The Potential of Blockchain-based Fraud Detection Systems in the Insurance Industry

A Critical Analysis Based on Real-World Solutions

15th of March 2023

Authors

Aaron Pozzi

Management

Premton Avdyli

BD/CRM

Silvan Müller

Publication

Kevin Bründler

Data Management

Luna Arnold

Website

Sena Mutlu

Operations

SMART CONTRACTS LAB

Abstract

Insurance fraud is a pervasive and costly phenomenon that has yet to be fully addressed. Blockchain technology has emerged as a promising solution to uncover and prevent fraud, but its full potential has yet to be realized. This report provides a comprehensive analysis of the application of blockchain technology for the detection and prevention of insurance fraud, with particular emphasis on Samsung SDS, an operational project that targets receipt fraud in the South Korean health sector.

Through a review of existing literature and analysis of real-world projects, this study demonstrates that blockchain's immutability and data integrity features make it well-suited for fraud prevention. However, the technology must overcome several limitations before it can be considered a trustworthy solution for fraud prevention. These include scalability and sustainability concerns, as well as legal and regulatory issues such as data privacy and deletion features.

The findings of this report reveal the potential benefits of using blockchain technology for insurance fraud prevention, such as increased transparency, efficiency, and cost reduction. Nevertheless, further research and development are needed to overcome the current limitation of the technology. Moreover, globally coordinated regulation is necessary to ensure that insurance records can be stored in a decentralized manner while complying with jurisdictions.

In conclusion, this report provides a valuable contribution to the literature on the use of blockchain for mitigating insurance fraud. Despite the challenges that must be addressed, we believe that blockchain technology has the potential to revolutionize the insurance sector and become an integral part of fraud prevention.

Table of contents

List of Figures

1. Introduction

The insurance industry is facing a momentous change. The advent of blockchain technology could revolutionize several aspects of the relationship between the parties associated with an insurance contract. The focus of this paper, however, is on how such technology can help in the prevention and identification of fraud with a focus on real-world examples.

According to the Coalition Against Insurance Fraud (2022), American consumers are estimated to lose roughly $ 309 billion yearly due to insurance fraud. One of the most prevalent techniques to commit fraud is taking out multiple insurance policies, essentially allowing claims to be filed in parallel at various insurance providers and thus collecting several proceeds for the same claim. Another case could be the withholding of various key medical information when compiling the application process for a life insurance policy. For instance, the omission of a history of diabetes or heart-related conditions (Deloitte, 2016). The problem arises since data such as claim records are stored in isolated legacy systems and not made accessible to other insurance providers. In this sense, blockchain technology can be used as a cross-sectoral distributed ledger with external and customer data to help detect identity fraud and dishonest claims of injury or damage. In addition, aspects such as validation of authenticity, ownership, the provenance of assets or data, and verification of police theft reports or claims history would be affected. Moreover, it would be easier to detect patterns of fraudulent behavior linked to a specific identity. Even more so, it would be possible to prove the date and time of issuance of a policy or purchase of a product/asset and confirm subsequent changes in ownership and location (Lorenz, et al., 2016).

All in all, by establishing a permissioned distributed network to store and share anonymized insurance records, blockchain technology can help mitigate the impact of fraud in the insurance sector. This comes hand in hand with the utilization of smart contracts that facilitate and speed up the process of recognition of fraud. Eventually, data integrity enhances the predictive analytics capabilities of machine learning classification algorithms, which are sophisticated approaches to combat fraud in the insurance sector. Throughout our report, the intention is to provide a general overview of the implementation of blockchain-based systems to prevent insurance fraud, with a specific focus on the research question: **Does blockchain technology help to reduce fraud in the insurance sector and how are different projects implementing it?**

Before this question can be answered it is necessary to give a general overview of how an insurance company works and how blockchain would work in this field. After this theoretical part, there is an analysis of several companies implementing this new technology and how they have reduced/expected to reduce fraud. This is followed by a comparison that weighs out the advantages and disadvantages of the different solutions presented in the previous chapter. Then, the legal implications of this blockchain implementation are discussed. Finally, the last section summarises the main findings and tries to provide a possible vision of the future per se, as well as hints for further research.

2. Methodology

The approach that was used to answer the research question of this report was to identify the appropriate literature by conducting a systematic query of research databases, including Google Scholar, ScienceDirect, and Swisscovery. The search was conducted using the keywords: "blockchain", "insurance", and "fraud prevention". We limited the search to papers and corporate research reports published between 2015 and 2023, except for three sources that were groundbreaking for blockchain technology and smart contracts. In addition, the bibliography of relevant research papers was reviewed to identify additional sources. Apart from the chapter on legal aspects, our focus was limited to the inclusion of literature in English. Indeed, in the legal chapter, since the focus was on Swiss jurisdiction, the relevant literature was only available in German.

In the section dedicated to real-world examples, we also considered articles published on websites due to the lack of academic and corporate literature. To better describe their relationship to fraud prevention in the insurance industry, our focus was based on identifying examples that were relevant to the industry and offered appropriate publications. More specifically, we focused on companies that represented joint ventures of major companies or companies whose purpose was exclusively on insurance fraud prevention.

To ensure readability for people without a technical background we first introduce the most fundamental theoretical and technical concepts to understand the content of this report. Furthermore, we conducted our research by searching for documents that also included terms such as “smart contract” and “machine learning” to ensure a thorough examination of the literature. Overall, the systematic literature review approach was chosen because it allows for a comprehensive and unbiased evaluation of existing research, providing an evidence-based foundation for the conclusion of the research report.

3. Theory Review

3.1. Classical Insurance Model

Insurance is a risk management tool that involves the transfer of risk from an individual or organization to an insurance company (Investopedia, 2022). Insurance policies typically involve a contractual agreement between the insurance company and the policyholder, whereby the policyholder pays a premium in exchange for the promise of financial protection in the event of a covered loss (Contracts Counsel, 2017). This involves a careful balancing act between charging enough to cover potential losses and ensuring that the premiums are affordable enough to attract customers. Insurance policies provide financial protection to policyholders in the event of unforeseeable events, such as accidents, illness, natural disasters, or other events that result in financial loss. The following section describes how insurance companies operate in the event of an insured event.

The general scheme of how insurance functions involve several key players: the policyholder, the insurance company, and the insured event. The policyholder purchases an insurance policy from the insurance company, which outlines the terms of the coverage and the premium payments required. In the event of an insured event, such as an accident or illness, the policyholder submits a claim to the insurance company. The insurance company then investigates the claim and assesses whether it is covered under the terms of the policy. If the claim is approved, the insurance company provides financial compensation to the policyholder, up to the limits of the policy coverage. There are various types of insurance policies, including health insurance, life insurance, property and casualty insurance, liability insurance, and more (The Balance Money, 2022). Furthermore, the insurance model is a critical component of the modern economy, providing individuals and organizations with financial protection as well as enabling businesses to manage risk and pursue growth opportunities. While the industry faces significant challenges, including changing customer preferences, regulatory constraints, and the ongoing threat of fraud & cyber-attacks (Top Insurance, 2022), it remains a vital part of the global financial system.

The insurance industry has long been a target for fraudulent activities, which result in significant financial losses for insurance companies and higher premiums for policyholders. The industry faces a significant challenge in combating fraudulent activities, which cost the industry billions of dollars every year. To combat this problem, the industry has been exploring various technologies and approaches. One way of classifying insurance fraud is by distinguishing between soft fraud and hard fraud. Soft fraud is the exaggeration or fabrication of claims, while hard fraud is the deliberate intentional creation of false claims (NAIC, 2022). Examples of soft fraud include exaggerating the extent of a car accident injury to receive more compensation from an insurance claim or inflating the value of lost or stolen items to get a higher payout. On the other hand, hard fraud may include staging a car accident or arson to receive compensation from an insurance claim. The incidence of soft fraud is greater than that of hard fraud (NAIC, 2022).

Both types of fraud have significant impacts on the insurance industry, leading to increased premiums for honest policyholders and increased costs for insurance companies. Detecting and

preventing fraud in the insurance industry requires a combination of advanced technologies, including data analytics and machine learning, as well as the expertise of fraud investigators (kbv Research, 2019). To detect fraud, insurance companies employ various techniques, such as investigation of claims, interviews with claimants, analysis of historical data, and collaboration with law enforcement agencies (i-Sight, 2019). These techniques aim to identify patterns of behavior or inconsistencies that may indicate fraudulent activity.

One popular method of fraud detection is data analytics. Insurance companies use software tools to analyze vast amounts of data, such as policyholder information, claim history, and external data sources, to identify anomalies and suspicious patterns (Management Events, 2023). For example, they may analyze the frequency and timing of claims, the relationship between claimants and other parties involved in the claim, and the consistency of information provided by the claimant. Another approach is to implement anti-fraud measures, such as checks and balances, to prevent fraudulent activity from occurring in the first place. For instance, insurance companies may implement policies that require claimants to provide documentation, such as police reports or medical records, to support their claims (Verivox, 2022). They may also use technology to verify the authenticity of the documentation provided.

To sum up, these methods are a good step in the right direction, but they are not foolproof. Nevertheless, the use of human expertise and judgment remains essential (Reuters Events, 2023). By implementing advanced technologies and analytics techniques, insurers can better detect and prevent fraudulent activities, helping to protect themselves and their customers. The industry is currently exploring new methods and technology for fraud detection. Advancing technology such as blockchain will be the subject of the next chapter.

3.2. Blockchain Technology

Blockchain is a digital, distributed ledger network that stores validated transactions with timestamps which eliminates the need for intermediaries (Nakamoto, 2008; Christidis & Devetsikiotis, 2016). Each transaction is linked together, creating a chain of data blocks that are secured with cryptography (Al-Jaroodi & Mohamed, 2019) and visible to anyone (Amponsah, Adekoya, & Weyori, 2022). For a transaction to be included in a block, it must go through a consensus mechanism which means that the network agrees on a single state of truth and verifies that this transaction is legitimate (Al-Jaroodi & Mohamed, 2019; Aste, Tasca, & Di Matteo, 2017). Consensus is achieved across network participants (so-called nodes) who maintain the distributed ledger (Al-Jaroodi & Mohamed, 2019; Aste, Tasca, & Di Matteo, 2017). There are several consensus mechanisms, but the most known ones are Proof-of-work (PoW) and Proof-of-Stake (PoS) (Casino, Dasaklis, & Patsakis, 2019; Wendl, Doan, & Sassen, 2023). PoW is the first mechanism that existed in blockchain, and its algorithm secures transactions through miners that need to use enough computing power to connect the last block of transaction data to the new one with encryption algorithms (Back, 2002; Nakamoto, 2008; Wendl, Doan, & Sassen, 2023). This will guarantee the authenticity and verifiability of the new transactions (Casino, Dasaklis, & Patsakis, 2019). However, the process of the PoW algorithm needs an immense amount of energy

and additionally, only one miner who was able to identify the right solution to a challenging mathematical riddle, that requires pure guessing first, will be rewarded (Casino, Dasaklis, & Patsakis, 2019; Wendl, Doan, & Sassen, 2023). As a result, the energy that was acquired from other miners through their attempts was not necessary after all (Casino, Dasaklis, & Patsakis, 2019; Wendl, Doan, & Sassen, 2023). The concern about the high energy consumption resulted in new consensus mechanisms such as PoS which is the most common alternative and is also implemented by Ethereum (Casino, Dasaklis, & Patsakis, 2019; Wendl, Doan, & Sassen, 2023).

In the last decade, the recognition of blockchain technology has widely spread and it has been mostly associated with cryptocurrencies such as Bitcoin or Ethereum (Nakamoto, 2008). However, recently there is a growing interest in this technology in other industries such as the insurance sector because it has great potential in other applications than in money transfer (Kar & Navin, 2021). Thanks to the anonymous and irreversible recording of digital assets, blockchain could also be a beneficial network to speak up in countries where there is a strict censorship system (Kar & Navin, 2021). All in all, blockchain technology stands for security, immutability, and transparency (Amponsah, Adekoya, & Weyori, 2022).

3.2.1. Smart Contracts

Smart Contracts were first introduced and defined as: "a computerized transaction protocol that executes the terms of a contract" (Szabo, 1996) and is mostly used on the Ethereum platform (Ouyang, Zhang, & Wang, 2022). In other words, smart contracts are digital agreements, between companies or parties in general, that run on the blockchain and are automatically executed when all the requirements are met, so consequently, there is no necessity for centralized authorities (Casino, Dasaklis, & Patsakis, 2019; Al-Jaroodi & Mohamed, 2019; Ouyang, Zhang, & Wang, 2022). This enhancement of Blockchain technology opens limitless application possibilities using complex processes that are traceable and unalterable (Casino, Dasaklis, & Patsakis, 2019). A good example would be in the medical sector, more specifically, it can be utilized for datasets of patient records that need to be updated continuously (Kumar, Arjunaditya, Singh, Srinivasan, & Hu, 2022). Consequently, it can reduce administrative costs and processing time in a more efficient way (Al-Jaroodi & Mohamed, 2019; Ouyang, Zhang, & Wang, 2022).

3.2.2. Permissioned and Permissionless Blockchain

Ledgers are the copies of the blockchain network that each participating node owns to have access to the network (Voulgaris, et al., 2019; Amponsah, Adekoya, & Weyori, 2022). It is also important to mention that there are different types of blockchain networks: Permissioned, permissionless, and federated ledgers (Casino, Dasaklis, & Patsakis, 2019; Voulgaris, et al., 2019). They stated that permissionless ledgers are used in a public blockchain such as Ethereum where anyone can set up a node, access the blockchain, or interact with the functionality the network provides. With a permissioned ledger, only a limited number of specific nodes have the authorization to access the blockchain, which makes it the preferred choice for corporate networks and the federated one contains private and public blockchains which makes it a hybrid of the former two (Casino, Dasaklis, & Patsakis, 2019; Voulgaris, et al., 2019). Private blockchains primarily reduce the risk of Sybil attacks, which occur when one user disguises himself as multiple peers in order to gain a

disproportional amount of influence compared to the remaining nodes (Swanson, 2015). Additionally, permissioned blockchains can be more flexible, efficient, and faster than public blockchains such as Bitcoin or Ethereum, because they don't need to use the time and energy-consuming consensus mechanisms like PoW (Andoni, et al., 2019; Casino, Dasaklis, & Patsakis, 2019; Tang, Torngren, & Wang, 2020). According to Tang et. al. (2020), it is also no surprise that permissioned blockchains are most appealing to enterprises. There are already existing projects and firms that started using federated or private blockchains such as the Hyperledger project by the Linux foundation or Nexledger by Samsung SDS. In this report, we will focus on the permission-based blockchain framework of Samsung SDS which was developed in 2017 and will be explained further as a real-world solution.

3.3. Blockchain and Artificial Intelligence: Machine Learning

Artificial Intelligence (AI) is used for machines that "perform ordinary tasks associated with human intelligence" (Kumar, Arjunaditya, Singh, Srinivasan, & Hu, 2022, p. 8). AI has several sub-divisions, one being Machine Learning which stands for self-learning computers that can act upon their own decisions without being programmed to do so (Kumar, Arjunaditya, Singh, Srinivasan, & Hu, 2022). Combining blockchain and AI enables multiple benefits. For example, blockchain-optimized AI includes blockchain and smart contracts that can contribute to AI with data traceability and resource sharing which are often referred to as Intelligent Contracts (Ouyang, Zhang, & Wang, 2022). In terms of AI-optimized blockchain, AI can obtain beneficial information that again can give blockchain and smart contracts the possibility to automatically learn and solve problems (Zibin Zheng, 2021; Ouyang, Zhang, & Wang, 2022). Unfortunately, there is still more research needed on how to properly constitute intelligent contracts from smart contracts and what kind of an impact they could have on AI-driven blockchain intelligence (Ouyang, Zhang, & Wang, 2022).

3.4. Blockchain in the Insurance Sector

There is a lack of transparency in the insurance sector in terms of data sharing between insurance companies which can also make it difficult to detect fraud (Kumar, Arjunaditya, Singh, Srinivasan, & Hu, 2022). As a result, fraud prevention is one of the primary use cases for blockchain in the insurance industry. (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018a). Using Blockchain and AI, there are already several proposals on how to secure insurance records on a blockchain and on how fraud can be prevented or detected using classification techniques (Shi, et al., 2016; Zhou, Wang, & Sun, 2018). When data records are stored on the blockchain, it can enhance the credibility of agreements and transactions between the parties involved in an insurance process (Kumar, Arjunaditya, Singh, Srinivasan, & Hu, 2022).

An example of a blockchain-based insurance storage system has been introduced by Raikwar et. al. (2018). They came up with an experimental storage framework on the private blockchain Hyperledger Fabric and show, how both the client and the agent of the insurance company can send their requests and transactions back and forth through the blockchain which is verified by the

validators. Below, there is an overview of the insurance framework proposed by Raikwar et al. (2018):

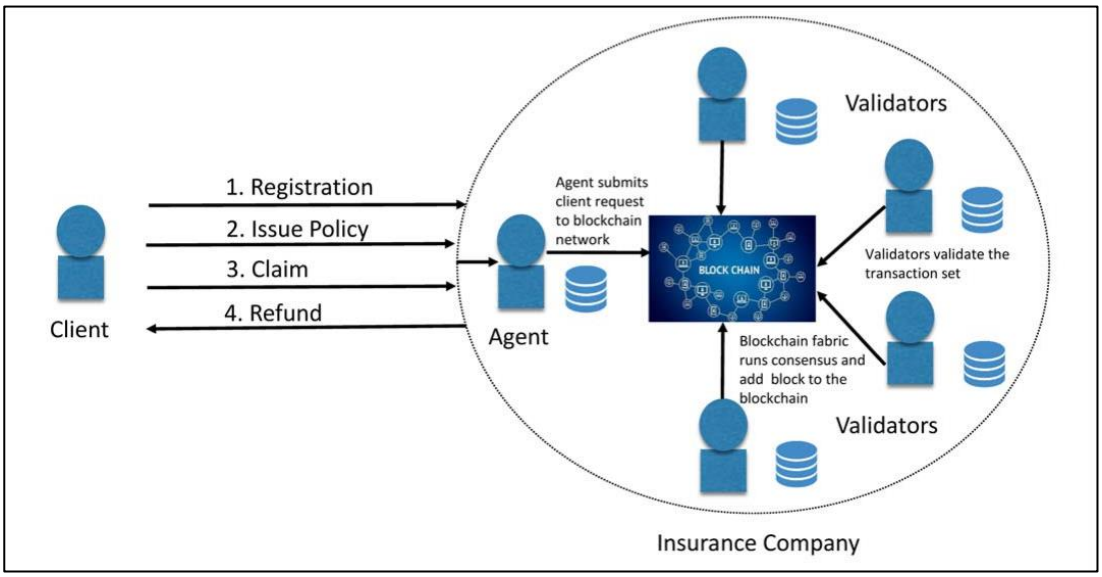

Figure 1: An overview of an insurance blockchain framework (Raikwar, et al., 2018)

More precisely, the scenario considered by the authors and explained in Figure 1 is that the core processes contain classic insurance transactions such as customer registration, policy assignment, premium payment, and reimbursement processing. Subsequently, the sored outcomes of each transaction are secured via blockchain technology thanks to the decentralized nature of the system. Any transaction is verified by the validators and executed when specific requirements are met. Hence, their proposed, blockchain-based solution guarantees that clients do not unreasonably accuse the insurance company. Furthermore, it ensures that the insurance firm is responsible for all the services it provides (Raikwar, et al., 2018). The presented scheme serves as a starting point to better understand how blockchain can be used in the insurance field. With the necessary modifications, such a scheme can also be implemented to replicate the functioning of specific types of insurance such as medical insurance, car insurance, or travel insurance.

4. Real-world Solutions

Blockchain technology has been widely investigated as a potential solution to prevent fraud in various industries. This chapter provides examples of how blockchain technology has been used for fraud prevention in the insurance and healthcare sectors.

The use of blockchain-based systems for fraud prevention in the insurance industry is exemplified by B3i, a consortium of insurance companies, and BigchainDB, a start-up that enhances existing databases with blockchain properties. On the contrary, the Lemonade Foundation has launched a blockchain-based system for delivering affordable and instantaneous climate insurance for farmers in emerging economies, which eliminates the need for intermediaries and reduces the potential for fraud. In the healthcare sector, Samsung SDS has launched a blockchain-based medical processing system that securely and accurately shares personal medical information, reducing fraud and the cost of processing medical claims.

These real world-examples illustrate the potential of blockchain technology to revolutionize existing insurance processes and create more efficient, secure, and transparent systems that are less prone to fraud.

4.1. BigchainDB / Interplanetary Database

According to the CEO of Swiss Re, one of the largest reinsurers in the world, one of the primary challenges of implementing blockchain technology is the lack of interoperability with current IT systems such as legacy databases (Howard, 2022).

Therefore, it seems particularly important to explore a blockchain startup that combines existing technologies with blockchain, as this allows the exploration of new use cases such as data sharing without compromising existing infrastructure. One such start-up is BigchainDB, which enhances database software such as MongoDB or PostgreSQL with blockchain properties (BigchainDB GmbH, 2018). The opensource codebase of BigchainDB is currently being expanded by the Interplanetary Database project (Interplanetary Database Association, 2023) as the focus of BigchainDB shifted to another project called Ocean Protocol, which focuses on a decentralized marketplace for data records of all kinds (Ocean Protocol Foundation Ltd., 2023).

Although BigchainDB is not developed explicitly for mitigating insurance fraud, it represents one of the main building blocks of a notable proof-of-concept study for fraud prevention conducted by Gokay et. Al (2020), which is elaborated further in this section. As such BigchainDB could play a crucial role in allowing insurance providers to adopt new technologies while minimizing disruptions to their existing infrastructure. In the context of BigchainDB, entries on the blockchain are classified as assets and can represent tangible or intangible assets, such as bicycles, health records, or insurance claims respectively. Furthermore, there is a metadata field that allows further specification of the asset (BigchainDB GmbH, 2018). In the example of an insurance claim, the corresponding metadata could be the date and time of the incident or loss, a description of the insurance claim, and if available a corresponding police report. BigchainDB also allows for the

encryption of part of the asset, allowing for the anonymization of a policyholder's claim record while still sharing relevant metadata with other insurance providers.

Using BigchainDB's metadata querying functionality, insurance companies can extract records based on date and time across the entire blockchain to identify cases of double-dipping. Double-dipping is a type of insurance fraud and refers to a policyholder filing multiple claims for the same incident at various insurance providers (Fourie, 2021). Since claim records are currently stored in isolation in each insurance company’s database, cases of double-dipping are hard to detect.

Gokay et al. (2020) implemented a proof of concept of a blockchain-based solution to detect fraud in health insurance using BigchainDB as one of their main backend components. While the authors highlight BigchainDB as one of the only viable solutions at the time of writing, they also elaborate on the difficulties of setting up the infrastructure due to a lack of community support and a stable version. As such it would be interesting to see if this has changed since the takeover by the Interplanetary Database Project. Nevertheless, Gokay et al. (2020) emphasize the benefits of greater data availability by using a blockchain-based architecture for storing insurance records.

4.2. The Lemonade Foundation

A decentralized autonomous organization (DAO) called the Lemonade Crypto Climate Coalition was established by the Lemonade Foundation with the goal of using blockchain technology to create and provide cost-efficient and immediate parametric weather insurance to farmers and livestock keepers in emerging economies (Lemonade Foundation, 2022). The climate insurance will be developed as a decentralized application (dApp) denominated in stablecoins on the sustainable proof-of-stake Avalanche blockchain (Wilard, 2022). The utilization of smart contracts, rather than conventional insurance policies, and the integration of oracles in lieu of claims adjusters will leverage the collaborative and decentralized features of web3 and real-time weather information (Lemonade Foundation, 2022). The DAO's smart contracts will be initially funded by the Lemonade Foundation, and over time, cryptocurrency investors will be allowed to contribute to the liquidity pool. The DAO will also release a governance token to encourage community participation (Lemonade Foundation, 2022).

The on-chain solution from the Lemonade Crypto Climate Coalition can have an immediate impact at scale and will enable farmers to obtain financial protection against the hazards that are becoming more frequent, including droughts., that are currently faced by the majority of the estimated 300 million smallholder farmers in Africa (Wilard, 2022). The Lemonade Foundation's use of blockchain technology to deliver affordable and instantaneous climate insurance to farmers in emerging markets is an example of how blockchain can be used in the insurance industry to prevent fraud and increase transparency. Even though this is not the main goal of this coalition, the use of blockchain technology, smart contracts, and oracles in this use case eliminates the need for intermediaries and reduces the potential for fraud (Evans, 2022).

The Lemonade Foundation once launched specifically a fraud detection system that was based on blockchain technology, but for unexplained reasons, they ended this project (Hsieh, 2021). As

Lemonade is a big player in the insurance industry in the U.S. it deserved to be mentioned even if their Crypto Climate Coalition doesn't directly focus on fraud detection.

4.3. B3i

Presently, data is perceived as a valuable commodity, which poses challenges for multinational insurance corporations to abandon authority over their data by sharing their claim records publicly on a decentralized ledger with other insurance providers. Gatteschi et al. (2018a) propose a permissioned blockchain run by a consortium of insurance companies as a potential approach to implementing a distributed database for claim records.

One notable example of a blockchain consortium in the insurance industry was B3i, established in 2018 with the aim of exploring the possible use of blockchain technology in the insurance industry. The initiative supported major insurance industry investors and its members included some of the biggest names in the insurance industry such as Allianz, Swiss Re, and Munich Re. A diverse community of over 40 companies and large investors in the insurance industry sponsored the global effort led by B3i. It was established in Zurich in 2018 with the intention of developing the primary insurance protocol to solve important insurance industry needs while also expanding its network and forming relationships with other projects. One of the key areas that B3i has focused on was also fraud detection. Their general vision was to deliver better solutions for the end consumers through more efficient and rapid access to insurance in general, creating fewer operational risks for the insurance focusing on better fraud prevention, and lowering administrative costs (Crunchbase, 2023).

Unfortunately, the startup B3i went bankrupt. They made a short statement saying that the reason for that was based on unsuccessful attempts to close further rounds of financing and that there was insufficient support for the venture at their development stage. According to an anonymous insurance analyst, no one had used B3i (Niklowitz, 2022). In the Critical Discussion chapter, we will talk about the potential outlook of companies in the insurance industry.

4.4. Samsung SDS

Samsung SDS, a subsidiary of South Korean tech conglomerate Samsung, has launched a blockchain-based medical claims processing system. This system is aimed at simplifying the complex process of medical claims processing in Korea, connecting hospitals, pharmacies, insurers, and other companies in the insurance industry (Ben-Hutta, 2019). The system uses blockchain technology to share personal medical information securely and accurately, reducing fraud and processing costs of medical claims by up to 70 percent (Ben-Hutta, 2019). The new system has been launched in partnership with various stakeholders in the healthcare industry, with plans to expand the scope of services provided. According to Samsung SDS (2020), policyholders now have the option to initiate claims directly after paying their medical bills, either at the hospital reception or via their mobile devices. Upon completion of payment, policyholders receive a message via KakaoTalk, a mobile messenger application, which contains a hyperlink to initiate the reimbursement process (Samsung SDS, 2020). The objective of the blockchain-powered system is

to mitigate receipt-related fraud, curtail expenses, and enhance productivity for healthcare establishments and insurers. A more detailed description of receipt fraud can be found in the appendix. We have summarized our understanding of their One-Stop Medical Claims System and illustrated it in the following figure:

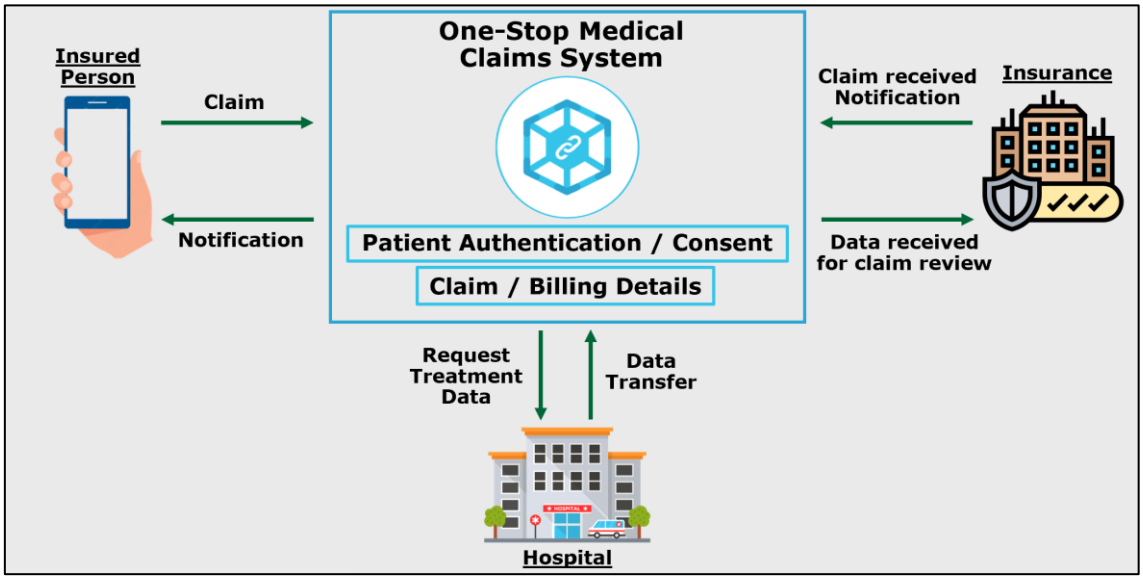

Figure 2: An overview of how Samsung SDS works (own illustration)

With the use of blockchain technology, personal medical information can be shared securely and accurately, eliminating the requirement for extraneous paper-based receipts and documents (Samsung SDS, 2020). Concurrently, healthcare providers can concentrate on proactively deterring receipt fraud at the point of origin and markedly decrease expenses via fraud identification, achieved by the elimination of manual document processing (Samsung SDS, 2020). The use of blockchain technology also makes the process of claims faster and more efficient, reducing the workload at medical institutions and shortening wait times for claims processing (Ben-Hutta, 2019). The mechanism speaks for trust and makes the common frauds by the provider and consumer much more difficult to achieve. This new system is built on the Nexledger blockchain platform, which was developed originally in 2017 by Samsung SDS. The platform is currently being utilized in the execution of 110 blockchain initiatives and possesses 51 patents (Meyer, 2019). The system is expected to expand to 30 health facilities, including Korea University Medical Center, Seoul Medical Center, and eight insurance companies (Pratap, 2019).

In conclusion, the launch of Samsung SDS's blockchain-based medical claims processing system marks a significant step towards simplifying the complex process of medical claims processing in Korea. This new system connecting all stakeholders in the industry to simplify the claims process creates a valuable platform for all parties involved. With plans to expand the scope of services provided, the new system has the potential to revolutionize the healthcare industry in Korea.

4.5. SWOT-Analysis of Samsung SDS

As we have seen, there aren't many successful projects that focus on fraud detection in the insurance industry. The only companies we analyzed that had enough resources and somehow had a focus on fraud detection, were Samsung SDS and BigchainDB. Whilst we realized that the medical claim management system of Samsung SDS was the most similar to what many theory sources described, a SWOT Analysis of their business model will give a deeper dive into the future of those companies & startups that want to interact in the insurance industry to prevent fraud. The analysis is rather pessimistic due to the reasons mentioned above. The following Figure weighs the four aspects and brings more objectiveness to this service:

Strengths	**Weaknesses**
• Secure and tamper-proof platform for storing/sharing sensible medical data which prevents fraud and data breaches • Workload reduction & shorter wait times for claims processing (which also improves customer satisfaction) • Samsung SDS's "home" blockchain platform Nexledger speaks for professionality and extensive experience • Network including major hospitals which indicate strong interest • Specific goal & not too overbearing	• System adoption may be slow as medical data sharing could bring user hesitation (even when it's encrypted) • Fraud effectiveness is limited as fraudsters may find new ways to manipulate the system or falsify data • Legal and regulatory issues, especially as it started in Japan. • Rather simplifying fraud detection than really trying to prevent it • Insider fraud is possible for individuals with authorized access to the system
Opportunities	**Threats**
• Expanding their system to other industries where the claims management process could be simplified • Integration with Machine Learning to create more powerful applications like verifying the authenticity of claims to prevent fraudulent "fake" claims • Collaborate with other blockchain projects/firms to improve their system and bring in new perspectives (also more trust as the B3i went bankrupt)	• Hype of Blockchain causing a short-term lifetime (see; critical discussion) • Companies might not be ready to invest much money if this system doesn't significantly lower their costs • Competition, maybe also insurance companies themselves integrate a solution like this in collaboration with smaller firms rather than Samsung SDS • Data breaches & cyber-attacks could cause reputational damage leading to fewer customers for all involved parties

Figure 3: SWOT-Analysis of Samsung SDS's blockchain-based medical claims system (own illustration)

Samsung SDS offers a system that is indeed very smart and widely useable. But as many arguments speak for the real product and business model, many of them also speak against it. A key takeaway that seems to be around in the current market situation is the hype of many blockchain-based startups that try to solve a problem without really solving it but rather just simplifying it. The following chapter will critically elaborate further on this.

4.6. Critical Review of Real-World Solutions

The implementation of blockchain technology has gained significant attention and interest in recent years due to its potential to revolutionize various industries. However, it is essential to acknowledge that the development of blockchain projects is often driven by hype, fueled by the speculative nature of cryptocurrencies. This can lead to unrealistic expectations and an overemphasis on the potential benefits of the technology, which may not always translate into useful applications. As such it comes as no surprise that projects are being discontinued or shifting focus, as the examples of B3i and BigchainDB suggest. The bankruptcy rate among blockchain startups is exceptionally high. According to an analysis of GitHub repositories, less than 10% succeed with the majority being in business for just one year (Deloitte, 2017). During our research, we stumbled across several failed startups committed to eliminating insurance fraud using blockchain technology.

Consequently, this gives rise to the question of whether blockchain protocols are developed enough for an application such as fraud detection or if blockchain technology remains a theoretical concept when it comes to preventing deception. On the one hand, there are impressive success stories of decentralized insurance solutions, disrupting entire industries. One such example is Insurwave Ltd. for cargo insurance (insurwave, 2023) which gained a remarkable 8% market share in maritime insurance. On the other hand, at the time of writing the only blockchain-based solution fully devoted to mitigating fraud in the insurance industry is Samsung SDS. However, as Samsung SDS focuses on a niche of digital prescriptions, it remains to be seen whether their approach can be scaled to prevent fraud in different parts of the insurance industry.

Intuitively it seems reasonable that blockchain startups focus on decentralized insurance solutions first, before approaching more specific problems such as insurance fraud. Streamlining a more efficient process between insurers and insurance companies appears economically more promising and easier to implement using existing solutions such as smart contracts. Nonetheless, proof of concepts such as the one proposed by Gatteschi et al. (2018a) indicates a continuing interest of academia in fraud prevention using blockchain.

Moreover, it is worth noting that the issue of fraud is not limited to the insurance sector alone. Therefore, a potential solution for fraud detection and mitigation could be implemented across various businesses. The implementation of such solutions for fraud prevention could potentially result in significant cost savings for the industries concerned.

5. Advantages and Disadvantages

As already mentioned in previous sections, blockchain is gaining increasing attention in both academia and industry and is seen as a disruptive technology for, among other things, detecting fraud in the insurance business. However, the growing excitement could bias an objective assessment of whether to invest in this technology. In addition to the numerous benefits of technology, the challenges and risks of implementation should be kept in mind. In the following, the main advantages, and disadvantages, as well as associated risks and opportunities of blockchain technology in the insurance industry are being discussed.

The adoption of blockchain technology in an insurance company for fraud prevention has the power to help eliminate errors and detect fraudulent activity in insurance businesses. A particular form of fraud is signing several insurance policies covering the same event at various insurance companies, intending to later fake a claim and obtain payouts from several insurance policies related to the same incident. To eliminate the risk of double coverage fraud, insurance companies are reaching out to the blockchain before creating a new insurance policy. This helps to ensure that there are no duplicate insurance policies for the same person and the same incident (Roriz & Pereira, 2019).

To detect identity fraud, fake injury, or falsified damage reports, blockchain may be used as a distributed registry of customer data. Blockchain enables the authenticity of documents to be validated, the identity of an individual to be verified, and patterns of fraudulent behavior associated with a particular identity to be uncovered (Lorenz, et al., 2016). As demonstrated by the example of Samsung SDS, personal medical information can be exchanged safely using the blockchain, making paper documents unnecessary. In addition, this example shows how an insurance company can use blockchain systems to detect fraud very quickly and save significantly on expenses by removing the need for manual processing of documents (Samsung SDS, 2020). A further advantage of using blockchain technology for fraud detection is the immutability of the data stored on the blockchain. The cryptographic system guarantees that data cannot be altered or deleted. Thus, each network node's duplication of the blockchain ensures that it will survive any unforeseen events, such as hacks and data manipulations, and therefore leads to increased data security (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018a).

In general, two important disadvantages of blockchain technology are the low scalability and the high energy consumption (Alshahrani, et al., 2023). However, it is worth noting that some blockchain projects designed the validation process of the blocks differently to save energy. Nevertheless, an insurance company needs to be aware of these issues in terms of sustainability and efficiency. Further limitations are the necessary technical skills of all participants on the blockchain combined with the fact that development tools are yet poorly established. Thus, the technology is still not familiar to many people, which does not strengthen users' trust in the technology (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018a). This drawback is well reflected in the failure of B3i. As discussed in the corresponding section, B3i was not used by anyone, which could be due to the lack of interoperability and the lack of trust in blockchain

technology, a concept that is still new to the market (Niklowitz, 2022). Current laws and legal considerations are other drawbacks that should be considered before implementing blockchain for fraud detection. In the public eye, digital ledger technology is seen as offering security, immutability, and transparency, so laws and regulations are viewed as unnecessary. When implementing blockchain applications in insurance for fraud detection, laws and regulations cannot simply be ignored. The legal risk will remain even though the data is distributed among multiple ledgers (Zetzsche, Buckley, & Arner, 2017).

Researchers agree that blockchain is an enormously valuable technology and can help detect fraud in the insurance industry. Since blockchain still has many limitations, an insurance company should comprehensively evaluate the implementation of the technology to detect fraud (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018b).

6. Legal and Regulatory Implications

As mentioned in previous chapters, by using blockchain technology, customer data can be stored in a decentralized manner and protected from manipulation and fraudulent actions. For insurers planning to implement distributed ledger technology in fraud detection, several legal implications regarding data responsibility are discussed in the next sections.

Before discussing the various implications of implementing a blockchain system to detect insurance fraud, the current situation regarding data protection laws in Switzerland should be clarified. In general, all companies in Switzerland that process personal data in any form must comply with the Swiss Federal Act on Data Protection (FADP). A business must adhere to the General Data Protection Regulation (GDPR) as soon as it begins processing data from EU citizens (Hauser, et al., 2017). According to Art. 3 lit. e. FADP, "processing" is defined as any form of handling personal data, in particular obtaining, storing, using, reworking, disclosing, archiving, and destroying it. Therefore, insurance companies in Switzerland are principally obliged to comply with the Federal Data Protection Act as well as, depending on their activities in the EU, the General Data Protection Regulation when working with customer data.

What does this mean for insurance companies using blockchain systems to prevent and detect insurance fraud? Regarding data protection responsibility, the difference between public and private blockchain systems must be mentioned. Depending on whether a private or public blockchain is used to store customer data, there are different legal consequences for the insurance company in terms of data protection. The data protection implication is clear for insurers using private blockchain systems to detect insurance fraud. In a private blockchain as a closed system, one or several central entities must undertake data protection responsibility. These central parties are, as mentioned, subject to the FADP and the GDPR respectively (Isler, 2017). The challenge now arises when using public blockchain systems, in which the nodes can be distributed all over the world. The globally distributed network makes it complicated to determine the data protection responsibilities as well as the applicable data protection law. Another challenge in applying blockchain technology for fraud detection is the right to deletion that applies under the GDPR, which is incompatible with the subsequent immutability of data in public blockchain systems. This problem could be avoided by insurers, for instance, with the usage of private blockchain systems or the nomination of a central authority among the participants of the blockchain a central body that manages GDPR compliance, establishes network participants' rights, and negotiates contracts with nodes for the processing of data (Guggenmos, Rieger, Wenninger, Fridgen, & Lockl, 2020).

In conclusion, the main obstacle regarding the use of blockchain applications for fraud detection under data protection law is the insufficient responsibility allocation of the data controller to all nodes of the blockchain platform as well as the lack of practicable options for the later deletion of stored data. Consequently, the optimal solution would be a regulation that assigns responsibility for the information processed on-chain and makes the deletion of stored data no longer necessary (Fridgen, Guggenberger, Hoeren, Prinz, & Urbach, 2019).

7. Conclusions and future perspectives

The hype surrounding cryptocurrencies has fueled interest in the underlying blockchain technology. While blockchain holds great promise for the insurance industry, it is important to approach its implementation with caution and careful consideration of legal and technical issues. Real widespread adoption in fraud detection remains yet to be seen, although there are initiatives such as Samsung SDS pushing in the right direction. Nevertheless, the high failure rate observed in blockchain projects intended to mitigate insurance fraud remains a point of concern. It is noteworthy that the involvement of renowned insurance providers did not appear to affect the negative outcome in a significant manner. This point would certainly be a suitable field for further analysis. Perhaps also using a more data-driven method, which was a limitation of this research. It would be interesting to get more insider information, obtained for instance through interviews, on why a certain project in this area fails, since the reasons for failure are usually communicated vaguely.

For blockchain to be established as a go-to solution for fraud prevention within the insurance sector, it is necessary to overcome various limitations. Notably, technology must address scalability and sustainability issues before achieving widespread adoption. Additionally, as insurance records contain confidential data, it is crucial to propose novel privacy regulations for decentralized data storage. Furthermore, deletion mechanisms should be implemented to provide insurers with control over their data. Despite these challenges, the potential benefits of using blockchain technology for fraud mitigation in the insurance industry cannot be ignored. The immutability and data integrity features of blockchain technology make it a suitable solution for fraud prevention.

In the long term, we believe that the full potential of blockchain technology for fraud mitigation in the insurance industry can only be realized through further research and development. This includes not only technological advancements such as scalability improvements but also the harmonization of legal and regulatory frameworks that support the use of blockchain technology in a privacy-preserving manner. Moreover, it should be of corporate interest to witness additional proof of concepts beyond the work of Gatteschi et al. (2018a) to assess whether blockchain technology has advanced concerning fraud detection solutions. Finally, we recommend that insurance companies continue to explore the use of blockchain technology in partnership with startups and other technology firms. Collaboration with regulators and policymakers can also help to address legal issues and provide a supportive environment for the adoption of this novel technology. We hope that our report has shed light on the potential of blockchain for fraud mitigation in the insurance industry and has provided a starting point for further discussion and research.

8. References

Al-Jaroodi, J., & Mohamed, N. (2019, April 2). Blockchain in Industries: A Survey. *IEEE Access, 7*, 36500-36515. doi:10.1109/ACCESS.2019.2903554

Alshahrani, H., Islam, N., Syed, D., Sulaiman, A., Al Reshan, M., Rajab, K., . . . Soomro, A. (2023). Sustainability in Blockchain: A Systematic Literature Review on Scalability and Power Consumption Issues. *Energies, 16*. doi: https://doi.org/10.3390/en16031510

Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology. *Decision Analytics Journal*, 100121.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., . . . Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable & Sustainable Energy Reviews*, 143–174.

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer (Long Beach, Calif.)*, 18-28.

Back, A. (2002). Hashcash-a denial of service counter-measure.

Ben-Hutta, A. (2019, November 1). *coverager.com*. Retrieved February 28, 2023, from Samsung SDS pilots blockchain for medical claims: https://coverager.com/samsung-sds-pilots-blockchain-for-medical-claims/

BigchainDB GmbH. (2018). *BigchainDB 2.0 The Blockchain Database.* Berlin. Retrieved from https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, 55-81.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 2292-2303.

Coalition Against Insurance Fraud. (2022). *Fraud Stats*. Retrieved February 24, 2023, from insurancefraud.org: https://insurancefraud.org/fraud-stats/

Contracts Counsel. (2017). *Insurance Agreement*. Retrieved March 14, 2023, from https://www.contractscounsel.com/t/us/insurance-agreement

Crunchbase. (2023). *crunchbase.com.* Retrieved February 27, 2023, from About B3i: https://www.crunchbase.com/organization/b3i

Deloitte. (2016). *Blockchain in insurance, Turning a buzzword into a breakthrough for health and life insurers.* Deloitte Development LLC. Retrieved from

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-in-insurance-ebook.pdf

Deloitte. (2017, November 6). *Evolution of blockchain technology - Insights from the GitHub platform*. Retrieved February 28, 2023, from https://www2.deloitte.com/us/en/insights/industry/financial-services/evolution-of-blockchain-github-platform.html

Evans, H. (2022, September 25). *Velvetech.* Retrieved February 26, 2023, from Blockchain-Powered Insurance Solutions: Disruption, Benefits, and Challenges.: https://www.velvetech.com/blog/blockchain-powered-insurance-solutions/

Fourie, R. (2021, September 3). Retrieved from modata: https://modata.com/insights/quantifying-double-dipping-fraud-for-the-first-time-ever/

Fridgen, G., Guggenberger, N., Hoeren, T., Prinz, W., & Urbach, N. (2019). *Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik [Opportunities and challenges of DLT (Blockchain) in mobility and logistics]*. Berlin: Bundesministerium für Verkehr und digitale Infrastruktur.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018a). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet*, pp. 1-16.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018b, April). To Blockchain or Not to Blockchain: That Is the Question. *IT Professional*, pp. 62-74.

Gokay, S., Reddy, V., Bojja, K. S., Gururaja, M. K., Doddaveerappa, Y., & Tawalbeh, L. (2020). Health Care Insurance Fraud Detection Using Blockchain. *2020 Seventh International Conference on Software Defined Systems (SDS).* Paris.

Guggenmos, F., Rieger, A., Wenninger, A., Fridgen, G., & Lockl, J. (2020). How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, pp. 4023-4032.

Hauser, C., Blumer, H., Christen, M., Hilty, L., Huppenbauer, M., & Kaiser, T. (2017). *Ethische Herausforderungen für Unternehmen im Umgang mit Big Data [Ethical challenges for companies in dealing with big data]*. Schweizerische Akademie der Technischen Wissenschaften SATW.

Highmark Western New York. (2022). *bcbcswny.com.* Retrieved March 02, 2023, from Health Insurance Fraud: https://www.bcbswny.com/content/wny/member-services/tools/fraud.html

Howard, L. (2022, July 29). *Industry's Blockchain Project, B3i, Ceases to Trade After Filing for Insolvency*. Retrieved from Insurance Journal: https://www.insurancejournal.com/news/international/2022/07/29/677926.htm

Hsieh, N. (2021, March 19). *voltequity.com.* Retrieved February 28, 2023, from Lemonade's AI Jim and Insurance Fraud Detection: https://www.voltequity.com/post/lemonades-ai-jim-and-insurance-fraud-detection

insurwave. (2023). Retrieved from insurwave: https://insurwave.com/

Interplanetary Database Association. (2023). Retrieved from https://ipdb.io/

Investopedia. (2022, July 18). *Insurance*. Retrieved February 24, 2023, from https://www.investopedia.com/terms/i/insurance.asp

i-Sight. (2019, November 4). Retrieved March 2, 2023, from https://www.i-sight.com/resources/insurance-claims-investigations-detecting-fraud-and-abuse/

Isler, M. (2017, Dezember 4). Datenschutz auf der Blockchain [Data protection on the blockchain]. *Jusletter*, pp. 1-18.

Kar, A. K., & Navin, L. (2021). Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Oxford: Elsevier Ltd*, 101532.

kbv Research. (2019, September). *Power of Data and Analytics in Insurance Fraud Detection*. Retrieved February 27, 2023, from https://www.kbvresearch.com/blog/power-of-data-and-analytics-in-insurance-fraud-detection/

Kumar, R., Arjunaditya, Singh, D., Srinivasan, K., & Hu, Y.-C. (2022). AI-Powered Blockchain Technology for Public Health: A Contemporary Review, Open Challenges, and Future Research Directions. *Healthcare (Basel)*, 81.

Lemonade Foundation. (2022, March 22). *lemonade.com.* Retrieved February 26, 2023, from Introducing the Lemonade Crypto Climate Coalition: https://www.lemonade.com/blog/crypto-climate-coalition/

Lorenz, J.-T., Münstermann, B., Higginson, M., Olesen, P. B., Bohlken, N., & Ricciardi, V. (2016). *Blockchain in insurance-opportunity or threat?* McKinsey & Company.

Management Events. (2023, March 1). *Insurance Fraud Detection using Maschine Learning*. Retrieved from https://managementevents.com/news/insurance-fraud-detection-using-machine-learning-what-you-should-know/

Meyer, R. (2019, October 17). *coindesk.com.* Retrieved February 28, 2023, from Samsung SDS Pilots Blockchain-Based Medical Insurance Network: https://www.coindesk.com/markets/2019/10/17/samsung-sds-pilots-blockchain-based-medical-insurance-network/

NAIC. (2022, December 19). Retrieved March 1, 2023, from https://content.naic.org/cipr-topics/insurance-fraud

Nakamoto, S. (2008). *Bitcoin: A Peer-To-Peer Electronic Cash System.* Manubot.

Niklowitz, M. (2022, October 24). *Das Ende einer Startup-Hoffnung: B3i ist pleite [The end of a start-up hope: B3i is bankrupt]*. Retrieved February 27, 2023, from Handelszeitung: https://www.handelszeitung.ch/insurance/das-ende-einer-startup-hoffnung-b3i-ist-pleite-540666

Ocean Protocol Foundation Ltd. (2023). Retrieved from https://oceanprotocol.com/

Ouyang, L., Zhang, W., & Wang, F.-Y. (2022). Intelligent contracts: Making smart contracts smart for blockchain intelligence. *Computers & electrical engineering*, 108421.

Pratap, J. (2019, October 17). *coinnounce.* Retrieved February 28, 2023, from Samsung SDS to introduce blockchain-based medical claims processing system – Blockchain News: https://coinnounce.com/samsung-to-introduce-blockchain-medical-network/

Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K.-Y. (2018). A blockchain framework for insurance processes. *IFIP International Conference on New Technologies, Mobility and Security*, 1-4.

Reuters Events. (2023, March 1). Retrieved from https://www.reutersevents.com/insurance/fraud/role-data-and-analytics-insurance-fraud-detection

Roriz, R., & Pereira, J. (2019). Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector. *Procedia Computer Science*, p. 211-218.

Samsung SDS. (2020, January 30). *samsungsds.com.* Retrieved February 28, 2023, from Samsung SDS launches one-stop medical claims processing service fueled by blockchain: https://www.samsungsds.com/en/news/samsung-sds-launches-one-stop-medical-claims-processing-service-fueled-by-blockchain.html

Shi, Y., Sun, C., Li, Q., Cui, L., Yu, H., & Miao, C. (2016). A fraud resilient medical insurance claim system. *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (AAAI-16)*, (pp. 4393-4394). doi:10.1609/aaai.v30i1.9825

Swanson, T. (6. April 2015). *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.* Tratto da http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, 28.

Tang, L., Torngren, M., & Wang, L. (2020). *A Permissioned Blockchain Based Feature Management System for Assembly Devices.* Tratto da IEEE access: https://doi.org/10.1109/ACCESS.2020.3028606

The Balance Money. (2022, May 3). *Get the Basics to Learn How Insurance Works*. Retrieved February 26, 2023, from https://www.thebalancemoney.com/basics-to-help-you-understand-how-insurance-works-4783595

Top Insurance. (2022, November). *Major Challenges facing Insurance Industry*. Retrieved March 2, 2023, from https://mytopinsuranceblogs.com/major-challenges-facing-insurance-industry/

Verivox. (2022). *Versicherungsbetrug [Insurance fraud]*. Retrieved February 28, 2023, from https://www.verivox.de/privathaftpflicht/themen/versicherungsbetrug/

Voulgaris, S., Fotiou, N., Siris, V. A., Polyzos, G. C., Jaatinen, M., & Oikonomidis, Y. (2019). Blockchain Technology for Intelligent Environments. *Future Internet*, 3-16.

Wendl, M., Doan, M. H., & Sassen, R. (2023). The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *Journal of environmental management*, 116530.

Wilard, J. (2022, March 22). *Reinsurance News.* Retrieved February 26, 2023, from Lemonade to Use Blockchain to Deliver Affordable and Instantaneous Climate Insurance.: https://www.reinsurancene.ws/lemonade-to-use-blockchain-to-deliver-affordable-and-instantaneous-climate-insurance/

Zetzsche, D., Buckley, R., & Arner, D. (2017, August 15). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *EBI Working Paper Series*.

Zhou, L., Wang, L., & Sun, Y. (2018). *MIStore: a Blockchain-Based Medical Insurance Storage System.* New York: Springer US.

Zibin Zheng, H.-N. D. (2021). *Blockchain intelligence : methods, applications and challenges.* Singapore: Springer.

Appendix A

The receipt frauds mentioned in chapter 4.4 are specifically very common in the health insurance industry. They can be committed by a doctor (provider) or a consumer (Highmark Western New York, 2022). The following table shows the three most common frauds that appear per committer:

Provider fraud	Consumer fraud
• Billing services never performed or billing for a more costly service than performed	• Using a false or expired identification card to receive medical services
• Falsifying diagnosis to justify the need for more medical procedures	• Forging/Altering medical bills or receipts
• Maximize the reimbursement by billing each stage of a procedure as if it were separate	• Adding an individual for coverage to a contract who is not eligible

Figure 4: Common Frauds by doctors and consumers (Highmark Western New York, 2022)