INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Faculty of Management

The new ecosystem of the digital age – Impact of blockchain technology on the accounting environment and financial statement fraud detection

Simon Müller

Master's in Management

Supervisor:

Prof. Paulo Viegas de Carvalho, Assistant Professor, ISCTE Business School

Department of Finance

November 2021

iscte

BUSINESS
SCHOOL

Faculty of Management

The new ecosystem of the digital age – Impact of blockchain technology on the accounting environment and financial statement fraud detection

Simon Müller

Master's in management

Supervisor:

Prof. Paulo Viegas de Carvalho, Assistant Professor, ISCTE Business School

Department of Finance

November 2021

INSTITUTO
UNIVERSITÁRIO
DE LISBOA

The new ecosystem of the digital age – Impact of blockchain technology on the accounting environment and financial statement fraud detection Simon Müller

Resumo

A teoria da agência é um quadro subjacente para a instalação de funções de governação empresarial em empresas comerciais. A sua função de protecção contra a fraude de declarações financeiras continua a ser um escudo com carências que permitem a ocorrência de comportamentos incorrectos não resolvidos e intrínsecos na conduta empresarial. Os desenvolvimentos tecnológicos não foram capazes de resolver esta questão, ainda à espera de um libertador destas bem conhecidas cadeias. Vê-se na utilização da tecnologia Blockchain, a estrutura que gera confiança entre os participantes não confiantes em redes como a Bitcoin ou a Ethereum. Desde a sua popularidade de mainstreaming, investigadores, empresas e defensores prevêem um grande impacto na indústria da contabilidade que resulta da utilização da Blockchain. Aproveitando esta oportunidade, este trabalho investiga estes pressupostos através da revisão da literatura sobre o domínio, utilizando estudos de caso de antigas fraudes em demonstrações financeiras para enquadrar o perfil do fraudador e aplicando-o no cenário sugerido de contabilidade baseada em cadeias de bloqueio. Ao fazê-lo, a utilização sugerida de cadeias de bloqueio autorizadas levanta dúvidas num cenário que é moldado por actividades de substituição da gestão, causando graves afecções negativas a camadas num ecossistema que confia numa tecnologia e nos seus registos "imutáveis".

Palavras-chave: Teoria da agência, fraude de demonstrações financeiras, tecnologia de cadeia de bloqueio, tecnologia de livro-razão distribuído, anulação de gestão

JEL: M4, L1, G3

Abstract

The agency theory is an underlying framework for the installation of corporate governance roles in business enterprises. Their function to shield from financial statement fraud remains a shield with lacks that allow the occurrence of unsolved and intrinsic misbehaviour in business conduct. Technological developments have not been able to solve this issue, still waiting for a liberator from these well-known chains. One is seen in the use of Blockchain technology, the framework that builds trust among untrusting participants in networks such as Bitcoin or Ethereum. Since its mainstreaming popularity, researchers, corporations, and advocates foresee a great impact on the accounting industry that stems from the use of Blockchain. Taking this opportunity, this work investigates on these assumptions by reviewing literature on the domain, using case studies of former financial statement frauds to frame the fraudster's profile, and applying it in the suggested scenario of blockchain-based accounting. By doing so, the use of permissioned blockchains raises doubt in a scenario that is shaped by management override activities, causing severe adversely affections to tiers in an ecosystem that trusts a technology and its "immutable" records.

Keywords: Agency theory, financial statement fraud, blockchain technology, distributed ledger technology, management override

JEL: M4, L1, G3

Index

Table of figures

"I have always acted on the principle that I would rather lose money than trust. The inviolability of my promises, the faith in the value of my goods and in my word, stood always higher to me than a temporary profit." Robert Bosch

1. Introduction

Trust is the determinant for relationships in business sense and has been dealt with initially in the agency theory. The theory underlies corporate governance as foundational framework and maintains conduct in such. However, to this day and across industries, the intrinsic urge of fraudulent behaviour is deeply anchored, causing corporate governance failure. Consequences, among others, are accounting and financial statement fraud. Impacts of such unpredictability induce negative effects on markets and can lead to significant losses if not bankruptcy. A distrust in the quality of financial information adversely affects the confidence in capital markets with its participants and undermines shareholder trust. Levitt (1998) raised awareness on the motivation of meeting earning expectations may override common sense business practices and thus, an erosion in the quality of financial statement reporting. He further states that a grey area exists, in which "accounting is being perverted; where managers are cutting corners; and, where earnings reports reflect the desires of management rather than the underlying financial performance of the company" (Levitt, 1998). Waste Management, Enron, WorldCom, Parmalat, and Satyam did not do Levitt wrong when they headlined newspapers due to betrayals laid open in the following 2000's. More demanding financial accounting standards, prevention, and detection schemes followed these events. Investigations from Rezaee (2002) on financial statement fraud raised serious concerns and questioned the role of corporate governance, ethical values of top management teams, and effectiveness of audit functions to detect frauds. However, the actions taken still do not inherit the desired outcome to shield from accounting fraud incidents as the case of Wirecard in 2020 proofs. What all cases synergise is the fraudulent energy from leading or top managerial positions, framing the fraudster's profile.

Unquestionable, business processes, particularly those involving accounting activities, need restauration. The accounting industry formulates specifications for appropriate solutions that must tackle technical, organisational, and legal issues with the capability to either detect or prevent the occurrence of accounting fraud while maintaining or restoring trust to all tiers in respective ecosystems of the line of business. In the digital era, the application of technology to improve business processes is nothing new. Previous generations of technology had the incentive to deliver and exchange information in a faster, yet more secure way, aiming to deliver the same objectives. Blockchain (BC) intends to enable the exchange of value with one another while no intermediary needs to be relied upon to manage transactions. This attribute marks a significant difference in contrast to previous technologies. BC may redefine the exchange of value associated with business processes within and between companies. Thus, according to Wolfson (2020), BC is frequently suggested as a technological solution and possibility to reshape corporate accounting by the “Big Four”**.** It is an immutable ledger for recording transactions in a distributed network of mutually untrusting participants in which algorithms, digital signatures, and encryption are securing mechanisms. Advocates of BC foresee that the “single source of truth” skyrockets the accounting profession into the digital age. Given the infrastructure of the technology, real time accounting enables immediate facilitation of financial records. Transactions become more reliable due to its decentralised nature and do not necessitate an intermediary which results in cost and time reductions. The combination of gains in transparency and the cryptographic securing imply immutability. It also guarantees that no record or transaction can be altered later and if so, the rate of detection raises significantly. Given these attributes, the execution of business dealings concerning financial activity through BC has the potential to successfully mitigate accounting misbehaviour, unlawful trading, and other means of data manipulation.

The exploitation of the technology and trials of its facilitation is spread across industries already. Use cases in business and respective ecosystems have demonstrated initial successes. However, new technologies do not solely come with opportunities, but offer challenges to overcome. BC must deal with misleading and overrated expectations that surrounds it, let alone make it rather difficult to live up to and develop reasoned and balanced solutions. In addition, the enthusiasm is damaging in the long-term and may harm incentives for future investments. One example is the assumption that data on BC is always immutable, neglecting a variety of factors, among others, such as network size and used consensus mechanism. Moreover, a hasty shift to BC may lead to irrecoverable costs when other technologies at hand incorporate higher sustainability. The technology finds itself still at a relatively early stage and inherits both, strong interest for adoption and confusion about the addressing of business needs. Especially the latter is detrimental if risks including costs, security, and regulatory environment of respective industries, among others, are not considered. The business rationale behind BC implementation is a sound decision that starts with the business need itself and is not merely of technological nature.

1.1 Research aim, research question, and research objective

A careful assessment of BC and its interaction with the environment of accounting is necessary to meet the business rationale. This dissertation focuses on processes behind financial statement misconduct as well as technological features of BC and beyond. With the creation and derivation of facts concerning both topics as a foundation of knowledge, it investigates whether BC is a useful tool for the detection of fraud in accounting. Notably, the investigation sets a theoretical framework that draws conclusion of the possible interrelation of the fields accounting and BC, whether those interrelations justify the use of BC in accounting, and, ultimately, whether the technology is useful in the detection of accounting fraud. Further, by enabling BC in accounting processes, changes in management paradigms are implied and need to be considered. In these considerations a balance in trade-offs of several facets must be profound to identify organisational and technological changes in avoidance of significant new threads. An incentive to add insights of associated actions from users committing accounting fraud within the environment of BC is given and shall be investigated. In order, conclusions from past accounting fraud incidents and conducted surveys are used to identify fraudsters and their patterns.

The remainder of this dissertation is laid out as follows. Section 2 reviews agency theory with its instruments, possible outputs, both positive and negative, and introduces the topic of BC. Section 3 gives an overview of the methodological approach in this work. Section 4 presents the contributions BC has and has not to offer the accounting domain. With the last section to conclude, most important insights of the research, limitations and suggestions for future research shall be given.

2. Literature review

In this section, detailed information on the framework shall be outlined on which the following dissertation is analysed. By initially reviewing the agency theory, it sets out to give an overview of corporate governance roles, defines possible failures of such by defining financial statement fraud and suggests actors in the domain of accounting fraud through insights in surveys. The awareness of the industry to act upon fraudsters and detection techniques shall be introduced and mark the way for the appearance of BC. Its core functionalities shall be displayed and possible contributions to accounting given, before a conceptual framework concludes on this section.

2.1 Agency theory

Among many theories is the principal-agent model highlighted by Adam Smith in his 1776 published book, The Wealth of the Nations. Deriving from his initial, it is probably one of the oldest in the literature of management and economics. Smith (1776) bases his theory on the assumption that chances of a managing body of an organisation, which is not working to the owner's benefits, exists, when it does not own the organisation (Grieve, 1983).

Berle and Means (1932) introduce in their conclusion of the model, that the agent can use the firm’s property to maximise own gains over those of the principal. A conflict derives as the sharing of risk is unbalanced. The principal takes the risk of generating economic gains through owning as opposed to the agent’s risk aversion and main goal of maximising own economic gains.

Ross (1973) saw the basis of the agency problem in incentives and identified it as a consequence of the compensation decision between principal and agent. Additionally, he opines the problem prevails not only in the firm but in society as well.

The institutional approach by Mitnick (1975) considered the problem occurs due to the firm’s structure and propagated that institutions form around agency. Further, they need to evolve to deal with the essential imperfection of the agent theory: an agent never behaves accordingly the principal’s wishes because the incentives are not perfect.

Jensen and Meckling (1976) consider contracts set between principal and agent as potential for conflict as both have their own economic self-interest in mind. To raise value and profitability, the maximisation of wealth derives from managing and coordinating work involved in the enterprise. However, interests between parties differ. Under those circumstances, the principal controls the agent's performance through various monitoring activities due to agency cost control. Agency costs equal the sum of monitoring costs, bonding costs, and residual losses. They are of internal nature and part of an agent’s employment and due to imperfect aligning interests between principal and agent. Monitoring costs are associated with control and assessment of an agent’s performance in the organisation. Costs of bonding involve set contractual obligations by the principal such as reaching benchmarks, targets, and milestones within the time of contract. Bonding costs increase with lower monitoring costs and vice versa. Residual losses are results of ineffective and not wealth maximising actions by the agent. The principal reduces these losses through monitoring and bonding costs.

Fame and Jensen (1983) divided the firm's decision making-process in two categories: decision management and decision control. Essential key position in the process is held by an agent. In non-complex firms, both categories are executed by the same body as opposed to complex firms. In those, the appearance of the principal as owner influences the decision management. The agency problem arises due to the agent as decision-maker who initiates and implements the decision but does not bear the real wealth of the firm. Again, the control of the agency problem is necessary for the firm’s survival.

Eisenhardt (1989) divides the theory, from which the principal-agent and positivist agency model derives. Both base their theory on the relationship between the two parties set by contracts. His principal-agent approach adds characteristics like risk-neutral and profit seeking to the principal, whereas the agent is risk averse and seeks for rent. The positivist model on the other hand explains the cause and the costs involved in the problem itself. The causes either appear solely or in interaction, such in separation of the ownership from control, unsatisfying incentives, information asymmetry, different attitudes towards risk, and time of involvement in the organisation. Further, two propositions are made, considering in the first an agent acting in favour of the principal when the outcome of the contract is based on incentives and in the second that the principal penalises the agent if he has information on him prior contracting.

Donaldson's (1990) stewardship theory stands against the principal-agent model. In his theory, humans are noble beings who act out tasks ethically for the firm's advancement. His model is based on Perrow (1986), who criticises that research only focuses on the agent’s perspective of the principal-agent model. He brings forward that those problems may also arise from the principal's side. In opportunistic manner the principal exploits and deceives the agent which are working in defenceless environments and must deal with intrusions. Those intrusions manifest in, for e.g., Jensen and Meckling’s (1976) calculation of agency cost control.

However, Panda and Leepsa (2017) investigated on the agency theory to bring evidence on problems and perspectives. In their findings on limitations of the theory, they see the director role’s limitations to monitoring agreements on contractual basis between the two parties. The contractual basis stems not only from the will of wealth maximisation in uncertain time periods, but also tries to cope with uncertain events. In other words, the theory assumes elimination of uncertainties by contracting via agreements, compensation, and monitoring. Practically, it must deal with hindrances such as rationality, transaction costs, information asymmetry and fraud.

2.2 Corporate Governance: structure, role(s), and principles

Corporate governance derives from the agency theory. It serves corporate purposes through diligence which stockholders, directors, and management go after to effectively reach the goals of a corporation. Additionally, it can be seen as a solution to prevent and detect fraudulent activities and spare from adversely affections. Figure 4.3 gives an overview of the hierarchical order; detailed information on the single bodies is to find in Appendix A**.** It is defined by the European Central Bank (ECB) as:

> "Procedures and processes according to which an organisation is directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among the different participants in the organisation – such as the board, managers, shareholders and other stakeholders – and lays down the rules and procedures for decision-making" (ECB, 2005).

According to Hacıoğlu and Aksoy (2021), effective corporate governance must follow the principles of fairness, accountability, responsibility, and transparency. Fairness is the quality of independent actions and serves to guarantee protection that corporate governance vows to do. Hence, fair decision-making processes require accountability, responsibility, and transparency and underline their centrally located and intertwined relationship in corporate governance. The principle of transparency limits information asymmetry between stakeholders of a company. The interaction of fairness and transparency is a necessity to establish high level institutional quality that leads to effective information systems. The information system used is known as accounting. Accounting converts an organisation's actions into information and reports, thus into understandable, meaningful, and comprehensive outputs. The board of directors is authorised to manage the organisation and presents their activities to the stakeholders. Additionally, the audit committee ensures transparency and controls the board's activities and provides an independent audit report. These mechanisms establish the realisation of principles, namely responsibility and accountability. Therefore, accounting is the most significant tool used to manifest each of the principles defining corporate governance. In the following, an emphasis on the functions of internal and external audit is given throughout literature as accounting may not be free of failure.

Watts and Zimmermann (1979) established an understanding of accounting and its importance to be monitored as financial reports produced by managing bodies do not solve the agency problem alone. Further, contracts between agent and principal neither solve possible information asymmetries nor conflicts of interests due to a lack in determining whether these have been breached. Therefore, a natural demand for monitoring arises with the goal to minimise an owner's risk of being exploited to information in financial reports, that do not purport to represent what they must. Monitoring, also referred to as auditing, performs its obligations at two places, internally and externally.

Adams (1994) sees internal audit as a bonding of the contractual relationship between principals and agents. It may vary due to nature, structure, and complexity of control mechanisms implemented, nevertheless vows to help overcoming information asymmetry caused by agents in cost efficient manner. However, costs of monitoring depend on the severity of information asymmetry within an entity.

Opposed performs external audit from outside an entity. Lee (1972) sees its most important requirement by raising credibility in financial statements that result through and from accounting. Chedrawi and Howayeck (2018) state that decisions by internal and external parties based on accounting information run the risk of lacking credibility when they have not been subject to external audit. Further, external audit's major objective lies in securing an agent's stewardship and accountability towards the contracting entity and his performance within the entity.

On this account summarise Watts and Zimmerman (1979) that the contracting of auditors follows the objective logic of the principal to oversee accounting numbers, check processes behind compensation and bonus schemes, and reveal breaches of contract between principal and agent of any kind.

Corporate governance therefore inherits oversight, managerial, audit, and monitoring functions. However, vain endeavours of its kind showcase possible erosions, among others, financial statement fraud.

2.3 Financial Statement Fraud

The term fraud derives from several sources. In context of this work, looking into court cases shall offer a best fit solution. Judge J.J. Smith (1934) defined fraud as follows:

> "Fraud is a generic term, which embraces all the multifarious means which human ingenuity can devise and are resorted to by one individual to get an advantage over another by false suggestions or by the suppression of the truth. No definite and invariable rule can be laid down as a general proposition defining fraud, as it includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated." (Smith, 1934)

This work deals with a branch of it, financial statement fraud. Financial statement fraud is defined by the Association of Certified Fraud Examiners (ACFE) as “the deliberate misrepresentation of the financial condition of an enterprise accomplished through the intentional misstatement or omission of amounts or disclosures in the financial statements to deceive financial statement users” (ACFE, 2021).

To misstate, generally accepted rules in the environment of accounting need to be circumvent. The International Accounting Standards Board (IASB), as an issuer of general accepted rules, has the goal to create a single set of global accounting standards. Their International Financial Reporting Standards (IFRS) offer a framework-based approach to accounting standards and is adopted in more than 160 countries worldwide. A set on qualitative characteristics on financial information is depicted and ordered by objectives in the following:

- General

> “If financial information is to be useful, it must be relevant and faithfully represent what it purports to represent. The usefulness […] is enhanced if it is comparable, verifiable, timely and understandable” (IASB, 2021, p. 25).

- Completeness

> “A complete depiction includes all information necessary for a user to understand the phenomenon being depicted, including all necessary descriptions and explanations” (IASB, 2021, p. 26).

- Neutrality

> “A neutral depiction is not slanted, weighted, emphasised, de-emphasised or otherwise manipulated to increase the probability that financial information will be received favorably or unfavorably by users” (IASB, 2021, p. 27).

- Faithfulness

> “Free from error means there are no errors or omissions in the description of the phenomenon, and the process used to produce the reported information has been selected and applied with no errors in the process” (IASB, 2021, p. 27).

2.4 Surveys that underpin the fraudster’s profile

Financial misconduct is not happening geared towards the media every once a year, but rather on a constant basis. PricewaterhouseCoopers (PwC) (2020) show that more companies face fraud as rates remain at record highs. They are being attacked in more diverse ways than ever before; economic crimes, cyber-attacks on companies with millions of data hacked, medical records unlawfully used, product failure blames on unconscionable acting corporations, short selling of shares, and price plummets on alleged fraudulent accounting practices. Their survey on fighting fraud reports losses of more than €36bn[1] in the last 24 months across industries. Also, it unveils that nearly half of reported incidences result in losses higher than €86m[1] and were committed by insiders. The 2019 survey was conducted in 99 countries, involved 5000 respondents, of which 62% are senior level, and 72% of the companies have a global revenue higher $10m.

Farrell and Healy (2000) state, that the actual costs of fraud are difficult, if not impossible, to measure for many reasons as the overall loss is often times double the amount of missing money and assets. Further, fraud is and remains a globally occurring element of offence.

An investigation of Deloitte's (2021) Forensic Department in Russia and CIS countries between 2019 and 2020 reported that 23 out of 41 respondents encountered fraud. The fraudsters were most frequently mid-level employees. Also, even if senior-level employees involved in fraud was not as often the case as for mid-level employees, their illicit patterns exceeded losses from mid-level employees by a much greater margin.

The investigation of Ernest & Young (EY) (2020) on integrity and the future of compliance revealed that the more senior an employee, the more likely he or she is involved in unethically behaviour. They justify their behaviour to boost their own career progression or renumeration. In order, they ignore unethical conduct in their team, mislead auditors or regulators, and even offer or accept bribes. The survey included 2,550 interviews with senior decision makers across 55 countries between October 2017 – February 2018.

2.5 The awareness of industries to act

With the industries aware of the impact and threat of fraud in day-to-day business as well as insiders' possible role as perpetrators, the development of solutions to better tackle incidents brought forward through present and history, are of much concern. Participating companies of all surveys see the mastery of fraud in the search for appropriate measures and, hence, in the transformation of business processes and even whole businesses. Transformation of processes and businesses, however, is a two-sided sword. Gordon (2018) states in an EY survey on integrity and the future of compliance:

> "The transformation of business models due to the rapid evolution of digital technology is making the landscape of fraud, bribery and corruption risk ever more complex. We are in

[1] To the price of 1 USD = 0,8619 EUR on 2nd of November 2021

> an era of digital transformation that continues to challenge how all aspects of business are conducted — and the implications for the legal, compliance and internal audit functions are significant" (Gordon, 2018, p. 7)

According to several surveys, industries push forward in the use of advanced technologies as they are forced to adapt when their relevance is in an ever-dynamic environment shaped by trends, innovation, and digitalisation. To succeed in the process, businesses need to become more agile, leverage technology effectively, and innovate consistently. Internal structures deem it best to install robust internal controls, gather business intelligence, and transparent governance. Simply, businesses cannot afford to sit back and procrastinate on limited preparedness and foreseeable changes that can make them vulnerable in the future. By doing so, digitalisation alters traditional risks. When out-of-date risk assessments and antiquated policies, procedures, and controls remain while the digital footprint grows, companies miss opportunities to comply with corporate governance. Arising lacks in the development of timely solutions may be exploited by rogue employees and end up in new (types of) frauds, data thefts or other illegal acts. A continuous adoption helps companies to operate more ethically by helping to detect and even prevent fraudulent acts in the enterprise and among third parties. The careful assessment of risks, whether traditional or ethical, positions companies well for future regulations and changes. Proportionate steps towards digitised corporate governance, changes in working conditions and resilient business processes mitigate the emergence of fraud in the future (A. Gordon, 2020; Sokolov et al., 2021; Mahajan et al., 2016).

2.6 Fraud detection techniques

Fraud is a concern of organisations, let alone research and science, that conduct investigations in the field. Even though it distinguishes between two main types of fraud detection techniques, their line becomes thinner, if not blur due to the widespread of information technology.

The first is statistical data analysis that deals with statistical parameter calculation, probability distribution and models, regression analysis, and data matching. Kanapickienė's and Grundienė's (2015) work on fraud detection in financial statements by means of financial ratios is well founded on previous research studies that range from 1991 to 2011, showing the 51 most fraud-sensitive ratios in financial reports that predict fraud. These ratios concern profitability (return of investment and return of sales), liquidity, solvency, activity, and structure (total asset, current asset, and property). A possible detection of fraudulent information happens through a logistic regression model.

The second type is artificial intelligence that deals with data mining, neural networks, pattern recognition, and machine learning. Jan (2018) established an artifact using several instruments on financial and non-financial data to detect financial statement fraud. The combined use of data mining, artificial neural networks, support vector machines, classification and regression tree, chi-square automatic interaction detector, and quick unbiased efficient statistical tree marks a reliable and innovative approach on the topic. The combination of neural networks with classification and regression tree showed an above 90% fraud detection accuracy in 22 chosen variables, complementing rigorous and accurate data mining techniques mentioned in the paper. However, the study was limited by size and scope of the Taiwan market and its legal frame.

2.7 Blockchain and the transformation of business processes (?)

In the financial sector, trust is of utterly significance and seen to be provided by BC in the future. The hype surrounding it geared towards the media and induced numerous companies and industries to start projects on the domain. Attaran and Gunasekam (2019) state the aim lies in increasing:

- operational, regulatory and validation efficiency
- settlement time
- fraud defence
- intermediary reduction

while overall transparency between market participants attains. With BC to better track and understand goods and logistic processes, the team up of Maersk and IBM turned into a novel example of how to digitise, secure, and scale supply chain management processes (Androulaki et al., 2018). Several further applications and projects continue the technology's examination in manufacturing and industrial solutions, government and public sector, healthcare and life science professions, consumer goods and retail industry, cybersecurity, and data management. Chronologically, forecasts of spending expenditures in BC are reconditioned constantly. As International Data Corporation's (IDC) Spending Guide (2019) states, that blockchain spending of €2.3bn[2] in 2019 are 80 percent higher than in 2018. Overall predictions see the market to reach €13.2bn[2] in 2023 and then peak at €17.7bn[2] in 2025. (Sweet & Daugherty, 2020; Peng, 2020). After all, the technology's biggest exploitation and recipients of opening opportunities

[2] To the price of 1 USD = 0,8619 EUR on 2nd of November 2021

are in financial services, given the fact of being the backbone to Bitcoin. It is therefore no surprise that Fortune 500 companies and especially the Big Four firms, in respect of being auditing entities, engage in this market. Wolfsen (2020) refers: “The Big Four firms immediately understood that the value of blockchain is in the digital transformation of enterprise business processes, rather than in the cryptocurrencies domain.” In order, the following explains BC.

2.8 The basics of BC

Gayvoronskaya and Meinel (2021) explain communalities and differences of intermediaries and network structures. Intermediaries are part of our daily lives. Banks, social networks, online traders, or cloud storage providers allow (free) access to their online platforms as well as support daily needs and connectivity with services and infrastructure to their customers. When an issue occurs, it is providers as central instances that are responsible and stand in. In a situation of transferring a high amount of money to an incorrect account number, the bank can easily track and reverse the false transaction. On the downside, personal data is stored on the banks network and in case of a hack easily accessible without permission. With the General Data Protection Regulation (GDPR), mediators ensure to tell what happens to personal data and who gets entrusted with it. By handing over personal data of any kind, the level of trust is high. This concept is called the client-server model. The customer (client) obtains services by requesting it (at the server).

On the other hand, a peer-to-peer (P2P) or decentralised network involves participants who are simultaneously service users (clients) and service providers (servers). In context of BC the term for participant is “node” and will be synonymously used in the remainder of this work. With the dissolution of an intermediary, the division of trust, management and resources is handled among its nodes. BC can handle issues related to untrustworthy nodes. It derives from Distributed Ledger Technology (DLT) and must be considered a branch of it. DLT is a special form of electronic storage and data processing. It allows participants in a multi-party system network to share access for reading and writing purposes. DLT is of much greater space than BC, as the latter uses a specific layout to structure data. Figure 1 illustrates the underlying ideas of the three theories.

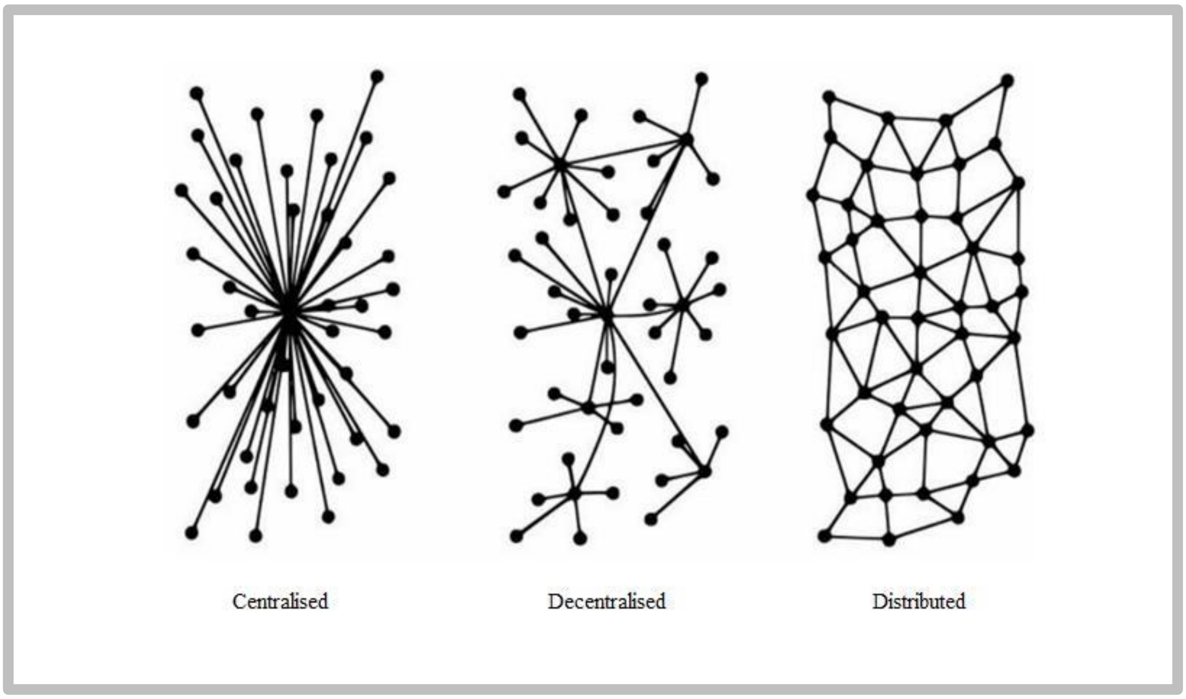


Figure 2.1: Difference between network types (Ruiqi, 2020)

Nakamoto (2008) introduced a whitepaper to a digital currency and cash system, namely Bitcoin, in the aftermath of the global financial crisis in late 2008. It further elaborated the idea of Haber and Stornetta's (1991) work, who developed cryptographically secured linked chains of blocks of data and transactions to certify creation and modification via timestamps. The terms Bitcoin and Blockchain are often used as synonyms which is incorrect. Bitcoin processes digital payments in its respective network that is running on the underlying technology of Blockchain. The Bitcoin system enables a robust and secure network for everyone free to join and to leave. Among others, there are several more Blockchain solutions such as Ethereum. In his whitepaper, Buterin (2013) explained what Ethereum is and wants to be. He states that it merges and improves the concepts of Bitcoin and different other BC solutions to provide an abstract foundational layer for developers. Those have the possibilities not only using its features, but also developing own solutions and rules on ownership or transactions formats, a part of which is now considered smart contracts and to find in Appendix B.

2.9 Types of BC

Over the course of time and development efforts, two types of BC established and are distinguished between, permissionless and permissioned.

Permissionless BCs are characterized in a way that anyone can join or leave the network at will. Participation in reading, writing, and verification of data is granted to all equally, which guarantees transparency as checks on records can happen at any moment. The examples given on consensus mechanisms (Appendix B) handle verification of transactions, namely proof-of-work and proof-of-stake. The most prominent permissionless BCs are Bitcoin and Ethereum, creating and using native digital assets, namely cryptocurrency (O'Leary, 2017; Liu et al., 2019; Beyer et al., 2018; Nakamoto, 2008).

Permissioned BCs are characterized that they are only available to a certain group of users. A delegated node or a delegation of nodes are responsible for the operability and access authentication. Additional rights are assigned, determining reading, writing and verification of the data. The proof-of-authority consensus algorithm (Appendix B), among others, is the preferred consensus algorithm (O'Leary, 2017; Liu et al., 2019; Beyer et al., 2018). An example for a permissioned BC is HyperLedger.

2.10 BC characteristics

The successful combination of existing technologies makes BC an innovative technology. It uses cryptography, decentralised network structure and consensus finding models to build trust among unknown nodes. Lakhani and Iansiti (2017) summarised the core characteristics as follows:

- *Distribution* of all entries and their history, with no intermediary present.
- *P2P* transmission allows the storage of all information in the system and division to all nodes.
- *Transparency* is provided through availability of transactions to everyone in the network under a pseudonym.
- *Immutability* A transaction entered in the database cannot be altered when it is updated. The transactions are linked with each other, hence the word "chain". A cryptographic hash function ensures that alteration will be unveiled.
- *Consensus* is reached through computational logic which further allows the programming of transactions itself. Users can set algorithms and rules to automatically trigger transactions between participants.

Understanding the characteristics of BC is to understand the characteristics of its single parts. Appendix B gives a detailed overview of these characteristics and their interrelations. Even though reading is highly advised by the author, the specifications mentioned in the following are sufficient to reach the conclusions in this work.

2.11 Contributions of BC to accounting

Literature, white papers, organisations, and authorities frequently propose BC as foundational infrastructure in the accounting environment, leading to real-time accounting. The rationale behind this proposal is the infrastructure of the technology that possibly enables immediate facilitation of financial records. Transactions become more reliable due to its decentralised nature and do not necessitate an intermediary which results in cost and time reductions. The combination of gains in transparency and the cryptographic securing imply immutability. It also guarantees that no record or transaction can be altered later and if so, the rate of detection raises significantly. Given these attributes, the execution of business dealings concerning financial activity through BC has the potential to successfully mitigate accounting misbehaviour, unlawful trading, and other means of data manipulation. (Yermack, 2015; Andersen 2016). The following introduces the main theme and its subordinates of BC contribution to accounting.

The double-entry accounting system is relied upon for more than 600 years, but also inherits flaws such as lack of transparency and time-consuming evaluation of transactions for auditors. In their profession, auditors influence the credibility of firms through the confirmation of an entity's private information with outsiders as well as examine and test internal controls. They are representatives of an occupation that demands faithfulness and trustworthiness which are relied upon. However, accounting information are still too concealed for external auditors. Records can fall victim to alteration or accounts do not resemble what they purport as internal manager oversight may facilitate fraudulent activities. That is why increasing transparency through the potential use of a triple-entry accounting method promises more efficient and fundamentally trust building improvements. (Cai, 2021; Inghirami, 2020)

On this account elaborated Ijiri (1986) further his idea on a triple entry solution for the double-entry approach in accounting. "Momentum accounting" records the currency per second in a set period that can be associated with assets and liabilities. The additional third layer, namely "force accounting" is introduced and actions, under a disciplined framework of measurements, the forced entry of two parties in a shared ledger. Grigg (2004) proposed a solution to tackle accidental errors and fraud in accounting. He further stated that companies should not be solely responsible for their records. With a cryptographically secured entry of a transaction between two entities, a third ledger gets filled with respective information and records one's debit as its counterparty's credit. The creditor signs a receipt with all transaction-related information on the third ledger which the debtor signs to approve the transaction. The third entry is immutably stored in a shared ledger and, hence, guarantees that later changes are impossible.

2.12 Conceptual Framework

The above-mentioned literature proved interrelations of two different topics on the core principle of trust in abstract manner. Thus, the following contribution needs to wander between theory, legislation, management, technology, and even psychology. Their boundaries blur throughout the section. This is due to a technology-centred approach that tries to deal with an issue occurring in human relationships; due to using technology as prolonged arm for utilising processes in business context. Consequently, having identified the carrying pillars behind two different topics, the elaboration of interrelating subordinates between these topics will justify or drop further assessment. The approach resembles a rather managerial than technical point of view. However, its elaboration requests technical understanding and necessitates understanding of information technology corresponding with requirements of all affected tiers in range of accounting and BC. Further, the objective consists of a joint technological-organisational development in the respective fields.

3. Methodology

The creation of concepts is essential in the global dialogue of science-based research. However, research is not purely conducted in the search of empirical evidence, but also through rhetorically based concepts. Reflecting, developing, and refining in a profound manner on both these concepts shape cultural dialogue in the long-term. Considering the degree of master's in management (M.Sc.), the following methodology is an essential component of research and a contribution to the global dialogue of what science represents.

The conceptual method, often referred to as "desk research", allows to identify patterns and create concepts from priorly conducted studies and their significant findings. This creates space for comparison, contrast, refinement, and reflection by "raising above" narrow and detailed investigations, using a wider angle, and reaching a holistic approach. It is shaped by both, an exploratory and descriptive nature and composed of scientific papers, journal entries, academic books, and white papers that use different frameworks. It must be mentioned that the exploratory ingredients outweigh descriptive ingredients. However, as part of this work, case studies have been conducted which are clearly defined as descriptive research methods.

The overall aim is to identify characteristics, patterns, and correlations. The data was found and gathered on platforms such as Google Scholar, SpringerLink, Researchgate, B-on, YouTube, and the ISCTE Repository. The latter can be classified as an internal desk research, the other mentioned are clearly definable as external, including online and governmental sources. They consist of both, qualitative and quantitative data. In terms of sampling, if to speak of sampling over the course of a desk research, a non-probability classification fits best as to the rather detailed information requested by literature about a specific context. The timescale is defined as a cross-sectional study that gathers data at a single point in time and tries to understand the current situation, even though using data from past centuries that allow the drawing of conclusions to the present of this study. The location can be clearly defined as flexible due to the overall general approach of the research and the development of topics throughout the data collection process.

Considering search terms and conditions, the evaluation of the research conducted followed the principles of reliability and validity. Reliability was claimed to the extent of consistency in the review of literature. Its validity is reached through the correspondence of the initial keywords and the use of reliable sources mentioned priorly. Due to the nature of this study being a desk research, reliability and validity are object to the subjectivity of the author, and hence, do not guarantee to be overall reproduceable. However, appropriate methods of measurement, their application, and the standardisation of conditions of the research conducted was handled to the best of the authors knowledge and abilities.

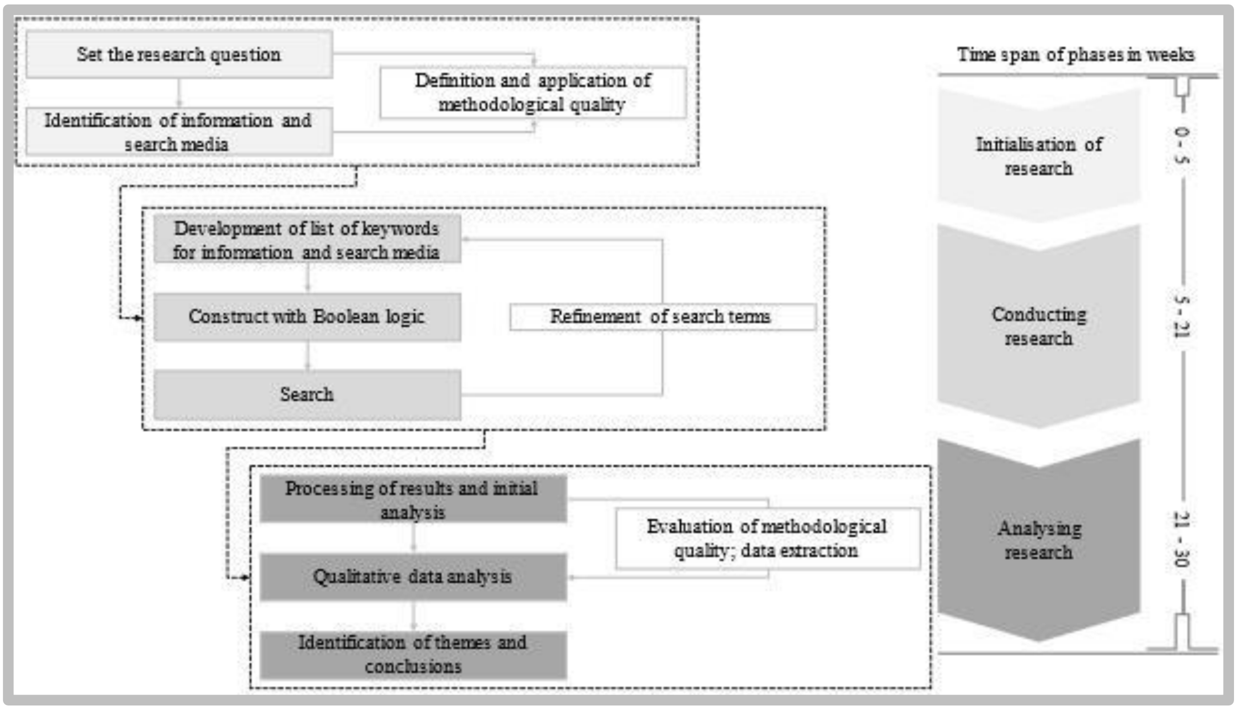

Set the research question
Definition and application of methodological quality
Identification of information and search media
Development of list of keywords for information and search media
Construct with Boolean logic
Refinement of search terms
Search
Processing of results and initial analysis
Evaluation of methodological quality; data extraction
Qualitative data analysis
Identification of themes and conclusions
Time span of phases in weeks
Initialisation of research
Conducting research
Analysing research
0 - 5
5 - 21
21 - 30

Figure 3.1: Schema of conducted literature research

Processing the results of the research conducted involved several steps. As indicated in Figure 2, qualitative analysis required an evaluation of the methodological quality on which the data extraction was based. Thereafter, the identification of themes and their conclusions mark the beginning of the section referred to as obtained results.

This approach was chosen because of several reasons. Topics concerning accounting and financial statement fraud are well researched. The gathering of profound information and insights did not require additional primary data. In terms of BC the reasoning is different as to the novelty of the technology and its use in business context. Despite profound information on the technology itself, inquiries for primary data concerning the accounting domain became victim to a high possibility of being biased. The use of BC in accounting is to a great extent brought forward by enthusiasts of the technology that lack professional criticism. Additionally, criticism on the technology form different perspectives does rarely exist, or the technology is not considered at all due to its still early stages in the development. Further investigation also unveiled significant lacks understanding the technology in its entirety.

Keywords chosen for Boolean logic: Beneish M model, Benford’s law, Bitcoin, Blockchain, blockchain evolution, blockchain technology, blockchain XBRL, business ecosystem, Business model, Cloud computing, continuous auditing, creative accounting, Distributed Ledger Technology, Ethereum, financial accounting, financial statement fraud, financial statement fraud detection, forensic accounting, fraud, fraud detection, HyperLedger, implementation blockchain accounting, management accounting, permissioned blockchain, principal agent theory, real time accounting blockchain, statistical parameter calculation, swiss cheese model, triple entry accounting, value creation, XBRL

3.1 Limitations:

Exploratory research brings value in understanding specific problems but lacks conclusive results. Further, it must be noted that the gathering of primary data was excluded. This comes with a limitation in controlling qualitative and quantitative data generated. An extra processing in the analysis to ensure fit to this work's purpose is also required and can result in erroneous transfer. Another issue goes along with a limitation on data itself, meaning the reliance and dependence on data sets. Qualitative data can neither be analysed statistically nor generalised to broader populations in prospect of future research. Additionally, they are subject of bias due to the interpretation of the author and hence, be judgemental. Considering quantitative data, preliminary goals, predictions, or causal relationships cannot be influenced and the existing dependence of primary research by other researchers may harm the success of one's own research goals.

4. Obtained results

In the following are results of the research displayed. To comply to this work's concept and enhance reading, the obtained results, findings, and the discussion will not only go hand in hand throughout this section, but blur in the process of reaching the section referred to as conclusion. The section inherits themes that pick-up topics found in literature as well as contribute to the overall research question of whether BC is a useful tool in financial statement fraud detection. These themes depict:

- Assessment of initial BC and accounting interrelations
- Assessment of in-depth BC transaction functionality and security
- Assessment of the fraudster's profile in BC accounting scenario
- Assessment on the literature concerning BC in accounting

4.1 Assessment of initial BC and accounting interrelations

Literature showed interrelations of several topics that shall be investigated in the following section. Trust, in abstract manner picked up by the agency theory and BC, is discussed and references back to the literature are drawn. Investigating on the interrelations of BC and the legal framework provided by IFRS accounting standards, shall give insights on the usage of the technology within parts of the legal framework surrounding the accounting domain. This step introduces the concept of triple-entry accounting, a framework that utilises BC in the accounting domain. The assessment of initial interrelations concludes on XBRL, a format to create electronic financial statements.

4.1.1 Assessment of BC and agency theory

The attributes of BC allow it to be chosen for further elaboration in an agency theory set environment. The agency theory is the leading theory of governance and therefore defines its development and implications. It deals with conflicts between shareholders, managing directors, legal authorities, and governing institutions. Corporate government's conflicts, one of which is trust, are still not solved through theoretical and legal frameworks. Historically, trustworthy and knowledgeable people were given the responsibility of integrity. Lemieux & Feng (2021) refer that this unquestionable trust is continuously eroding due to manipulation of records and information. Trust is at an all-time low when it comes to data and records as the confrontation with willingly provided misinformation happens daily. This complements both, Berle and Means' (1933) and Ross' (1973) assumption of the agency problem as a matter of trust, its share in society, and compensation models. Agency builds around a firm's structure and needs to evolve to deal with imperfections and its problems. This structure is the structure of agency control involving monitoring, bonding, and residual costs which exceed in decision management and decision control environments (Mitnick 1975; Jensen & Meckling 1976; Fame & Jensen 1983). On this note used Hacıoğlu and Aksoy (2021) accounting as the deliberate translation of corporate governance, hence agency theory. Taipaleenmäki & Ikäheimo (2013) (2013) framed a concept that deals with the convergence of management accounting (MA) and financial accounting (FA) and what role information technology holds in the process. They found information technology serves as a facilitator, catalyst, motivator, or an enabler in the respective field. Their outcomes showed that the technological domain, related to standard setting in FA, precedes the organisational domain, related to internal reporting practices of MA, that possibly motivates to realise changes in MA and in which IT has had a dominant role in doing so. In this context, IT, in the shape of BC, becomes the foundational structure of accounting. It builds an environment that no longer needs to rely on internal and external control mechanisms as it inherits necessary corporate governance while substantially increasing efficiency in the agency relationship and lowering controlling costs. Its ecosystem is shaped by the absence of intermediaries and presence of a majority of truthful computing power, encryption, and consensus algorithms. However, this could only be the case in a self-containing universe with native digital assets. In a scenario of full native digitality, another qualitative shift is the one towards information symmetry in financial disclosures, causing the incentive-based contracting in the agency relationship (Eisenhardt, 1986) to become rather risk averse for management pressured from stock performances and investors.

4.1.2 Assessment of legal framework

When BC is put in context with company environments, the need to address current theoretical and legal frameworks becomes mandatory. In the case of accounting, the information processed within the BC ecosystem becomes a subject of public interest and, hence, is subject to auditing since legal authorities, as part of corporate governance, have a share in controlling accounting standards. From an information point of view, conceptual frameworks allow to consider uncertainty, multiple agents, demand for information, and multiple information sources. Accordingly, it must comply to IFRS as this work's conceptual framework for accounting standards. With their set on qualitative characteristics on financial information, it subtly provides necessities to be met from Accounting Information Systems (AIS), a system that BC claims to become. Those objectives derive from the following perspectives:

- General

> "If financial information is to be useful, it must be relevant and faithfully represent what it purports to represent. The usefulness […] is enhanced if it is comparable, verifiable, timely and understandable (IASB, 2021, p. 25)."

Quality in financial information inherits high relevance and makes a difference in the decisions made by MA. Moreover, conceptual frameworks and its approach can result in a comparative advantage over other sources of information.

- Completeness

> "A complete depiction includes all information necessary for a user to understand the phenomenon being depicted, including all necessary descriptions and explanations (IASB, 2021, p. 26)."

In understanding the complete depiction of accounting information provided, the ability to assess management performance and its implied decisions, both financial and material, is given. The AIS's design supposedly guarantees its users to understand how information got collected, processed, and reported.

- Neutrality

  “A neutral depiction is not slanted, weighted, emphasised, de-emphasised or otherwise manipulated to increase the probability that financial information will be received favorably or unfavorably by users (IASB, 2021, p. 27).”

Representational faithfulness in information provided in an AIS should be free of any error or bias. Therefore, the major goal of an AIS must be the elimination of any bias or error.

- Faithfulness

  “Free from error means there are no errors or omissions in the description of the phenomenon, and the process used to produce the reported information has been selected and applied with no errors in the process (IASB, 2021, p. 27).”

The process of an error free creation of representational faithfulness in financial information is represented by the process of BC itself and applies to all objectives of the IFRS qualitative characteristics. However, the process within applied BC’s is coherent. This is due to its native ecosystem. To successfully assess its establishment, it needs to be assessed in an accounting environment consisting of a legal framework leading to financial statements based on which it is audited.

4.1.3 Triple-Entry accounting

BC has the potential for automation in processes. Transactions embedded in triple entry accounting environments may even make use from smart contracts to predetermine payment rules on a self-executing digital contract. The "third-party" involved is resembled by the blockchain ledger and avoids errors or fraud. Chronologically ordered and permanent without change, transactions are not maintained on a centralized system. This approach guarantees a higher degree of security. Additionally, the linkage between internal records makes them easily identifiable and creates an audit trail that is different to double entry accounting. Approaching accounting through a triple entry solution adds transparency, and reduces audit times with its associated costs while enhancing overall operational efficiency (Dai & Vasarhelyi, 2017; Mosteanu & Faccia, 2020; Cai, 2021)

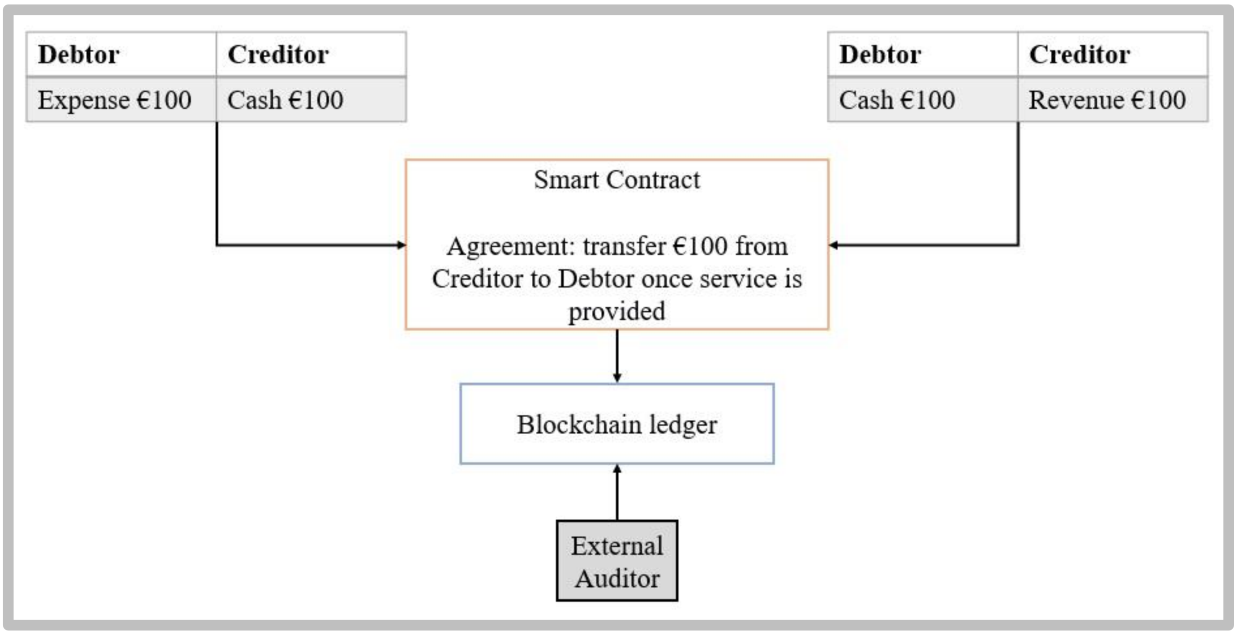


Figure 4.1: Triple-entry accounting system with blockchain - own illustration (Cai, 2021, p. 10)

However, the implementation of a third ledger with BC as foundational system brings other issues. Significant from a business point of a view is privacy of data and information that presents conclusions on a corporation's strategy. Several approaches try to deal with this issue by different means; records only consist of hash values from their respective transaction, receive verification through a trusted third party, or contents are hidden with cryptographic schemes (Narula et al., 2018). The first approach eliminates the core attribute of a distributed ledger as it eliminates public verifiability. Verification through trusted third parties in the second approach reveals transaction contents to the auditor, therefore revealing strategic information. It does offer public verifiability but neglects corporate privacy concerns. Scalability concerns also need to address performance setbacks due to many distributed ledger copies. The throughput of merely 15 transactions per second on one of the most popular blockchains that is considered for this very approach, Ethereum, is limited in comparison to VISA with a throughput of 30,000 per second (Cai, 2021). Tackling the issue of scalability is brought forward constantly in blockchain designs. One hurdle to take in terms of accounting is performant semantics, meaning to use a "language" of data that is understood worldwide. Current accounting information or business systems in general have their own data sources and languages that vary between companies. Harmonisation of semantic information not only offers faster performance, but also adds potential to interoperability of BC ecosystems.

A possibility is seen in eXtensible Business Reporting Language (XBRL). The language transforms paper written reports into an electronically unique information format by tagging individual disclosure items within financial statements (Tie, 2005). It is the standard set for digital exchange in financial information and enables data modelling, financial data examination, visualisation of information, and ultimately creates a taxonomy such as the IFRS (Beerbaum, 2020). The standards it provides allow standardised methods application such as historical analysis that reclassifies statements and their indices in financial statements as well as prospective analysis and proforma statements that MA uses. The most promising literature in the field remains with Duncan *et al* (2019). Introducing and testing their system architecture that used the combined efforts of BC, smart contracts, XBRL, and statistical data analysis for further verification in the process, they evaluated a system that could possibly run on the Ethereum BC. The study was limited to the Italian market and was based on an offline system. Cost approximates and performance evaluation showed a linearity which initiated further research on file compression and "on-chain" transactions.

4.1.4 Assessment of BC and XBRL

The legislation on auditing and auditing standards have not agreed upon any rules, yet verifying and auditing financial statements in XBRL when committed and disclosed (Mosteanu & Faccia, 2020). According to the International Auditing and Assurance Standards Board (IAASB) the auditor is not required to verify the conversion from written financial statements into XBRL. Since XBRL is used only to transform the financial statement into electronic data, the format is not considered "other information" in this process. According to ISA 720, international audit principles:

> "This ISA requires the auditor to read and consider the other information because other information that is materially inconsistent with the financial statements or the auditor's knowledge obtained in the audit may indicate that there is a material misstatement of the financial statements or that a material misstatement of the other information exists, either of which may undermine the credibility of the financial statements and the auditor's report thereon." (IAASB, 2015, p. 6)

Further stating in the definitions chapter of application and other material: "eXtensible Business Reporting Language (XBRL) tags do not represent other information as defined in this ISA" (IAASB, 2015, p. 12). Hence, an auditor's assessment for any inconsistencies of financial statements and XBRL submitted is not required.

4.2 Assessment of in-depth BC transaction functionality and security

This section provides detailed information on a core principle of transaction creation within BC systems and uses former research on the security of BC systems to introduce the principle of layers in such. Both topics have been neglected on the broad literature of BC and accounting so far and will bring new perspectives to an overall evaluation.

4.2.1 From Transaction to Ledger – the concept of the ledger

Key concepts on the terminology of how transactions enter DLT systems can vary. A ledger in terms of BC can be defined in two different ways according to the authors, either describing a "set of data held by an individual network node, or the set of data held in common by the majority of nodes" (Rauchs et al., 2018, p. 25). Transactions that ultimately lead to a ledger are processed always in the same way. These key concepts shall be outlined.

A transaction must not necessarily contain a transfer of assets between nodes but can also inherit exogenous data. Exogenous data represents data that is exclusively existing outside the boundaries of BC systems, contrary endogenous data that only exist in a self-containing universe such as to find in the Bitcoin system. A proposed transaction enters the BC system by deliberate enforcement of the sender. It then enters the Mempool, a pool for unconfirmed transactions, waiting to be processed and subject to testing of validity. A series of tests for validity is concerned with conditions set in the protocol. Every node in the system has a Mempool, offering their computing power to the network for processing and validity testing. As every node inherits a Mempool, they inherit a different set of unconfirmed transactions due to every node's different computing power to offer. All nodes/Mempools create peering relationships and share pending transactions. These relationships can vary between 20 – 100. If a sender wants to ask: where is my transaction? it needs to ask all nodes in the network. If the "mindset" about transactions being on-chain is a single-source of truth, the truth about pending transactions is a truth spread across all nodes in the network. The testing of validity of a transaction is subject to the network consensus algorithm, which makes it compete against all transactions for block space. Reaching a block space means to have passed the test for validity. In simple words, transactions compete against transactions to be chosen for a block. This competition determines the time to confirmation. Each node/Mempool arbitrarily selects a set of unconfirmed transactions from the Mempool and creates a candidate record. The candidate record gets broadcasted to connected nodes when it is valid. Validation is reached when meeting the specified conditions in the protocol. Next step is the testing of each node verifying the candidate record for compliance with the protocol, adding it to its own journal when passing the test. The BC ledger represents agreed-upon journals of individual nodes by synchronising individual journals (Deneuville, 2016; Blognative, 2021; O'Connor, 2020)

4.2.2 Layers and their security in BC systems

The BC system contains of several layers, upon which the literature has not entirely agreed upon. However, standardisation models, such as the Open System Interconnection (OSI) model led to reference models that are used by practitioners as well as researchers. Popescu-Zeletin (1983) states about the model:

> "it is an efficient framework for developing complex hard- and software in networks; is mandatory for future changes and integration in the domain to set new standards and develop products; active participation in the standardization shortens implementation time; formal description is mandatory to achieve compatible implementations by different teams on different machines; testing procedures and reference implementations is a necessity for heterogenous networks and has to be considered in the design from the beginning" (Popescu-Zeletin, 1983, p. 62).

The following investigations summarise general threats and countermeasures of which Homoliak *et al* (2021) proofed to be the most profound due to its holistic approach. Homoliak *et al* (2021) used a security reference architecture which adopts the OSI model. It stacks four layers (Figure 4) in a BC system to describe the nature and hierarchy of various security and privacy aspects. Its hierarchy is shaped by a next-level principle that starts on the network layer, meaning its sequences defined in the protocol can overrule the layers above. By identifying known threats, origins, and countermeasures, several dependencies from a cross-layer-point-of-view were also analysed. In their observations they identified substantial smaller incidents than described in overall literature. In case of the application layer most incidents occurred due to exploitation of central components. These exploitations were based on internal and external attackers. In case of the consensus layer, 51% attacks occurred due to temporary violation of protocol assumptions. A 51% attack makes an attacker possess most of the computing power within the network and raises the probability of creating a block before all other participants significantly.

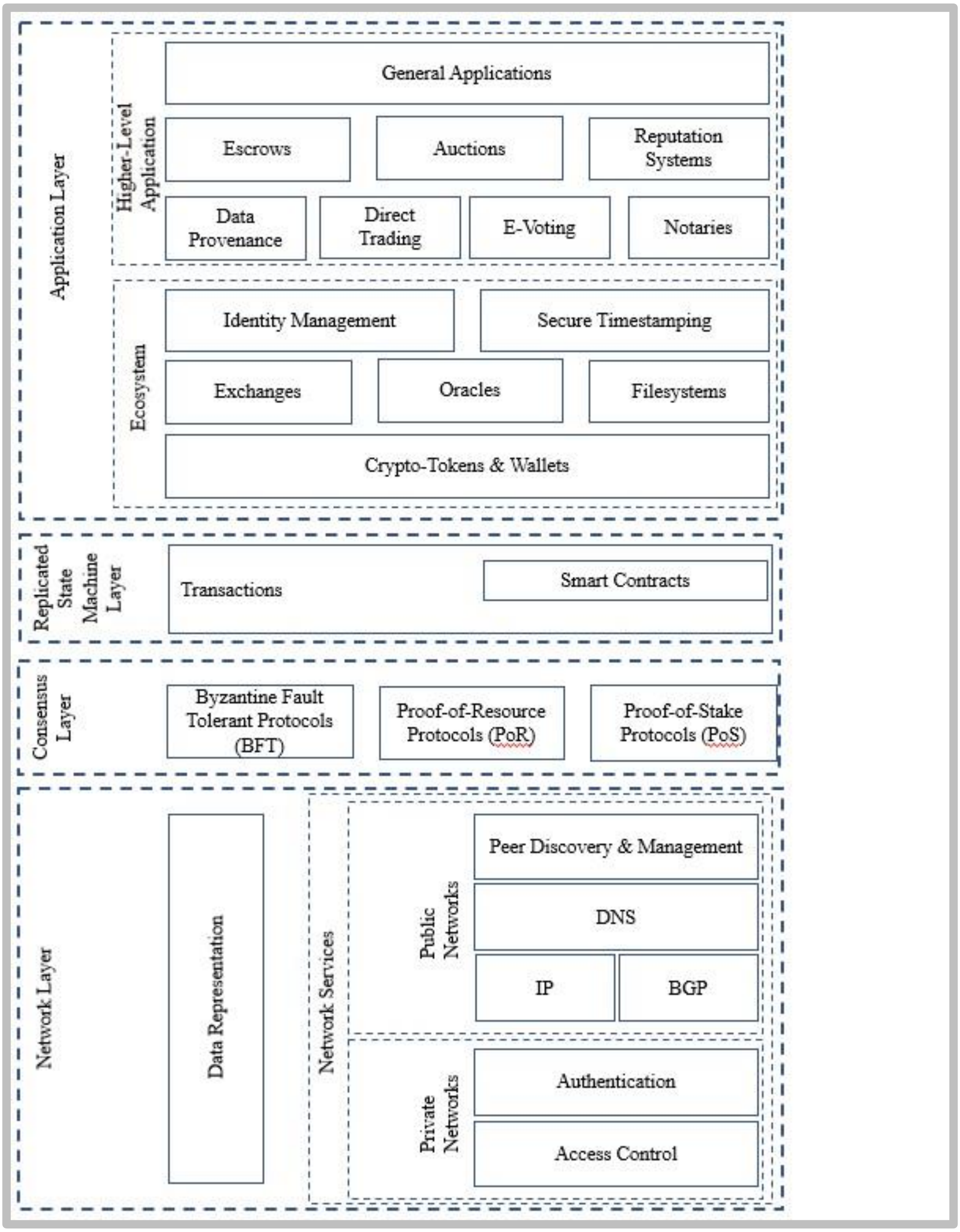


Figure 4.2: Stacked model of BC architecture - own illustration (Homoliak et al., 2021, p. 5)

However, among others, researchers proposed different types of layer indications and amounts. Wang *et al* (2019) propose a "network implementation stack" that resembles a perspective of system design in which the BC network got abstracted into four layers initially. Chen *et al* (2019) used a four-layer model to investigate on vulnerabilities in Ethereum, identifying 44 of them, in which most of them belong to the network layer. However, not all the vulnerabilities are specifically inherited by the Ethereum architecture. Zhang *et al* (2019) used in their study a six-layer model. Characterising security and privacy attributes of blockchain, they tested the application against several inherent techniques, concluding in their argue that an in-depth understanding of security and privacy properties is crucial for enhancing the degree of trust that BC may provide as an innovative and robust system as well as technological developments on defence techniques and countermeasures.

4.3 Assessment of the fraudster's profile in BC accounting scenario

The following section gives insights into former cases of financial statement frauds by investigating on them and laying key take-aways open. By using these key take-aways and overlapping them with the research conducted in this work, an answer to the overarching research question is provided.

4.3.1 Case studies on financial statement fraud

Financial statement frauds in history of business show significant failure of agency theory in corporate governance and neglect, at least, qualitative characteristics on financial information mentioned priorly. Ranging from 2001 to 2009, they include Enron Corporation, Worldcom Inc., Tyco International Inc., Parmalat Finanziaria SpA, and Satyam Computers Services Limited. In all cases the board of directors showed a lack of independence. Additional subjects involved were compensation model abuses, weak detection infrastructure, compromised auditors, bribery, and ineffective whistle-blower policy (J. N. Gordon, 2002; Beresford et al., 2003; Sadka, 2006; Kemmerer & Shawver, 2007; A. Ross & Berenson, 2002; Srivastav & Uzma, 2010). Detailed information of the case studies conducted are to find in Appendix C. Figure 5 gives a general idea of matter of facts in their respective element of crime.

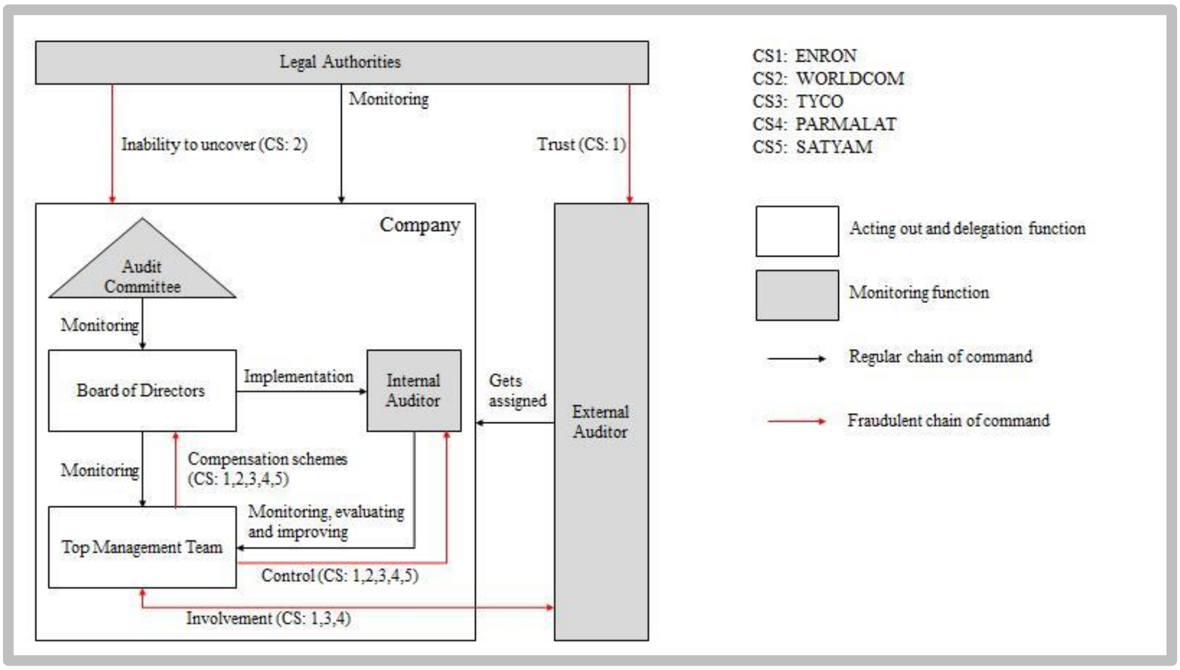


Figure 4.3: Generalisation of fraud patterns - based on Rückeshäuser (2017)

4.3.2 End of the line – the first mile problem

BC systems considering business processes face an issue that is known as first mile problem (Alles & Gray, 2020). It arises when the data to store is not natively digital, meaning it is about a physical item in the real world. The best example of a native digital construction is the Bitcoin network. Its reality is a self-contained universe in cyberspace that reflects to the real world. All extends in the literature on BC and accounting in this work could not overcome this issue. By building a BC based universe within company structures, they all faced the issue of whether the data put in a system is trustworthy. The agency theory installs monitoring instances as it argues that people and their actions, one of which is accounting, may be untrustworthy and do not reflect reality in form of the financial statement. This puts the financial statement and accounting actions that led to the issuing of the statements into the spotlight. Auditors, contracted by principals to verify financial statements, can be compromised too, and verify falsified information. As the enforcement of records is of exogenous nature in corporate BCs, the validity of the data is linked to the enforcing entity**.** Thus, the agency problem in corporate governance was and remains persistently present which puts BC in the corner of being questionable for the use in accounting and hence, for fraud detection. Even further, the use of BC in corporate context may give space to management override activities, a phenomenon highlighted by Rückeshäuser (2017). She states that management could override internal control mechanisms, especially through choosing the strength of them.

The suggested use of BC's as internal control mechanism becomes questionable in such a scenario. As investigations on BC security undertaken by Homoliak *et al* (2020) laid open, incidents occurred on the exploitation of central components from internal or external attackers on the application layer. Considering the proposed stacked model, within the application layer are oracles to find. Oracles transmit external data to the system (Rauchs et al., 2018). Management must be considered throughout the process of accounting as oracle. This is due to being the last instance in the hierarchical order, in charge of financial statement creation, and especially due to the lack of a native digital environment. In addition, Homoliak *et al* (2020) brought forward 51% attacks occurred due to temporary violation of protocol assumptions in the consensus layer. The continuous suggestion of permissioned BCs in corporate context, considering this kind of attacks, neglects key concepts of consensus finding between nodes. As stated by (Deneuville, 2016; Blognative, 2021; O'Connor, 2020), nodes find consensus by sending their own journal to at least 20 nodes. This process happens in permissionless BC environments. In terms of permissioned BC's, Rauchs *et al* (2018) brought capabilities of properties in DLT systems forward that are crucial for its reliability, among others, multi-party-consensus in which it is stated: "If permissioned, through multiple record producers who have been approved and bound by some form of contract or other agreement." Due to this contracting, an additional principal-agent relationship arises between management and record producer or embodies both in one person. In a more realistically scenario, more than one record producer will be appointed. However, restating Gordon (2018) "the transformation of business models due to the rapid evolution of digital technology is making the landscape of fraud, bribery and corruption risk ever more complex". The case studies conducted showed not only significant lacks in the board's independence, but additional other controlling failures of instances, either being compromised, too, or not functioning accordingly. A situation that prevails to this day as the study conducted by PwC (2020) indicates. With a high number of questioned employees and the global range of the survey, it compliments Rückeshäuser and vice versa. Highlighted in red were misconducts that were presented in the chapter 4.3.1 Case studies on financial statement fraud. They are significant as actions, among others or in different constellation, happened additionally to the case studies on financial statement frauds.

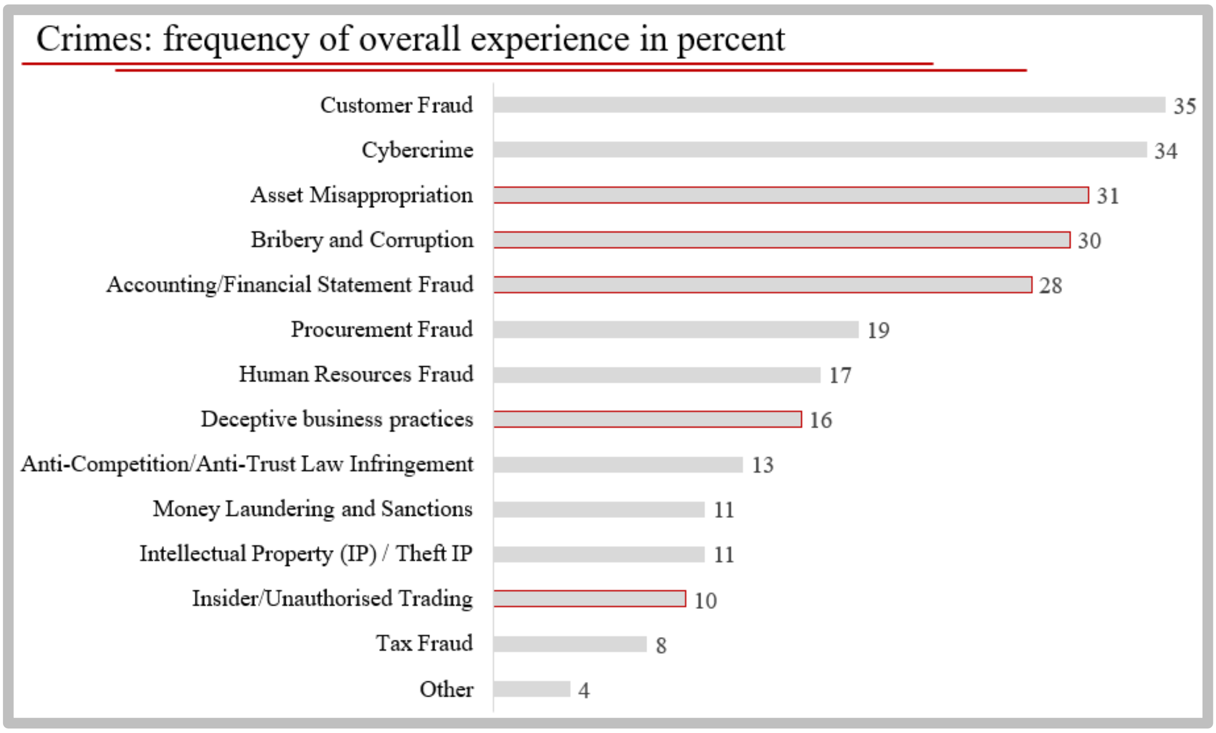


Figure 4.4 Crimes: frequency of overall experience in percent – own illustration (PwC, 2020)

Additionally, in a case of management override, the external auditor possesses no need to revise evaluation on the management's integrity, which ultimately leads to inefficiencies in the overall control system. It essentially harms not only Lee's (1972) basic requirements on external auditors but also Chedrawi and Howayeck's (2018) statement that financial information lack credibility if they have not been subject to external auditors.

In conclusion, "off-chain" agreements, trivial in their origin, may cause the same if not worse adversely affections stemming from accounting and financial statement frauds as their records are represented by a system that, according to Lakhani and Iansiti (2017), implies immutability.

4.4 Assessment on the literature concerning BC in accounting

The suggestion of BC in accounting is not new in the field but lacks serious holistic approaches. The term Blockchain is used in an inflationary manner as every distributed solution seems to inherit all attributes that define a Blockchain. However, this is not true. The span of attention and detail wanders between fractions of the system and deals with issues related on the surface, rather than diving deep into the Materia. Focal points of research in the management domain gather mainly around the application layer and suggest topics, among others, such as triple-entry accounting, or a change in the auditor's role. It suggests taking place in an already existing ecosystem in which either one and the same DLT system across all participants of an industry is used, or interoperability remains a question of when and not how.

4.4.1 The misconception of BC and DLT

As mentioned at the beginning, BC systems are a branch within the domain of DLT systems. A major misconception derives from the fact that literature deals with BC but means DLT. This may be due to missing generics in their definitions but also to lacking attention of distinguishment. Rauchs *et al* (2018) brought forward that

> “decentralisation is often treated as a binary feature of DLT systems, instead of a continuous variable resulting from the interplay of the various layers and nested subsystems within them. This is partially due to examples in the current literature which do not break down the system into different components and examine the relationships, dependencies, and interactions between these different elements” (Rauchs et al., 2018, p. 21).

However, as highlighted by Xu *et al* (2019), research on the topic of BC is still in its infancy. Figure 7 portrays the effort and aspiration research puts into the domain, trying to delve into deeper spheres. Their systematic review comprises of 925 papers in the Web of Science (WOS) database, of which 756 were WOS articles and 119 related to business and economics. It did not find papers prior 2015 and ended in 2019.

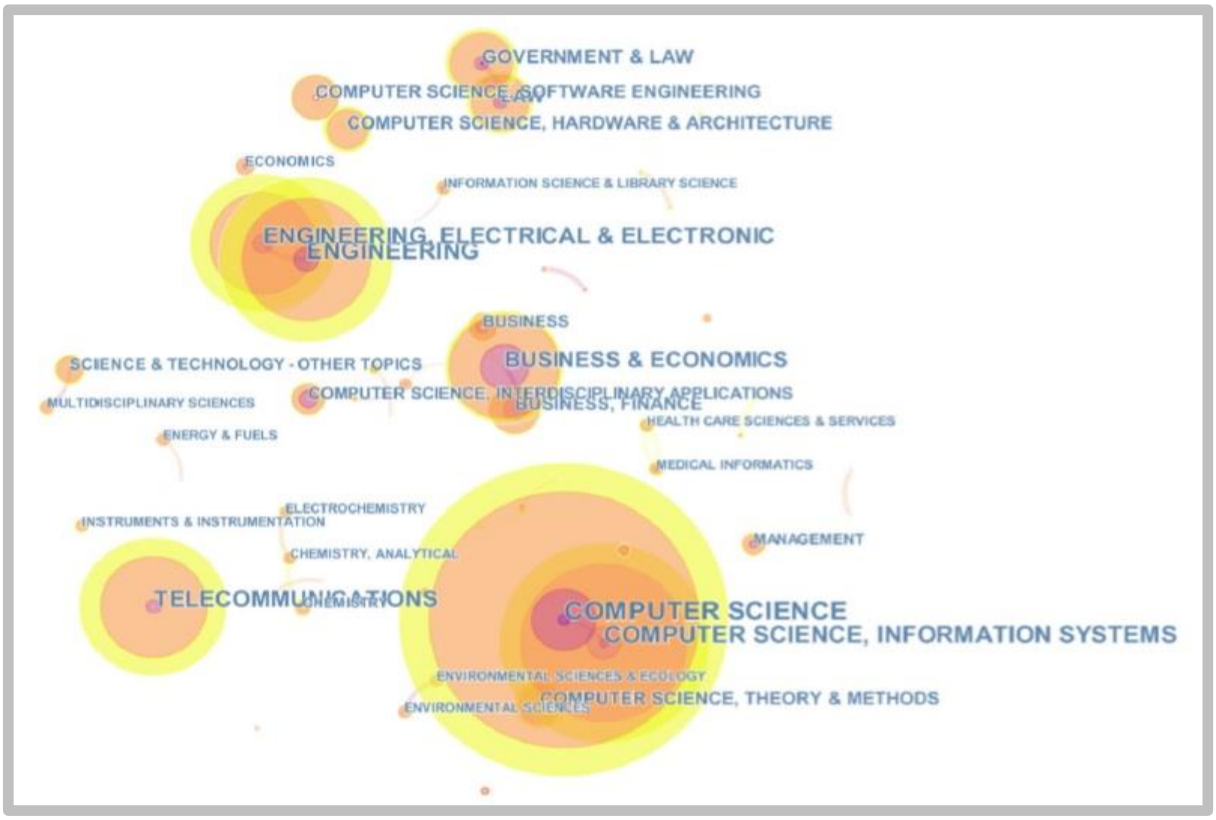


Figure 4.5: CiteSpace: BC related articles in Web of Science Core Collection (Xu et al., 2019, p. 3)

Ante (2020) undertook a similar approach and retrieved a total of 9672 articles within the WOS database in July 2019. His findings relate to the keywords blockchain and cryptocurrency in the business and economic domain. Concluding on five major strands of research, the last three comprise of the principles and applications of blockchain technology, transactions and anonymity, and monetary theory. These facts resemble the findings in this work and introduce the concluding marks.

5. Conclusions

This research was set out to find answers to the question of whether BC can be a useful tool in the detection of financial statement fraud. Based on qualitative investigations in the shape of desk research and conducted case studies, it can be concluded that BC and accounting interrelate in theory but lack practical scalability to meet the business rationale. Most predecessors in research of this domain see BC as an end rather than a mean to an end. To a certain extent, focus is set to narrowly and neglects specific technological implications, considering their impact in joint technological-organisational developments. Underlined by case studies on financial statement fraud and their implications, it becomes obvious in a scenario of intentionally wrong-acting participants within a BC-accounting set environment that is proposed by literature, that the use of BC to detect financial statement fraud may be rather harm- than purposeful.

While limitations on the used approach of this work are laid out in the respective chapter already, it clearly illustrates what the literature is missing. The overall understanding of what BC is, what it does, what it can do, and what it cannot do is crucial for finding answers to questions related to whether BC's use can be of purpose in the investigated domain. False expectations are detrimental for research and are misleading. A proper distinguishment between BC and DLT is necessary to nurture future research positively.

This work's contribution can be defined as one that brings insights to a topic that is still in its infancy. Even though investigated in, from, and by many perspectives, a common and recommended course of action of the topic is still missing. Streamlining the narrative of BC's use in accounting is incumbent on those who see its implementation as turning point in the industry to deliver it.

References

Adams, M. B. (1994). Agency Theory and the Internal Audit. *Mangerial Audit Journal*(Vol. 9, No. 8), 8–12.

Alles, M., & Gray, G. L. (2020). “The first mile problem”: Deriving an endogenous demand for auditing in blockchain-based business processes. *International Journal of Accounting Information Systems*, *38*, 100465. https://doi.org/10.1016/j.accinf.2020.100465

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. de, Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., . . . Yellick, J. Hyperledger fabric. In *Proceedings of the Thirteenth EuroSys* (pp. 1–15). https://doi.org/10.1145/3190508.3190538 (Original work published 2018)

Ante, L. (2020). A place next to Satoshi: foundations of blockchain and cryptocurrency research in business and economics. *Scientometrics*, *124*(2), 1305–1333. https://doi.org/10.1007/s11192-020-03492-8

Association of Certified Fraud Examiners. (2021, August 8). *Financial Statement Fraud, Part One*. https://www.acfe.com/article.aspx?id=4294967876

Attaran, M., & Gunasekaran, A. (2019). *Applications of Blockchain Technology in Business*. Springer International Publishing. https://doi.org/10.1007/978-3-030-27798-7

Beerbaum, D. (2020). *Blockchain and XBRL-A merger of equals?* Aalto University School of Business, Helsinki.

Beresford, D. R., Katzenbach, N. d., & Jr., C. R. (2003). Report of Investigation: Special investigative committee of the board of directors of Worldcom, Inc., 1–348.

Berle, A., & Means, G. (1932). *The modern corporation and private property*. Macmillan. https://doi.org/10.4324/9781315133188

Beuteslpacher, A., Schwenk, J., & Wolfenstetter, K.-D. (1999). *Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge* (3rd ed.). Viewg und Teubner Verlag.

Beyer, S., Hofman, Prof. Dr. Georg Rainer, Lundborg, M., Märkel, C., Mundo, A., Pohlmann, N., Steffen, L., & Zimprich, S. (2018). *BLOCKCHAIN IN SMEs*.

Blognative. (2021, January 14). *Mastering the Mempool: Your Intro to In-Flight Transactions*. https://www.blocknative.com/blog/mempool-intro

Buchanan, B., & Yang, T. (2005). The benefits and costs of controlling shareholders: the rise and fall of Parmalat. *Research in International Business and Finance*, *19*(1), 27–52. https://doi.org/10.1016/j.ribaf.2004.10.002

Buterin, V. (2013). A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/

Cai, C. W. (2021). Triple-entry accounting with blockchain: How far have we come? *Accounting & Finance*, *61*(1), 71–93. https://doi.org/10.1111/acfi.12556

Chedrawi, C., & Howayeck, P. (2018). Audit in the Blockchain era within a principal-agent approach. *International Conference ICTO2017*.

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2019, August 13). *A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses*. http://arxiv.org/pdf/1908.04507v1

Dai, J., & Vasarhelyi, M. A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems*, *31*(3), 5–21. https://doi.org/10.2308/isys-51804

Deneuville, M. (2016). *An in-depth guide into how the mempool works*. https://blog.kaiko.com/an-in-depth-guide-into-how-the-mempool-works-c758b781c608

Donaldson, L. (1990). The Ethereal Hand: Organizational Economics and Management Theory. *Academy of Management Review*, *15*(3), 369–381. https://doi.org/10.5465/amr.1990.4308806

Duncan, B., Lee, Y. W., Westerlund, M., & Aßmuth, A. (Eds.). (2019). *Cloud COMPUTING 2019: The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization : May 5-9, 2019, Venice, Italy*. IARIA. https://www.thinkmind.org/index.php?view=instance&instance=CLOUD+COMPUTING+2019

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*(14(1)), 57–74.

European Central Bank. (2005). *OECD Glossary of Statistical Terms - Corporate governance Definition.* European Central Bank, Annual Report 2004. https://stats.oecd.org/glossary/detail.asp?ID=6778

Fame, E., & Jensen, M. (1983). Agency problems and the theory of the firm. *Journal of Political Economy*(88(2)), 288–307.

Farrell, R. B., & Healy, P. (2000). White Collar Crime: A Profile of the Perpetrator and an Evaluation of the Responsibilities for Its Prevention and Detection. *Journal of Forensic Accounting*(January/June, Vol. 1, No.1).

Gayvoronskaya, T., & Meinel, C. (2021). *Blockchain*. Springer International Publishing. https://doi.org/10.1007/978-3-030-61559-8

Gordon, A. (2018). *Integrity in the spotlight: The future of compliance*. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-integrity-in-spotlight.pdf

Gordon, A. (2020). *Is this the moment of truth for corporate integrity? Global integrity report 2020*. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-is-this-the-moment-of-truth-for-corporate-integrity.pdf

Gordon, J. N. (2002). What Enron Means for the Management and Control of the Modern Business Corporation: Some Initial Reflections. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.305343

Grieve, R. H. (1983). Adam Smith's 'Wealth of Nations': the Legacy of a Great Scottish Economist. In *Understanding the Scottish Economy* (pp.41-54). https://www.researchgate.net/publication/254560449_Adam_Smith%27s_%27Wealth_of_Nations%27_the_Legacy_of_a_Great_Scottish_Economist

Grigg, I. (2004). *Triple entry accounting*. https://iang.org/papers/triple_entry.html

Haber, S., & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document. In A. J. Menezes & S. A. Vanstone (Eds.), *Lecture Notes in Computer Science. Advances in Cryptology-CRYPT0' 90* (Vol. 537, pp. 437–455). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-38424-3_32

Hacioglu, U., & Aksoy, T. (2021). *Financial Ecosystem and Strategy in the Digital Era*. Springer International Publishing. https://doi.org/10.1007/978-3-030-72624-9

Hinckeldeyn, J. (2019). *Blockchain-Technologie in der Supply Chain*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-26440-6

Homoliak, I., Venugopalan, S., Hum, Q., Reijsbergen, D., Schumi, R., & Szalachowski, P. (2021). The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. *IEEE Communications Surveys & Tutorials*, *23*(1), 341–390. https://doi.org/10.1109/COMST.2020.3033665

IAASB (2015). The Auditor's Responsibilities Relating to Other Information and Related Amendments: International Standard on Auditing (ISA) 720 (Revised).

IDC: The premier global market intelligence company. (2019). *IDC - IDC Customer Insights & Analysis - Home*. https://www.idc.com/promo/customerinsights?modal=tile-Blockchain&modal-ytb=nObc-jvPQA4&modal-ytb-api=1

Ijiri, Y. (1986). A Framework for Triple-Entry Bookkeeping. *The Accounting Review*(Vol. LXI, No. 4).

Inghirami, I. E. (2020). Accounting Information Systems: The Scope of Blockchain Accounting. In R. Agrifoglio, R. Lamboglia, D. Mancini, & F. Ricciardi (Eds.), *Lecture Notes in Information Systems and Organisation. Digital Business Transformation* (Vol. 38, pp. 107–120). Springer International Publishing. https://doi.org/10.1007/978-3-030-47355-6_8

International Association Standards Board (2021). Conceptual Framework for Financial Reporting (2018) – 2021 Issued IFRS Standards (Part A).

Jan, C. (2018). An Effective Financial Statements Fraud Detection Model for the Sustainable Development of Financial Markets: Evidence from Taiwan. *Sustainability*, *10*(2), 513. https://doi.org/10.3390/su10020513

Jensen, M. C., & Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.94043

Kanapickienė, R., & Grundienė, Ž. (2015). The Model of Fraud Detection in Financial Statements by Means of Financial Ratios. *Procedia - Social and Behavioral Sciences*, *213*, 321–327. https://doi.org/10.1016/j.sbspro.2015.11.545

Kemmerer, C. H., & Shawver, T. J. (2007). Tyco: A Top-Down Approach to Ethical Failure. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.1010558

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal Des Sciences Militaires*(9), 161–191.

Lakhani, K. R., & Iansiti, M. (2017). The Truth About Blockchain. *Harvard Business Review*.

Lee, A. T. (1972). *Company Auditing; concepts and practices.*

Lemieux, V. L., & Feng, C. (2021). *Building Decentralized Trust*. Springer International Publishing. https://doi.org/10.1007/978-3-030-54414-0

Levitt, A. (1998). *"The Numbers Game": 1998 SEC chair from the speech*. https://www.sec.gov/news/speech/speecharchive/1998/spch220.txt

Liu, M., Wu, K., & Xu, J. J. (2019). How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain. *Current Issues in Auditing, 13*(2), A19-A29. https://doi.org/10.2308/ciia-52540

Mahajan, R., Bansal, A., Saran, J., Karthik, K. V., Bedi, N., Vig, R., & Makhija, S. (2016). #letstalkfraud: India Fraud Survey, *2016*, 1–76 (Edition II).

Mitnick, B. (1975). The theory of agency: The policing 'paradox' and regulatory behaviour. *Public Choice*(24 (1)), 27–42.

Mosteanu, N. R., & Faccia, A. (2020). Digital Systems and New Challenges of Financial Management – FinTech, XBRL, Blockchain and Cryptocurrencies. *Journal of Management Systems*(21), 159–166.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Narula, N., Vasquez, W., & Virza, M. (2018). zkLedger: Privacy-Preserving Auditing for Distributed Ledgers. *Undefined*. https://www.semanticscholar.org/paper/zkLedger%3A-Privacy-Preserving-Auditing-for-Ledgers-Narula-Vasquez/95734d753b0bb945f9fd0c8d05897f41d3ecbb5b

O'Connor, S. (2020). *Mastering the Mempool [A How to Guide]*. https://hackernoon.com/mastering-the-mempool-a-how-to-guide-zs7u32ou

O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intelligent Systems in Accounting, Finance and Management*, *24*(4), 138–147. https://doi.org/10.1002/isaf.1417

Panda, B., & Leepsa, N. M. (2017). Agency theory: Review of Theory and Evidence on Problems and Perspectives. *Indian Journal of Corporate Governance*, *10*(1), 74–95. https://doi.org/10.1177/0974686217701467

Peng, T. (2020, May 13). Enterprise Blockchain Market Will Hit $21.07 Billion by 2025, Says Fortune Business Insights. *Cointelegraph*. https://cointelegraph.com/news/enterprise-blockchain-market-will-hit-2107-billion-by-2025-says-fortune-business-insights

Perrow, C. (1986). *Complex organizations: A critical essay* (3. ed. [Nachdr.]. Echo Point Books & Media.

Popescu-Zeletin, R. (1983). Implementing the ISO-OSI reference model. *ACM SIGCOMM Computer Communication Review*, *13*(4), 56–66. https://doi.org/10.1145/964661.800902

Professor Messer. (2018). *Hashing and Digital Signatures - CompTIA Security+ SY0-501 - 6.1*. https://www.youtube.com/watch?v=OBdEhSPoDaY

Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. (2018). *Distributed Ledger Technology Systems: A Conceptual Framework.* University of Cambridge.

Rezaee, Z. (2002). *Financial statement fraud: Prevention and detection*. Wiley.

Rivera, K., Rohn, C., Donker, J., & Butter, C. (2020). Fighting fraud: A never-ending battle: PwC's Global Economic Crime and Fraud Survey, 1–14.

Ross, A., & Berenson, A. (2002, December 31). CORPORATE CONDUCT: THE OVERVIEW; Tyco Admits Using Accounting Tricks To Inflate Earnings. *The New York Times*. https://www.nytimes.com/2002/12/31/business/corporate-conduct-overview-tyco-admits-using-accounting-tricks-inflate-earnings.html

Ross, S. (1973). The economic theory of agency: The principal's problem. *Anerican Economic Review*(63 (2)), 134–139.

Rückeshäuser, N. (2017). *Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls.* 13th International Conference on Wirtshcaftsinformatik, St. Gallen.

Ruiqi, Z. (2020). *A Decentralized Resource Allocation System - DLC Group Project.* https://doi.org/10.13140/RG.2.2.18728.52481

Sadka, G. (2006). The Economic Consequences of Accounting Fraud in Product Markets: Theory and a Case from the U.S. Telecommunications Industry (WorldCom). *American Law and Economics Review*, *8*(3), 439–475. https://doi.org/10.1093/aler/ahl012

Sixt, E. (2017). *Bitcoins und andere dezentrale Transaktionssysteme*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-02844-2

Smith, J. J. (1934, December 18). *Johnson v. Mcdonald: Case Number: 21895*. https://law.justia.com/cases/oklahoma/supreme-court/1934/39408.html

Sokolov, A., Grechanik, L., Sokolova, A., Rykalin, P., Ivlev, A., Gordienko, N., & Neboga, K. (2021). Countering corporate fraud: Survey findings (A study by Deloitte Forensic Russia).

Srivastav, N., & Uzma, S. h. (2010). Satyam Fiasco: Corporate Governance Failure and Lessons Therefrom. *The IUP Journal of Corporate Governance*, *2010*(Vol. IX, No. 4), 30–39.

Sweet, J., & Daugherty, P. (2020). Technology Vision 2020: We, the post-digital people, *2020* (Can your enterprise survive the tech-clash?).

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Taipaleenmäki, J., & Ikäheimo, S. (2013). On the convergence of management accounting and financial accounting – the role of information technology in accounting change. *International Journal of Accounting Information Systems*, *14*(4), 321–348. https://doi.org/10.1016/j.accinf.2013.09.003

Tie, R. (2005). XBRL: It's Unstoppable: A Conversation with the Father of the Digital Language of Business. *Undefined*. https://www.semanticscholar.org/paper/XBRL%3A-It%27s-Unstoppable%3A-A-Conversation-with-the-of-Tie/71c31ad53956c987c73bc750ba3673df12a469c9

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. in (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*, *7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

Watts, R. L., & Zimmerman, J. L. (1979). The Demand for and Supply of Accounting Theories: The Market for Excuses. *The Accounting Review*(Vol. LIV, No. 2).

Wolfson, R. (2020, May 29). The Big Four Are Gearing Up to Become Crypto and Blockchain Auditors. *Cointelegraph*. https://cointelegraph.com/news/the-big-four-are-gearing-up-to-become-crypto-and-blockchain-auditors

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, *5*(1). https://doi.org/10.1186/s40854-019-0147-z

Yermack, D. (2015). *Corporate Governance and Blockchains*. Cambridge, MA. https://doi.org/10.3386/w21802

Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, *52*(3), 1–34. https://doi.org/10.1145/3316481

Appendix

Appendix A

The following bullet points refer to Rezaee's (Rezaee, 2002, pp. 126–127) work on roles in corporate governance:

- *Board of Directors* fulfils its requirements by overseeing managements activities; acting as initiator of independent decisions to create shareholder value; developing operations for its own functioning; meeting periodically for the assessment of organisation and management; examining their own performance and of its professional independence

- *Audit Committees* are mandatory in publicly traded companies to strengthen and oversee corporate governance, financial reporting, and improve quality of information flow between principal and agent. This standing committee acts as intermediary between the board, internal, and external auditors and consists of non-executives and independent members.

- *Top Management Team* ensures to create shareholder value by acting out effectively and responsibly the delegated authority from the board of directors. This includes managing the business of an organisation through development and execution of strategies, protecting financials, follow and respect laws and regulations, ensure efficient operational success via an internal control system, and provide financial reports of high quality and reliability.

- *External Auditors* give credibility to decisions made by management considering financial resources about their use, planning, and actioning. They assure, that the contractual relationship between principal and agent are free of any errors, material misstatements or misconduct concerning financial statements and their derivation from the business process. In order, they are responsible to bring forward any concerns as users of financial reports, especially investors and creditors, rely on their judgements.

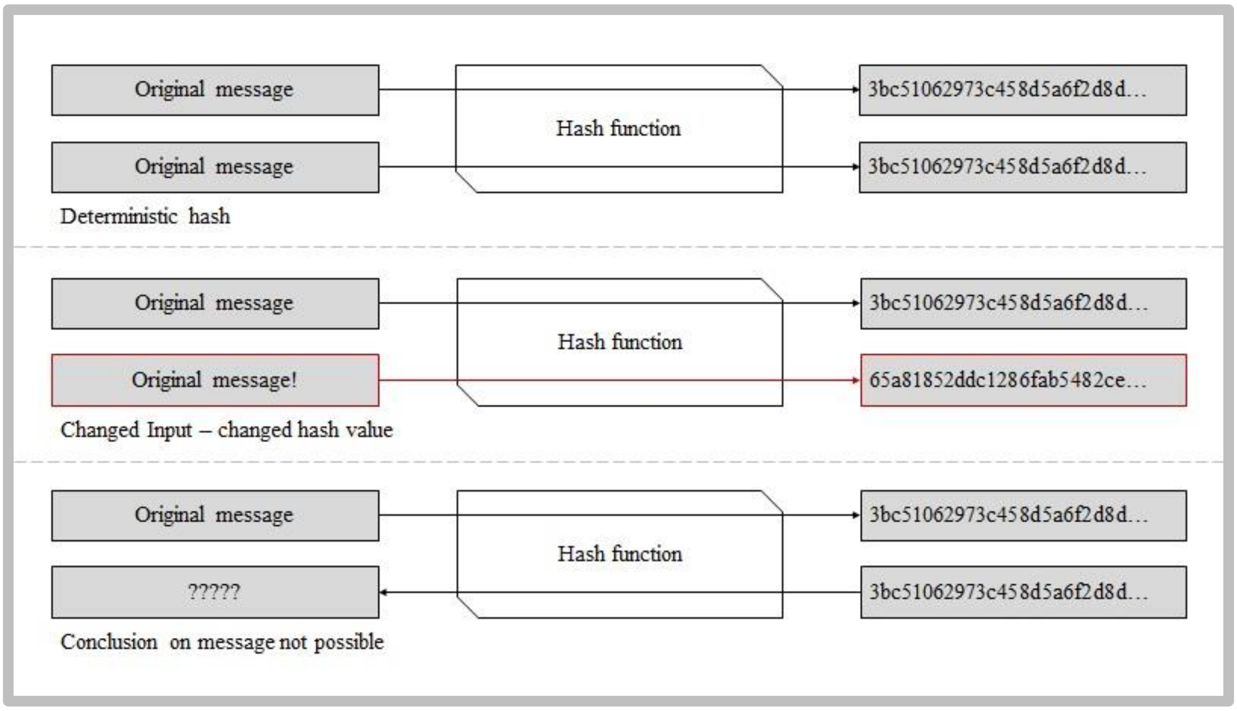
- *Internal Auditors* follow objective auditing and advisory activity in an organisation. They are independent of day-to-day operations. It assists the organisation in achieving its objectives through a systematic and disciplined approach by evaluating and improving the effectiveness of risk management, the internal control environment and governance.

- *Legal Authorities* monitor companies' and external auditors' action. Their task is to ensure high quality financial reporting through accordance of the prevalent form of accounting standards such as IFRS, GAAP etc. Further, they can issue legal investigations, sue, or charge misconduct. In the United States of America legal authorities dealing with corporate financials is the Security and Exchange Commission (SEC), in Europe it is the European Securities and Market Authority (ESMA), and some additional local country authorities.

Appendix B

Hash Values

Hash functions and hash values are considered central elements in BC and are widely used. They are one-way mathematical calculations and convert amounts of data of various length into hexadecimal strings of a fixed length. One way means that it is easy to calculate them forward but difficult, if not impossible, to calculate backwards. Conversion into hexadecimal strings means that a combination of numbers between 0 and 9 (10 figures) and letters between A and F (6 figures substitutional for hexadecimal numbers 10 to 15) are carried out. Hashing the original message encrypts its content while its identification remains clearly and easily possible. Hash functions are deterministic, which means that an identical data input results in an identical hash value. However, if a change occurs when a hash function is entered, this will lead to an unpredictable change in the resulting hash value. Most BC's use the SHA-256 algorithm, where 256 indicates the length of the hash value in bits. (Gayvoronskaya & Meinel, 2021, pp. 14–17).


Original message
Hash function
3bc51062973c458d5a6f2d8d…
Original message
3bc51062973c458d5a6f2d8d…
Deterministic hash
Original message
Hash function
3bc51062973c458d5a6f2d8d…
Original message!
65a81852ddc1286fab5482ce…
Changed Input – changed hash value
Original message
Hash function
3bc51062973c458d5a6f2d8d…
?????
3bc51062973c458d5a6f2d8d…
Conclusion on message not possible

Appendix B.1: Hash functions – based on (Hinckeldeyn, 2019, p. 7) – own illustration

Asymmetric encryption and digital signatures

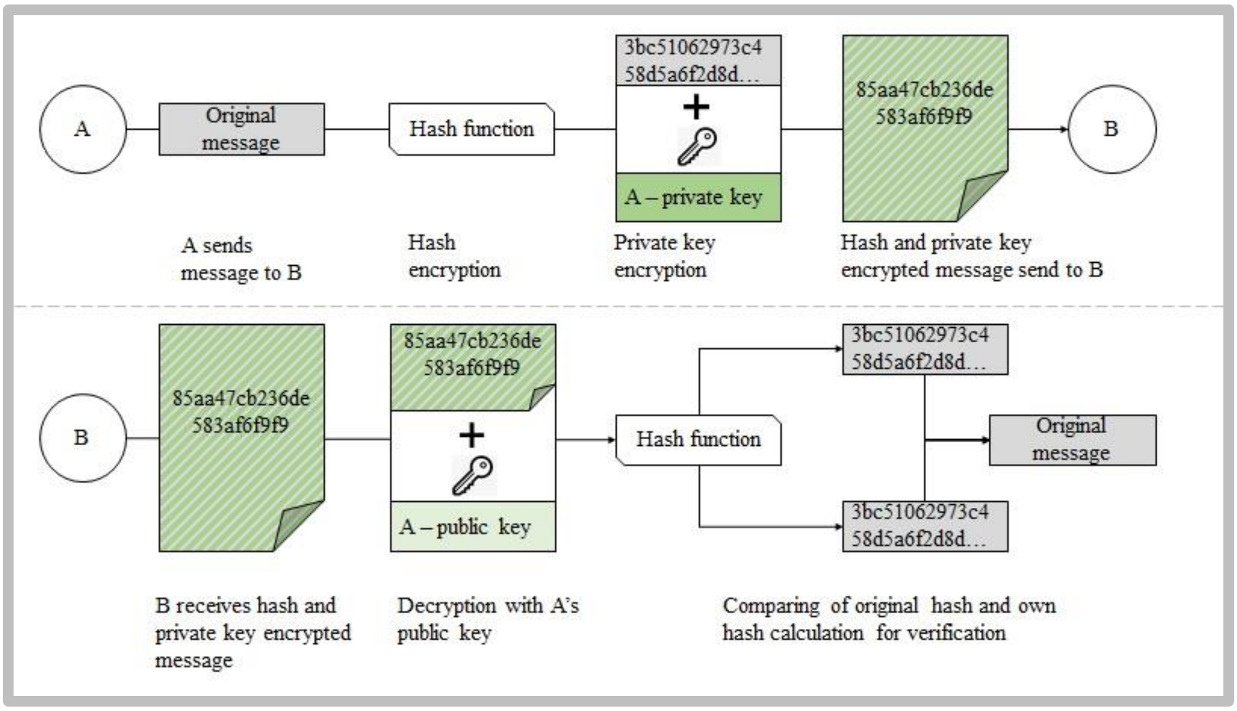
In Kerckhoffs' principle, a cryptographic sequence or message is only as secure as its key. The symmetric-key algorithm is encrypted and gets decrypted with the same key. In order, the sender and the recipient use the same one. For this to successfully happen, the exchange of key must be secured as well (Kerckhoffs, 1883). However, communication in a P2P network requires multiple encrypted messages opposed to one. The solution is the asymmetric-key algorithm that relies on a key pair – a public key to encrypt messages and a secret, private key to decrypt them.

> "In an asymmetric encryption scheme, anyone can send an encrypted message to a recipient - without having any secret information. But only the recipient can undo the encryption. One can imagine the sender dropping the message into the receiver's "mailbox". Throwing the message into the letterbox is equivalent to encrypting it with the recipient's public key: any participant can do this. But only the recipient is able to open the letterbox with his secret key and read the message." (Beuteslpacher et al., 1999, p.)[3]

The identification of sender and receiver happens through addresses or account numbers. The sender encrypts his message with the recipient's public key. The recipient, in turn, can only decrypt the received message with his private key, which ensures secure transmission.

A digital signature offers an additional protection mechanism and is considered a fingerprint or electronic signature of a transaction. The sender calculates a hash value of the message and simultaneously encrypts it with his private key, which is known only to him. The recipient in turn uses the senders the public key. He uses it to decrypt the signature and compares the hash value of the message with the hash value calculated on his or her machine. This ensures that the message really comes from the original sender and is thus verified (Gayvoronskaya & Meinel, 2021, pp. 17–19).

[3] Translation to the best of the author’s knowledge (German – English)

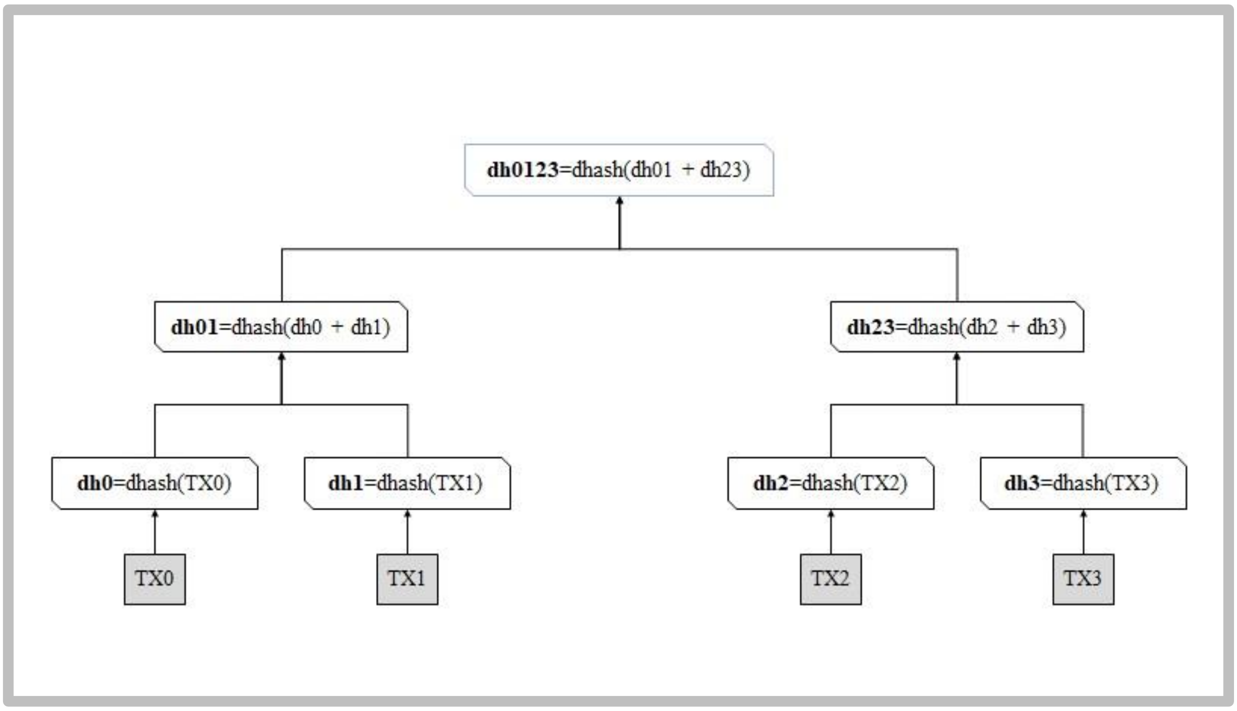

A
Original message
Hash function
3bc51062973c4 58d5a6f2d8d…
A – private key
85aa47cb236de 583af6f9f9
B
A sends message to B
Hash encryption
Private key encryption
Hash and private key encrypted message send to B
B
85aa47cb236de 583af6f9f9
85aa47cb236de 583af6f9f9
A – public key
Hash function
3bc51062973c4 58d5a6f2d8d…
Original message
3bc51062973c4 58d5a6f2d8d…
B receives hash and private key encrypted message
Decryption with A's public key
Comparing of original hash and own hash calculation for verification

Appendix B.2: Principle of signatures – based on Professor Messer (2018) – own illustration

Overall, this results in double security for the parties involved. The public key is an identification number, the private key serves to authorise and sign transactions. However, the security gained in this way is only guaranteed if decryption takes place in a secure environment.

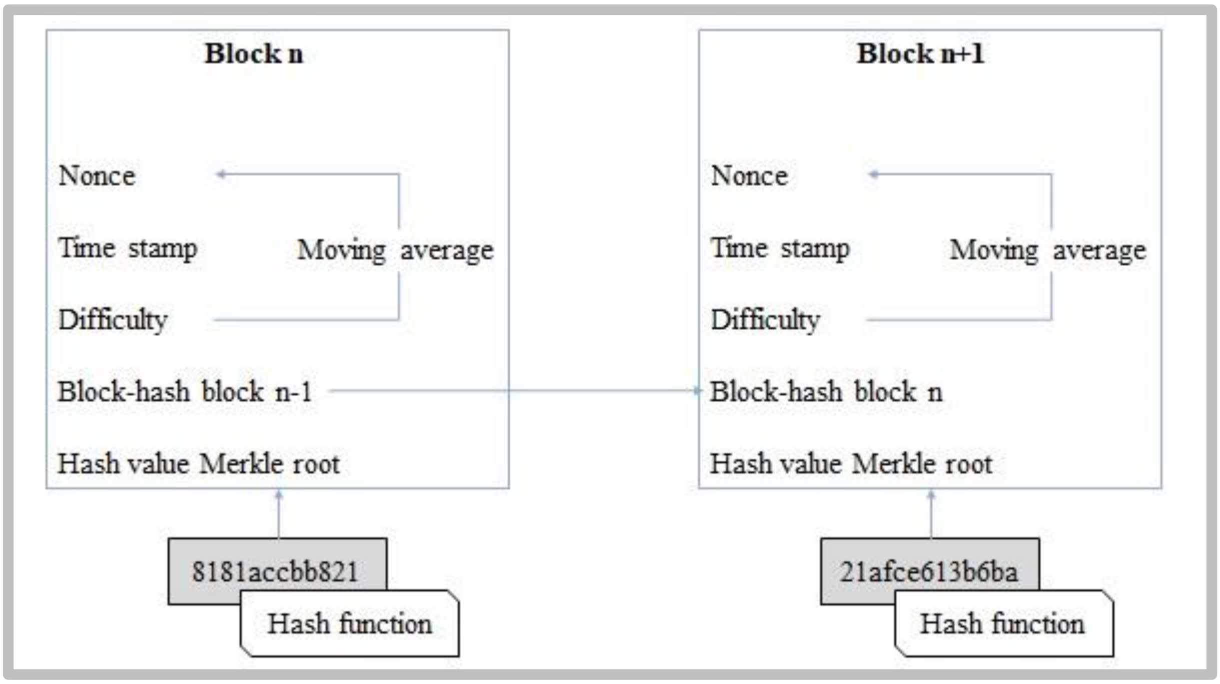
Merkle Trees and chaining blocks

The blockchain contains several transactions that are linked to each other. Single transactions are stored in a hash tree and form the so-called Merkle Tree. The repeated addition of two hash values not only creates the tree, but also leads to a single hash value - the Merkle Root. If the content of a transaction is subsequently changed, this would affect all other transactions. An attempted manipulation can thus be identified immediately. The chaining of Merkle trees gives the blockchain its name, as the chained elements are additionally reflected in blocks or created by the nodes of the network.



Appendix B.3: Merkle Root – based on (Gayvoronskaya & Meinel, 2021, p. 44) – own illustration

In addition to the Merkle tree, the created block contains a block header, which in turn also consists of several components. The random value “Nonce” (Number used once) is used to validate the block. For it to be valid, a hash value must have a system-defined number of leading zeros (a certain nonce). The algorithm does not provide the possibility of determining this nonce by calculation, but only by constantly testing random nonces to find the correct one. If the matching hash value is found, the block is created and forwarded to all nodes in the network. The block hash gets included as a link in the next block created and links them. If one of the blocks is changed, the containing Merkle root and thus the cumulative hash values of all transactions in it, plus all the other hash values change. This methodology makes the blockchain an (almost) completely tamper-proof construct, as all nodes would have to confirm the change to validate it.



Appendix B.4: Creation of blocks – based on (Hinckeldeyn, 2019, p. 10) – own illustration

Consensus algorithm

Due to the equal rights of the nodes and the lack of a central authority that has control over the data, a "single source of truth" that is approved by all must be found. The consensus algorithm as source achieves through a protocol consensus in the system by addressing and solving the problem of the Byzantine generals. It describes the problem of finding consensus in a decentral system with possible untrustworthy participants. In the Byzantine general example, a castle is surrounded by several, spatially separated generals with their armies. A coordinated and simultaneous attack by the generals enables the successful capture of the castle. The coordination and transmission of instructions is done by messengers. However, the trustworthiness of the generals and messengers, thus the messages, must be questioned in the process. So how can the generals reach an agreement without having to douSS the messengers and their delivered message?

The blockchain faces this problem through its structure as everyone is free to join and leave. Furthermore, the trustworthiness of new nodes must be questioned. Despite the possibility of manipulation, consensus must be found for all participants. By using consensus algorithms, the blockchain solves this problem and thus is endowed with the Byzantine Fault Tolerant attribute. (Gayvoronskaya & Meinel, 2021, pp. 27–28)

Proof of work consensus algorithm

The Nakamoto consensus assumes that in free to join networks, most of the computing power is in hands of honest participants and not most users are honest (Gayvoronskaya & Meinel, 2021, p. 28). The random value (nonce) plays a decisive role. On platforms like Bitcoin, nodes who help to find a random value are called miners. A miner who wants to create a new block does this by constantly generating new random numbers (nonce) for the block and then forming the hash value of this block together with the nonce. If he has found a nonce for the block that leads to a hash value with enough leading zeros, he has created a valid block. This process of finding a nonce that meets the requirements is called proof-of-work. By making the nonce known, the miner proves that he has spent work in the form of computational effort to test many nonces (Sixt, 2017, pp. 40–41). This approach also unambiguously establishes a temporal sequence of transactions. The difficulty is determined by a moving average, which is derived from the average number of blocks per hour. If the number of nodes and the CPU power used increase below the 10 min algorithm, the difficulty of the proof-of-work is adjusted (Sixt, 2017, p. 41). A high computing capacity is expressed as hash-rate per time unit. This protects the network from manipulation. If an attacker tries to change parts of the blockchain, he will need to have most of the computing capacity to increase the probability of finding the nonce before all other nodes. This case is called a 51% attack and immediately removes the decentralisation of the system (Chen et al., 2019, p. 10). Securing the network via computing capacity proves to be successful for large networks. However, the need for high computing capacities also comes with disadvantages. For example, the throughput, or in other words, the amount of data units per time span, is quite limited. In addition, the high energy consumption results in corresponding emissions. These disadvantages are attempted to be circumvented by other consensus algorithms (Gayvoronskaya & Meinel, 2021, pp. 30–32).

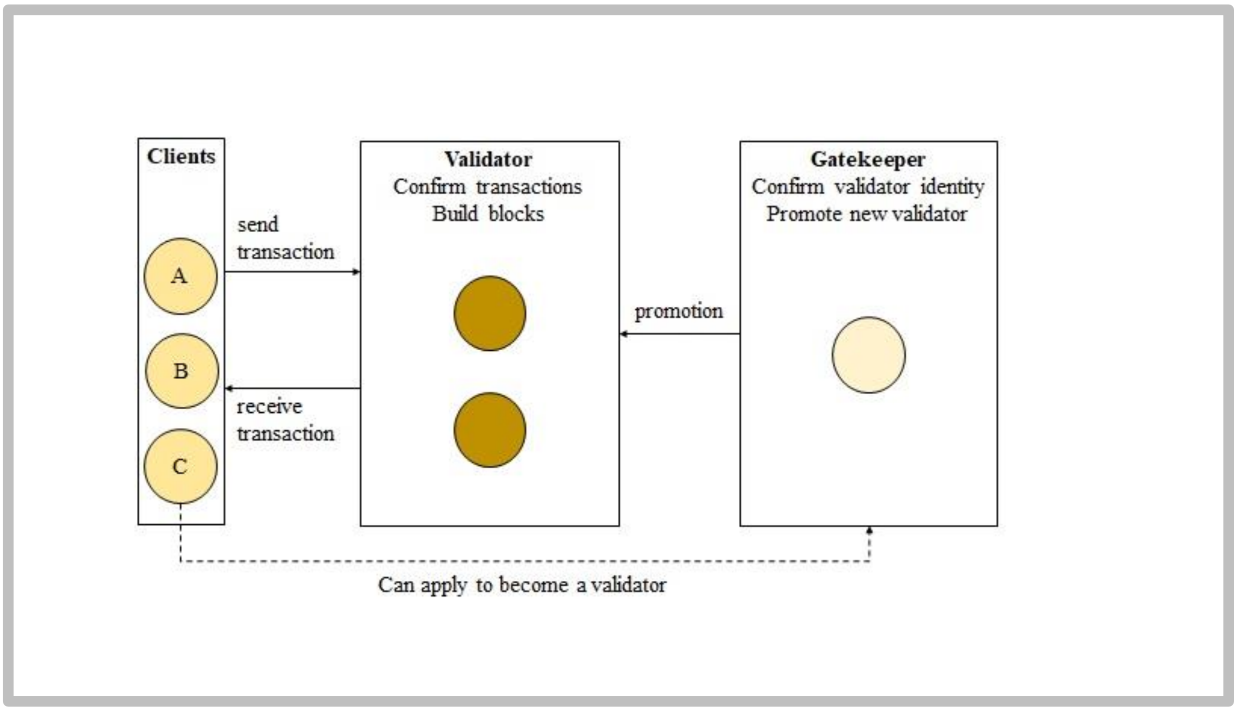
Proof of stake consensus algorithm

The proof of stake algorithm approach attempts to decouple the use of computing capacity in consensus building. Certain nodes also validate the blocks here, but they are determined with the help of a stake. In this case, the participants are called validators and not miners. By depositing a certain stake, they receive the potential right to create blocks. However, the probability of being involved in the creation of a block is linked to the deposited value. A distinction is made between two variants of consensus building. In the Chain-Based Proof of

Stake variant, a single validator is selected at random. The other variant describes the Byzantine Fault Tolerance Proof of Stake, in which a group of validators is randomly selected and, in addition to checking a block, also votes on its authenticity. The vote requires a pre-determined majority to create the block. Proof of Stake thus decouples computing capacity from energy consumption and at the same time ensures a higher throughput of the data volume. However, another problem comes to light with the deposit of a value. The higher the value deposit, the higher the probability of the validator creating a block, which centralises the system to a certain extent (Gayvoronskaya & Meinel, 2021, pp. 30–32).

Proof of authority consensus algorithm

With the Proof of Authority consensus algorithm, participants also act as validators. They benefit from a leap of faith from the rest of the network, as they are a selected group. It must be ensured that a validator is neither manipulated nor compromised. Due to this procedure, the group is kept small. This results in a high throughput, as there is no high computing effort in finding the block hash. The nodes send their transactions to the validators for verification. Thus, the effectiveness and credibility of the entire network depends on the group of validators. Besides the lack of broad decentralisation, the small group of selected nodes may exert power on the rest of the network and thus influence it.



Appendix B.5: Proof of authority – based on (Hinckeldeyn, 2019, p. 17) – own illustration

Smart Contracts

Transactions can transmit programme code for decentralised applications. Going back to the idea expressed by Nick Szabo (Szabo, 1997) of executing contracts automatically, the blockchain with its special security properties offers a good basis. Szabo called this type of automatic execution of legal transactions "smart contracts". Transactions here act as the core for settlement and describe a change in advance; a parameter is defined to describe the occurrence of an event and an output variable to be changed is defined as the result of the contract. Another important aspect of smart contracts is that all conditions can also be viewed by third parties and can no longer be changed after successful publication. This is also referred to as the "law" of the smart contract. This publicity thus makes it possible to record behaviour or activities or changes in a value-neutral way and to implement them contractually (Cai, 2021, pp. 77–78).

Appendix C

CASE 1: ENRON (2001)

Enron used to be an energy trading and distribution company and was the 7th largest company in the United Stated of America. They were famous for their advocacy role of energy deregulation and valued for over $70bn. In 1997, they were losing money and accumulated debt which was the initial to conduct fraud.

- The board of directors showed a lack of independence
- The stock-based compensation model was used by top management team to boost own gains at the stock market
- External Auditor (Anderson) was compromised and misused the legal authority’s trust (J. N. Gordon, 2002)

CASE 2: WORLDCOM (2002)

Worldcom was an international telecommunications service provider based in the US. Their business was run in several segments of services related to data, internet, local and international communicating, and customer management. By the time of the fraud, the company supposedly pushed through half of the US' internet and communication demands in their cables. The overstating of EBITDA was laid open in June 2002. A month after, the company filed for bankruptcy with debt of $41bn (Sadka, 2006, p. 452).

- The board of directors showed a lack of independence by making use of compensation schemes
- Bonus schemes enforced workforce loyalty
- Internal and external auditors to fail detection of fraud (Beresford et al., 2003)

CASE 3: TYCO (2002)

Tyco International Inc. is a global acting conglomerate that manufactures a wide range of products in segments such as electronic components, healthcare products, fire, and security systems. As of the year 2004, reported net income was $14.5bn. CEO Dennis Kozlowski and CFO Mark Swartz were led by individual greed, manipulated corporate loan programs, circumvent shareholder and board approvals to hand themselves unauthorised bonuses of $170m (Kemmerer & Shawver, 2007, p. 3).

- The board of directors showed a lack of independence by overriding internal control mechanisms
- Bribery of workforce to hide fraud
- Weak corporate governance procedures in documentation (A. Ross & Berenson, 2002)

CASE 4: PARMALAT (2003)

The case of Parmalat is different due to the corporate governance structure. Italy's corporate governance system has its origins in the French civil law tradition. Its characterizations distinguish it from its counterparts in the European Union: antiquated capital markets and smaller firms, on average, than other industrial economies, which are mainly run by family and therefore concentrate ownership. Italy's economy equals a family capitalism with nearly 99 percent of firms run by families. “The result is a business culture that is rooted in blood ties, friendship, reciprocal favours, and sometimes, corruption.” (Buchanan & Yang, 2005, p. 32). In terms of institutional investors and banks, the economic landscape of Italy differs in comparison to the U.S and other European states significantly as well. Small fractions of equity in family run Italian firms between 0.5 and 6 percent are opposed to family investments in other European states which range between 50 and 60 percent. Additionally, in the wake of the Enron scandal, the Sarbanes-Oxley Act increased prison sentences for false accounting to up to 20 years in the U.S., whereas the regulatory institutions in Italy reduced jail time from 5 to 4 years (Buchanan & Yang, 2005, pp. 30–33).

In this scenario happens the incident of Parmalat, a family run business and international food company. Starting in 1990 and with losses in a South American subsidiary, CEO Calisto Tanzi was successfully cooking the books until 2003. Family members running corporate subsidiaries were also compromised. In the end, there was an accounting hole of €14bn missing and a filing for bankruptcy.

- Ownership structure due to Italian business ecosystem and composition of family members in leading positions of subsidiaries

- The board of directors showed a lack of independence
- The audit committee showed a lack of independence
- Weak corporate governance and accounting standards
- External auditor showed lack of objectivity (Buchanan & Yang, 2005, p. 28)

CASE 5: SATYAM (2009)

Satyam Computer Service Limited was an Indian corporation and provided services in information technology such as programming, consulting, and outsourcing to cheaper prices. It was founded in 1987 by Ramalinga Raju. In the wake of 2009, the accounting scandal of Satyam got public due to a confessing letter of the CEO, in which he stated his inflating measures over the course of recent years. Those included non-existent bank balances, fake interest receipts and customer billings as well as borrowings on a fabricated board.

- The board of directors showed a lack of independence
- CEO and internal audit were compromised and engaged in fraud
- External auditor was unable to detect the fraud
- Whistle-blower policy was not effective (Srivastav & Uzma, 2010)