shareholders are liable for their voting behavior within the consensus finding process. However, liability for shareholders in a distributed ledger accounting system is hardly conceivable, when considering large companies with thousands of minor shareholders that would be enforced to be fully informed about all conducted corporate transactions. Consequently, the incorporation of shareholders as consensus participants in the distributed ledger based accounting system seems to be neither practically nor feasible, given the far reaching consequences and responsibilities for shareholders that possible strive for mere passive investment opportunities.

A second concern of the proposed scenario is its restriction to a intra-corporate ledger and the associated strictly permissioned peer-to-peer network. Notably, one might argue that this is in contrast to the intended effect of decentralization, since the restriction of consensus participants already implies a high probability for centralization of transaction validation. However, a network without any restrictions with respect to network access as well as transparency is not conceivable, given the sensible nature of corporate financial data. This holds, especially, when assuming that transparency of financial data is provided by one corporation but not from a competing corporation. The competing corporation could then use the information provided by the other firm for their own benefit, i.e. by analyzing business relationships or making competitive offers to the respective business partners, which would possibly threatens the corporation, which employs the transparent accounting ledger.

An alternative to the two previously described extreme scenarios is a blockchain based accounting system that is shared by two or more corporations that exert mutual controls of the transaction records. Notably, this scenario was proposed by Andersen (2016), whereas the underlying rational for the expectation of fraud reduction is that each firm can be sure that a competing firm will declare fraud once detected. However, similar to the analytical results previously presented in this chapter, in this scenario there exist no proper mechanisms that prevents the companies from cooperation. Indeed, if corporations want to conduct fraud, decentralized consensus will not prevent them from establishing cooperation for the joint conduction of accounting fraud.

Eventually, additional mechanisms might be employed that are intended to increase security and integrity of ledger entries. A possible mechanisms to prevent data manipulations through ex post manipulations is, for instance, partitioning (Croman et al.,
2016). Thereby, the blockchain or distributed ledger is partitioned into smaller chunks, whereas one part is stored on a centralized, secure storage location (where ledger entry alterations should not be feasible anymore), and the other part of the chain is used as foundation for further validation activities. However, while the stored part may be secured and not prone to changes, alteration of the blockchain in use may be easier to conduct, especially, directly after the partitioning and given the fewer resources or effort that is contained in the remaining chain. Despite security issues, however, this approach also implies that a centralized storage location is used, which is actually in contrast to the decentralized approach of the blockchain.

Given these considerations, overall, it is assumed that the results received from the simple scenario proposed in this thesis are transferable to other settings. Whether or not distributed ledger technology is able to prevent accounting fraud in general, cannot stated with certainty. However, the analysis and subsequent discussion suggest that at the end, the determining factors are, whether the management has the capability and the resources to have the majority of voting rights within the consensus finding process or is capable of convincing or enforcing other entities and consensus participants to vote in the management’s interest. Notably, this was not prevented by the analyzed distributed consensus mechanisms.

5.6 Concluding Remarks

The assessment of different distributed consensus mechanisms in the proposed scenario of distributed ledger based accounting leads to the conclusion that distributed ledger based accounting and, more precisely, accounting based on blockchains, will not prevent the emergence of accounting fraud. In particular, all analyzed decentralized consensus mechanisms that are applicable to the propose scenario do not prevent the management from conducting fraud either by themselves, e.g. by acquiring the majority of resources in a network or trough cooperation, i.e. by convincing or enforcing control entities to conduct fraud jointly or to tolerate fraudulent activities. Moreover, the subsequently conducted debate on the transferability of these results showed that, even if the scenario is modified, accounting fraud is probably not prevented.

Notably, there exist other possible solutions in order to prevent accounting fraud as well as further issues related to the blockchain based accounting system. For instance, partitioning of the blockchain would not only increase the speed of validation, since the blockchain would be shortened, but also would prevent single entities from changing ledger entries on the centrally stored part of the blockchain. However, on the other side this probably reduces the effort necessary to change ledger entries on the chain, given the short blockchain that is actually in use, provided that a resource based approach is
employ. Nevertheless, as already indicated, such approaches require to store the partitioned part of the blockchain on a central and secure storage location, which is in contrast to the initial attempt to employ a decentralized, blockchain based accounting information system.

It is, furthermore, worth noticing that the proposed scenario and the inability of decentralized consensus to prevent accounting fraud, merely refers to malicious behavior of nodes within the blockchain based accounting system. What is not discussed and potentially also not avoidable, is accounting fraud that happens outside of the system. An example for such fraudulent behavior is the creation of, for instance, documents or invoices for business partners or of business events that never exist or happened in reality. However, it is generally questionable, whether any information system is capable of preventing non-systemic fraud, especially, if not all business processes and the associated business activities, such as payments, are completely digitalized.

**Key Points Chapter 5:**

- The proposed scenario of blockchain based accounting raises expectations that accounting fraud is prevented through organization restructuring and the associated compliance-by-design approach.
- Ultimately, the ability to prevent accounting fraud is determined by the fact, whether or not the protocol sets appropriate incentives for nodes to behave according to the rules.
- Currently, there exist no mechanism that prevents nodes from exploiting the protocol characteristics for their own benefits, i.e. conduct accounting fraud. Consequently, accounting fraud is possible using blockchains.
- Accounting fraud by internal override of controls is even facilitated through distributed ledgers, at least given the investigated distributed consensus mechanisms and the proposed scenario.
- Fraud prevention might be possible or enhanced by applying additional security mechanisms, however, most of them imply centralization.
6 Conclusion and Outlook

The findings of this doctoral thesis appear to be somewhat pessimistic. The application of distributed ledger technology in the realm of accounting does not lead to the desired effects and the prevention of accounting fraud. What does this mean for the future of distributed ledger technology? First and foremost, this thesis is not a proposal to abandon the idea to implement and apply distributed ledger technology in the context of a business environment to facilitate business activities as well as processes. In contrast, this thesis seeks to bridge the gap between strict advocates of distributed ledger technology and opponents, by stressing the importance for comprehensive analysis of possible applications. In particular, both, investigations that focus solely on the technical details in contrast to investigations that care merely about existing as well as possible future applications, without considering the concrete implementation and adjustment processes in regard to organizational structures as well as individual behavior, should be avoided. To achieve a fair assessment of the potentials and suitability of distributed ledger technology for a particular use case, the implementation process as well as trade-offs implied by implementations of the technology must be considered. Eventually, challenges for corporations that need to balance these costs against potential benefits must be taken into account, if proposed distributed ledger applications should not only be theoretically advantageous, but also beneficial from a corporate perspective.

6.1 Main Findings and Discussion of the Results

In the following, the main findings of this thesis will be emphasized and discussed.

i. The unleashing of the potentials of distributed ledgers and, especially the degree of disruptiveness, are hard to predict and will depend on the business strategy as well as the applied business models.

A lot of works consider distributed ledger technology as highly disruptive and as ‘game-changer’ in various industries. This assumption is mainly based on the expectation that the features of the technology that are, particularly, decentrality and transparency, will lead to the replacement of existing business models, which ultimately results in significant transaction cost reductions. The investigation of business models based on distributed ledger technology, however, showed that business models features, such as the customer value proposition, the positioning of the company within the value network as well as the competitive strategy does not significantly vary from traditional business models and in particular, from contemporary IT-enabled business models. Notably, this allows two alternative conclusions: Either distributed ledgers do not possess the disrup-
tive potential that advocates of the technology expect or the disruptive potentials of the technology did not unfold so far. Further theoretical investigation showed that, beside the technology seems not to affect business models, business strategy is significantly affected. The, thereby, expected resulting economic effects of distributed ledger use, justify the usage of the technology in a business environment. Notably, given the associated changes of business relationships as well of organizational structures, it can be anticipated that distributed ledger posses disruptive potentials that did not unlash so far, owing to the adjustment processes that are necessary for a successful application of the technology. Consequently, the speed of the unfolding of the potentials of distributed ledger technology is determined by related integration and adjustment processes and hard to predict. The degree of disruptiveness, however, depends on the applied business model and strategy. For instance, the business strategy and model of a particular corporation is more affected, if the distributed ledger is used a digital infrastructure underlying business activities and processes, rather than, if distributed ledgers are used as an technology, which facilitates an application that is provided by a third party.

ii. Distributed ledger technology implies a range of paradigm changes that need to be addressed properly in order to foster overall corporate goals.

The inherent logic of distributed ledger technology and business logic are divergent and diametrical opposed. Most importantly, distributed ledgers imply decentralization of consensus finding, which is in heavy contrast to the hierarchical structure of a firm and the associated responsibilities with respect to decision making. Given these differences, the application of distributed ledger technology in business is not straightforward and needs to be discussed, especially, referring to the advantages but also disadvantages, resulting from technology use. For instance, the fact that distributed consensus requires every participating node to possess a copy of the ledger on his or her computer has positive effects, which is among others resilience, but also negative effects. For a corporation a resilient database system is favorable, assuming that a possible down turn or other unforeseeable events will probably have only minor effects, such that stored data of a corporation is not threatened. However, resilience of the distributed ledger simultaneously implies data redundancies that are typically avoided, owing to the risks stemming from possible data inconsistencies or simply costs, which are implied by holding a myriad of copies, implying associated storage capacity needs. Another paradigm change is implied be the feature process integrity, meaning that rules are implemented in the protocol and automatically enforced. Notably, this limits the ability of a corporation to make ad hoc rule making and requires that an IT department is responsible to adapt and implement new rules in the protocol as fast as possible, which comes as well at costs. Given paradigm changes implied by distributed ledgers, corporations must identify the
right strategy for mitigation as well as to exploit technological, organizational as well as social paradigm changes to facilitate existing infrastructures and business processes.

iii. **The application of distributed ledger in accounting does not lead to the prevention of accounting fraud.**

Given the developed scenario of blockchain-based accounting and the applied alternative consensus mechanisms in addition to proof-of-work, decentralized consensus did not lead to the expected or, more precisely, the desired outcome of the prevention of accounting fraud. The main reason therefore is that an individual that wants to commit fraud will, with high probability, be able to acquire the majority of necessary resources to possess the majority of votes within the consensus finding process, or is otherwise able to build coalitions, either on a voluntarily basis or by enforcing collaboration. Given these possibilities for a potential attacker, fraud is not prevented by applying distributed ledger technology and the commitment and concealment of fraud is even simplified. In particular, whereas the case studies of accounting fraud incidents revealed that perpetrators of fraud typically must override internal controls to conduct fraud, e.g. through the exertion of pressure or monetary rewards (e.g. bonus schemes), using distributed ledgers, override of internal controls is not necessary anymore, since ledger entries can possibly be overwritten, which simultaneously conceals the traces that may be left otherwise.

These results hold, given the developed scenario, the associated assumptions as well as applied consensus mechanisms, however, a certain degree of transferability of these result to other scenarios or alterations of the proposed scenario is expected. Alterations include for example the inclusion of shareholders within the consensus finding process or the extension of the scenario to a two firm setting. Although the possibility that fraud is prevented in one of these scenarios cannot be excluded, the conditions for a potential perpetrator of fraud do not change and imply that the majority of votes within the consensus process must be acquired. Based on the discussion of the possible scenario changes, however, there seems to be no mechanism that prevents a perpetrator of fraud from doing so. For instance, in a setting with two firms using a shared blockchain based accounting system as proposed by Andersen (2016), decentralized consensus mechanisms cannot prevent the two firms from committing accounting fraud jointly.

iv. **Other decentralized consensus mechanisms are needed to prevent fraud – however, a main problem is the assumption of a majority of altruistic or reciprocal behaving nodes.**

In order to prevent fraud in the defined or similar scenarios of distributed ledger based accounting, other decentralized consensus mechanisms need to be developed and implemented that deter network participants from the conduction of fraud by simply ac-
quiring the majority of votes in the consensus process or by building coalitions for the joint conduction of fraud. A major problem that must be solved, however, is that the analyzed consensus mechanisms are all based on the assumption that the majority of nodes will behave honest, which implies that nodes show either reciprocal or even altruistic behavior. Especially in a business context, this assumption seems not to be realistic and, instead, rational acting agents are typically assumed. Thus, new distributed consensus mechanism must take care of rational acting individuals and find a solution for consensus without assuming that the majority of consensus participants will behave honest. Focusing solely on individuals, dynamic weighting of voting rights could be a solution. This means that voting weights are adjusted to the network size, the particular consensus mechanism and other determinants of the consensus finding process, such that nobody is able to acquire the majority of voting rights. However, this would still not rule out the possibility of coalition building, which obviously, cannot be prevented by dynamic weighting of votes given the unpredictable nature of spontaneous alliance building. Overall, the possibility that distributed ledger technology could prevent accounting fraud, given alternative and newly emerging distributed consensus mechanisms cannot be denied. However, so far, it must be stated that literature that currently proposes the application of this technology in accounting, neglects the weaknesses of currently existing consensus mechanisms. Therefore, instead of further promoting untested characteristics implied by distributed ledger technology, further research should focus on the development of consensus mechanisms that take up these vulnerabilities.

v. Overcoming the normative premise to apply distributed ledgers is vital to the distributed ledger’s future development and successful applications.

Not only in the case of accounting applications, there seems to exist a normative premise to apply distributed ledger technology in various industries and for numerous purposes, however, without a fundamental analysis concerning the actual effects of the technology once applied in a corporate context. In particular, evaluations of the technology’s capabilities mainly refer to economic analysis based on untested assumptions, i.e. that distributed ledger impose decentralization of consensus without the need of a validating trusted third party, full transparency as well as immutability of ledger entries. As shown in this thesis, these assumptions not hold always and are heavily determined by the actual design of the distributed ledger. It can be assumed that this assessment applies to other application areas as well.

Applying untested assumptions can occasionally lead to significant economic losses, for example, as already apparent in the case of the research project R3 CEV. In particular, R3 CEV started as a research project to develop a distributed ledger based inter-bank ledger to store financial agreements transparently. However, recently the speaker of the project acknowledged that their efforts, which were finance through large investment
sums, led to the development of a ledger that ‘does not need a blockchain or distributed ledger’ (Suberg, 2017). Certainly, the failure of such projects as well as the associated economic losses send pessimistic signals to the market and provide a poor starting point for further research projects. Thus, it is vital to the future development of distributed ledgers to avoid research projects that apply a normative premise to use the technology. Instead, fundamental research should be conducted in order to explore the possibilities opened up by distributed ledger technology as well as comprehensive assessing whether and if so, how distributed ledgers can be applied in a corporate environment.

vi. Distributed ledger research needs appropriate analysis techniques to avoid misjudgments over potential application areas and the associated economic benefits.

As described in this thesis, analyzing techniques to assess the potential of distributed ledgers are predominantly limited to either a technical-infrastructural viewpoint, or make use of economic analysis methods. Most importantly, these two views are typically not combined, resulting in two viewpoints that separated, probably, will not lead to the desired outcomes and a fair assessment of the technological capabilities. Consequently, new frameworks that comprise both approaches as well as a corporate perspective must be developed. In particular, a combination of those three viewpoints is expected to lead to improved assessments in regard to the questions, in which business areas and how the application of distributed ledger technology is actually reasonable, without referring to mere assumptions about the previously mentioned potentials capabilities of distributed ledgers.

6.2 Limitations

Several limitations apply to this thesis and the associated results that are partially discussed in the respective chapters. However, in the following the main limitations should be highlighted. Especially, these limitations refer to the result that a blockchain based accounting information systems cannot prevent accounting fraud, owing to the vulnerabilities that are induced by the respectively applied decentralized consensus mechanism. This result holds for the most part, however, needs to be interpreted with respect to the following constrains:

i. Proposed scenario of blockchain based accounting

Certainly, one of the major limitations of this study is the restriction of the scenario to an intra-corporate setting and the associated distributed ledger design decisions. In particular, the restriction to a permissioned peer-to-peer network accelerates some of the later identified vulnerabilities of distributed consensus mechanisms, i.e. the ability of one individual or a group of individuals to acquire the majority of network power and,
thereby decision-power. Also the decision to allow only a restricted number of consensus participants to validate information is a limitation to the proposed setting that implies centrality tendencies in the distributed network. Thus, it can be questioned, whether the restrictions of the scenario to the intra-corporate setting is reasonable at all. However, it can be argued that, if distributed ledgers are applied in a business context, networks must be somehow restricted, either in regard to network access and the ability to validate information or in regard to the provided transparency. A completely unrestricted distributed ledger otherwise could lead to the threatening of business secrets, such as information on particular business partners or other collaborations, research and development efforts or expansion endeavors, that consequently, could lead to the loss of competitive advantages. Moreover, the expansion of the scenario was proposed and discussed, including the proposal to extend the blockchain based accounting system to a two- or multiple firm setting. However, as already discussed, the results are expected to stay the same or, at least, similar to the initially proposed setting. Nevertheless, a conclusive clarification of the outcomes in other scenarios necessitates separate evaluations.

ii. Investigated decentralized consensus mechanisms

The ability of a blockchain based accounting information system to prevent accounting fraud was, eventually, reduced to the functioning of distributed consensus mechanisms and the respective interaction with the behavior of consensus participants based on the prevailing incentives in the network. Notably, only five distributed consensus mechanisms were investigated that were applicable to the proposed setting. Thus, the results stated in this thesis hold only with respect to the proposed scenario in combination with the analyzed consensus mechanisms. Other scenarios may allow the application of different distributed ledger mechanism that are potentially more suited to prevent the emergence of accounting fraud in a blockchain based accounting system. Moreover, the emergence of new distributed consensus mechanisms may challenges the results found in the course of this thesis. This applies not only to the proposed scenario, but also to modified scenarios of blockchain based accounting, in which an alternative distributed consensus mechanism may prevents the emergence of accounting fraud.

iii. Focus on a particular type of fraud

The present evaluation of a distributed ledger based accounting information system and its ability to prevent fraud is conducted based on the premise that fraud is always committed by the management as well as through override of internal controls. The restriction to one attacker scenario was necessary, since this thesis constitutes one of the first attempts to conduct an in-depth analysis of the technology’s abilities to prevent fraud, without relying on mere assumptions about the unreserved immutability and transparency of logged data entries. At the same time, the investigation of only one at-
tacker scenario implies that the founded results hold only with respect to the defined attack scenario. Thus, potentially, other attacks as well as fraud conducted by other entities or individuals within or outside a company could be prevented by using the blockchain based accounting system and respective consensus mechanisms. Simultaneously, through this restriction, especially, the incentives of the management and the internal control system were investigated. However, the applied technology may also alter the incentives of other entities within and outside the company, whereas the effects in the proposed scenario may be either positive or negative. Looking at the external auditor, for instance, and assuming a different attacker scenario, possibly there is an increased incentive for more accurate and in-depths auditing of the corporate financial transactions, given increased transparency and the thereby improved oversight on financial statements. Thus, not only alternative attacker scenarios should be included in future analyses, but also considerations on the modification of the incentives of further entities within the proposed scenario, since changed incentives potentially balance each other or lead to mutual reinforcement.

iv. Negligence of fraud that happens outside of the system

Focusing on accounting fraud that is conducted through the offsetting of internal controls through the management, neglects fraud that is prepared and conducted outside the system. As already indicated, accounting fraud may also happens through the creation of fictitious documents or events and the subsequent settlement within the accounting system. Fraud that happens outside the system, probably, cannot be combated by a distributed ledger based accounting system; however, by assuming that corporate transactions are completely digitally and the placement of payments with cash is not allowed, then, some of these fraudulent activities can be avoided, by including the associated actions into the system. However, these considerations were not considered in this thesis so far. Consequently, further research must also take into account that fraud may happens outside an information system and, consequently, must find answers to the question, how these fraudulent activities may be prevented by a distributed ledger based accounting system.

6.3 Implications for Further Research: Towards Process-Centered Research on Distributed Ledger Technology

The present thesis emphasized some of the most urgent drawbacks of contemporary distributed ledger research and illustrates its effects by using the example of blockchain-based accounting and the refutation of the expected effects. As highlighted at several points, distributed ledger technology, its functioning and the associated economic outcomes, when applied in a business context or by substituting existing digital infrastruc-
tures, is mainly investigated from an either technical or economic viewpoint, without reconciling both views. The direct transfer of the technical architecture and functioning on the economic domain, however, led to the rise of misleading expectations concerning the technology’s capabilities for fraud prevention. The effects of misleading expectations and the resulting development and implementation efforts were already emphasized and occasionally lead to severe economic losses. However, misleading expectations are not only economically bad, the failure for correct assessment of the abilities of the technology also provides a poor starting point for further research endeavors.

Given these drawbacks, further research must place a greater focus on the factors that mediate between the technical and economic domain that is the implementation of the technology within businesses. The business value of distributed ledger is expected to be a joint technological-organizational phenomenon and, thus requires a simultaneous perspective on the technology, economic effects, organizational implementation as well as their interactions. Moreover, a greater focus must be placed on the effects of distributed ledgers on operational and management processes, whereas distributed ledger technology is expected to have especially an influence on management processes that are, according to Mooney, Gurbaxani and Kraemer (1996), enhanced by improvised availability and communication of information. Consequently, a perspective on distributed ledger as a coordination tool is proposed for further research, which implies business process re-engineering and, thereby, the redesign of operational and management processes. However, before the redesign of the business processes can be explored, more foundational research must be conducted that, especially, refers to the question, how distributed ledger technology is implemented into a corporation and adjusted to associated business processes. Consequently, the degree to which business processes are affected by the technology is heavily determined by the implementation mode of distributed ledgers that first must be defined for the particular application case, including investigations on the thereby induced trade-offs for corporations and the associated implications. All in all, this process-centered view on distributed ledger technology should lead to enhanced findings on the potentials of distributed ledgers, and especially to new insights in regard to applications of the technology that are actually reasonable and do not depend on mere expectations.
Appendix

Appendix A: Online Survey for the Evaluation of Trust in Bitcoin

Introduction

Bitcoin is a globally available decentralized payment system, which probably will become the dominant payment system in business-to-consumer (B2C) e-commerce. Owing to its characteristics, the existing financial infrastructure (e.g., banks, credit card companies) is obsolete in order to conduct transactions. Therefore, an essential change of the landscape in B2C e-commerce can be obtained and transaction cost are reduced. Consumer acceptance, however, is still low compared to other online payment systems such as PayPal. The following survey is, therefore, concerned about a comparison of user attitudes and perceptions towards PayPal and Bitcoin.

Information

This survey is solely about your attitudes and perceptions. Thus, in order to answer the questions no prior knowledge about PayPal or Bitcoin is necessary. Please answer according to your subjective assessment.

Definitions

PayPal is an online payment system, leveraging the existing bank infrastructure in order to process transactions. Transactions are, therefore, processed using existing bank accounts.

Bitcoin is an alternative payment system that is not based on the existing bank infrastructure. Transactions are verified and processed over a distributed network and without a central authority.
Part I: PayPal

Please answer the following questions concerning the ONLINE PAYMENT SYSTEM PAYPAL.
Please note that you do not have to answer all questions in order to complete the survey.

How often do you use PayPal to shop online?
- Never
- Rarely
- Regularly
- Frequently

How would you assess your knowledge about the general functioning of PayPal?
- Very good knowledge
- Good knowledge
- Neither good nor bad knowledge
- Bad knowledge
- Very bad knowledge

How would you assess security of PayPal?
Please use the scale below to indicate agreement or refusal regarding the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>strongly disagree</th>
<th>disagree</th>
<th>rather disagree</th>
<th>rather agree</th>
<th>agree</th>
<th>strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is unlikely that someone else is able to gain access to my PayPal account without my approval</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>It is unlikely that someone else withdraws money from my PayPal account or shops without my approval</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Payment reversals are possible</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Payment reversals are easy to conduct</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>All services and functions are constantly available</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>My overall perception of the degree of security is high</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>
### Appendix

#### Seite 07

**How would you assess privacy of PayPal?**

Please use the scale below to indicate agreement or refusal regarding the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Rather Disagree</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is unlikely that an uninvolved party is able trace my payment behavior</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>It is unlikely that personal data are transmitted to a uninvolved party during a transaction</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>My overall assessment of the degree of privacy is high</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

#### Seite 08

**How would you assess usefulness of PayPal?**

Please use the scale below to indicate agreement or refusal regarding the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Rather Disagree</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is possible to transact micropayments (&lt;€1) with PayPal</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Micropayments are commonly accepted by merchants</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Payments with PayPal are commonly accepted by merchants</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Appropriate mechanisms for consumer protection are implemented</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Within the payment system, it is possible to choose between different payment methods (e.g., giro-card, credit card etc.)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>PayPal credits can easily be converted into other funds</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>My overall perception of the degree of usefulness is high</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

#### Seite 09

**How would you assess the ease of use of PayPal?**

Please use the scale below to indicate agreement or refusal regarding the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Rather Disagree</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions are easy to conduct</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Usage is intuitive</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>A clear representation of product and payment detail is essential</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
Part II: Bitcoin

Please answer the following questions concerning the ALTERNATIVE PAYMENT SYSTEM BITCOIN.
Please note that you do not have to answer all questions in order to complete the survey.

How often do you use Bitcoin to shop online?
- Never
- Rarely
- Regularly
- Frequently

How would you assess your knowledge about the general functioning of Bitcoin?
- Very good knowledge
- Good knowledge
- Neither good nor bad knowledge
- Bad knowledge
- Very bad knowledge

How would you assess security of Bitcoin?
Please use the scale below to indicate agreement on or refusal of the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>strongly disagree</th>
<th>disagree</th>
<th>rather disagree</th>
<th>rather agree</th>
<th>agree</th>
<th>strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is unlikely that someone else gains access to my Bitcoin account without my approval</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>It is unlikely that someone else withdraws money from my Bitcoin account or shops without my approval</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Payment reversals are possible</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Payment reversals are easy to conduct</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>All services and functions are constantly available</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>My overall perception of the degree of security is high</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
### How would you assess privacy of Bitcoin?

Please use the scale below to indicate agreement or refusal regarding the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Rather Disagree</th>
<th>Rather Agree</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is unlikely that an uninvolved party is able trace my payment behavior</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>It is unlikely that personal data are transmitted to an uninvolved party during a transaction</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>My overall perception of the degree of privacy is high</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

### How would you assess usefulness of Bitcoin?

Please use the scale below to indicate agreement or refusal regarding the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Rather Disagree</th>
<th>Rather Agree</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is possible to conduct micropayments (&lt;€1)</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Micropayments are commonly accepted by merchants</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Payments with Bitcoin are commonly accepted by merchants</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Appropriate mechanisms for consumer protection are implemented</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Within the payment system, it is possible to choose between different payment methods (e.g., giro-card, credit-card, etc.)</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Coins can be easily converted into other funds</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>My overall assessment of the degree of usefulness is high</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>
Appendix

How would you assess ease of use of Bitcoin?  
Please use the scale below to indicate agreement or refusal regarding the following statements.

<table>
<thead>
<tr>
<th>强烈不同意</th>
<th>不同意</th>
<th>中立</th>
<th>同意</th>
<th>强烈同意</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment transactions are easy to conduct</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usage is intuitive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A clear representation of product and payment detail is essential</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Part III: General questions

Please answer the following general questions.

What is your sex?

- Male
- Female

1. What is your highest educational achievement?

- Doctorate or postdoctoral education
- University degree – Master
- University degree – Bachelor
- Apprenticeship
- High school graduation
- Secondary school certificate
- Secondary modern school certificate
- None
- Other

In the future, do you (furthermore) want to use PayPal?

- Yes
- No

In the future, do you (furthermore) want to use Bitcoin?

- Yes
- No
I want to gain additional Information/knowledge about....

☐ PayPal
☐ Bitcoin

Thank you for your participation!

I would like to thank you for your participation.

All your answers are saved. You can close the browser window now.
B: Questionnaire for Assessing Distributed Ledger Backed Business Models

<table>
<thead>
<tr>
<th>Case Study</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Short Description of your Business Objective:</strong> ...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Customer Value Proposition | • What is the service or product you provide to your customers?  
• What is the main benefit for customers using your service?  
• What is the problem/need you try to solve/fulfill for your customers? |
| Market Segment | • Who are your customers?  
• How do you address them (channels)? |
| Cost Structure | • What are the costs of doing your business, how do they emerge/for what business activity? |
| Revenue Stream | • How do you generate profits?  
• What is your pricing structure?  
• Do you have different revenue flows? |
| Value Network Positioning | • How do you position yourself in the value chain?  
• At which point of the value chain do you create value for your customers? |
| Value Network Structuring | • Who are your business partners?  
• Do you have any substantial business relationships or cooperation?  
• Do you have any necessary business relationships that are vital to your business? |
| Competitive Strategy | • What gives you a competitive advantage, what is your key competence?  
• What is your competitive strategy?  
• Do you have any key business partners delivering you competitive advantages? |
### C: Overview over Contacted Companies and Descriptive Statistics

#### Case Study: Business Models Based on Distributed Ledger Technology

<table>
<thead>
<tr>
<th>Company No.</th>
<th>Company Name</th>
<th>Industry</th>
<th>Location</th>
<th>Employees (up to)</th>
<th>Answer Received</th>
<th>Rejected</th>
<th>No Reaction</th>
<th>Additional Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BitPay</td>
<td>Infrastructure</td>
<td>Netherlands</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>BlockCypher</td>
<td>Infrastructure</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ConsenSys</td>
<td>Infrastructure &amp; Business Applications</td>
<td>USA</td>
<td>200</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Eris Industries</td>
<td>Infrastructure &amp; Smart Contracts</td>
<td>UK</td>
<td>n/a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Ellureum</td>
<td>Infrastructure &amp; Smart Contracts</td>
<td>n/a</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Hyperledger</td>
<td>Infrastructure</td>
<td>UK</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>NeoNova</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Nxt</td>
<td>Payments</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Pl</td>
<td>France</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>TeraBlock</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Next</td>
<td>Business Applications</td>
<td>Canada</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SI</td>
<td>Infrastructure</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Ripple</td>
<td>Payments</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Ledger Labs</td>
<td>Business Applications</td>
<td>Canada</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>MultiChain</td>
<td>Infrastructure</td>
<td>n/a</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>MultiMantra</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>OpenChain</td>
<td>Infrastructure &amp; Finance</td>
<td>n/a</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>R3</td>
<td>Blockchain &amp; Finance</td>
<td>USA</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Rigi</td>
<td>Infrastructure</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Chain</td>
<td>Infrastructure</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Digital Asset</td>
<td>Finance</td>
<td>USA</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Digital Currency Group</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Enternaut</td>
<td>Smart Contracts</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>firmchain</td>
<td>Infrastructure &amp; Business Applications</td>
<td>Luxembourg</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Finchain</td>
<td>Business Applications</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>SolidX</td>
<td>Infrastructure &amp; Business Applications</td>
<td>n/a</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>SecurCard</td>
<td>Identity Management</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>SmartContact</td>
<td>Smart Contracts</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>PayHer</td>
<td>Payments</td>
<td>UK</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Alphapage</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Digital Payment</td>
<td>Finance</td>
<td>Canada</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>SETL</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>TLEX</td>
<td>Exchange</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Token Digital Asset Exchange</td>
<td>Exchange</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Flamingo</td>
<td>Infrastructure</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Pase</td>
<td>Commerce</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Snapcard</td>
<td>Payment</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Stingle Labs</td>
<td>Infrastructure</td>
<td>UK</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>HfF</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Ellipta</td>
<td>Security</td>
<td>UK</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Numerex</td>
<td>Security</td>
<td>Malaysia</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Blockchain Innovation Labs</td>
<td>Governmental</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Bazar</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>Infra</td>
<td>Infrastructure</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Keremos</td>
<td>Business Applications</td>
<td>Singapore</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Atlas</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Chrona</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>HashLab</td>
<td>Infrastructure</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Secure Asset Exchange (SAE)</td>
<td>Exchange</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Lbta</td>
<td>Business Applications</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Info</td>
<td>Infrastructure</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Stor.ai</td>
<td>Security</td>
<td>USA</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>The Decentralized Library of Alexandria</td>
<td>Property Rights</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Stempay</td>
<td>Smart Contracts</td>
<td>Spain</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>IcyPay</td>
<td>Smart Contracts</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Billibit</td>
<td>Finance</td>
<td>Canada</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>TeraBlock</td>
<td>Finance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Blackstream</td>
<td>Payment</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>BitNexo</td>
<td>Payment</td>
<td>China</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Apergi</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Cardinal</td>
<td>Payments</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>Lightning</td>
<td>Payment</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Cavennower</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Chamaliyas</td>
<td>Business Applications</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Cipherflex</td>
<td>Infrastructure</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>Cryptaly</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>KeeK</td>
<td>Payment</td>
<td>Canada</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>Unipay</td>
<td>Infrastructure</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>The Verge Group</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>World Libra</td>
<td>Business Applications</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>Perimstance</td>
<td>Business Applications</td>
<td>UK</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>Scope</td>
<td>Business Applications</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>Africrypt</td>
<td>Payment</td>
<td>UK</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>Cloudbreach</td>
<td>Security</td>
<td>USA</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>Compact</td>
<td>Insurance</td>
<td>USA</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>Cipherpay</td>
<td>Property Rights</td>
<td>Italy</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Company</td>
<td>Industry</td>
<td>Country</td>
<td>Website</td>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---------</td>
<td>----------</td>
<td>---------</td>
<td>---------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>Furos Limited</td>
<td>Payment</td>
<td>China</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>Credits</td>
<td>Infrastructure</td>
<td>UK</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>Symant</td>
<td>Infrastructure</td>
<td>France</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>Moxin</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>BitNation</td>
<td>Infrastructure &amp; Business Applications</td>
<td>UK</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>Blockchainly</td>
<td>Business Applications</td>
<td>UK</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>Medallion Labs</td>
<td>Property Rights</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>Ethere</td>
<td>Infrastructure &amp; Business Applications</td>
<td>UK</td>
<td>na</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>Bitproed</td>
<td>Notary</td>
<td>USA</td>
<td>na</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Coincele</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>Money2</td>
<td>Payment</td>
<td>France</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>DXMarkets</td>
<td>Finance</td>
<td>Singapore</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>BlockNotary</td>
<td>Notary</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>Endemint</td>
<td>Infrastructure</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>Sumatra</td>
<td>Infrastructure</td>
<td>UK</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>Chainsmiths</td>
<td>Infrastructure &amp; Business Applications</td>
<td>Ireland</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>Singular</td>
<td>Property Rights</td>
<td>USA</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>Cryptones</td>
<td>Infrastructure</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>Uptxi</td>
<td>Identity Management</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>Entrepreneur</td>
<td>Business Applications</td>
<td>Canada</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>Shifu</td>
<td>Infrastructure</td>
<td>Germany</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>CoinCorner</td>
<td>Infrastructure &amp; Business Applications</td>
<td>Ireland</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>Exictchain</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>E-Biz</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>Blocks</td>
<td>Infrastructure</td>
<td>South Korea</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>RSK Labs</td>
<td>Smart Contracts</td>
<td>Argentina</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>Cambridge Blockchain</td>
<td>Identity Management</td>
<td>UK</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>Asia Global Finance</td>
<td>Finance</td>
<td>Singapore</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>Forex</td>
<td>Payment</td>
<td>Thailand</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>Agileledger</td>
<td>Business Applications</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>Muhrich</td>
<td>Infrastructure</td>
<td>Austria</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>Viveat</td>
<td>Property Rights</td>
<td>Italy</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>Link</td>
<td>Infrastructure</td>
<td>Germany</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>GeoPay</td>
<td>Payment</td>
<td>South Africa</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>Centref</td>
<td>Business Applications</td>
<td>Poland</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>Leidum</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>Compt</td>
<td>Finance</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>114</td>
<td>Blocker</td>
<td>Property Rights</td>
<td>UK</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>115</td>
<td>GeoCoin</td>
<td>Payment</td>
<td>UK</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>116</td>
<td>CryptMail</td>
<td>Business Applications</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>The Cryptocurrency Store</td>
<td>Payment</td>
<td>Canada</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>RightsBlock</td>
<td>Property Rights</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>Leading Knowledge</td>
<td>Business Applications</td>
<td>Canada</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>Bill</td>
<td>Infrastructure &amp; Finance</td>
<td>France</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>121</td>
<td>VelTrade</td>
<td>Business Applications</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>Bitcoin</td>
<td>Infrastructure</td>
<td>6c</td>
<td>X</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>The Hive</td>
<td>Business Intelligence &amp; Insights</td>
<td>USA</td>
<td>na</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>124</td>
<td>Manaro</td>
<td>Property Rights</td>
<td>UK</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>Open Trade Docs</td>
<td>Finance</td>
<td>Singapore</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>Centexo Labs</td>
<td>Finance</td>
<td>Vietnam</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>BlockPlume</td>
<td>Health</td>
<td>6c</td>
<td>X</td>
<td>6a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>Biimark</td>
<td>Property Rights</td>
<td>China</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>129</td>
<td>Affair</td>
<td>Identity Management</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>130</td>
<td>PeerHealth</td>
<td>Health</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>131</td>
<td>ChainReactor</td>
<td>Security</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>132</td>
<td>Cryptore Payment Technologies</td>
<td>Payment</td>
<td>India</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>133</td>
<td>Avalanchain</td>
<td>Business Applications</td>
<td>UK</td>
<td>na</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134</td>
<td>ChainCrowd</td>
<td>Finance</td>
<td>Netherlands</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>135</td>
<td>Jupi Software</td>
<td>Smart Contracts</td>
<td>South Africa</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>136</td>
<td>Sino-Reader</td>
<td>Identity Management</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>137</td>
<td>Fomar</td>
<td>Infrastructure &amp; Business Applications</td>
<td>na</td>
<td>200</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>138</td>
<td>My ID Store</td>
<td>Identity Management</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>Coinlca</td>
<td>Finance</td>
<td>South Korea</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>140</td>
<td>Slove</td>
<td>Biotechnology</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>CoinSpace</td>
<td>Payment</td>
<td>Malta</td>
<td>na</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>142</td>
<td>Zaniati</td>
<td>Payment</td>
<td>UK</td>
<td>na</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>143</td>
<td>Node40</td>
<td>Finance</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td>Cannova Base</td>
<td>Infrastructure</td>
<td>Japan</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>145</td>
<td>Linus</td>
<td>Business Applications</td>
<td>Japan</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>146</td>
<td>BigChainDB</td>
<td>Infrastructure</td>
<td>Germany</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>147</td>
<td>Vital Identity</td>
<td>Identity Management</td>
<td>USA</td>
<td>50</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>148</td>
<td>Clause</td>
<td>Smart Contracts</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>149</td>
<td>ChainLink</td>
<td>Property Rights</td>
<td>USA</td>
<td>10</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>150</td>
<td>UniCrypt</td>
<td>Property Rights</td>
<td>USA</td>
<td>6a</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TOTAL: 0 6 133 2
Descriptive Statistics

<table>
<thead>
<tr>
<th>Location</th>
<th>Absolute Number</th>
<th>Relative Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>79</td>
<td>53%</td>
</tr>
<tr>
<td>UK</td>
<td>21</td>
<td>14%</td>
</tr>
<tr>
<td>Canada</td>
<td>5</td>
<td>3%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Germany</td>
<td>5</td>
<td>3%</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>South Africa</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>South Korea</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Singapore</td>
<td>4</td>
<td>3%</td>
</tr>
<tr>
<td>Spain</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>France</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>China</td>
<td>4</td>
<td>3%</td>
</tr>
<tr>
<td>Italy</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Australia</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Ireland</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Argentina</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Thailand</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Poland</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>India</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Malta</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Japan</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Austria</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>n/a</td>
<td>7</td>
<td>5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employees</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 10</td>
<td>69</td>
</tr>
<tr>
<td>11 to 50</td>
<td>30</td>
</tr>
<tr>
<td>51 to 200</td>
<td>8</td>
</tr>
<tr>
<td>n/a</td>
<td>43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responses</th>
<th>Absolute Number</th>
<th>Relative Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer</td>
<td>9</td>
<td>6%</td>
</tr>
<tr>
<td>Reject</td>
<td>6</td>
<td>4%</td>
</tr>
<tr>
<td>No Reaction</td>
<td>133</td>
<td>89%</td>
</tr>
<tr>
<td>Additional Information</td>
<td>2</td>
<td>1%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry</th>
<th>Absolute Number</th>
<th>Relative Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>33</td>
<td>22%</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>26</td>
<td>17%</td>
</tr>
<tr>
<td>Smart Contracts</td>
<td>7</td>
<td>5%</td>
</tr>
<tr>
<td>Identity Management</td>
<td>6</td>
<td>4%</td>
</tr>
<tr>
<td>Property Rights</td>
<td>11</td>
<td>7%</td>
</tr>
<tr>
<td>Security</td>
<td>5</td>
<td>3%</td>
</tr>
<tr>
<td>Payment</td>
<td>19</td>
<td>13%</td>
</tr>
<tr>
<td>Business Applications</td>
<td>20</td>
<td>13%</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Exchange</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Infrastructure &amp; Finance</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>Infrastructure &amp; Business Applications</td>
<td>8</td>
<td>5%</td>
</tr>
<tr>
<td>Business Intelligence/Insights</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Health</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Notary</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Biotechnology</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Governmental</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Infrastructure &amp; Smart Contracts</td>
<td>2</td>
<td>1%</td>
</tr>
</tbody>
</table>
## Case Study 1 – Symbiont

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Costumer Value Proposition   | • Smart contract platform for institutional financial markets  
• Solves the problem of duplicated ledgers in the financial industry and the associated problem of cost and latency as well as high error rate due to manual entries  
• Reduction of operational costs by streamlining and automating complex business processes  
• Reduction of disputes  
• Reduction of counterparty risks  
• Improved IT security |
| Market Segment               | • Allianz and State of Delaware  
• Other Customer, not disclosed |
| Cost Structure               | n/a |
| Revenue Stream               | • Different revenue flows, not disclosed |
| Value Network Positioning    | • Software Providers |
| Value Network Structuring    | • Ipreo (financial market infrastructure provider, joint venture)  
• Pillsbury (State of Delaware Blockchain Initiative) |
| Competitive Advantages       | • Smart contract platform for financial sector use case (purpose build)  
• Smart contracts can be amended by consensus (in contrast to other smart contract platforms e.g. Ethereum)  
• Smart contracts in written in mature programming language making it auditing and understanding easier (reduces disputes)  
• No key business partner delivering competitive advantage, platform build total internally |

## Case Study 2 – Fuzo

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Costumer Value Proposition   | • Bitcoin and Blockchain Services on a SIM card including Identity and KYC before SIM activation  
• Lead Application Remittance services on any mobile phone to the Fuzo SIM Wallet  
• Fuzo Mobile Platform – SIM Appstack, plan to deploy over the air and other SIM after issuance  
• Service for unbanked by offering an international form of Mobile money which can be send from person to person directly |
| Market Segment               | • Unbanked/Underbanked in Emerging Economies  
• Channels: In-country players with financial |
licenses to handle money services business requirements in the particular destination area
• Other players able to ship/bundle SIM Cards (local banks, carriers or local MVNO)

| Costs Structure | • Hardware costs: Hardware SIM plus enrollment terminals
|                | • SMS Gateway Costs
|                | • Consulting and project costs

| Revenue Stream | • Share ARPU average revenue per unit with channel partners and financial settlement partners
|                | • Platform as a Service Model is a Fee for service (note: Bitcoin is used as protocol not currency), our costs is SMS Messaging and Gateway costs plus small bitcoin transaction costs used for Omni-Layer Transaction payloads
|                | • Deployment of a customer bundle for local country partner to sell (nominal costs recovery on SIM package)
|                | • Point spread on local exchange rate and flag fall per reload transaction
|                | • Charging of developers of third parties apps with hosting fee and revenue share

| Value Network Positioning | • Fuzo provides new nexus (pivot point) in the value chain
|                          | • The carrier can act as bank or the bank can act as carrier
|                          | • Fuzo as last hop off point to customers (customer is Fuzo’s customer)
|                          | • Provide a secure platform for key management and chip to cloud value added service layer for the ecosystem

| Value Network Structuring | • SIM Manufacturers
|                          | • Security Vendors
|                          | • POS Terminal Manufacturers
|                          | • Blockchain Experts
|                          | • Channels: channel to market (path to customer) and Carrier Key (MCNO) deal sourcing are vital

| Competitive Strategy | • Virtual SIM tech stack that harmonizes key management layer fused with Identity
|                      | • Key competence: Industry experience in building solutions that use Fuzo’s secure approach
|                      | • First mover advantage
|                      | • Strong and key business partners delivering competitive advantages
|                      | • Unique Value Proposition in the Bitcoin-Blockchain space, able to work on any mobile phone

### Case Study 3 – Factom

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Costumer Value Proposition | • Blockchain enabled tools and services build on top of an open source Blockchain network
|                         | • Customers do not need to implement on custom tools to take advantage of Blockchain trust trail |
### Business Model Feature

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Costumer Value Proposition** | - Provision of a software platform for deploying blockchain-based applications  
- Each organization using a particular chain installs a Multichain node either free or as (future) premium version  
- Eases to build blockchain applications and to deploy it across multiple parties  
- Offering od deployment models with APIs/commands that are tailored for blockchain applications  
- Offers people to see the blockchain as “black box”, use the blockchain without the need to know every technical details (equivalent to SQL or NoSQL databases)  
- Specialized and niche database architecture  
- Reduced development time for blockchain applications |

| **Market Segment** | - Enterprises  
- Government  
- Public Infrastructure Companies |

| **Cost Structure** | - Derived from Software as a Service offerings  
- Licensing and Consulting |

| **Value Network Positioning** | - De facto experts in implementing Factom based technology solutions  
- Continuing to Steward open source developments  
- Development of products that solve specific problems in the industry |

| **Competitive Strategy** | - Large companies that want to build blockchain applications internally  
- Consulting companies that want to serve these companies  
- Startups building blockchain applications  
- Channels: Search engines and blog posts  
- As software also natural viral, as one organization has to work with another |

| **Value Network Structuring** | - Employee costs, especially for developers  
- Legal and accounting costs  
- Conference costs (small) |
### Appendix

<table>
<thead>
<tr>
<th>Revenue Stream</th>
<th>• Lean cost structure (expecting that blockchain are overestimated especially for its application in finance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Network Positioning</td>
<td>• Software platform</td>
</tr>
<tr>
<td>Competitive Strategy</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case Study 5 – DX Markets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Model Feature</strong></td>
</tr>
</tbody>
</table>
| Costumer Value Proposition | • Professional grade trading platform for digital currencies  
• Low latency trading, real-time charting, profit and loss tracking, bulletproof security  
• Increased efficiency and reduced costs by integrating blockchain technology into enterprise-based financial process |
| Market Segment | • Art Owners and Investors  
• Channels: B2B Events |
| Cost Structure | • Costs stemming from compliance, technology, sales, marketing |
| Revenue Stream | • Commission on the transacted volume  
• 6% on sell-side, 2% on buy-side |
| Value Network Positioning | • As a platform/marketplace connector of supply and demand side  
• Value capture at the point of transaction |
| Value Network Structuring | • Relevant business partners: Insurance companies, banks  
• No other vital business relationships |
| Competitive Strategy | • Access to distributed channels, expertise in innovative technologies  
• Strategy: Achieve largest liquidity pool, first-mover advantages |

<table>
<thead>
<tr>
<th>Case Study 6 – SETL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Model Feature</strong></td>
</tr>
</tbody>
</table>
| Costumer Value Proposition | • Institutional payment and settlement infrastructure based on blockchain technologies  
• SETL enables to move cash and assets directly between each other, facilitating immediate and final settlement of market transactions  
• Permissioned distributed ledger of ownership and transaction records, simplifying the process of matching, settlement, custody, registration and transaction reporting  
• Most flexible and cheapest system compared to other public or private blockchain solutions |
### Appendix

<table>
<thead>
<tr>
<th><strong>Market Segment</strong></th>
<th><strong>Cost Structures</strong></th>
<th><strong>Revenue Stream</strong></th>
<th><strong>Value Network Positioning</strong></th>
<th><strong>Value Network Structuring</strong></th>
</tr>
</thead>
</table>
| • Reduction in costs to operate the system and capital charges participants need to pay  
  • Provide technology and work with regulators and compliance professionals for a better post trade infrastructure | • All people within the value chain: Asset Manager, Market Makers, Brokers, Exchangers, and Registrars, etc.  
  • Channels: Direct approach and relationship with clients | - | - | - |

### Market Segment

- All people within the value chain: Asset Manager, Market Makers, Brokers, Exchangers, and Registrars, etc.
- Channels: Direct approach and relationship with clients

### Cost Structures

- Mainly staff costs

### Revenue Stream

- -

### Value Network Positioning

- -

### Value Network Structuring

- -

### Competitive Advantages

- Only DTL finance grade system available on the market, the OpenCSD

---

### Case Study 7 – Uniquid

#### Business Model Feature

<table>
<thead>
<tr>
<th><strong>Business Model Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Costumer Value Proposition | • Software that removes the need of passwords to access digital systems  
  • Using smart phones, wearables, and other connected devices it helps human operators to manage and interact with hundreds of devices and remote cloud services |
| Market Segment | • Enterprise Software for big companies that need to manage hundreds or thousands of customers and/or that connect things (sensors, meters, vehicles, actuators, etc.)  
  • Channels: Business Development, content marketing, and PR |
| Cost Structure | • Mainly R&D and software development  
  • Marketing (limited part of monthly budget)  
  • Some G&A costs from double offices in Italy and California |
| Revenue Stream | • Software as a Service revenue stream model  
  • Big marginality on licensing software  
  • Pricing is a flexible trade-off between setup fee and maintenance fee (dependent on market and customer needs)  
  • Minor revenue flow from consulting services (lot of demand from financial and insurance sector) |
| Value Network Positioning | • B2B2B, offering a service to system integrators and big enterprises  
  • Market channel for Identity and Access Management is longer than in other markets, but value in the hand of end users |
| Value Network Structuring | • Business partners are system integrators and device manufacturers (focus on the latter)  
  • No substantial or vital cooperation’s, only commercial partnerships |
<table>
<thead>
<tr>
<th>Competitive Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Significant reduction to infrastructure complexity, can be leveraged for higher security or lower costs</td>
</tr>
<tr>
<td>• Higher pricing flexibility due to the blockchain backbone for customer tailored sales models</td>
</tr>
<tr>
<td>• Two experimental business partners, authorized to test innovative revenue models on the market with the goal to scale up the “open model” with every customer</td>
</tr>
</tbody>
</table>

### Case Study 8 – Singular

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Costumer Value Proposition | • Blockchain entertainment studio that produces, acquires and distributes films, TV, and software projects  
• Rights, revenue and royalty platform powered by a series of smart contract modules  
• Combination of content and infrastructure to build a transparent and decentralized entertainment industry  
• Users (audience and content creators) are able to interact in a decentralized manner for a new an innovative experience never seen before on a centralized computer network  
• Audience benefit from an array of emergent decentralized experience  
• Content producers benefit from assigning terms and conditions right and usage policies to heir content, instantaneously being paid for their property  
• Centralized computer systems are grossly ineffective and “not smart”  
• Monopolistic and obfuscated structures extract value from creators and consumers |
| Market Segment | • Audience  
• Content Creators |
| Cost Structure | • Personnel costs  
• Software development  
• Marketing  
• Production of film/TV content |
| Revenue Stream | • Entertainment content  
• Software licensing/sell  
• Transaction fees from users interacting with smart contract modules in the ecosystem |
| Value Network Positioning | • Creation of own ecosystem  
• Strategically placing Singular to benefit from the proliferation of decentralized scaling  
• Creation of value throughout the process |
| Value Network Positioning | • Business Partner: ConsenSys  
• Balance3  
• uPort |
| Competitive Strategy | • Being ahead of the curve in decentralized/crypto space  
• Building rights management platform and tokenized ecosystem |
<table>
<thead>
<tr>
<th>Case Study 9 – VARcrypt</th>
</tr>
</thead>
</table>
| **Costumer Value Proposition** | • Global content distribution, encryption, and payment processing of content via blockchain technology  
• Customers distributed and consume content that is completely outside every existing forms of content distribution, monetization, and encryption through traditional forms of content distribution  
• Protection of artist’s content give consumer the flexibility to purchase content via micro-transactions outside the banking system  
• User-friendly and simple interface for an easier adoption of the technology  
• Offering of compelling content created by both consumers and content creators |
| **Market Segment** | • Costumers of any age and demography, currently enjoying content at YouTube, Netflix, Amazon, the Internet traditional content gaming consoles, and cable television  
• Channels: Content is globally available to all customers as soon as it is published on the blockchain  
• Content is permanent and will no longer have to be sold off for distribution territory by territory |
| **Cost Structure** | • Mainly hard fixed costs (staff, software, start up costs)  
• Paying miners of the blockchain with cryptocurrency |
| **Revenue Stream** | • Charging of distribution fees for content distribution through the blockchain  
• Different revenue streams are planned but not disclosed at the moment |
| **Value Network Structuring** | • Creation of new content ecosystem that distributes and monetizes content as well as protects intellectual property rights and access to flexible micro-transactions  
• Value creation for customers at every point of the value chain from a digital rights management/encryption perspective, content monetization and a global distribution perspective |

<table>
<thead>
<tr>
<th>Case Study 10 – Provenance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Costumer Value Proposition</strong></td>
</tr>
</tbody>
</table>
### Appendix 199

- Platform empowering brands to take steps toward greater transparency by tracing the origins and histories of products
- Gathering and verifying of stories, keep them connected to physical things and embed them anywhere online
- Not a social network but marketing tool for businesses that want to use their data

| Market Segment | • Businesses  
|                | • Non-profit organizations |
| Cost Structure | • Payment for services on a monthly basis  
|                | • Three costs structures: Starter, Pro, Enterprise  
|                | • Differ according to the usage of tools offered by Provenance either used off-the-shelf or through working with an expert team on a custom solution suited to a particular business |
| Revenue Stream | • Monthly revenue from accounts and the offering of tools |
| Value Network Positioning | • Value Creation for the customer throughout the whole supply chain  
| | • Information published on the blockchain may be on product or rare material purchase, production or selling, etc. |
| Value Network Structuring | - |
| Competitive Advantages | • Blockchain as disruptive technology changing the way to trace materials and to ensure trustworthy data  
| | • Provenance as a new system where everyone in the supply chain can be part of it  
| | • Fulfillment of the increasing demand for transparency and perfectly auditable systems |

### Case Study 11 – StringLabs

<table>
<thead>
<tr>
<th>Business Model Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Costumer Value Proposition | • Crypto Studio, incubator and investor for advanced decentralized protocols and DAPPS  
| | • Realization of different projects: e.g. Phi (De-centralized commercial banking and stable currency) or Dfinity (Infinite Trust Machine)  
| | • Customers profit from professional experience and capital to build open protocol ventures |
| Market Segment | • Entrepreneurs  
| | • Developers, Engineers, etc. |
| Cost Structure | - |
| Revenue Stream | • Return on investment |
| Value Network Positioning | - |
| Value Network Structuring | • Business relationship to founded ventures  
| | • No other significant business relationships |
| Competitive Advantage | • Team of experts including researchers, engineers, law professors etc.  
| | • Experience in building new ventures |
References


AICPA (2005) Management Override of Internal Controls: The Achilles’ Heel of Fraud
References


Andersen, N. (2016) Blockchain Technology A game-changer in accounting?


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-


References


References


References


References


Rückeshäuser, N. (2017c) “Typology of Distributed Ledger Based Business Models,” in *ECIS.*


References(6,15),(991,995)


