Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls

Nadine Rückeshäuser

Institute of Computer Science and Social Studies, Department of Telematics, Freiburg, Germany
nadine.rueckeshaeuser@iig.uni-freiburg.de

Abstract. Research proposing the application of blockchain technology in accounting assumes the utilization of decentralized consensus mechanisms based on the exertion of scarce resources (Proof-of-Work; PoW), leading to the validation of transactions without the need of any third party. Together with the blockchain, a shared database, PoW is expected to lead to nearly immutable and, therefore, fraud-resistant, real-time financial registers. This conclusion must be reconsidered, taking into account recurrent top-management involvement in accounting scandals, often conducted through deliberate exposures of internal and external control systems. This paper asserts that blockchain-based accounting using PoW-based consensus paves the way for the suspension of controls by the management, since exerting the majority of computer power is easier than circumventing internal and external control systems in conventional accounting systems. Alternatives to PoW must be considered for blockchain-based accounting that prevents the management from conducting fraud and, thereby, qualifies the blockchain for its application in accounting.

Keywords: *Decentralized Consensus, Blockchain Customization, Blockchain-Based Accounting, Accounting, Management Override of Controls*

1 The Blockchain: The New Cure All?

Today, blockchain technology in combination with decentralized consensus mechanisms (DCMs) and its application in various business sectors is on everyone's lips. Blockchains are shared databases that are maintained and verified amongst actors that participate in a network, ensuring digital transparency and confidence of records of information without a trusted third party [26]. Whereas the financial sector was an early adopter, the demand for the technology has increased over the past years and comes from diverse industries, such as health care or logistics. This demand is not surprising, given the blockchain's ability to enable decentralized autonomous business models, defined by self-governed programs through decentralized governance and collective consensus [27]. In particular, this allows the execution of

13th International Conference on Wirtschaftsinformatik,
February 12-15, 2017, St. Gallen, Switzerland

Rückeshäuser, N. (2017): Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls, in Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S. 16-30

Turing-complete codes for so-called smart-contracts, leading to self-executing programs that automatically enforce properties of digital contracts [35].

One major business sector expected to benefit from the features of the blockchain is accounting. In particular, blockchains may facilitate the maintenance of permanent and timely records of financial transactions [36]. Its decentralized and transparent nature further implies potential immutability, meaning that financial records cannot be altered ex post and, if so, the probability of detection will be very high [2]. Thus, blockchain-based accounting could possibly rule out the conduction and concealment of improper accounting methods, illicit structuring of transactions and financial database manipulations [16]. The possibility of blockchain-based accounting, therefore, has recently become an intensively discussed issue, not only in an industrial [2, 34] but also in an academic context [8, 25, 36]. The growing interest in this topic is also reflected by the formation of several start-ups offering blockchain-based services for decentralized bookkeeping, such as *Factom* [37] or *Scorechain* [38]. Overall, the application of blockchain technology in the context of accounting could be conducive to the industry, which is still mainly based on standardized technology such as computer assisted audit techniques [2]. As the digitization of accounting is still in its infancy, the application of blockchain technology may leads to the technological progress needed.

However, industrial and academic advocates of blockchain-based accounting seem to neglect the still present and well-known challenges of proper accounting that is top-management involvement in accounting fraud [17, 32]. The severity of this topic gets obvious when looking, for instance, at fraud incidents in the United States, where accounting fraud conducted by the management amounts to 89 percent of all financial statement fraud cases of public companies [3]. The following paper investigates whether the blockchain is qualified for an application in accounting. To this end, it is investigated how the management is able to conduct fraud and whether the proposed intra-corporate blockchain application is able to decrease the opportunities to commit fraud. Accordingly, it is assumed that there exist incentives for the management to commit fraud, however, there might be technical mechanisms for its actual prevention. Most of all, this implies an investigation of DCMs regarding their ability to impede the management from conducting accounting fraud.

The paper is structured as follows: The next section provides a case study of the Comroad accounting scandal and investigates the used manipulation and concealment techniques. Based on this case study, a generalization of the fraud pattern and the relationships between internal and external control systems is deducted, using additional scientific literature to support the identified relationship in the case of Comroad. Section 3 subsequently presents a layer model for blockchain customization, on which basis a scenario for blockchain-based accounting systems is developed. Using the scenario as well as the general fraud pattern and opportunities to commit fraud, identified in section 1, various DCMs are investigated concerning their ability to serve as technical mechanism for fraud prevention.

2 How to Conduct Accounting Fraud: A Case Study & Analysis

Accounting fraud is the deliberatively attempt to prepare and disseminate material that misstates a company's financial situation [32]. Involvement of the top management, such as Chief Executive Officers (CEOs) and/or Chief Financial Officers (CFOs), in accounting fraud (hereafter: management accounting fraud, MAF) is frequently observed [3]. Thereby, MAF includes either direct involvement of top-management in conducting accounting fraud or indirect involvement by convincing or enforcing the provision of fraud by other parties. To identify the requirements on blockchains in respect to MAF prevention, a case study of the Comroad accounting fraud scandal and a generalization of this case for a further analysis are provided.

2.1 The Comroad Accounting Scandal

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 [15]. 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 [15].

Comroad's success story, however, turned out to be one of the major accounting scandals of publicly traded firms in Germany. 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 [11]. One of those trading partners was a company named *VT Electronics*, which was allegedly in charge of the production and deliver 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 [15]. 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.

2.2 The Manipulation and Concealment Techniques of Comroad

Dorin [15] describes several incidents of MAF and also the previously presented case study of Comroad by using the so-called *swiss cheese* model. The model shows, how

systems may breakdown due to human intended or unintended as well as technical failures [28]. Accordingly, MAF may 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 [15].

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 [1]. Despite this top-down approach of control, additional internal controls are legally required, for example, according to the AktG [13], the Act for Control and Transparency in the Corporate Sector (KonTraG) [7], as well as auditing standards such as IDW PS 261 [18]. Internal controls are measures and methods adapted to safeguard assets of a company as well as to check the accuracy of bookkeeping [7]. 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 includes internal auditors and/or an audit committee [7].

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 to suspend the internal control system – a practice called management override of internal controls [9] – 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 [15] as well as the internal auditor, who received monetary remuneration for the maintained silence [10]. 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 [11, 15].

2.3 Generalization: Dependencies in Control Systems and Accounting Fraud

The described hierarchy of the company, the external and internal control system as well as the associated relationships between the control systems and organs in the context of the Comroad scandal are transferred to an arbitrarily chosen stock company *i*, to which the German Stock Corporation Act applies. The identified loopholes in the control systems of Comroad are generalized and crosschecked by the economic literature, among others [1, 3, 6, 15] as well as [32], and combined in Figure 1. For example, existing theoretical or empirical work about the management's influence on the board of director's independence [1] and other relationships [4, 9] were reviewed, by which the management is able to exert control over the board. Solid lines indicate

that there is a broad consensus about the indicated relationship in the examined literature, whereas dashed lines emphasize controversies. The influence of the management on the board of directors is determined by a variety of factors, such as the geographically disparity or career perspectives of board members. However, the strong influence of the management on the board of directors in the case of Comroad can be substantiated by a large part of the literature and is, therefore, assumed within Figure 1. It should be noted that the emphasized relationships are not generally true, but may be part of the problem when considering the emergence of MAF.

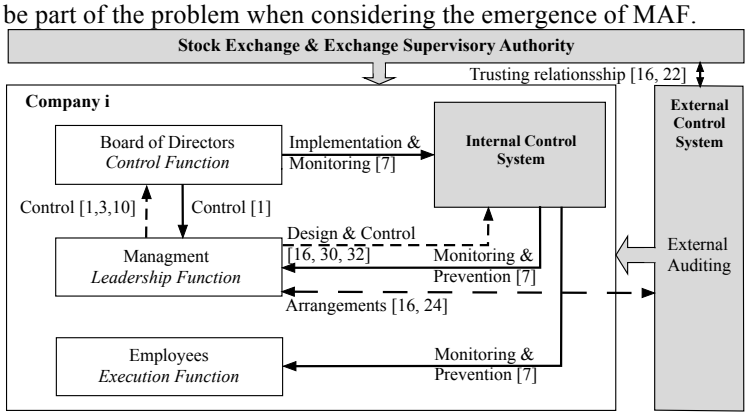

Figure 1. Stylized illustration of a company's control system and dependencies

Analyzing Figure 1, the existence of circular references between the management, the board of directors and the internal control system get apparent. 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 prevent the management from conducting accounting fraud by the exertion of effective controls. This observation is supported by the findings of Sawyer [30] as well as Caplan [9], noticing that the management will always be able to override internal controls, especially because they are able to choose the strength of these systems through its influence on the board. Moreover, if management override of controls happens, there is no obvious reason for external auditors to revise their evaluation of management integrity [9, 22], leading to additional negative effects for the effectiveness of controls. Despite the effects of external auditors are controversial discussed, the observations of [9, 22] coincide with those in the case of Comroad, where the assurance service of external auditor seems to have deteriorated and, therefore, was not able to deter management fraud [15]. Moreover, these inefficiencies are expected to exert further negative effects on the external control system, that is, first of all, external auditors, as well as the market, which typically trust (at least to a great extend) third-party financial audit [22].

Overall, this leads to the conclusion that the core of the management's ability to conduct and conceal accounting fraud is an inefficient internal control system resulting from a dependent board of directors, which is strongly influenced by the management. Based on this observation, a first step towards the prevention of MAF seems to be the strengthening of the independence of both mechanisms. This can be

done in terms of impeding the management's influence on the internal control system and the board of directors as well as by the avoidance of interdependencies between those entities and control systems. Second, MAF can also be prevented by decreasing the probability of successful concealment of fraud through the covering up of tracks, i.e through database manipulations and the circumvention of technical precautions. Consequently, an effective strategy for the prevention of MAF must take into account an organizational as well as a technical perspective.

2.4 Could Blockchains Prevent Accounting Fraud?

In view of the above considerations, the suitability of the blockchain for accounting must be discussed, as several academic and industrial research papers propose this, e.g. [2, 8, 36]. Certainly, the blockchain in combination with decentralized consensus induces organizational transformation through the decentralization of single business processes and by the potential increased involvement of employees because of high transparency. For instance, decentralized consensus could potentially raise employee involvement in accounting issues and the validation of business transactions, leading to more diversified controls through the transparency induced by the blockchain. Financial transparency is a major issue in accounting and for the internal control system, which is concerned about the openness and availability of information [20] that could potentially be moderated by the blockchain. Moreover, facilitating the involvement of employees could solve a frequently mentioned problem in internal control systems, which are claimed to be design, using an excessive agency view that promotes a strong adversarial relationship between the management and shareholders, but leaves out the relationship of the management and employees [32]. Summarized, given the potential organizational changes induced be the blockchain, it can be concluded that it is worthwhile to have a closer look on the technology and the impact of organizational restructuring. From a technical view, the blockchain is expected to introduce immutability of data stored on the blockchain, a feature that is frequently mentioned not only in the context of its possible application in accounting, e.g. [2, 8, 25]. This argument is based on the assumption to apply a proof-of-work (PoW) based DCM, which is a cryptographic puzzle, consisting of solving a mathematical problem by the exertion of computer power. In particular, PoW is a mechanism to ration resource access in client-server relationships and consist in finding a byte string combined with a block header, which results in a cryptographic hash that can only be done by the exertion of computer power [12]. Given this assumption, the suitability of an application of the blockchain for accounting will be analyzed not only with respect to the organizational transformations but also concerning the applied DCM.

3 Blockchain Customization and Organizational Restructuring

In this section, the structure and possible customization of the blockchain will be discussed in the context of a business environment. Based on the blockchain design decisions, a scenario for blockchain-based accounting will be presented.

3.1 The Blockchain in a Business Environment: Structure and Customization

Using a very basic definition, a blockchain is a synchronized global log of events between nodes in a peer-to-peer network. Particularly, a blockchain is replicated at every node and assists nodes in reaching consensus on the state of all accounts [26]. Blockchains can be customized for special use cases and adjusted to business environments, which is illustrated by a layer model presented in Figure 3. It is assumed that the layers overlap and are partially interconnected. The layer model provides an overview on how blockchains may fit in and support a company by providing deployment choices and by enabling flexibility.

At the lowest layer the blockchain provides a **digital infrastructure**, called distributed ledger. This basic infrastructure consists of three elements: The peer-to-peer network consists of homogenous nodes and is characterized by the ability to exist without a central node, responsible for network control. In the context of the blockchain, each node keeps a complete replica of all data needed to independently verify the validity of any data that should be incorporated into the distributed ledger. Before data are incorporated they must be broadcasted through the network. After broadcasting, a common order over data has to be agreed among the nodes, which is a non-trivial problem in a distributed network, known as the Byzantines generals problem [21]. This problem is solved by a cryptographically puzzle and the exertion of computer power by which a particular target value must be found (PoW; note that this mechanism will be explained in greater detail later). After reaching consensus, data are logged and permanently stored in the distributed ledger. At this level the customization of the blockchain for a business environment and/or application may happens by the choice of general rules according to which consensus is found.

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. Blockchains can either feature permission-less access or permissioned access. In the former case, everyone is able to participate as node and no prior authorization is needed [25]. Contrarily, blockchains that are characterized by permissioned access pre-select their participating nodes, e.g. through white- or blacklisting and some type of gatekeeping mechanism [31]. 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. Despite this sounds counterintuitive using a DCMs, 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, for instance, to avoid too much overhead and to allow for low latency. 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, permission-less 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 [31]. This definition excludes unintended centralization, for instance, through the undesired accumulation of the majority of computer power in the case of PoW.

On the third level, the blockchain is shaped by system design decisions in regard to the **foundation and integration** of the envisaged application. This includes that rules within the application must be designed in accordance to the particular business process or compliance requirements. In contrast to the general rules mentioned in the first layer that, these *specific* rules state additional, technical feasible requirements. For example, these rules may obey requirements referring to a specific section of the AktG. Moreover, a service-oriented architecture (SOA) might be taken into accounting, if a blockchain application must be integrated within an existing enterprise systems [33]. However, most likely not only the interaction of the blockchain and decentralized consensus with other information systems must be considered, but also user interaction. Nevertheless these system design decisions are only exemplary and customization may include numerous other aspects.

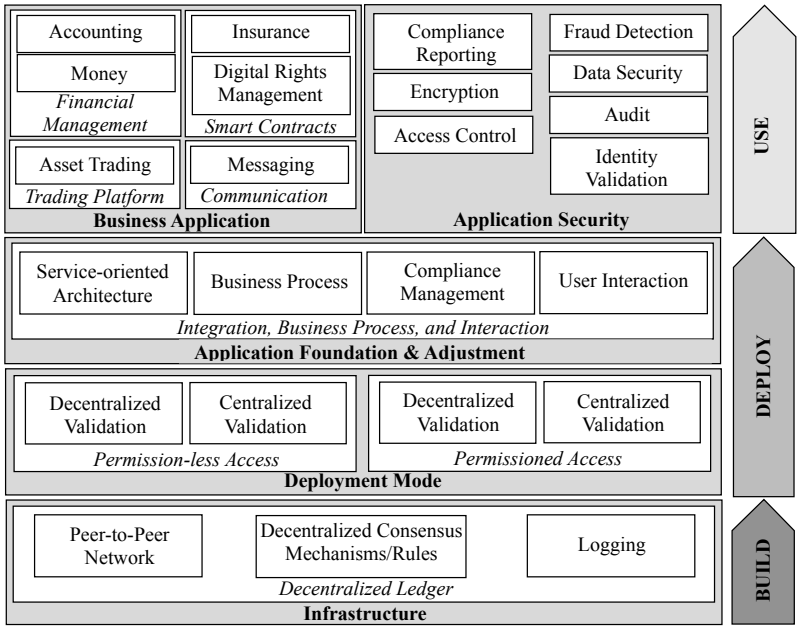

Figure 2. Blockchain layer model and customization in a business environment

Lastly, on the top layer particular **applications** are built on the basis of the preceding layer decisions. For example, smart contracts can be implemented for insurance services or digital rights management. However, as depicted in Figure 3, applications of the blockchain can relate to various business sectors, whereas this list is not exhaustive. Lastly, apart from the fact that the blockchain itself offers particular **security features** through cryptography, 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 to audit, whereas, again, this list is not exhaustive.

3.2 Scenario: Blockchain-Based Accounting and Organizational Changes

Proposed applications of the blockchain for accounting vary significantly from joint registers [2] to intra-firm blockchain-based record keeping [8, 34, 36]. However, industrial and academic literature lack a description on the concrete implementation of the blockchain as well as application scenarios, on which basis the blockchain and the proposed DCM can be evaluated. Contrarily, this paper develops a scenario for a blockchain-based accounting system using the layer model for customization.

As depicted in Figure 3, the basic infrastructure of the proposed accounting system is the distributed ledger, where business transactions are referenced on as monetary value and not as tokens. The deployment model of the blockchain is a private blockchain maintained by a network of individuals within the company that validate transactions, here called intra-corporate blockchain. Particularly, intra-corporate blockchains are chosen in this paper, since full transparency of sensitive financial data to particular companies or - in an extreme scenario - to the general public could lead to severe losses in competitive advantages for an individual company. For example, lawfully discretionary accounting practices would be no longer feasible, which could be exploited by competitors, whose financial data are not completely transparent. Thus, the following scenario is inspired by the facts from the Comroad study and the obligation of German stock companies for publishing annual accounts (AktG), which not implies full and real-time transparency. A comparison of intra- and inter-corporate ledgers is purposely excluded by referring to the associated strong focus of this study.

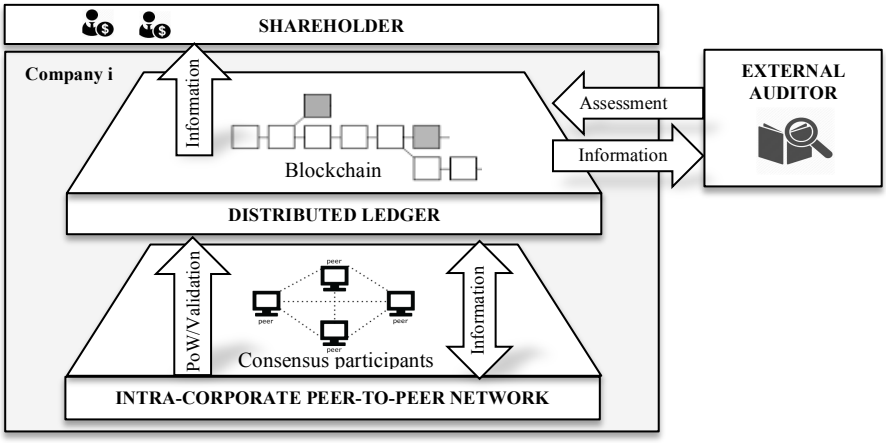

Figure 3. Scenario of a blockchain-based accounting

The network is assumed to consist of employees, especially, the accounting department, the management, and associated control entities that are the board of directors and an optional internal auditor or an audit committee, which together build the pool of consensus participants. Employees are likely to be enforced to participate on the consensus, as part of their work assignment. In contrast, executives and shareholders are assumed to act in their own interest and participate either because they want to influence the consensus protocol in a negative way, e.g. to conduct fraud,

or in a positive way, as shareholder are likely to be concerned about the accuracy of the financial situation. Consensus is found in accordance to the PoW mechanism, which is assumed as DCM in all identified papers that propose an application of blockchain technology for accounting, e.g. [2, 8, 36]. In this system, 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 (e.g. external auditors). 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.

4 Can We Prevent Management Accounting Fraud?

In the following, PoW as well as alternative DCMs will be investigated and assessed concerning their ability to prevent MAF. According to the previously presented scenario the decentralized consensus cannot be separated from the peer-to-peer network. Thus, it is acknowledged that there exist threats that result from the peer-to-peer network. Related attacker scenarios are, among others, Sybil attacks, Eclipse attacks, Byzantines Joint attacks as well as Churn attacks [14]. Secure blockchain-based accounting system must account for those attacks. However, given numerous works dealing with the security of peer-to-peer networks, it is assumed that there exist mechanisms to provide a considerable security level for the network. Thus, in the following the focus lies on DCMs and their ability to prevent MAF.

4.1 Management Override of Controls and Proof-of-Work Based Consensus

PoW is a mechanism to rationing resource access in client-server relationships, consisting of solving a mathematical puzzle, using computer power [5]. Particularly, PoW 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. A block contains all transactions, which have been committed on the previous block. Finding a nonce, can only be done by calculating the hash of the block for all possible nonces [12]. 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. Thus, if someone wants to revert the history, an alternative reality must be created (blockchain fork), which occurs if not all nodes agree on the same blockchain header [12]. 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 to be altered (51% attack). This requires not only computational power but also faster data processing than the rest of the network [26].

While PoW seems to provide a reasonable level of security in large networks, small-scale networks have been proofed to remain vulnerable of 51% attacks [5]. In

particular, this holds for intra-corporate blockchain-based accounting systems, where the management is potentially able to deliberately reach the majority of computer power. Without convincing, enforcing or circumventing exiting internal and external control systems as well as technical barriers, the management could simply use computers or a single server, which have more computing power than the remaining participants of the network for the effortless override of internal controls. Moreover, if logged transaction can be altered or possible deleted ex post, transparency of financial information is useless. This leads to the aforementioned negative effects on the external control system, as retrospective fraud detection mechanisms that may be conducted through external auditors are getting ineffective and subsequently also large parts of investors or exchange market participants, which rely on disclosed and allegedly external audited financial information. Consequently, using PoW as DCM for blockchain-based accounting, MAF will not be impeded, neither from an organizational perspective by decentralization nor through immutability of data, i.e. the technical perspective. Notably, PoW would even ease the override of controls, as the management does not need to convince others to support and conceal the fraud such as in the case of Comroad. This especially holds in the absence of direct monetary incentives that encourage honest behavior such as in the case of Bitcoin.

4.2 Alternative Decentralized Consensus Mechanisms

Table 1 provides an overview over DCMs developed after the emergence of PoW. For the sake of completeness PoW-based consensus is also included. A differentiation of the DCMs is conducted according to their ability to allow for permission-less or permissioned access of nodes as well as whether the mechanisms facilitate decentralized validation or not. This differentiation is done in accordance to the second layer of the model presented in Figure 3.

Table 1. Overview of decentralized consensus mechanisms after the emergence of PoW

	Permission-less Access	**Permissioned Access**
Decentralized Validation	• Proof-of-Work • Proof-of-Stake • Proof-of-Work based derivatives • Federated Byzantines Agreement	• Proof-of-Work • Proof-of-Stake • Proof-of-Work based derivatives • Federated Byzantines Agreement
Centralized Validation	• Delegated Proof-of-Stake	• Redundant Byzantines Fault Tolerance • Ripple consensus • Bilateral node-to-node (N2N) • RAFT and derivatives • Delegated Proof-of-Stake

Certain DCMs enable both, permissioned as well as permission-less access (although they might designed to be used in a permission-less system at first). 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. In the following, DCMs will be analyzed, if they feature permissioned access as well as decentralized validation and are, therefore, suited for an application according to the preciously presented scenario of blockchain-based accounting.

Proof-of-Stake

Proof-of-Stake (PoS) is based on the assumption that PoW's dependence on energy consumption creates unnecessary cost overhead in networks. PoS is a form of proof of ownership of the currency in the network [19]. 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 [26]. In a blockchain-based accounting system stakes will most likely be stocks. As the management will probably have the majority of stocks (this was also observed in the case of the Comroad scandal [15]), the management would be enabled to change financial transaction registers at their will, without having to respect any control system. Thus, despite the Proof-of-Stake is initially designed to promote decentralized validation, in practice the validation of transaction using this mechanism will be centralized and most likely led by the management. Moreover the protocol exhibits other general security issued, such as the so-called "nothing at stake" attack, where attackers can commit collateral as they can go back and rewrite history from a point where they still had stake [19].

Proof-of-Work Based Derivatives

Proof-of-Activity (PoA) is a combination of PoW and the PoS and described as one example of different PoW derivatives. Finding consensus by using PoA consists of the transformation of a pseudorandom value into a satoshi, which is the smallest unit of the cryptocurrency Bitcoin. According to [6], 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. Only active stakeholders, who maintain a node, get rewarded in exchange for the service they provide for the network. Despite PoA induces less overhead in terms of communication, it does not prevents "nothing-at-stake"-attacks [6] and therefore, does not guarantee for the fraud resistance of data on the blockchain. For the sake of completeness it should be mentioned that there exist further DCMs such as proof-of-capacity or proof-of-burn that are based on or are related to PoW. However, they are rather used for distributed payment systems and rarely discussed for other appliances in a scientific context.

Federated Byzantines Agreement

Federated Byzantines Agreement (FBA) 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. Nodes may select those participants based on arbitrarily criteria such as repudiation. To find consensus, a node waits for the vast majority of trusted nodes (quorum slice set) to agree on a transaction before considering the transaction settled. In turn, those nodes do not agree to the transaction until the participants they consider as important agree to the transaction as well, and so on. The key distinction between the FBA and prior Byzantines Agreements is the individual and decentralized trust decisions. If enough network nodes accept a transaction, it becomes infeasible for an attacker to roll it back [23, 29]. Moreover, security rest on digital signatures and hash families whose parameters can realistically be tuned to protect against adversaries with unimaginably vase computing power [23].

Notably, the FBA is a majority voting system, related to the decisions of selected trusted nodes. As in every voting system and, especially, if voting nodes are known to each other in a closed system, strategic voting cannot be excluded. Thus, 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 to cover up traces. Consequently, FBA is not able to prevent the occurrence of MAF.

5 Conclusion and Outlook

Academic and industrial work proposing the application of blockchain technology for accounting emphasize the immutability of financial recording based on a proof-of-work based decentralized consensus, probably leading to fraud-resistance. After identifying one of today's core problems of proper accounting, i.e. MAF, and proposing a scenario for blockchain-based accounting within a public company, this paper asserts that PoW is not effective in terms of preventing MAF. This conclusion is based on the assumption that there exist no incentive that prevents the management from committing fraud in accordance to [9, 16, 32], rather it is the mechanism, here distributed consensus that probably could prevent the commitment of MAF. Moreover, proof-of-work is even expected to ease the conduction and concealment of MAF, owing to the prevailing centrality tendencies within the system. Alternative decentralized consensus protocols were examined in accordance to the presented scenario of blockchain-based accounting. This paper concludes that currently, there exist no DCMs that promote permissioned systems, featuring decentralized validation and simultaneously preventing MAF. Overall, the ability of the blockchain and DCMs in the proposed scenario might be overestimated or even overhyped, even if a certain general potential of the technology in accounting could be attested owing to its decentralized and transparent nature. However, proposals for concrete applications must be strongly oriented on the de facto problems such as in the case of accounting

and MAF. Accordingly, further research should focus on the development of advanced consensus mechanisms that take into account the above-discussed issues, and especially, the ability of management override of controls. Variations in the proposed scenario are also conceivable. Overall, a special emphasis should lie on the cost-efficiency of such systems as well as security as basic requirements. Without these two prerequisites it is hard to imagine that any such system will be implemented in the future. Moreover, a comparison of intra- and inter-corporate solution as well as other possible scenarios should be pursued, in order to receive a more compressive evaluation of the potential of blockchain-based accounting.

References

1. Adams, R.B., Ferreira, D.: A theory of friendly boards. J. Finance. 62, 1, 217–250 (2007).
2. Andersen, N.: Blockchain Technology A game-changer in accounting? (2016).
3. Beasley, M.S.: An empirical analysis of the relation between the board of director composition and financial statement fraud. Account. Rev. 71, 4, 443–465 (1996).
4. Beasley, M.S. et al.: Fraudulent Financial Reporting. Committee. 12, 60 (2010).
5. Becker, J. et al.: Can we afford integrity by proof-of-work? scenarios inspired by the bitcoin currency. In: The Economics of Information Security and Privacy. pp. 135–156 (2013).
6. Bentov, I. et al.: Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. (2014).
7. Bungartz, O.: Handbuch Interne Kontrollsysteme (IKS): Überwachung und Steuerung von Unternehmen. Erich Schmidt Verlag, Berlin (2012).
8. Byström, H.: Blockchains, Real-Time Accounting and the Future of Credit Risk Modeling. (2016).
9. Caplan, D.: Internal Controls and the Detection of Management Fraud. J. Account. Res. 37, 1, 101–117 (1999).
10. Daum, R.: Phantompartner und Phantasieumsätze in Asien - Enttarnung eines Börsenstars. In: Leif, T. (ed.) Mehr Leidenschaft Recherche: Skandal-Geschichten und Enthüllungsberichte - Ein Handbuch zur Recherche und Informationsbeschaffung. pp. 134–143 Westdeutscher Verlag, Wiesbaden (2003).
11. Daum, R.: Phantompartnern in Asien auf der Spur. In: Schröder, C. and Sethe, R. (eds.) Kapitalmarktrecht und Pressefreiheit. pp. 9–30 Nomos (2011).
12. Decker, C., Wattenhofer, R.: Information propagation in the Bitcoin network. In: 13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings. (2013).
13. Deutschland, B.: Aktiengesetz (AktG), (2015).
14. Dinger, J., Hartenstein, H.: Die vermeintliche Robustheit von Peer-to-Peer-Netzen. (2006).
15. Dorin, M.: Institutionelle Maßnahmen zur Verbesserung der Qualität von Abschlußprüfung. Bielefeld University (2006).
16. Feng, M. et al.: Why do CFOs become involved in material accounting manipulations?

J. Account. Econ. 51, 1–2, 21–36 (2011).
17. Harrast, S.A., Mason-Olsen, L.: Can Audit Committees Prevent Management Fraud? CPA. 77, 1, 24–27 (2007).
18. IDW: IDW PS 261: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken. WPg Suppl. 2, (2012).
19. King, S., Nadal, S.: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Ppcoin.Org. (2012).
20. Kuizick, R.S.: Sarbanes-Oxley: Effects on Financial Transparency. SAM Adv. Manag. J. 69, 1, 43–49 (2004).
21. Lamport, L. et al.: The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4, 3, 382–401 (1982).
22. Lennox, C., Pittman, J.A.: Big five audits and accounting fraud. Contemp. Account. Res. 27, 1, 209–247 (2010).
23. Mazières, D.: The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus. (2016).
24. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted. 1–9 (2008).
25. Peters, G.W., Panayi, E.: Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. arXiv Prepr. arXiv1511.05740. 1–33 (2015).
26. Pilkington, M.: Blockchain Technology: Principles and Applications. In: Olleros, F.X. and Zhegu, M. (eds.) Research Handbook on Digital Transformations. Edward Elgar, Cheltenham, UK (2016).
27. Probst, L. et al.: Blockchain Applications & Services. (2016).
28. Reason, J.: The contribution of latent human failures to the breakdown of complex systems. Philos. Trans. R. Soc. Lond. B. Biol. Sci. 327, 1241, 475–484 (1990).
29. Rubin, J.: Federated Systems. , Massachusetts (2015).
30. Sawyer, L.B. et al.: Sawyer's Internal Auditing: The Practice of Modern Internal Auditing. Institute of Internal Auditors (2012).
31. Swanson, T.: Consensus-as-a-Service: a brief report on the emergence of permissioned, distributed ledger systems. (2015).
32. Topgos, M.A.: Why Management Fraud Is Unstoppable: Certified Public Accountant. CPA J. 12, 34, 34–41 (2002).
33. Tsai, W.-T. et al.: A System View of Financial Blockchains. In: IEEE Symposium on Service-Oriented System Engineering (SOSE). pp. 450–457 , Oxford.
34. Van de Velde, J. et al.: Blockchain in Capital Markets: The Prize and the Journey. (2016).
35. Vukolic, M.: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In: International Workshop on Open Problems in Network Security. pp. 112–125 Springer International Publishing, Zürich, Switzerland (2016).
36. Yermack, D.: Corporate Governance and Blockchains, http://www.nber.org/papers/w21802, (2015).
37. Factom - Apollo, https://www.factom.com.
38. https://www.scorechain.com.