Blockchain Solutions for Fraudulent Claims in Healthcare Insurance

Zurich, 15th March 2023

SMART
CONTRACTS
LAB

UZH
Blockchain
Center

Blockchain
Presence

Abstract

This paper aims to make blockchain-based solutions for healthcare insurance fraud accessible to insurers that have no or little knowledge of blockchain technology. In recent years a lot of research papers showed concepts to solve certain kinds of fraud using blockchain technology. This paper is a literature review of these sources, presenting the solutions and evaluating the strengths and risks of the utilization of blockchain technology in the healthcare insurance industry. While the strengths outweigh the weaknesses and the implementation could be very profitable in big markets, this paper concludes that implementation will not happen in the immediate future.

This paper shows why blockchain-based solution are more effective and more efficient than the current system. Many types of fraud can be prevented successfully with the solution of blockchain-technology. It also shows that the more efficient the solution is, the less insurance companies must trust the insureds. Additionally, the cost for the insureds can be reduced. Finally, the strengths outweigh the risks. All this means that blockchain-based solutions could be an interesting opportunity in the future for insurance companies.

Table of Contents

Abbreviations

DApps	Decentralized applications
DLT	Distributed Ledger Technology
IPFS	InterPlanetary File System

List of Figures

1 Introduction

Healthcare insurance companies (hereafter “insurance companies”) claim fraud is a pervasive problem that costs the healthcare industry billions of dollars annually (FBI, 2016). Fraudulent claims are a severe threat to the financial situation of healthcare providers and insurance companies, as well as the well-being of patients who rely on accurate and timely healthcare services. Traditional methods of preventing and detecting fraud, such as audits, investigations, and compliance measures, have proven ineffective and resource intensive. However, recent advances in blockchain technology and smart contracts have the potential to revolutionize the way healthcare insurance claims are processed, making it easier to prevent and detect fraudulent activities.

Blockchain technology provides a decentralized and immutable ledger that allows multiple parties to access and verify data without the intervention of a centralized authority. Smart contracts are self-executing digital contracts that can automate the execution of agreements and provide transparency, efficiency, and security that traditional contracts cannot offer. Together, blockchain technology and smart contracts can help to address some of the key challenges facing the healthcare insurance industry, including fraud prevention, claims processing, and data security. We hypothesize that blockchain technology offers a better solution than the status quo at combatting healthcare insurance fraud. Based thereon, we hypothesize that blockchain technology effectively detects healthcare insurance fraud and therefore saves money that otherwise would have been lost to fraudulent behavior. Further, we hypothesize that there are certain limitations to blockchain-based technologies. However, we assume that the advantages outweigh the disadvantages.

This paper is aimed at insurance companies that are considering implementing blockchain technology but do not have experience with blockchain technology. There are a lot of papers about the use cases of blockchain in the healthcare insurance industry, many of whom look at fraud prevention. The problem is that all these papers are single-present concepts. There is a lack of papers that regard different documents or concepts and make them broadly accessible.

This research paper aims to explore the potential of blockchain technology and smart contracts to mitigate healthcare insurance claims fraud and improve the overall efficiency and effectiveness of the healthcare system. The paper examines how these technologies work, what benefits they offer, and what their limitations are in the context of healthcare insurance claims. It also provides a critical analysis of the current state of healthcare insurance claims and how blockchain technology and smart contracts can address the challenges faced by the industry. Finally, the paper discusses the implementation of this technology.

2 Methodology

This chapter gives an outline of the methods implemented and the most important sources that this paper relies on. The paper uses a literature review as its method because the conditions are optimal for writing one. In recent years a lot of research has been conducted in the field of blockchain technology. A large part of that research consists of looking for new or improved use cases for blockchain. This is the same in the healthcare industry and healthcare insurance specifically. To find the sources, two methods are utilized.

First, keyword searches are used, where the web is scoured for journal papers, books, and other articles that include certain keywords such as "blockchain" and/or "healthcare insurance industry". After building a solid base of sources, applying a more specific method makes more sense. The sources found in the keyword search are then looked through to find more fitting sources.

The most important sources for this paper are the solutions for different existing problems. Saldamli et al. (2020) and Liu et al. (2019) solve problems like doctor shopping by using blockchain to introduce transparency to the system. Chen et al. (2021) created a solution to detect individuals with wrong intentions. Zhang et al. (2022) worked on improving traceability. Novikov et al. (2018) and Liu et al. (2019) use the immutability of blockchain to their advantage to prevent corruption and fraud in the healthcare system. Lamba et al. (2022) focused their work on identity management and thus the problem of identity theft. To round out the most critical sources, Alnuaimi et al. (2022) and Mackey et al. (2020) focus on the strengths and risks that the implementation of blockchain technology brings.

3 Healthcare Insurance Industry

In order to understand why insurance companies should rely on a blockchain-based solution, it is essential to acknowledge what problems the market is facing as well as their consequences.

3.1 General

Healthcare insurance is a contract between the insurance company and the policy holder (hereafter "the insured".), in which the insurance company compensates the insured for healthcare expenses (United Healthcare, n.d.). The compensation is triggered by the submission of a medical claim which is subsequently forwarded to the insurance company, who reviews it and decides, depending upon the terms of the contract, to pay a reimbursement. Consequently, the submission of the medical claim can be made by either the insured or the healthcare provider.

The term medical claims can be understood as any claim for which the insurance company reimburses the insured or the healthcare provider (Goundar et al., 2020). This includes claims pertaining doctors' consultations, prescribed medication, or overseas treatment costs. The total amount of money of all claims submitted annually is very large and should therefore be carefully examined when setting up annual financial budgets.

3.2 Problems in the Current State

Perhaps the most significant concern (i.e., costs) in such a system is claim-abnormality (Lu et. al, 2020). Thus, detecting anomalies is of great importance for both insurance companies and governments. Three types of anomalies exist in the context of healthcare insurance claims: fraud, abuse, and error. Fraud refers to the intentional act of deceit, misrepresentation, or concealment in order to obtain payment from the insurance company. Abuse indicates an unreasonable or inappropriate use of services that results in excess costs. Errors are mistakes made unintentionally while processing claims by one or more parties. It is not always clear what the boundaries between the three categories are (Lu et. al, 2020). All three types of anomalies deserve special attention.

However, this paper will focus on fraud issues. Fraud has a significant impact on governments and insurance companies across the globe. Recent research has shown that fraudulent claims account for 15% of the total claims in the insurance sector (Kareem et al., 2017). According to the U.S. Department of Health and Human Services' Centers for Medicare and Medicaid Services' data from 2010, the amount claimed from healthcare fraud in the US was between $77 billion and $259 billion (FBI, 2016). In the UK, over one billion pounds are lost annually due to fraudulent insurance claims (Kirlidog & Asuk, 2012). Another report indicates that the Indian industry loses between 6 and 8 billion Indian Rupees per year due to counterfeit claims (Rawte & Anuradha, 2015). This fraud is made possible by the fact that the system is built upon a certain degree of trust (Alhasan et al., 2021). Insurance companies tend to trust the information offered by the patient and the health provider (Alhasan et al., 2021). Sometimes dishonest actors take advantage of this trust in order to enrich themselves (Chu & U.S. Attorney's Office, 2020). For instance, in 2020, a total of 345 defendants were charged for fraud in connection with healthcare insurance in the US. This included over 100 doctors, nurses, and medical professionals.

Below is a highlighted summary of the most typical types of healthcare insurance frauds or fraud-like practices. Not all of them are easily classified as fraud because certain practices are not easy to classify as fraudulent.

3.2.1 Kickback Schemes

Kickbacks are one of the most common types of fraud (Rabecs, 2006). There are many different kinds of kickbacks and not all of them are illegal. For example, apothecaries can hand out a prescription with a specific brand of medicine, which will yield a bonus from the drug company instead of offering another brand of medication. This does not only have explicit financial implications, but the drugs might not be optimal or necessary for the patient (Morris, 2009). It is possible for doctors to write prescriptions that are not medically warranted in exchange for money, which could essentially lead to the unlawful sale of these drugs (Morris, 2009).

3.2.2 Self-referral

This involves patients being transferred to a doctor or clinic with whom the referring healthcare organization has a financial relationship (Li et al., 2008). If the healthcare organization receives part of the money that was given to the referred doctor or clinic this could involve a kickback scheme, but other financial relationships are conceivable (Liu, 2013).

3.2.3 Double Billing

Many healthcare providers send identical claims several times for the same service to get paid multiple times (Ogaboh & Osuchukwu, 2010; Margret & Sreenivasan, 2013).

3.2.4 Phantom Billing

Insurance companies receive claims for medical services and products which were not provided (Rashidian et al., 2012).

3.2.5 Identity Fraud

When an individual who is not insured takes over the identity of a person who is covered by an insurance company in order to obtain medical attention or hide a certain malady, identity fraud can occur (Plomp & Grijpink, 2011). This is often done with the cooperation of the insured, who is trying to help a friend or family member (Thornton et al., 2015). Identity fraud can have a negative impact on the individual lending their identity, as their health records could contain unrelated and potentially contradictory information (Thornton et al., 2015).

3.2.6 Doctor Shopping

Doctor shopping is where a person is intent on receiving a certain type of medication and will consult one doctor after another, sometimes feigning symptoms, until the medication is obtained (Thornton et al., 2015).

3.2.7 Improper Coding or Upcoding

One of the most relevant fraud topics is improper coding which is also known as upcoding (Agrawal et al., 2013). This takes place when the service billed is more expensive than the service that was performed. This is not always done with a fraudulent intent. Sometimes the cause is an administrative error.

3.2.8 Unbundling

Unbundling happens when medical services or products that would belong to the same claim are split up into separate claims (Cady, 2007).

4 Blockchain Technologies

This chapter introduces the reader to the basics of blockchain technology. It intends to establish a foundation for understanding blockchain to make the concepts that will be introduced in later chapters accessible. As previously mentioned, this paper is addressed to insurance companies that might not be familiar with blockchain technology yet. The explanation is conceptual and not technical. It focuses on what happens with a transaction from the execution until it is fixed in a block on the blockchain. Later on, the most important attributes will be outlined.

4.1 Basics

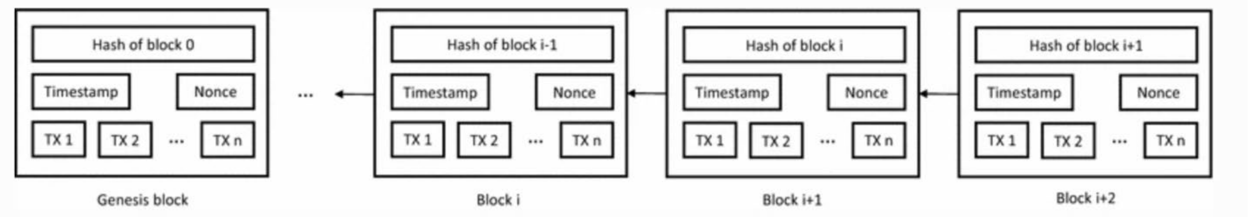
Blockchain Technology has been the focus of much attention in recent years, primarily because of its use in cryptocurrencies. This started in 2008 with Satoshi Nakamoto's whitepaper on Bitcoin (Nakamoto, 2008).

Blockchain is a distributed ledger technology (Lipovyanov, 2019). Crosby et al. (2016) describe it as follows "A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties" (p. 7).

The sender cryptographically signs these transactions (Laurence, 2019). The blockchain uses the cryptographic signature to confirm that the sender has the authority to initiate the transaction. Afterward, multiple transactions are combined into a block. Once the maximum number of transactions has been reached, or no more transactions are available, the block is added to the blockchain. This is done by linking the newest block to the previous one through hashes, creating a blockchain as is shown in Figure 1 below. Hashes, which are created using hashing algorithms, are a way of securing data. They are fixed-length strings of characters, and have crucial attributes for blockchain. This process is one-way, meaning it is not feasible to get to the input by having the output, and if a small part of the input is changed, the output will be very different (Laurence, 2019).

Figure 1

Example of a blockchain



Note. From "Blockchain challenges and opportunities: A survey", by Z. Zheng, S. Xie, H. N. Dai, X. Chen, & H. Wang, 2018, *International Journal of Web and Grid Services, 14*(4), p. 355 (https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf). Copyright 2018 by Inderscience Enterprises Ltd.

Who gets to create the new block and how this is decided depends on the consensus mechanism (Zhang et al., 2020). An in-depth description of the different mechanisms would be out of proportion for this paper. Therefore, only a short overview is provided. The most common mechanisms are Proof-of-Work and Proof-of-Stake. Proof-of-Work requires a complex computational puzzle to be solved and is a competition among miners to be the first to complete a block. Proof-of-Stake, which Ethereum now uses, is not based on computational power like Proof-of-Work, but instead on the pledging of currency (Zhang et al., 2020).

This makes it hard to control or manipulate a blockchain network. For example, in the Proof-of-Work consensus mechanism, you need to have 51% of the network under your control to gain full control over the network (Laurence, 2019).

The following paragraphs outline the most important attributes of blockchain technology.

The ledger is stored on all nodes in the blockchain, so there is no central point where all the data is saved (Engelhardt, 2017). This leads to the fact that no single person or organization has any kind of authority over the data, which means that blockchain is decentralized.

Different blocks on the blockchain are linked through hashes, as previously mentioned (Engelhardt, 2017). If data in a block were changed, it would lead to the block's hash changing and breaking the blockchain, which would be very easy to detect. Therefore, blockchains are considered immutable.

All verified transactions are contained in the blockchain ledger (Crosby et al., 2016). In addition, this ledger is public which makes it accessible to everyone (Schär & Berentsen, 2020). This allows for traceability of transactions on the blockchain (Sunny et al., 2020).

Privacy is the last major attribute of blockchain technology (Nakamoto, 2008). Another attribute is traceability. At first, traceability and privacy seem to contradict each other. However, privacy can be guaranteed by keeping the displayed addresses (also called public keys) anonymous, revealing the true identities of users only to certain parties that are supposed to have that information.

4.2 Smart Contracts and Oracles

The rise of blockchain technology has opened up the possibility of many applications in companies and markets where centralized systems were traditional leaders (Zheng et al., 2018). Other than storing static data, blockchain technology can be exploited to create decentralized applications (DApps) that often rely on smart contracts. They make DApps transparent, secure, and autonomous. This chapter will explore the theory behind smart contracts and oracles and how they work.

Smart contracts are computer programs running on the blockchain that express conditions to automate the execution of certain agreed-upon contracts (Parizi et al., 2018). In other words, they are self-executing programs stored on the blockchain that automatically enforce the terms of an agreement when certain predefined conditions are met.

The use of smart contracts eliminates the need for intermediaries such as lawyers or banks that can reduce the efficiency of ordinary contracts (Mohanta et al., 2018). What makes smart contracts very attractive as well as practical are their advantageous features, such as transparency and immutability, which are derived from the underlying blockchain technology.

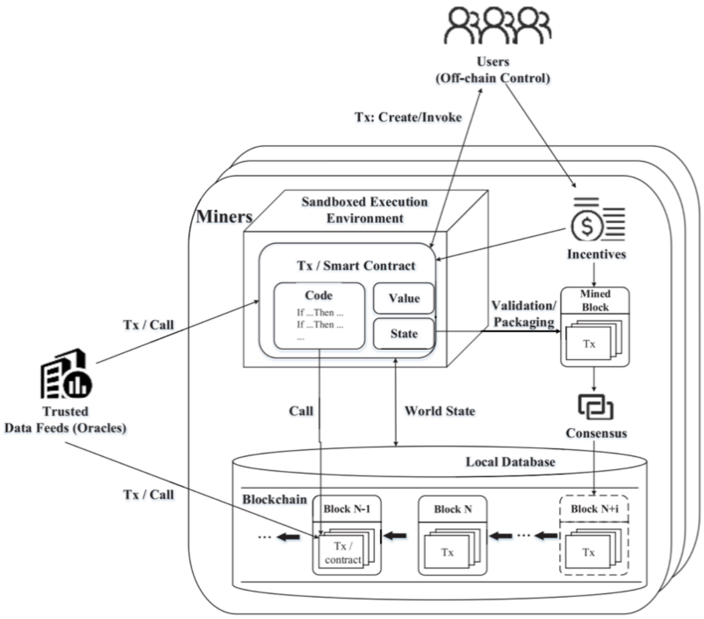
Smart contracts are built using programming languages designed explicitly for blockchain, and they always entail a triggering condition statement, most of the time the “If-Then” statement (Wang et al., 2019). They are agreed upon and signed by all parties and afterwards they are submitted to the blockchain network. After the validation of the miners, smart contracts are securely stored in specific blocks of the blockchain. When the data that triggers the conditions is transmitted to the smart contracts, the response actions are executed and stored in a new block that is added to the blockchain after the whole network reaches consensus.

Although smart contracts entail all the benefits of blockchain technology, they are not limited to decentralized systems (Schär, 2022). The same standard execution environments can be used on centralized ledgers.

On the other hand, while smart contracts are powerful tools for automating agreements, they are limited by the information available on the blockchain (Al-Breiki et al., 2020). Smart contracts cannot access data outside of the blockchain, which limits their ability to execute complex agreements that rely on external information. Oracles are the connection between off-chain information and on-chain smart contracts. An oracle is a trusted third-party service that provides verified external information to a smart contract. Oracles can be centralized, meaning that they are controlled by a single entity, or decentralized, meaning that they are run by a network of nodes (Al-Breiki et al., 2020). They work by receiving data from external sources and verifying the data before sending it to the smart contract, which ensures that the data is accurate and tamper-proof (Beniiche, 2020).

Figure 2

Operational Mechanism of Smart Contracts



Note. From “Blockchain-enabled smart contracts: architecture, applications, and future trends” by S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, & F.-Y. Wang, 2019, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49* (11), p. 2267 (https://doi.org/10.1109/TSMC.2019.2895123). Copyright 2019 by IEEE.

In conclusion, smart contracts could lead to several advantages in the healthcare insurance industry compared to traditional ones (Mohanta et al., 2018). Firstly, smart contracts eliminate the need for intermediaries such as lawyers, brokers, or banks, making the entire process faster and more efficient. Secondly, smart contracts are transparent and public, with all parties being able to view and verify the terms of the contract. The use of smart contracts can reduce the number of disputes and increase trust among parties. Finally, besides being accurate, smart contracts use blockchain technology, which is secure and decentralized, making them less susceptible to fraud, hacking, and other security breaches.

5 Blockchain as a Solution

In this chapter of the report, we demonstrate what solutions and benefits blockchain technology offers insurance companies. It provides an overview of the possible implementations. The aim is to enable insurance companies to weigh up the advantages and the drawbacks of the addressed blockchain benefits for combatting fraudulent claims and to come to an informed conclusion about whether they intend to implement a blockchain solution in the future.

5.1 Benefits of Blockchain-based Solutions

5.1.1 Collaboration through Transparency

The fact that transactions stored on a blockchain are transparent to all involved parties means that patients' healthcare data can be viewed by everyone (Saldamli et al., 2020). This ameliorates collaboration and the sharing of healthcare data between insurance companies, doctors, and other authorized parties. Insurance companies would have better and easier access to medical records and be able to verify patients' claims before agreeing to a settlement. Additionally, reducing the complexity by having a sole source of medical information could avoid fraudulent behavior such as doctor shopping.

However, not only could collaboration between different insurance companies be facilitated, but also that between insurance companies and external actors such as traffic control departments and judicial organs (Liu et al., 2019). In these cases, the external actors would also serve as nodes in the blockchain network. They would record details of accidents and incidents caused by third parties, and write these to the blockchain, making it possible for insurance companies to use this information to counter fraudulent claims pertaining to third-party responsibility.

5.1.2 Trust

Chen et al. (2021) note that storing patient data transparently on the blockchain can be used to create an industry-wide blacklist for individuals who do not act in good faith. Identifying such bad actors would serve as valuable feedback to other parties in the healthcare insurance industry.

5.1.3 Traceability

Zhang et al. (2022) propose a concrete way to implement such a blockchain-based medical data storage and management system using smart contracts for data storage and query. Doctors would digitally sign medical data collected before initiating a transaction to write the data to the blockchain (Zhang et al., 2022). Then, the doctor's hospital would check and digitally sign the medical data again, adding another layer of protection. Signing the data enables the blockchain participants to see who collected which records, thus allowing potential fraud to be traced to its origin. In the last step of the process, the insurance company uses a “diagnosis verification smart contract” to call an external diagnosis verification service through an oracle.

5.1.4 Immutability

Immutability on the blockchain means that any information uploaded to the blockchain by a doctor would not be able to be manipulated (Engelhardt, 2017).

Even by making additional new entries, existing ones can never be removed or altered and stay on-chain forever, leaving an irrefutable and eternal link between a medical record and the individual doctor or hospital responsible for entering it (Novikov et al., 2018). Also, the possibility of false claims is reduced since the increased visibility deters healthcare professionals from engaging in corrupt behavior.

Another way to prevent fraud committed by healthcare providers is to use smart contracts to compare on-chain information about medical treatment procedures to the commonly used medical procedures pertaining to the respective diagnoses (Liu et al., 2019). This would prevent healthcare providers from wishing to commit fraud by pretending to have conducted unnecessary or unconventional medical treatment.

5.1.5 Data Availability

Kapadiya et al. (2022) suggest the use of smart contracts to incentivize insureds to share their personal healthcare data. They propose a system in which insureds give their consent to their data being shared by using a predefined smart contract, a solution made possible through blockchain technology. The smart contract rewards the patient for sharing their data in the form of cryptocurrency. The healthcare data is then stored in a decentralized manner and is ready to be analyzed.

For example, Amponsah et al. (2022) show that one way insurance companies can leverage the vast amounts of data on a blockchain-based application to combat fraud is through the integration of machine learning in smart contracts. They used a decision tree model for the machine learning algorithm. This enabled them to combat various kinds of fraud. They detected fraud at a rate of roughly 98%.

5.1.6 Identity Management

The main concerns in digital identity management are security and privacy (Lamba et al., 2022). Identity management created with blockchain technology is a decentralized and safe solution which allows individuals to have more control over their identity information. Identity theft can be divided into the subtypes of financial, criminal, and synthetic identity theft. In this paper, we focus on medical identity theft. An example would be for an injured person without a legal insurance contract to apply with the identity of an insured who has a valid insurance to gain access to benefits like medical treatments, check-ups by a doctor and operations etc., thus abusing the healthcare insurance system at someone else's expense (Lamba et al., 2022). The vast number of medical records makes it more difficult to have an overview of each record.

According to Lamba et al. (2022), a possible solution to avoid any form of identity fraud would be for insureds to manage their own identity for healthcare insurance. The insureds must check and confirm their identity via a blockchain app for identity management. After creating a profile on the app, the users receive a unique ID number which gives the healthcare providers access to the users' identity paper. As soon as the users get their unique IDs, they must upload them for self-certification. The users are the sole owners of their personal information and insurance data. The app assists the users by making decisions about which data can be shared with the insurance company. Based on how much personal and relevant information users admit to the insurance company, smart contracts can determine a trust score. This lets the healthcare providers better verify the users' identities. This score represents the trustworthiness of users. The higher the score, the more trustworthy the users are. Whenever healthcare providers need access to get specific information about the authentication, the users will be informed via a message. This ensures that only the rightful users are able to gain access to all services of the healthcare insurance contract. Another benefit of blockchain technology is that users can monitor and track how and when their personal data was used in the past. All this helps to combat healthcare insurance fraud caused by identity theft (Lamba et al., 2022).

5.2 Strengths and risks

A possible disadvantage inherent to the use of blockchain solutions for any kind of fraud prevention is the fact that data written to the blockchain cannot be changed (Gatteschi et al., 2018). This characteristic is commonly referred to as immutability. For this reason, it is important to put in place thorough error management systems. However, due to the immutability of blockchain-based solutions, information cannot be modified retrospectively (Alnuaimi et al., 2022). Therefore, blockchain-based solutions are less prone to attacks compared to the current centralized solutions.

Depending on the implementation, another disadvantage of a blockchain-based solution may be the lack of scalability due to limited storage capacity (Alnuaimi et al., 2022). However, Alnuaimi et al. (2022) show in their solutions that this can be remedied by adding an off-chain layer. They use an off-chain memory solution for this purpose, which is called InterPlanetary File System (IPFS).

Basically, with a blockchain solution, the patient record, as well as the claims process, are traceable (Alnuaimi et al., 2022). However, due to asymmetric encryption, it is ensured that the information cannot be clearly assigned to a person. It should be noted here that privacy cannot always be maintained when off-chain layers are used (Alnuaimi et al., 2022). However, one approach to ensuring this, even with so-called off-chain layers, such as off-chain storage systems, is to work with various interface application filters (in the context of DApps) and encryption methods. Another way to ensure confidentiality and privacy in smart contract applications is by using the Quorum platform, whereby transactions can only be viewed by selected users (Alnuaimi et al., 2022).

Saldamli et al. (2020) show that a blockchain-based solution is suitable not only because of the prevention of fraud in the healthcare industry but also because this industry involves many different parties (doctors, hospitals, pharmacies, insureds, insurance companies, etc.). In particular, the advantageous features of blockchain-based solutions, which arise from the decentralized structure, would minimize the risks and simultaneously offer new opportunities.

Mackey et al. (2020) show that one of the big challenges which blockchain-based solutions face are the interfaces to the various applications. Thus, the blockchain-based solutions must be compatible with the insurance companies' data storage application as well as the internal billing system of the healthcare provider.

One of the major strengths compared to the current system lies in the more active role of the insureds (Mackey et al., 2020). In the future, they can be part of the claims process based on blockchain technology since they can actively validate certain steps (Mackey et al., 2020). By getting insureds more involved in the validation process, the system will be less fraudulent (Mackey et al., 2020).

Unlike the current system, where often only one party, the insurance company, does the validation, a blockchain-based solution involves multiple parties in the validation process (Mackey et al., 2020). This provides more trust in the system from the perspective of all parties involved.

Another advantage resulting from the implementation of a blockchain-based solution lies in the creation of a solid database for further applications (Mackey et al., 2020). According to them, it might be possible to identify regional patterns or other anomalies that are not necessarily related to the claims process in the future.

6 Discussion

In this section, we summarize our findings and discuss their implications and limitations in a broader context. Furthermore, this section shows the insurance companies whether a blockchain-based solution is superior to current solutions for effectiveness and efficiency reasons.

It turns out that the various blockchain-based solutions are more effective and efficient compared to the current system at combatting fraudulent claims. According to our research this is reflected by the fact that blockchain-based solutions proactively detect fraudulent claims rather than reacting to them. An example of this is the facilitated collaboration between parties noted by Saldamli et al. (2020) who show that broad availability of information makes certain fraudulent claims easier to detect in advance. Saldamli et al. (2020) mention how this can be used to combat doctor shopping, however we suggest that the same logic could be applied to also prevent double billing. We contend that the use of smart contracts to incentivize insureds to share their healthcare data posited by Kapadiya et al. (2022) will increase the amount of distributedly stored medical data and therefore add significant value to blockchain solutions striving to reduce healthcare fraud. Another aspect that illustrates that blockchain-based solutions are more effective and efficient is shown by Mackey et al. (2020). They show that patients are more involved in the verification process of claims and therefore take an active role in verifying the services they were provided with.

Another example would be an industry-wide blacklist as postulated by Chen et al. (2021). It is clear to see how such a blockchain-based, transparent blacklist could detect patients prone to submitting fraudulent claims very efficiently. We argue that this ability to protect insurers pre-emptively would reduce the need for trust between insurance companies and insureds, creating a more trust-less system than is currently in place. This leads to an increase in efficiency, as fewer money has to be spent on the verification of claims.

According to our findings, many types of fraud can be successfully eliminated by using blockchain-based solutions. This is especially true for double billing, phantom billing, identity fraud and doctor shopping. For example, we argue that the comparison of on-chain information about medical procedures with commonly used real-world procedures described by Liu et al. (2019) could significantly reduce the frequency of phantom billing. However, certain types of fraud might not be addressed thoroughly by implementing a blockchain-based solution, such as particular types of kickback schemes. As shown in chapter 5, the current blockchain-based solutions focus on combatting specific types of fraud, which is why not all types of fraud are usually addressed to the same extent.

Although the advantages clearly outweigh the disadvantages, we assume that the implementation of blockchain-based solutions will not take place in the near future. Many different providers as well as the many insurance companies must first create an interface to their own software applications. Experience shows that this can be a very long and complicated process. According to our literature review, there are no meaningful analyses on the implementation costs of blockchain-based solutions. However, we estimate that the cost savings brought about by blockchain-based solutions will exceed the implementation costs, especially in large healthcare markets such as the US. However, it is questionable whether this is also true for smaller healthcare markets such as Switzerland. The healthcare industry is very country-specific, since each country has its own legislation and regulation concerning insurance. Based thereon, in our opinion, only in very rare cases are blockchain-based solutions transferable without modification. For this reason, any blockchain-based solution must be tailored to the specific country.

Blockchain-based solutions are also attractive from a broader economic perspective. This is because they eliminate many administrative tasks, such as the tedious checking of invoices. This increase in efficiency should therefore lead to smaller premiums.

Overall, we can establish that blockchain-based solutions are both more effective and more efficient. The implementation costs thereof have not been analyzed yet. However, according to our analysis, it can still be stated that with a fraudulent claims volume of several billion US dollars (depending on the size of the country-specific market), even a very small increase in efficiency and effectiveness can save an enormous amount of money. Therefore, we have come to the conclusion that the advantages outweigh the disadvantages in the long term.

7 Conclusion

In conclusion, the issue of fraudulent claims in the healthcare insurance industry has been a significant problem for both insurance companies and policyholders for many years. However, the emergence of blockchain technology and smart contracts provides a viable solution to this problem.

Smart contract usage in the healthcare insurance sector could significantly reduce costs and time currently spent on avoiding or reducing fraudulent claims (Novikov et al., 2018). They are built on-chain which enables the creation of a secure, transparent, and tamper-proof ledger that ensures data integrity, immutability, and confidentiality. Smart contracts can facilitate automated claims processing and reduce the need for intermediaries, resulting in faster and more accurate claim settlements. This eliminates the need for manual interventions, reduces the risk of errors and fraud, and speeds up the claims settlement process (Hewa et al., 2021). Overall, smart contracts enhance the efficiency and accuracy of the claims process.

The uncertain implementation costs of blockchain-based solutions and the uncertain costs due to organizational changes needed within the companies represent an issue. This pressing matter needs to be further investigated to determine how high the efficiency gains are.

In conclusion, this technology has the potential to reduce fraudulent claims, improve claims processing times, and enhance customer satisfaction. However, as the technology continues to evolve, it will slowly gain acceptance in the healthcare insurance industry, benefiting all stakeholders involved.

8 References

Agrawal, S., Tarzy, B., Hunt, L., Taitsman, J., & Budetti, P. (2013). Expanding Physician Education in Health Care Fraud and Program Integrity. *Academic Medicine*, *88*(8), 1081-1087. https://doi.org/10.1097/acm.0b013e318299f5cf

Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access*, *8*, 85675-85685. https://doi.org/10.1109/ACCESS.2020.2992698

Alhasan, B., Qatawneh, M., & Almobaideen, W. (2021). Blockchain Technology for Preventing Counterfeit in Healthcare insurance. *International Conference in Information Technology*. https://doi.org/10.1109/icit52682.2021.9491664

Alnuaimi, A., Alshehhi, A., Salah, K., Jayaraman, R., Omar, I. A., & Battah, A. (2022). Blockchain-Based Processing of Healthcare insurance Claims for Prescription Drugs. *IEEE Access, 10*, 118093-118107. https://doi.org/10.1109/ACCESS.2022.3219837

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, 4, 100122.* https://doi.org/10.1016/j.dajour.2022.100122

Beniiche, A. (2020). A study of blockchain oracles. *ArXiv, 2004.07140v2*. https://doi.org/10.48550/arXiv.2004.07140

Cady, R. F. (2007). Healthcare Fraud. *JONA's Healthcare Law, Ethics, and Regulation*, *9*(2), 54-61. https://doi.org/10.1097/01.nhl.0000277202.16864.aa

Chen, C. L., Deng, Y. Y., Tsaur, W. J., Li, C. T., Lee, C. C., & Wu, C. M. (2021). A Traceable Online Insurance Claims System Based on Blockchain and Smart Contract Technology. *Sustainability*, *13*(16), 9386. https://doi.org/10.3390/su13169386

Chu, V. & U.S. Attorney's Office, Southern District of California. (2020, September 30). National Health Care Fraud and Opioid Takedown Results in Charges Against 345 Defendants Responsible for More Than $6 Billion in Alleged Fraud Losses. *San Diego Defendants Charged [Press release]*. https://www.justice.gov/usao-sdca/pr/national-health-care-fraud-and-opioid-takedown-results-charges-against-345-defendants

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *71* (2), 6-10. https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review*, *7*(10), 22-34. https://timreview.ca/article/1111

FBI. (2016, June 27). *Financial Crimes Report 2007*. https://www.fbi.gov/stats-services/publications/fcs_report2007/

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaria, V. (2018). *Future Internet, 10*(2), 20. https://doi.org/10.3390/fi10020020

Goundar, S., Prakash, S., Sadal, P., & Bhardwaj, A. (2020). Healthcare insurance Claim Prediction Using Artificial Neural Networks. *International Journal of System Dynamics Applications*, *9*(3), 40–57. https://doi.org/10.4018/ijsda.2020070103

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *177*, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. *IEEE Access*, *10*, 79606–79627. https://doi.org/10.1109/access.2022.3194569

Kareem, S. L., Ahmad, R., & Sarlan, A. (2017). Framework for the identification of fraudulent healthcare insurance claims using association rule mining. *2017 IEEE Conference on Big Data and Analytics (ICBDA)*. https://doi.org/10.1109/icbdaa.2017.8284114

Kirlidog, M., & Asuk, C. (2012). A Fraud Detection Approach with Data Mining in Health Insurance. *Procedia - Social and Behavioral Sciences*, *62*, 989–994. https://doi.org/10.1016/j.sbspro.2012.09.168

Lamba, S., Singh, M., & Kapoor, A. (2022). Use of Blockchain to prevent identity theft. *International Research Journal of Modernization in Engineering Technology and Science, 4*(4),1362–1367. https://www.irjmets.com/uploadedfiles/paper/issue_4_april_2022/21248/final/fin_irjmets1650966793.pdf

Laurence, T. (2019). *Introduction to Blockchain Technology: The many faces of blockchain technology in the 21st century*. Van Haren Publishing.

Li, J., Huang, K. Y., Jin, J., & Shi, J. (2008). A survey on statistical methods for health care fraud detection. *Health Care Management Science*, *11*(3), 275–287. https://doi.org/10.1007/s10729-007-9045-4

Lipovyanov, P. (2019). *Blockchain for Business 2019: A user-friendly introduction to blockchain technology and its business applications*. Packt Publishing.

Liu, Q. (2013). Healthcare fraud detection: A survey and a clustering model incorporating Geolocation information. 29th WORLD CONTINUOUS AUDITING AND REPORTING SYMPOSIUM (29WCARS). http://raw.rutgers.edu/docs/wcars/29wcars/Health%20care%20fraud%20detection%20A%20survey%20and%20a%20clustering%20model%20incorporating%20Geo-location%20information.pdf

Liu, W., Yu, Q., Li, Z., Li, Z., Su, Y., & Zhou, J. (2019). A Blockchain-Based System for Anti-Fraud of Healthcare Insurance. *2019 IEEE 5th International Conference on Computer and Communications (ICCC),* 1264-1268. https://doi.org/10.1109/iccc47050.2019.9064274

Lu, J., Fung, B. C. M., & Cheung, W. K. (2020). Embedding for Anomaly Detection on Healthcare insurance Claims. *2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA)*. https://doi.org/10.1109/dsaa49011.2020.00060

Mackey, T. K., Miyachi, K., Fung, D., Qian, S., & Short, J. (2020). Combating Health Care Fraud and Abuse: Conceptualization and Prototyping Study of a Blockchain Antifraud Framework. *Journal of Medical Internet Research, 22*(9), e18623. https://doi.org/10.2196/18623

Margret, J., & Sreenivasan, S. (2013). Implementation of Data Mining in Medical Fraud Detection. *International Journal of Computer Applications*, *69*(5), 1–4. https://doi.org/10.5120/11835-7556

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1-4. https://doi.org/10.1109/ICCCNT.2018.8494045

Morris, L. (2009). Combating Fraud In Health Care: An Essential Component Of Any Cost Containment Strategy. *Health Affairs*, *28*(5), 1351–1356. https://doi.org/10.1377/hlthaff.28.5.1351

Nakamoto, S. (2008, October 31). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Bitcoin.org. https://bitcoin.org/bitcoin.pdf

Novikov, S. P., Kazakov, O. D., Kulagina, N. A., & Azarenko, N. Y. (2018). Blockchain and Smart Contracts in a Decentralized Health Infrastructure. *2018 IEEE International Conference - Quality Management, Transport and Information Security, Information Technologies*, 697-703. https://doi.org/10.1109/itmqis.2018.8524970

Ogaboh, A., & Osuchukwu, U. (2010). National Healthcare insurance Scheme (NHIS) and Employees' Access to Healthcare Services in Cross River State, Nigeria. *Global Journal of Human-Social Science*, *10*(7), 9-16. https://socialscienceresearch.org/index.php/GJHSS/article/ view/100046/101

Parizi, R. M., Singh, A., & Dehghantanha, A. (2018). Smart Contract Programming Languages on Blockchains: An Empirical Evaluation of Usability and Security. *Blockhain – ICBC 2018, 10974.* https://doi.org/10.1007/978-3-319-94478-4_6

Plomp, M., & Grijpink, J. (2011). Combating Identity Fraud in the Public Domain: Information Strategies for Healthcare and Criminal Justice. *The Proceedings of the 11th European Conference on e-Government*, 451-458. https://books.google.ch/books?id=cIkxJXGyhv8C&pg=PA451&lpg=PA451&dq=Combating+Identity+Fraud+in+the+Public+Domain:+Information+Strategies+for+Healthcare+and+Criminal+Justice.+The+Proceedings+of+the+11th+European+Conference+on+e-Government&source=bl&ots=Rh1b6HqhAS&sig=ACfU3U1VVkaXJ6S0UWQhOe1lrpYg24YBvA&hl=de&sa=X&ved=2ahUKEwim7cmN2N79AhVv7rsIHemDagQ6AF6BAgeEAM#v=onepage&q=Combating%20Identity%20Fraud%20in%20the%20Public%20Domain%3A%20Information%20Strategies%20for%20Healthcare%20and%20Criminal%20Justice.%20The%20Proceedings%20of%20the%2011th%20European%20Conference%20on%20e-Government&f=false

Rabecs, R. N. (2006). Health Care Fraud Under the New Medicare Part D Prescription Drug Program. *Journal of Criminal Law & Criminology*, *96*(2), 727–756. https://dialnet.unirioja.es/servlet/articulo?codigo=2245119

Rashidian, A., Joudaki, H., & Vian, T. (2012). No Evidence of the Effect of the Interventions to Combat Health Care Fraud and Abuse: A Systematic Review of Literature. *PLOS ONE*, *7*(8), e41988. https://doi.org/10.1371/journal.pone.0041988

Rawte, V., & Anuradha, G. (2015). Fraud detection in health insurance using data mining techniques. *International Conference on Communication, Information & Computing Technology*, *4*(1), 404-412. https://doi.org/10.1109/iccict.2015.7045689

Saldamli, G., 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)*, 145-152. https://doi.org/10.1109/sds49854.2020.9143900

Schär, F., & Berentsen, A. (2020). *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction*. MIT Press.

Schär, F. (2022). DeFi's Promise and Pitfalls. *Finance and Development (IMF)*, *59*(3), 33-35. https://www.imf.org/en/Publications/fandd/issues/2022/09/Defi-promise-and-pitfalls-Fabian-Schar

Sunny, J., Undralla, N., & Madhusudanan Pillai, V. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Computers & Industrial Engineering*, *150*, 106895. https://doi.org/10.1016/j.cie.2020.106895

Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015). Categorizing and Describing the Types of Fraud in Healthcare. *Procedia Computer Science*, *64*, 713–720. https://doi.org/10.1016/j.procs.2015.08.594

United Healthcare Student Resources (n.d.). *Healthcare insurance 101*. Retrieved March 3, 2023, from https://www.uhcsr.com/insurance101

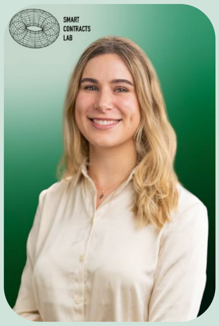
Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277. https://doi.org/10.1109/TSMC.2019.2895123

Zhang, C., Wu, C., & Wang, X. (2020). Overview of Blockchain Consensus Mechanism. *Proceedings of the 2020 2nd International Conference on Big Data Engineering,* 7-12. https://doi.org/10.1145/3404512.3404522

Zhang, G., Zhang, X., Bilal, M., Dou, W., Xu, X., & Rodrigues, J. J. (2022). Identifying fraud in medical insurance based on blockchain and deep learning. *Future Generation Computer Systems*, *130*, 140–154. https://doi.org/10.1016/j.future.2021.12.006

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352-375. https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf

Authors



Cendrine Wagner

Marco Pecoraro

Oliver Erni

Gavaskar Parameswaran

Valentin Leuthard

Liam Kane

SMART
CONTRACTS
LAB