Journal of Mathematics and Modeling in Finance (JMMF)
Vol. 4, No. 2, Summer & Autumn 2024
Research paper

Fraud detection in supplementary health insurance based on smart contract in blockchain network

Abbas Raad[1], **Reza Ofoghi**[2], **Ghadir Mahdavi**[3]

[1] ECO College of Insurance, Allameh Tabataba'i University, Tehran, Iran
a-raad@sbu.ac.ir

[2] ECO Collage of Insurance, Allameh Tabataba'i University, Tehran, Iran
r.ofoghi@yahoo.com

[3] ECO college of Insurance, Allameh Tabataba'i University, Tehran, Iran
mahdavi@atu.ac.ir

Abstract:
This study aims to examine the function of blockchain technology to detect fraud in health insurance. we consider the literature on fraud in health insurance, blockchain, and smart contracts to to test a newly structured software system based on blockchain technology for this purpose. Different blockchain platforms, consensus algorithms, and structures have been used to pick the proposed system's best structure based on blockchain. Eventually, the best techniques to put the system to the test and evaluate the findings were assessed. we propose a standardized system, where blockchain is applied to store data and smart contracts are used to automate insurance policies. Furthermore, a web-based application, which acts as core insurance software, is proposed for all stakeholders to communicate with the blockchain and smart contracts. Therefore, the proposed system comprises a blockchain, web app, and standardized smart contracts. The proposed system mainly focuses on fraud detection in insurance claims while maintaining a standard data storage and transfer structure. The system proved to be thriving once claim data can be created, read, and analyzed (i.e. fraudulent data are caught) effectively in a standard way. The web app consists of a front-end and back-end section. The front-end enables users to interact with the proposed system, and the back-end allows the insurance company to store records on the blockchain and increase the chances of detecting fraud in insurance claims, especially Digital Insurance Claims. Finally, a blockchain-based web application that can be used as core insurance software for any health insurance company is proposed.

Keywords: Health Insurance, Fraud Detection, Blockchain Technology, Smart Contract.
Classification: 00-XX, 00-01, 00-02, 00AXX, 00BXX

[2] Corresponding author

Received: 08/06/2024 Accepted: 05/10/2024
https://doi.org/10.22054/JMMF.2024.79731.1136

1 Introduction

In the recent technological era, several latest technologies are emerging in different sectors of the global economies. Therefore, blockchain technology is one of the top leading emerging technologies widely used in institutions. The insurance industry as one of the important parts of the financial industry needs this technology seriously. The insurance industry has big data, which needs to be analyzed to deliver high-quality services to clients and to manage this industry effectively. Health insurance is one of the key fields in insurance because of offering the pace and financial help to the people. Insurance companies like AXA and Generali have started investing in blockchain applications. Allianz has recently announced its successful pilot of a blockchain-based smart contract solution to automate catastrophe swap transactions. A critical lever for improving customer engagement through blockchain lies in the area of personal data. Customers fears about losing control of personal data as soon as it is handed over to a company and their frustration with the need to repeat data entry processes can be addressed by a customer-controlled blockchain for identity verification (see KYC use case) or medical/health data. Personal data does not need to be stored on the blockchain; it remains on the users device. Only its verification, e.g., through a doctor, and related transactions (e.g., an examination that has taken place on a specific date) are registered in the blockchain. Here, scale is critical to reaping the benefits of blockchain as it requires a sufficient number of parties involved to reuse the verified data.

Health insurance fraud is complex, as multiple parties can initiate it, including the beneficiary, the provider, or any intermediaries. Furthermore, the nature and structure of health insurance claims are quite different. For example, various medical services may be provided at each medical appointment and are likely to be filed separately. Due to a lack of data, this situation makes healthcare fraud investigations unique and limited.

According to the National Health Care Anti-Fraud Association (NHCAA) report in 2023, [1] healthcare costs the United States over $4260 billion (16 percent of the GDP) yearly, while hundreds of billions of dollars are lost due to health insurance frauds. So, we can summarize the consequences of fraud in Health Insurance as below:

- Increase in the cost of the companies
- inflated premium
- threatening the viability of the insurance companies
- An adverse effect on the profit the company make
  For fighting against fraud, we need blockchain technology because:
- Healthcare data and cyber-attacks

Because of complexities of defining fraudulent behavior and detecting fraudulent cases, measuring fraud losses in health care is difficult. According to existing literature undetected frauds remain a problem; in many individual cases, it may not be possible to determine whether a claim is fraudulent or not. Still, it has been estimated that three to ten per cent of health care spending is lost to health care fraud and abuse, amounting to billions of dollars per year [2]. In Iranian insurance industry according to experts opinion 20 to 30 percent of health insurance is fraud. Last year (2023) total loss payed by insurance industry to insued was 160 thousand billion Toman which is a huge amount of money.

Health insurance fraud is complicated, as it can be initiated by multiple parties, including the beneficiary, the provider, and/or any intermediaries. Furthermore, the nature and structure of health insurance claims are quite different. For example, at each medical appointment, various medical services may be provided and are likely to be filed separately. Due to a lack of data, this situation makes healthcare fraud investigations unique and limited. Having a central authority over a database containing healthcare data can be a major security threat.

2 Litrature Review

We develop a taxonomy of frauds in health insurance based on various fraud scenarios and create relationships between insurance claim contents and associated fraud categories. These senarios are based on literature [3] and expert opinions. This paper has 17 scenarios in 9 categories (some categories have more than one scenario) which are showed at table1. It consists of these participants: Head Medical Insurance Company (HMIC); Branch Medical Insurance Company (BMIC); Patients; Hospitals; Allied Health Professionals; Pharmacists; Pharmaceutical Companies; Medical Equipment Suppliers;Diagnostic Centers.

Category	Scenario	Fraudster	Other entities involved in the claim
C1 = Pinging the system	S1=Referring to a patient within the same healthcare organization for laboratory tests, medications, and pharmacy	Healthcare Provider	Patient
C2 = Waiving co-payments	S2=Routinely waiving patients co-payments and overbilling the health insurance provider. Patient co-payment is a fixed amount paid by the patient to the healthcare provider as defined by the health insurance policy.	Doctor	Patient
C3 = Managed care	S3= Denial of service, substandard care, and creation of administrative obstacles for patients by the managed care organization	Managed care organization	Patient
	S4= Charging for a more expensive service, such as a visit to a specialist, when the patient saw a nurse or an intern.		
	S5=Billing for professional services rendered by personnel lacking appropriate credentials		
	S6= Using insurance for a service that fails to meet coverage requirements		
C4 = Self-referral	S7= A doctor refers the patients to clinics, healthcare organizations, hospitals, or pharmacists with which the referring doctor/ physician has a financial relationship	Doctor	Patient
C5 = Doctor shopping	S8= An addicted individual is visiting multiple healthcare providers to buy unprescribed medical drugs	Patient and Doctor	Doctor
C6 = Identity theft	S9=Obtaining and using another persons health insurance card or identification, by theft or deception, to obtain health care or other services or to impersonate that individual	Patient	Doctor
C7 = Prescriptions = S10,S11	S10= Patients have falsely stated that they have lost their prescriptions and obtained duplicates	Patient	Doctor
	S11= Patients claim exemption from prescription charges when they are not, in fact exempt		
C8 = Commission based = S6, S7, S8	S12=Referring patients to specific hospitals, clinics, pharmacists, medicines, or equipment to get a commission	Healthcare Provider	Patient
	S13=providing specific brands of medicines to get a commission from the pharmaceutical company	Pharmaceutical and Pharmacists	Patient
	S14=A pharmaceutical company provides incentives to doctors to promote unapproved or off-label drugs	Pharmaceutical and Doctor	Patient
C9 = Billing Manipulation = S9, S10, S11, S12	S15=Manipulation of diagnosis in the claims without the knowledge of the patients	Doctor	Patient
	S16=Providing unwanted care to the patients, increasing service hours in the bills, duplicate claims, phantom billing, or replacing codes of diseases with one more price	Healthcare Providers	Patient
	S17=Increasing the price of medical equipment for patients whose insurance covers equipment costs or claiming for expensive equipment while providing the ones with less expense	Medical Equipment Provider	Patient

Table 2: The fraud scenarios and their categories in health insurance

For many years, trust and privacy had a vital role in commerce. Duo to this matter, a third party such as banks, governments or any other central authority has always been introduced. Brokers and claim agents as a part of classic process of health insurance claims led to some problem like decrease in speed, increase in cost vulnerability to attacks and sometimes even fraud. Replacing the classic process of health insurance claims with the automated blockchain process, will be result in improve the process and eleminite the role of intermediaries. Many fraudulent claims might end up successfully without insurance companies notice them as frauds so to suatain the system, we needs the collaboration of all parties such as: doctors, health care centers, brokers, insurers, reinsurers. Faced with these challenges, IBM [4] puts forward blockchain technology as a solution which was first introduced in the insurance sector in 2016. Some of the advantages of blockchain in the health insurance domain are as below:

(i) Accessibility and interoperability;

(ii) Automated helthcare insurance claims;

(iii) Faster process and reduced cost;

(iv) Privacy-assured health insurance.

(v) Combat the health care fraud and abuse

Blockchain has the versatility of transporting smart contracts, which are receiving great attention in new business applications and the scientific community, because they allow untrusted parties to manifest contract terms in program code and thus eliminate the need for a trusted third party. The health insurance claim process uses smart contracts to automate the claim process. When the patient is diagnosed with some health issue and the insurance policy covers that issue, and patient visits any doctor or some other healthcare provider, the doctor or the healthcare provider updates the medical record of the patient which is stored on the blockchain. If the insurance policy bought by the patient covers any issue in the diagnostic report, then this acts as a trigger for the event in the smart contract [4]. Smart contracts take transaction as a input, executes the corresponding code and triggers the output events. They have interfaces to handle input from contract participants. Because they run on the blockchain, smart contracts run exactly as programmed, without any possibility of censorship, downtime, fraud or third party interference [5, 6].

Fraud in health insurance system is widespread and very costly. Manual detection of frauds in the healthcare industries would be a tough going work. Health insurance fraud is committed through insurance companies, service providers, and insurance subscribers. Consequently, financial industries are forced to continually improve their fraud detection system [7]. Blockchain technology minimize fraud in health insurance by using smart contracts through the client information, premium collection and detailed analysis of data collected to identify the fake claims. A fraud can happen in any phase of an insurance life cycle [8] for example, Individuals applying for insurance; Policyholders; Third-party claimants; Professionals who provide services to claimants.

Trust in the health care claims system could be significantly improved by automating the execution of rule-based logic through smart contracts. For example, a specific action can be automatically invoked if a patient disputes a health care claim in our system, whereas current systems require detection and auditing of fraud mostly retrospectively [9].

There is a large variety of application domains in a specific blockchain using smart contract, so it may not be able to meet the requirements for all use scenarios. Therefore, choosing the proper blockchain platform to execute smart contracts in a business context is a strategic decision. Each platform has its own features that makes it more or less suitable to be used for particular application. There are three architectures for blochchain as below:

(i) Single-Ledger-Based Architecture

(ii) Multi-Ledger-Based Architecture

(iii) Interoperability-Based Architecture

A classification of these three architecture based on their characteristics presented in [9]. Based on their study the single-ledger-based is sutable for this research. They indicated that this architecture is reasonable for healthcare system.

In healthcare domains which the transactions (images and laboratory results) are big in size, the blockchain network reduces the number of transactions in a block, so that the throughput issue is a problem for the blockchain architecture.

The solution for that chalange is to use credits platform to compress the transactions. Also in healthcare domains which ledger should be replicated among most of the network entity, the scalability is another issue because of heavy computation and communication. Lightweight blockchain architecture as in [10] is the solution. This architecture divides the network participants into clusters and selects a cluster head(s) for each cluster. The ledger can only be replicated on the cluster heads which are selected either based on voting or on the number of incident edges from a node [11]. The remaining participants can query the ledger to get the transactions information.

To build blockchain within a trusted healthcare domain, single-ledger-based blockchain architecture for a private network can be used. Private network has fewer encryption/decryption operations than the public one because of its defined access control to the blockchain. The proper benefit of hybrid architecure is less encryption/decryption operations than public and private architectures (which store all the transactions data in the ledger) becuase only the transaction hash are stord in node in hybride arctecture. healthcare, research, real estate, social networking, and retail industry, can be some examples of this architecture. The multi-ledger-based blockchain architecture for a private network divides the blockchain network into channels to enable private transactions between the members of a channel. This architecture can be used in applications domains that require confidentiality of data while several collaborating organizations such as health insurance and hospitals are involved [12].

According to above statement, healthcare application can be built in private and hybrid type of network in single-ledger-based architecture and multi-ledger-based architecture.

A framework with a set of quality attributes have been proposed in [13] to define identify the expected comparing blockchain platforms for smart contracts peculiarities of a blockchain platform and to highlight objective differences among different platforms. Regard to the attributes, decision maker can select the platform based on perceived quality (product), and attractiveness of it in the specific business context.

Based on the framework which introduced in [13] and chractristics of health insurance which is discussed and fraud detection context, the most sutable platform will be hyperledger fabric and it is supported in the literature.

Some senarios for health insurance claims frauds presented in [14]. They proposed a framework for healthcare fraud detection based on smart contract in blockchain. They used Practical Byzantine Fault Tolerance (PBFT) consensus mechanism and NS3 as a simulator to form the blockchain network. In this paper we use more senarios and real blockchain. A framework for fraud detection in health insurance in blockchain technology proposed in [15]. Patient acts as a validator and only one frauds scenario is contained. It uses ethereum platform and proof-of-authority (POA) consensus mechanism. They used 3 layes in their work: front-end user interface framework, a back-end processing server, and a blockchain network. Two frauds scenario are included in [16]. By defining a set of rules, the misleading information is removed. They used MVC arcitecher, BigchainDB and Neo4J (Graph Database) for creating distributed database, Python flask framework as bakend and React.js and Redux as frontend on blockchain. They used EDI validator to verify if the data follow National Health Care Anti-Fraud Association (HIPPA) guidelines. The model supported with web application. They didn use smart contract. Selecting the databases for HIPPA validation is a problem in this work. A blockchain system with five layers predented in [17]: cloud platform layer, network layer, core layer, interface layer and application layer. Three blockchains each with different organization nodes, designed to provide different services based on three types of frauds, fraudulent data, concealing third-party liability accident fraud, false electronic bill reimbursement. These three blochchain are relevant, so it need cross-blockchain solution to help interat among them and to enables the health insurance agency to obtain necessary information. In the system architecture, smart contract include multi-channel service by which cross-chain can be achieved. Offering a blochchan for any fraud make problem particulary when the number of fraud increses. It propsed to use hyperledger in future works to build the intended system. To mitigate health insurance fraud, in [18] researchers enable (Transport layer security-non repudiation)TLS-N in conversation between insurance company, policy holder and medical institution. They used smart contract in TLS-N to reckons the Merkle tree and recreate the hash chain and verifies the signature. Two adversary models are considered as below:

- The pationed getting his/her claim settled by manipulated documents.
- Insurance company manipulation the proof to reject genuine claim.

A model with four layers presented in [19]. Firstly, P2P mining pool layer for consensus mechanisem. Secondly, blockchain layer where nested transaction blocks are included. Thirdly, a smart contract layer for detecting feauds. It used seven smart contracts for authorization rules and authentication, data access audit logs, health insurance fraud cases, health insurance fraud patterns, personal healthcare record, personal policy and personal claim. Fourthly, a user layer for represents the five final entities such as patient, insurer, healthcare service provider, healthcare supplies provider and anti-fraud decentralized service. Trust on some entities such as doctors in this paper which may lead to fraud activity is not the case. Manipulated medical prescriptionsand fake certificates to a billing for services not provided or overused. A blockchain and smart contract presented in [18] to detect fraud in vehicle insurance sector. They presented the most common types of fraud senarios: Ditching, Cash for Crash and Double Dipping, which they considered the last one in blochchain. Their prototype of blockchain has been developed using the ethereum technologies. it offers three smart contract for main functionalities. These functionalities are creation and termination of insurance policies, creation of Claims and record of the life of a vehicle. Some frauds related to doctore shopping and false certification of medical necessity were described but did not cover a spectrum of scenarios along with a classification.

The machine learning approaches require a medical insurance claims dataset to train the learning models for fraud detection. This leads to security and privacy concerns as the dataset might expose patients identities to attackers. Consequently, in this research, we focus on blockchain technology to detect fraud in the health insurance sector. So now we focus on literature that is done for fraud detection using blockchain technology. A blockchain system with five layers proposed by [17]:

cloud platform layer, network layer, core layer, interface layer, and application layer. Three Blockchains, each with different organization nodes, are designed to provide different services based on three types of fraud: fraudulent data, concealing third-party liability accident fraud, and false electronic bill reimbursement. These three Blockchains are relevant, so they need a cross-blockchain solution to help interact among them and to enable the health insurance agency to obtain necessary information. In the system architecture, smart contracts include multi-channel services by which cross-chain can be achieved. Offering a Blockchain for any fraud creates significant problems when the number of frauds increases. It proposed using hyperledgers in future works to build the intended system. Blockchain and smart contracts used in [3] to detect fraud in the vehicle insurance sector. They presented the most common types of fraud scenarios. Ditching, Cash for Crash, and Double Dipping, which they considered the last one in Blockchain. Their blockchain prototype has been developed using Ethereum technologies. It offers three smart contracts for main functionalities. These functionalities are the creation and termination of insurance policies, the creation of claims, and the record of the life of a vehicle. Interventions to combat healthcare fraud and classified the interventions for prevention and detection of fraud and response to fraud has been discussed in [19]. Some frauds related to doctor shopping and false certification of medical necessity were described but did not cover a spectrum of scenarios or a classification. So, based on the literature review, our contribution to this study will be as follows:

- Identifying the different categories and scenarios of fraud in the healthcare sector
- Considering the different platform and consensus algorithms in the literature and selecting the most used one for healthcare fraud detection
- Design the smart contracts based on transactions in the system
- Proposing a framework for fraud detection in the healthcare sector

3 Research Method

A Quantitative Research Method is used to test the proposed system through software models and applications. For this research paper, we evaluated different blockchain platforms, consensus algorithms, and structures to choose the proposed system's best structure. Furthermore, we are going to evaluate the best ways to put the system to the test and assess the findings. We will analyze different methods to simulate the proposed system and choose the closest option for this research paper. The research data will be primary data collected by the author through experience and programming knowledge. This choice is because other research papers have not entered the world of software programming to model/simulate a blockchain-based application, making this research method

the first of its kind. We now introduce hash and hashing function respectively in blockchain terminology. A hash is an encrypted text output, usually in hexadecimal format or hex for short, which cannot be reverse-engineered. A hash is always of fixed length, no matter the input size. Consequently, if we were to hash the text ”hello,” the output hash (using the SHA256 function) will always be:
”2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824”.

Meanwhile, the hash of the text ”Blockchain-based Application in health Insurance Industry” will always be:
”23fdc23761ed4a049465e0ed5d31b83fe0815d1b94d1044dec25f0ccb966d9cc”.

Although the length of input texts is different, as you can notice, the size of both encoded outputs is 64 characters. Hashes cannot be reversed. If you were given a hash output, calculating the input is almost impossible. The only way to figure out the input is by test and trial, which means going through all the possible text combinations, or worse yet, text mixed with other types of data, like numbers, to get the input. Lastly, the resulting hash is always the same for every input data. However, two input data may output the same hash. The main reason behind this is that when data is hashed, part of the data is lost, which makes it impossible to retrieve data from a hash. This mechanism explains why a hash is always of fixed length and why two input data may result in the same hash. A function that defines an algorithm that hashes data is called hashing function. The act of using a hashing function is called ”hashing”. There are a few types of blockchain, such as public, private, hybrid, and consortium. A public blockchain, as the name suggests, is accessible to everyone. Any person who wishes to can copy the blockchain and run a node. On the other hand, a private blockchain is only accessible to a particular group of people and may or may not be publicly viewable. A hybrid blockchain is a mixture of a public and private blockchain. Some parts of the blockchain are general, and some are not. A consortium blockchain is similar to a private blockchain, but multiple groups of people can access the blockchain. For example, if a single company runs a blockchain, it is private since only the company has access to it. Meanwhile, if multiple companies agree to create a blockchain, then the blockchain is a consortium blockchain. Blockchain technology has three main aspects: security, network, and speed. These three aspects make up the concept of blockchain trilemma. This concept states that a blockchain can never reach an optimum level in all three aspects. An optimum-level blockchain is considered to be a blockchain that is a truly decentralized network, completely secure, and extremely fast. A blockchain attempting to reach all these three levels will eventually fail because it has to sacrifice one aspect to reach the optimum level for the other two. As the block difficulty lowers, so does the security since the time it takes to mine a block reduces, giving malicious nodes a chance to either spam the blockchain network or create faulty blocks that benefit them unfairly. A process during which the nodes of a blockchain reach an agreement on the state of the blockchain, even if new transactions or blocks are added to it, is called a consensus algorithm/protocol. This algorithm is vital in distributed networks where reliability between nodes needs to be achieved. The same applies to centralized private networks, but in these types of networks, the algorithm's security is less significant. Many consensus algorithms are being used in the blockchain industry such as POW, POS, DPOS,POC,POA,POET, POAtivity, PBFD, DPBFT, IBFT. An application that runs on the web is called a web-based application or web app for short. A web app has a front-end and a back-end. The app's front-end is the web app components that a user can see and interact with. The back-end consists of the processes behind the scenes on the server side, such as system structure, flow of data, and data storage.

4 Modelling the system

In this paper a standardized system is presented where blockchain is used to store data, and smart contracts are used to automate insurance policies. Also a web-based application (web app) is suggested that acts as Core Insurance Software for all stakeholders to communicate with the blockchain and smart contracts. The Core Insurance System can manage its day-to-day operations. It can be used to track and process policies and claim information, manage administrative operations, and detect fraud. The proposed system consists of a front-end, back-end, and storage system. The blockchain is the primary storage system, and the web app is the front-end and back-end. The web app allows stakeholders to interact with the blockchain, smart contracts, and other data related to them. It acts as a gateway to the rest of the system. The proposed blockchain has a run-time environment that can run smart contracts on the proposed system. Much like the Etherium Virtual Mashine (EVM), this run-time environment enables an insurer to create Digital Insurance Policies with the help of the proposed smart contracts. The proposed smart contracts will act as off-the-shelf programs that are secure, optimized (in terms of speed and energy costs), and private. The web app uses two storage systems: the proposed blockchain and a storage server. The proposed blockchain will store all permanent data, while the storage server will store all temporary data. Notably, the web app is simply a model of the proposed web app. A Digital Insurance Policy (or DIP, coined by the author) is a smart contract that acts as an agreed insurance policy between the insurer and policyholder. Therefore, the proposed smart contracts are general digital insurance policies that will turn into an agreed insurance policy between the parties involved upon deployment to the blockchain. The proposed smart contracts are programmed to include the basic terms of any insurance policy, including coverage, declarations, agreements, exclusions, conditions, endorsements, and third-party involvements. However, unlike a traditional insurance policy, the terms in the proposed smart contract are automated and enforced under the right conditions. For instance, if the policyholder stops paying their premiums, the smart contract will automatically disallow them to make insurance claims. Similarly, if the policyholder has not made insurance claims in a long time, the smart contract will automatically calculate the discounted premium they must pay. The proposed blockchain is a private blockchain with a Proof of Authorized Work (PoAW) consensus algorithm. This consensus algorithm is a mix of the PoA and PoW algorithms. In this algorithm, all the nodes on the blockchain need to be verified by the insurance company running the blockchain. Like the proposed blockchain, the PoA algorithm is exceptionally suited for a centralized blockchain network. The PoA section of the system will allow the insurance company to benefit from high security and scalability, fast transactions, and low energy costs. The PoW section of the system requires verified nodes (specifically miners) to perform a relatively straightforward calculation process to mine a block. The verified validators will then validate the mined block and include it in their copy of the blockchain if it is valid. It is emendable note that each node is randomly chosen as a miner each time a block is mined. Using a centralized blockchain network with verified nodes will ensure the security and confidentiality required in the health insurance industry. Consequently, patients, health professionals, and other entities involved in healthcare will no longer worry about their privacy.

Consider an insured patient visits a health professional in direct contact with a health insurance company. Assuming the insurance company has implemented our proposed system, the health professional sends a request to the insurance company via the proposed web app. The web app forwards the request to the blockchain nodes, in our case, the operators employed by the insurance company. Then, the nodes gather and send the required data to the web app. The web app will then show the data to the trusted health professional for a more accurate medical diagnosis. Lastly, the proposed system holds an up-to-date data record of the blockchain in relational databases that refer to specific topics. This data record is temporary and is created for faster and smoother access to short-term data. The typical of the propsed model is shown at FIGURE 1.

To explain the fraud detection system, we must understand how policyholders create insurance claims in the proposed system. As explained earlier, all interactions with the proposed system are completed via the proposed web app. The web app has many sections (web pages), including the "Claims" section. On this webpage, users can create and sign Digital Insurance Claims. A DIC is simply an insurance claim that has been digitally created, but in our case, a digital insurance claim is incomplete without a digital signature. The proposed system mainly relies on digital signatures for insurance claim validation. In this section, we will assume a scenario where a patient must visit a trusted health professional and purchase pharmaceutical drugs due to a common flu. After logging into the "Claims" section of the web app, the insured patient has to fill out details about their sickness and

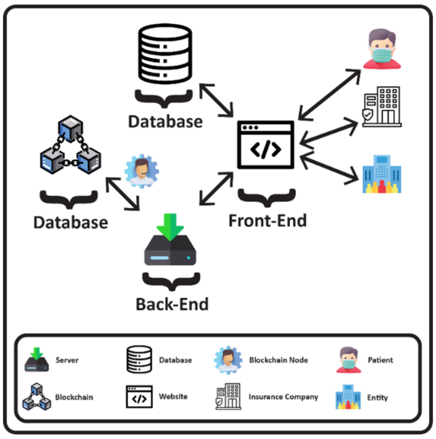


Figure 1: A typical of the proposed model

symptoms. The description of these details has to be thorough. The health professional will now examine the patient and record their diagnosis on the same webpage using their account. After completion, the data filled out on this webpage has to be digitally signed by the patient. Later, the healthcare professional, the entity involved in the healthcare process, has to digitally sign the claim data as well. As a result, two digital signatures are created along with the claim data. The patient will now have to visit a pharmacy to purchase the drugs the health professional prescribes. After providing the prescription drugs, the pharmacy can log onto the web app and add the data to the form. Consequently, the claim data contains information about the patient's symptoms, the health professional's diagnosis, and the pharmacy's prescribed drugs. At this point, the pharmacy must sign the data and give it to the patient. Similarly, the patient has to sign the claim data to confirm the data.We are left with three digital signatures and completed claim data. The patient will send the bundle of claim data (signed claim data along with all the digital signatures) to the insurance company. This claim data bundle is in a text format that is easily typed and read, hence the reason we call them digital insurance claims. The insurance company will begin validating the claim data and looking for possible misrepresentations. This process is much faster in the proposed system since it is mainly automated with the help of smart contracts. When the patient sends the bundle of claim data to the insurance company, the web app forwards the bundle to a smart contract. The smart contract will validate the claim data by recovering the public address of the signer who signed the message using the EC Recover algorithm. If the signers' claim data, digital signatures, or public addresses have been altered in the minor ways possible, then the smart contract will detect this change and flag the claim data as fraud. Otherwise, the smart contract will flag it as truthful and store it on the blockchain for further investigation. Once the insurance company is satisfied with the logic of the claim data, they can either automatically reimburse the patient using cryptocurrency via the smart contract or transfer the amount via regular banking systems. Digital signature verification ensures whether collected data indeed originates from the sender. It creates a barrier for intruders or malicious nodes that plan to generate data on someone else's behalf. It also allows the blockchain nodes to easily track the origin of data if it contains malicious information. In the proposed system, the digital signature verification is processed automatically, removing the need for human interaction and possible human errors. Consequently, reducing claim processing time and increases efficiency.

There are different ways users can interact with the web app, which are categorized as:

(i) Internal interactions

(ii) External interaction

(iii) Trusted external interactions

Internal interactions refer to any interactions performed by a trusted party that works for the Insurance Company. This party may use the system to execute core policy management and processing such as rating, quoting, issuance, endorsements, and renewals. It may be noteworthy to mention that although the insurance company trusts this party, it is still necessary for them to own an asymmetric key and interact with the app through that key. The proposed system is fault tolerant (i.e., if the trusted parties acted maliciously for any particular reason, the system would not crash or fail). As a result, even trusted parties require asymmetric keys to sign any data they create. This system ensures trust even within the Insurance Company since one trusted party (for ex., an employee) cannot generate and sign data on behalf of other trusted parties.

External interactions refer to any interactions performed by an untrusted party, i.e., a person or entity that is a stakeholder of the Insurance Company but does not work for them, such as a policyholder or a hospital in contract with the Insurance Company. These entities will have different access rights in the proposed web app. For example, the policyholder will have access to digital insurance policies, and the hospital will have access to further patients' health records. However, these entities will not have access to other parts of the system that are unrelated to them. All these access rights are managed by the proposed web app that the administrators of the Insurance Company control. Trusted external interactions refer to interactions performed by trusted parties that do not directly work for the Insurance Company, such as individual claim adjusters and insurance underwriters. These entities will have limited access to the web app, such as being able to post images related to a claim.

In the proposed system, the insurance company's administrators have complete control over not only the blockchain and blockchain nodes but also the access controls of different system users. They can decide every entity's access controls through the web app. When users log in to their account, the web app processes the relatable web page and delivers it to the user. The user's information is then stored on the webpage so that the user will not need to sign in again. If the user is an internal employee, such as an admin, the webpage will show all the options that allow them to interact internally. If an admin logs in, they will have a few more options, such as generating a key for an employee or any other entity. This webpage allows the admin to create an identity for a new user. After sending the request, the web app will forward the request from the front-end to the back-end of the web app using the fetch API in JS. The request is received through the addUser port via the express JS app. The request is then processed in the app to ensure authenticity to fulfill the request. In this case, the user interacting with the app should be a valid admin. In the web app, authenticity is ensured through usernames and passwords. After authentication, the app generates an asymmetric key using the 'crypto' library available in Node JS. This library allows us to generate asymmetric keys using the 'secp224r1' Elliptic Curve Cryptography that is highly similar to the curves used by the Bitcoin and Ethereum blockchains. After generating a private and public key, similar to how Ethereum operates, an 'address' key is also generated by hashing the public key. I.e., the public key (in its hex form) is hashed using the SHA256 hashing algorithm to generate a hash, which is used as an address key. This address key is then used to identify users in the network, hence used as a username. The generated keys will then be stored in a JSON file, assuming the key does not exist or an error did not occur while generating asymmetric keys. After storing the keys, the app will check whether the new user is an admin. If the user is an admin, the login data will be stored in the admin folder of the app's local database. Otherwise, another relatable folder will be chosen.

The web app will later use these files and directories to authenticate users through the login port. This port forwards the request body (which contains the username and password of the user) to the 'isValidEmployee' and 'isValidAdmin' functions that compare the request information with the data in the directories mentioned above. Once the user information is validated, the app will send the results to the front-end. At this point, the user has logged in to their account, and the web app presents the relevant screen to them. The user can view different records (based on their control access) but is unable to update records. I.e., the user cannot create transactions on the blockchain. The main reason is that the user does not have the key to sign transactions. To retrieve the key, the user must send a request to the web app through the 'getKey' port. It is noteworthy to mention that in implementing this web app, the port currently retrieves the key from the directories mentioned before. In contrast, in the proposed web app, the user is responsible for maintaining the keys locally for more security. As a result, the keys are not stored in the proposed web app. Moreover, when the keys are generated, they are securely presented to the new users via cryptographic encryption. In the web app, after sending a request through the 'getKey' port, the app will return the requested keys, assuming the user has correctly logged in to their account. Once the key has been successfully retrieved, the user can create transactions. Transactions may include creating a DIP, interacting with an existing DIP, creating a DIC, etc. Every user must maintain a key to create transactions and have them in the blockchain. The transactions cannot be signed without a key, and unsigned transactions will never be included in the blockchain. In addition, the miner and validator nodes of the blockchain validate signed transactions before including them on a block. Consequently, if a transaction has been signed using randomly generated or invalid keys, the nodes will alarm the network, and the transaction will never be finalized. In the proposed web app, the users sign a transaction locally and then send it to the web app. After sending the request, the app validates the user through the 'isValidAdmin' and 'isValidEmployee' functions. Assuming the user is authentic, the web app will then create a transaction using the data signed by the user and their key.

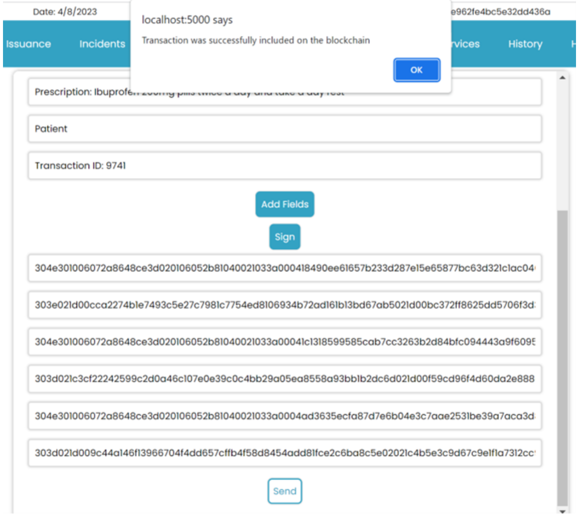
Once the transaction joins the pending transactions of the blockchain, the user will have to wait until the transaction is successfully included in a block. Once the miner nodes include the transaction in a block and mine it successfully, the web app will notify the user. Once the miner node validates a bundle of transactions, it will add it to a block and start mining it. Once mined, the miner will broadcast the block to the network, and then the validator nodes (branches of the insurance company) will validate the miner's work. After block validation, the block will be included in the blockchain, and the state of data and records will be updated. However, in the case of digital insurance claims, the included transaction must be investigated before the state is updated. Notably, the relatable records will be marked as being "pending update" for reference during the investigation period. In the proposed system, the insurance claim investigation process is different from traditional methods. In the proposed system, the insurance company has the ability to use the proposed smart contracts to investigate a DIC. The proposed smart contracts automatically get triggered once a new transaction related to DICs gets included in the blockchain. The smart contracts will perform trials on the claim data using predefined rules and functions in this part. Initially, the proposed smart contracts will verify the signatures in the DICs and compare the results with those involved in the healthcare process. In the proposed system, as the number of entities involved in the healthcare process increases, the chances of adding fraudulent data to the digital insurance claim rise. Although this situation also stands true for traditional systems, since it is more challenging to act fraudulently when more people are involved, this process becomes twice as hard in the proposed system.

The main reason is that entities have to sign data before sending it to another entity in the proposed system. Without these digital signatures, essential messages, especially digital ones, can be easily altered without the sender's notice, allowing policyholders to change other entity's messages for their benefit. However, this risk can be reduced to null once entities digitally sign their messages using the proposed web app.

After validating the signatures in the claim, the proposed smart contract performs other predefined calculations. For example, in the health insurance industry, usually policyholders, with the help of physicians, attempt to misuse the insurance policy and purchase medical equipment that is not required. The proposed smart contracts will be programmed in such a way as to detect these irregularities and alarm the claim validators. For example, in this case, the proposed smart contract analyses the records of the policyholders and realizes that the policyholder has been purchasing specific equipment in the recent insurance claim; as a result, alarming the validator nodes to take a closer look at the claim. Consequently, the proposed smart contract can judge DICs based on algorithms declared by the insurance company. Along with validating DICs, proposed smart contracts can run DIPs as well. DIPs will provide a safe, secure, and fast method for managing policies. Through blockchain technology, insurance companies can use DIPs to track and manage all policies. DIPs are smart contracts stored on the blockchain that automatically process policy-related transactions. With the help of DIPs, insurance companies will no longer need to spend long hours validating insurance policies. In the traditional methods, insurance companies use labor to analyze an insurance policy to check whether it is valid. Meanwhile, using DIPs, these smart contracts will automatically perform these checks and validations. For example, the DIP will immediately alarm the validator nodes if an expired insurance policy is issued. In addition, if a policyholder requests an insurance claim (digital or not), the DIP will ensure the policy is valid during the claim validation process. In other cases, the DIP can automatically renew itself upon premium payment. DIPs also have risk management abilities. When a policyholder attempts to renew their policy, they will send their request to the web app, requesting a policy renewal. The policy renewal request is forwarded to the relatable DIP via the proposed web app and blockchain. The DIP will initially analyze the risks associated with the policy and later return an assessment of the premium that needs to be paid. The premium assessment is sent to the web app to send a payment request to the policyholder. Once the policyholder completes the payment, the web app will alarm the DIP to store the payment information and update the state of the DIP. In this manner, there is little human interaction, removing human errors or potential fraudulent activities. However, not all insurance policies can be automatically processed via the DIP. For example, in the case of insurance covering airplanes, it is not recommended to calculate risk via a smart contract since many other factors need to be considered before calculating premium payments. These types of insurance have extremely sensitive factors that need to be considered, making automatic risk measurements an ineffective approach. On the other hand, this research paper concentrates on health insurance, which does not have extremely sensitive risk management calculations.

5 Data Analysis

In this section, we will analyze a few scenarios where we put the model to the test and show how the proposed system can detect fraudulent actions while creating digital insurance claim . In the first scenario, it is assumed a policyholder (patient) is feeling ill and needs to visit a health professional (doctor) working in a health center (hospital). In addition, we assume that no entity involved in this healthcare process is malicious. For demonstration purposes, in this scenario, it will be showed the users public keys and signatures so that the reader can follow along with the processes happening behind the scenes. In other scenarios, these fields will be hidden, similar to how the proposed system is designed. Note that other entities in the following scenarios also have access to the web app; however, they cannot perform actions that an employee or admin of the insurance company can. In Scenario1 the patient visits the hospital and registers their details, username, and symptoms in the hospital. Initially, the hospital, assuming it is in direct contact with the insurance company, logins into their account using the web app, The hospital should then enter their login details as well. In the insurance companys records, the address is registered as the hospital. For this scenario, we are going to set the password of the account to hospital. After successful login, the hospital asks for the patients policy ID in order to enter. After entering the policy ID, the hospital needs to fill in the fields with as many details as possible.Once the data has been filled in, the hospital signs it and sends it to the doctor for a medical examination.Once the hospital clicks the 'Sign' button, the system signs the messages and provides us with two fields, one is the users public key, and the other one is the users signature. At this point, the patient checks the claim data and visits the doctor for a medical examination. Assuming the doctor prescribed the patient to rest and consume ibuprofen pills, the doctor needs to log in to the system, similar to how the hospital did, and complete the required details.Once filled in, the doctor clicks the sign button to sign the data. The doctor will then send details to the hospital and the patient. The patient will then visit the hospital's cashier and pay the amount charged by the hospital (declared in the receipt ID). After payment, the patient can add the transaction ID to the fields of data and sign the data. Once patients complete the healthcare process, they can send all the data using the 'Send' button. Once clicked, the system gives the following message, indicating that the transaction has been sent:
When this message is received, it indicates that the signatures are valid and the claim has not been altered in any way possible. If we query the blockchain and



Date: 4/8/2023

e962fe4bc5e32dd436a

localhost:5000 says

Transaction was successfully included on the blockchain

Prescription: Ibuprofen 200mg pills twice a day and take a day rest

Patient

Transaction ID: 9741

304e301006072a8648ce3d020106052b81040021033a000418490ee61657b233d287e15e65877bc63d321c1ac04

303e021d00cca2274b1e7493c5e27c7981c7754ed8106934b72ad161b13bd67ab5021d00bc372ff8625dd5706f3d

304e301006072a8648ce3d020106052b81040021033a00041c1318599585cab7cc3263b2d84bfc094443a9f6095

303d021c3cf22242599c2d0a46c107e0e39c0c4bb29a05ea8558a93bb1b2dc6d021d00f59cd96f4d60da2e888

304e301006072a8648ce3d020106052b81040021033a0004ad3635ecfa87d7e6b04e3c7aae2531be39a7aca3d

303d021d009c44a146f13966704f4dd657cffb4f58d8454add81fce2c6ba8c5e02021c4b5e3c9d67c9e1f1a7312cc

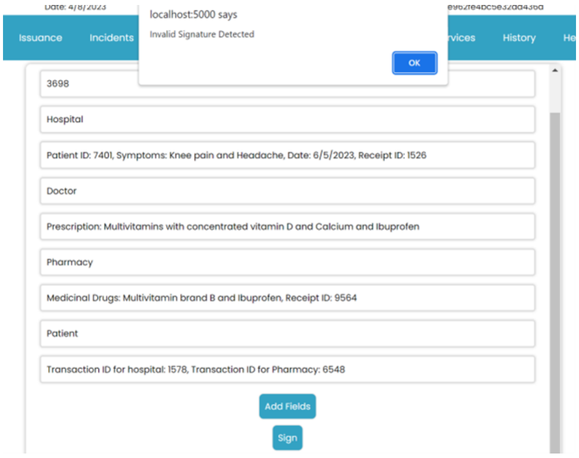
Figure 2

check the transactions, we are able to see that the latest block on the blockchain relates to the transaction. At this point, the Insurance Company can take a closer look at the claim data to ensure that the data logically makes sense as well. Since the claim is valid, the Insurance Company will reimburse the patient as soon as possible and mark the claim as complete.

In next scenario, we will assume one of the entities will attempt to act maliciously and alter claim data in their favor. As mentioned earlier, the two fields related to the users public key and signature are removed, but behind the scenes, these fields will be sent along with the claim data. In this scenario, the patient visits the hospital and requests for treatment.The patient is assumed to have a knee pain and needs to visit a doctor. The hospital registers the patient and signs the data. The app alerts the hospital that they have signed the data. Now, the patient visits the doctor, and the doctor prescribes multivitamin pills. The doctor, too, will sign the data and return it to the patient. In this scenario, the patient will take the signed prescription and visit the pharmacy to purchase the pills. The pharmacy will now have to login to the system and add their data to the fields. Now the pharmacy will sign the data and return it to the patient. The patient is now responsible in completing the data and then sending it to the insurance company. This claim data has not been altered and will be accepted by the system.

The patient attempts to alter the data and changes his 'Symptoms,' the doctors prescription, and the pharmacys drugs. In this way, the patient can request extra reimbursement from the Insurance Company due to the added cost of buying an

Ibuprofen pill. The system returns the following message once the patient sends the altered data to the Insurance Company.



localhost:5000 says

Invalid Signature Detected

3698

Hospital

Patient ID: 7401, Symptoms: Knee pain and Headache, Date: 6/5/2023, Receipt ID: 1526

Doctor

Prescription: Multivitamins with concentrated vitamin D and Calcium and Ibuprofen

Pharmacy

Medicinal Drugs: Multivitamin brand B and Ibuprofen, Receipt ID: 9564

Patient

Transaction ID for hospital: 1578, Transaction ID for Pharmacy: 6548

Figure 3

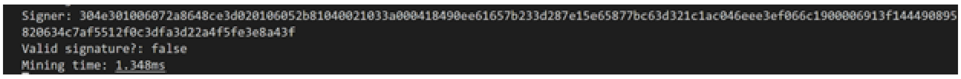
This indicates that an error has occurred in the back-end, showing that the data has somehow been altered. In the back-end, the console has printed the following message:

```
Patient ID: 7401, Symptoms: Knee pain and Headache, Date: 6/5/2023, Receipt ID: 1526
```

This message shows that this part's claim data has been altered. It is remarkable to note that the proposed system only notifies the insurance company of potential fraud. In the model, the transaction has not been reverted. As a result, the blockchain contains the fraudulent claim. There are two reasons for this functionality. The first one is if the claim is mistakenly marked as fraudulent, then the insurance company should be notified and mark the transaction as valid. The second one is if the claim is accurately marked as fraudulent, like in our example, then the data should be saved so that the Insurance Company can keep a record of all fraudulent activities and also potentially use this significant data for further technological advancements, such as training an Artificial Intelligence.

Entities may also try to alter data in other ways. In our system, this may include altering the signatures or the public keys so that a user may bypass the system. For this purpose, we will create a signature from the hospital and send it to the patient. In this case, we assume the patient must send the data to the insurance company. However, the patient decides to alter the hospitals signature (assuming the patient has a software engineering background).

The patient attempted to alter the data and sign it using their key, but the system showed the same error. In addition, in the background of the system, the server has printed the following message:



```
Signer: 304e301006072a8648ce3d020106052b81040021033a000418490ee61657b233d287e15e65877bc63d321c1ac046eee3ef066c1900006913f144490895
820634c7af5512f0c3dfa3d22a4f5fe3e8a43f
Valid signature?: false
Mining time: 1.348ms
```

Figure 4

It can be seen that the system has managed to detect a signature alteration. Notably, the Insurance Company may have discovered this fraud by talking to the pharmacy or the hospital. However, usually, insurance companies ignore small transactions and reimburse the patient either way, which results in never detecting fraud in smaller transactions. Moreover, even if the Insurance Company wanted to contact other entities and examine the claim, they would have to spend hours, sometimes days, communicating with other entities. However, in the proposed system, we can notice how quickly the system can flag alterations in data, reaching speeds of 1.348ms or less than a second! Now, if we consider other scenario cases where a patient may visit more healthcare entities such as clinics, medical group practices, individual practice associations, individual practitioners, emergency care facilities, laboratories, or even surgery centers, the data validation may take months before being completely processed. Adding to the importance of the proposed system, any data alteration can be marked as a fraud detection; these include:

(i) Altering claim data, even by simply adding a dot

(ii) Altering any entitys signature

(iii) Altering any entitys public key

(iv) Altering the public key and the signature at the same time

(v) Altering the claim data along with the public key and the signature

As explained in earlier parts, altering signed data will change the resulting hash of the data. As a result, when a piece of data is altered, the hash also changes, which means the digital signature is no longer valid. In addition, hashes are extremely sensitive, which means that with minor changes to data, the hash completely changes. Hence, this is why even adding a dot to a claim data will invalidate the signature. However, for the last case, case number 5, data is altered, hashed again, and then signed by another entity, so how can the proposed system detect this type of fraud? After all, the original signature has been replaced by the entitys signature so that signature verification will result in a valid signature. For the last case, it will not work because the insurance company holds a record of all registered public keys (in both a trusted and trustless network) and will detect fraud if someone tries to impersonate another entity. Consequently, if a patient tries to sign a data and then claims that the hospital signed in, the system will flag it as fraud since the patients public key differs from the hospitals public key. In the last scenario, we will concentrate on how the system can detect irregularities in the claim data using pre-defined rules and checks. In this scenario, the patient directly visits a health professional (doctor), assuming the doctor is in contract with the insurance company. Notably, in all scenarios, we assumed that the entities are in contract with the Insurance Company. However, if an entity is not in contract with the insurance company, then with the Companys consent, they could still create claims through the proposed web app, assuming the company provided them with login information and asymmetric keys. The patient is assumed to have high cholesterol levels and requests the doctor for a medical prescription, which the doctor prescribes Atorvastatin pills. The doctor signs the prescription and hands the data to the patient. The patient will now visit the pharmacy to purchase the prescribed drugs. However, the patient and the pharmacy are assumed to act maliciously and decide to take advantage of the Insurance Company. Consequently, the patient decides to place an irregular order for the prescribed drugs with the help of the pharmacy. Since both entities are malicious, the pharmacy charges higher than usual for the prescribed drug. In our scenario, Atorvastatin pills are generally priced at 2 dollars, but the pharmacy decides to charge each at 3 dollars. After the pharmacy has signed the data, the patient will also add his/her details and sign the data. Now, the patient will send the details to the insurance company. As it can be noticed, the web app has successfully included the transaction in the blockchain since the signatures had no issues. However, the following messages have been printed in the back-end of the web app, where the nodes control it. The back-end has been programmed to search for unusual quantities of drugs bought at unusual prices. These programmed rules are simple in our model and scenario; however, in the proposed method, these rules can become highly complex since, for every medicinal drug, a different regular price and quantity are defined. In our case, we programmed the software to alert when the quantity of drugs bought exceeds 5, and the price exceeds 2. In this manner, without missing a beat (in 1.667ms), the Insurance Company can detect whether the claim data contains irregular data. In the proposed system, the web app can also connect to other APIs. As a result, the web app can connect to a banks API and query the transaction the patient has sent via an API request. In this way, even bank transfers can be analyzed via the system. Consequently, if a patient pays an amount that is less than claimed to profit from the difference, the system can query the bank transfer and detect fraud.

6 Conclusion and policy implication

Fraud detection in the health insurance industry is a critical issue that demands innovative solutions. Blockchain technology offers promising advantages, including transparency, immutability, smart contracts, and secure data sharing. The proposed system is a blockchain-based web application that consists of several sections, such as the proposed blockchain, proposed smart contracts, and the proposed web application. The web application consists of a front-end and back-end section. The front-end enables users to interact with the proposed system. The back-end enables the Insurance Company to store records on the blockchain and increase the chances of detecting fraud in Insurance Claims, especially Digital Insurance Claims. In this research paper, we proposed and evaluated fraud detection methods using blockchain and smart contract technology. We proposed a blockchain-based web application that can be used as Core Insurance Software for any health Insurance Company. The main issue with the proposed system is the high initial cost. Therefore, we recommend the proposed system to large, established Insurance Companies with at least 1’000 employees and 20 branches. Due to the lack of capital and labor in smaller companies, it would not be an ideal choice to opt for the proposed system. Another reason for our recommendation is that large insurance companies already own many hardware devices that can become blockchain nodes. On the other hand, smaller companies will need to consider investing large amounts of capital in purchasing hardware devices to run nodes. Much like all other research papers, this paper has certain limitations that will be explained here. The first limitation is that we could not test the model in a real-life health Insurance environment. In this paper, we could only simulate a healthcare scenario. Our second recommendation is to develop the model of the proposed system further. Although we have completed the model for this research paper, there is still room for further development. The recomandation for Iranain insurance company and other organization which are related to health insurance is to transfer theire IT system to blockchain system, so that they can get a good benefit from it and a lot of money can be saved.

Bibliography

[1] http://www.nhcaa.org

[2] Sparrow, Malcolm K, *Health care fraud control: understanding the challenge*, JOURNAL OF INSURANCE MEDICINE-NEW YORK- 28 (1996): 86-96.

[3] A. Rashidian, H. Joudaki, and T. Vian, *No evidence of the effect of the interventions to combat health care fraud and abuse: A systematic review of literature*, PLoS One, vol. 7, no. 8, 2012, Art. no. e41988, doi: 10.1371/ journal.pone.0041988.

[4] IBM, *Blockchain: The Chain of Trust and its Potential to Transform Healthcare Our Point of View*, 2016, unpublished.

[5] M. Wohrer and U. Zdun, *Smart contracts: security patterns in the ethereum ecosystem and solidity*, Blockchain Oriented Software Engineering (IWBOSE) 2018 International Workshop on, pp. 2-8, 2018.

[6] Mendoza-Tello, J. C., Mendoza-Tello, T., & Mora, H, *Blockchain as a Healthcare Insurance Fraud Detection Tool. In Research and Innovation Forum 2020: Disruptive Technologies in Times of Change*, Springer International Publishin, pp. 545-552, (2021).

[7] https://doi.org/10.37896/jxu14.6/096

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

[9] Ismail & Materwala, *Article A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions*, Symmetry, 11(10), 1198, (2019). https://doi.org/10.3390/sym11101198

[10] Ismail, L., Materwala, H., & Zeadally, S., *Lightweight blockchain for healthcare*, IEEE Access, 7, 149935-149951, (2019).

[11] Kousaridas, A., Falangitis, S., Magdalinos, P., Alonistioti, N., Dillinger, M., *SYSTAS: Density-based algorithm for clusters discovery in wireless networks*, In Proceedings of the 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Hong Kong, China, 30 August2 September 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 21262131.

[12] Oracle, Available online: https://cloud.oracle.com/en_US/blockchain, (accessed on 20 January 2022).

[13] L. Ismail and S. Zeadally, *Healthcare Insurance Frauds: Taxonomy and Blockchain-Based Detection Framework (Block-HI)*, in IT Professional, vol. 23, no. 4, pp. 36-43, 1 July-Aug. 2021, doi:10.1109/MITP.2021.3071534.

[14] Mackey, T. K., Miyachi, K., Fung, D., Qian, S., & Short, J., *Combating Health Care Fraud and Abuse: Conceptualization and Prototyping Study of a Blockchain Antifraud Framework*, Journal of medical Internet research, 22(9), e18623, (2020).

[15] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa and L. Tawalbeh, *Health Care Insurance Fraud Detection Using Blockchain*, Seventh International Conference on Software Defined Systems (SDS), 2020, pp. 145-152, (2020). doi:10.1109/SDS49854.2020.9143900

[16] W. Liu, Q. Yu, Z. Li, Z. Li, Y. Su and J. Zhou, *A Blockchain-Based System for Anti-Fraud of Healthcare Insurance*, IEEE 5th International Conference on Computer and Communications (ICCC), pp. 1264-1268, (2019).

[17] Mohan T., Praveen K., *Fraud Detection in Medical Insurance Claim with Privacy Preserving Data Publishing in TLS-N Using Blockchain. In: Singh M., Gupta P., Tyagi V., Flusser J., Ören T., Kashyap R. (eds) Advances in Computing and Data Sciences. ICACDS 2019*, Communications in Computer and Information Science, vol 1045. Springer, Singapore. https://doi.org/10.1007/978-981-13-9939-8_19

[18] Mendoza-Tello J.C., Mendoza-Tello T., Mora H., *Blockchain as a Healthcare Insurance Fraud Detection Tool. In: Visvizi A., Lytras M.D., Aljohani N.R. (eds) Research and Innovation Forum 2020. RIIFORUM 2020.*, Springer Proceedings in Complexity. Springer, Cham. https://doi.org/10.1007/978-3-030-62066-0_41

[19] Rui Roriz, José Luis Pereira, *Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector*, Procedia Computer Science, Volume 164, 2019, Pages 211-218.

How to Cite: Abbas Raad[1], Reza Ofoghi[2], Ghadir Mahdavi[3], *Fraud detection in supplementary health insurance based on smart contract in blockchain network*, Journal of Mathematics and Modeling in Finance (JMMF), Vol. 4, No. 2, Pages:33–56, (2024).

Journal of Mathematics and Modeling in Finance (JMMF)
Vol. 4, No. 2, Summer & Autumn 2024
Research paper

Stochastic portfolio optimization by diversity-weighted portfolio approach

Shokoofeh Banihashemi[1]

[1] Department of mathematics,Faculty of Mathematics and Computer Science, Allameh Tabataba'i University, Tehran, Iran.

shbanihashemi@atu.ac.ir

Abstract:
The portfolio optimization problem, including portfolio selection, typically aims to maximize return and minimize risk. In this paper, we discuss about increasing use of stochastic portfolios in investments and aim to create optimal portfolios. It follows the relative wealth process of these portfolios, outperforms the market portfolio over sufficiently long time-horizons. In this regard, initially, a model of the market is presented by the stochastic portfolio theory (SPT) and features like Growth rate, Excess growth rate are mentioned. Then, functionally-generated portfolios are defined by using diversity weighted portfolios with parameters $p \in (0, 1)$, $p < 0$ and combination of them. Finally, by obtaining the daily closing price of 10 stocks in Tehran Stock Exchange (TSE) ,the performance of diversity weighted portfolios is investigated.

Keywords: Diversity-weighted portfolios, Portfolio generating functions, Portfolio, Stochastic portfolio theory, Sharpe ratio.
Classification: Primary: 91G10; Secondary: 91B70, 91G80.

1 Introduction

Investing in financial markets is inherently risky and investors try to increase returns and reduce their risks. Stochastic Portfolio Theory (SPT), was introduced by Fernholz in 1999, which provided insights into the structure and behavior of stock portfolios and market arbitrage. In the early 1950s, Markowitz [11] developed a theoretical framework for the systematic combination of optimal asset portfolios, which became the basis for modern theories of portfolio management. Markowitz sought a portfolio that had less risk and produced greater returns. Subsequently, the stochastic portfolio theory began in 1995 with a linear version regarding stock market diversification, which was eventually published by Fernholz in 1999 in the Journal of Mathematical Economics [2]. This theory provides a flexible framework

[1] Corresponding author

Received: 23/04/2024 Accepted: 06/10/2024
https://doi.org/10.22054/jmmf.2024.78741.1131