Asia-Pacific Journal of Science and Technology: Volume: 29. Issue: 02. Article ID.: APST-29-02-10. Research Article

Asia-Pacific Journal of Science and Technology

https://www.tci-thaijo.org/index.php/APST/index

Published by the Research and Graduate Studies,
Khon Kaen University, Thailand

Using blockchain oracle for data management: A case study on health insurance network

Sorawid Juntachat[1], Eknarin Lerdnuntawat[1], Tham Thearawiboon[1], and Supakit Prueksaaroon[1,*]

[1]Department of Electrical and Computer Engineering, Faculty of Engineering, Thammasat School of Engineering, Thammasat University, Pathum Thani, Thailand
[*]Corresponding author: psupakit@engr.tu.ac.th

Received 10 October 2022
Revised 3 August 2023
Accepted 13 September 2023

Abstract

The health insurance network represents a collaborative ecosystem involving hospitals and health insurance companies, jointly providing medical services while managing their customers' electronic health records (EHR). Presently, health records are typically confined to individual providers, hindering real-time data sharing with insurance entities and resulting in delayed claims processing. Blockchain technology, renowned for its distributed and decentralized nature, confers essential attributes such as immutability, tamper resistance, and transparency, rendering it a promising solution for enhancing insurance record management and event transactions. By incorporating data security and privacy features, blockchain establishes trust among network participants and effectively addresses interoperability challenges prevalent in current technologies. The proposed health insurance framework adopts R3 Corda, a peer-to-peer permissioned distributed ledger technology, introducing a novel model for sharing health insurance data on the blockchain while automating claim processes. Central to this framework is utilizing a blockchain oracle, a pivotal component facilitating the seamless integration of existing health insurance databases with the blockchain, leading to enhanced efficiency and streamlined claims processing.

Keywords: R3 Corda, Insurance, Permissioned blockchain, Healthcare, Blockchain oracle

1. Introduction

The health insurance industry plays a crucial role in society, providing financial security and mitigating the potentially devastating impact of unforeseen events such as accidents or pandemics like COVID-19. By covering medical costs, health insurance contributes to reducing mortality rates and improving individuals' overall quality of life. The health insurance network operates through three key stakeholders: hospitals, insurance companies, and customers. Despite technological advancements, the claim process still faces inefficiencies. Approval of insurance claims tends to be protracted, mainly due to manual transaction processes and interactions between parties involved in the system, resulting in prolonged refund times and slow processing rates. Additionally, the insurance network incurs substantial annual costs for processing claims and suffers losses due to fraud [1]. Researchers have proposed leveraging blockchain technology to address these challenges within the health insurance industry. [2,3]

Blockchain technology has emerged as a highly disruptive force across diverse industries. It functions as a decentralized database, structured by verified nodes, and maintains a series of blocks with immutable information, facilitating secure data exchange without the need for intermediaries [4,5]. Key elements such as digital cryptographic signatures, consensus algorithms, and data hashing are instrumental in ensuring data integrity and security [6]. The common structure of the blockchain is shown in Figure 1. This inherent capability to preserve sensitive information makes blockchain particularly promising for application within the healthcare network. For example, by converting insurance policies into smart contracts, the automation of claim processing, data verification, and payment processes can be significantly improved, saving both time and expenses, as well as providing enhanced fraud prevention. Smart contracts, written on the blockchain, are crucial in customer assistance by enabling policy purchases, claim tracking, and automatic fund disbursement for insurance customers. Currently, smart contracts are actively employed in blockchain-based solutions to streamline asset transfers, combat fraud, and minimize administrative overheads.

Moreover, hospitals are responsible for managing EHRs containing highly sensitive personal medical information on patients. Due to regulatory constraints, sharing such sensitive information with other healthcare providers becomes challenging.

The current blockchain technology primarily emphasizes the dissemination of data within public or private networks, where all nodes possess identical information, resulting in a lack of selective data sharing between nodes within the same network. The collaboration of multiple parties in the insurance network has raised concerns about the visibility of data on the ledger among participating entities. As one of the most intriguing and noteworthy technologies, R3 Corda presents a scalable and permissioned peer-to-peer (P2P) distributed ledger technology (DLT) platform that facilitates the development of applications fostering digital trust among cooperative entities in the general business context [7]. Unlike conventional centralized databases, Corda adopts a decentralized approach whereby data are not stored in a centralized repository. Instead, each individual Corda node maintains a specific set of data, referred to as "facts." A network comprising five nodes (Alice, Bob, Carl, Demi, and Ed) is depicted in Figure 2. When two or more nodes share certain data, they are represented by numbered circles at the intersection points. For example, Facts 1 and 7 are shared by both Alice and Bob. Importantly, data sharing is selective, with each node determining which facts to share with others. Alice, for instance, shares her facts solely with Bob, withholding any information from Carl, Demi, or Ed [8]. Consequently, each node perceives only a specific subset of facts based on its internal set of data and the facts it has opted to share with other nodes. As a result, no single node within the network possesses a comprehensive view of the entire ledger. For instance, in the given figure, Alice and Demi cannot access each other's respective data due to their lack of shared facts. This innovative approach enhances data privacy, security, and confidentiality, rendering it particularly suitable for diverse applications, including insurance networks, where protecting sensitive information is essential while still facilitating efficient collaboration and data exchange among participants.

To address the health insurance limitations, we propose the implementation of a blockchain-based health insurance network in collaboration with insurance companies and hospitals to automate claiming procedures and replace traditional underwriting processes. This proposed framework leverages the R3 Corda platform and integrates a blockchain oracle as a pivotal component. Blockchain oracles act as intermediaries, connecting blockchains to external data sources, referred to as off-chain data, enabling smart contracts to process real-world data as inputs and outputs. While the Corda blockchain directly stores EHRs as on-chain data, the blockchain oracle is instrumental in aggregating off-chain data from external sources such as relational databases (RDBMS) or NoSQL databases. Insurance providers and hospitals with shared facts selectively exchange specific data within this collaborative ecosystem. These proposed measures are expected to yield several benefits, including expedited claim processing, streamlining the traditional underwriting process through reduced manual intervention, enhanced transaction transparency, and bolstered data security among the participating parties. The primary contributions of this paper can be summarized as follows:

1. We present a blockchain-based peer-to-peer (P2P) network that facilitates collaboration between insurance providers and hospitals to enable the sharing of 1:1 private data. This collaborative approach aims to enhance the automated claims process, reducing the time spent and facilitating quicker refunds.
2. We introduce an automated claims process utilizing a blockchain oracle for off-chain connections. This oracle enables the verification of insurance policies from insurance providers while enhancing the efficiency and accuracy of the claims processing system.

The remainder of this paper is structured as follows. Section 2 provides a brief overview of the blockchain-based framework in the health insurance and healthcare domains. Section 2.1 presents the framework for using blockchain-based in the insurance network, while Section 3 provides the blockchain-based implementation in the proposed case study. The conclusion of this paper is presented in Section 4.

2. Materials and methods

2.1 Literature background

Blockchain technology can be applied to diverse domains, spanning the finance industry and beyond, encompassing the Internet of Things (IoT), cryptocurrencies, supply chain management, insurance, and healthcare. Among these domains, the health insurance industry stands out as being particularly challenging due to the sensitive nature of EHRs. The limitations associated with EHRs are effectively addressed by the inherent characteristics of blockchain, including decentralization, transparency, privacy, security, and data verifiability, as discussed in the research conducted by Agbo et al. [9]. Consequently, considerable research efforts have been directed toward exploring the potential of blockchain in the health insurance sector, considering both permissioned and public blockchain frameworks.

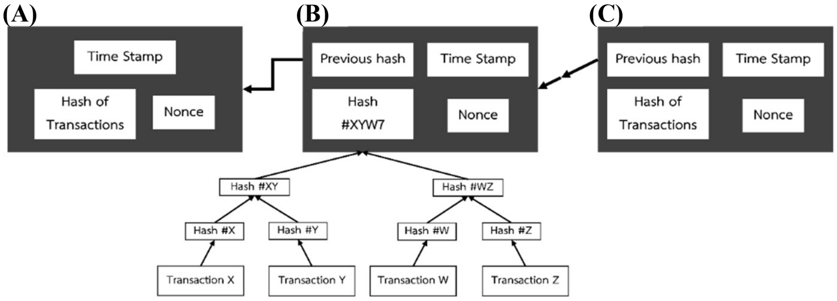

Figure 1 An overview of the blockchain structure: (A) Block 1, (B) Block 2, and (C) Block n.

The MedRec system [10] is a large-scale data management blockchain platform designed to manage EHRs through the Ethereum blockchain. MedRec leverages Ethereum's smart contracts to manage three distinct types of contracts, which in turn handle a multitude of records. These create relationships between all contracts, facilitating efficient and secure management of EHRs within the platform.

In their study, Aleksieva et al. [11] conducted a comparative analysis of two distinct use cases for the insurance claim process, utilizing both public and private blockchains, specifically Ethereum and Hyperledger Fabric (HLF), respectively. The researchers propose a combined solution that harnesses the strengths of both blockchain types. Hyperledger Fabric (HLF) is leveraged as a database for efficiently collecting data and executing automatic claims operations, offering greater flexibility and faster processing compared to a public blockchain. On the other hand, Ethereum is employed for enabling automatic payments on claims through the utilization of smart contracts, facilitating the seamless transfer of ETH as a payment in the claims process. Integrating these two blockchain technologies presents a comprehensive solution that optimizes data management and payment operations within the insurance claim process.

Saldamli et al. [12] present a prototype of a comprehensive healthcare insurance fraud detection system that harnesses the capabilities of blockchain technology and a graph database. The system's architecture integrates BigchainDB as the blockchain platform, serving as a secure and immutable repository for healthcare data while facilitating data sharing among relevant stakeholders. The use of blockchain technology ensures the integrity and security of the stored data. Additionally, the researchers employ Neo4j as the graph database, enabling real-time fraud detection by establishing relationships among healthcare providers, hospitals, and patients. This innovative combination of blockchain and graph database technologies empowers the system to efficiently and effectively identify instances of fraud within the health insurance domain.

MedBloc [13] introduces a blockchain-powered solution designed for the sharing and management of EHR data. The system is implemented using HLF, a popular blockchain framework. MedBloc incorporates an authentication server with an encryption mechanism to enhance privacy and security. This combination ensures that data access and protection are securely managed. The system further enforces controlled access to EHRs through smart contract-based access control, ensuring that only authorized parties can interact with the sensitive medical records. By leveraging blockchain technology and smart contracts, MedBloc offers a robust and secure platform for efficiently sharing and managing EHR data, safeguarding patients' privacy, and providing a trustworthy infrastructure for healthcare providers and stakeholders.

Marinho et al. [14] propose an intriguing hybrid framework named MOON, designed to manage data in relational databases (RDBs) and blockchain within the domain of clinical testing laboratories. MOON facilitates interaction between client applications and the system through familiar SQL language constructs, such as insert, select, update, and delete statements. The framework acts as an intermediary, converting SQL statements into requests for data on the blockchain. Additionally, MOON is responsible for transforming the JSON format data stored on the blockchain into table format in the output of the SQL language. Although the MOON framework may not always outperform traditional RDBs in certain circumstances, the research results highlight its utilization of blockchain properties, including immutability and transparency. By leveraging these characteristics, MOON offers an innovative and practical approach to sharing and managing data, effectively merging the advantages of both relational databases and blockchain technology in the context of clinical testing laboratories.

2.2 Advantages and disadvantages of the blockchain oracle in the health insurance framework

The blockchain oracle [15] serves as a critical network service, facilitating the retrieval of external data to invoke smart contracts enabling the execution of off-chain data processing in the blockchain. Blockchains' inherent decentralization and immutability present a challenge in directly accessing external data sources, which typically reside in centralized environments and are subject to alterations or updates. The external data encompasses a wide range of real-world information, including flight status, weather conditions, temperature data, and currency exchange rates. [16] Importantly, the blockchain oracle functions as a data conduit and does not retain any information, its sole purpose being to query off-chain data sources and provide such data to the corresponding smart contracts within the blockchain network.

By leveraging the blockchain oracle, manual operations are eliminated, leading to significant time saving in processing health insurance claims, as outlined in [17]. This integration of off-chain data via the blockchain oracle augments the capabilities of smart contracts, expanding their reach beyond the blockchain and enhancing the efficiency and automation of various processes, including those within the health insurance domain. [18]

Another advantage lies in the enhanced privacy and security measures ensured by the blockchain oracle. The oracle restricts access to sensitive off-chain data, such as customer information and insurance policies, exclusively to authorized entities like insurance providers and hospitals. This controlled access reinforces data privacy and bolsters the security of the health insurance network, safeguarding it against potential data breaches and unauthorized access.

However, certain drawbacks are associated with the utilization of a blockchain oracle. One significant concern pertains to potential centralization risks introduced by the oracle. If the blockchain oracle relies on a single service provider, the vulnerability of the entire system may increase since the oracle service provider could become a single point of failure. Therefore, ensuring a decentralized and robust oracle infrastructure is crucial for mitigating such centralization concerns.

Moreover, the trustworthiness of the blockchain oracle is paramount [16], given its pivotal role in handling sensitive off-chain data. Any malicious or unreliable behavior by the oracle could lead to inaccurate data validation, potentially compromising the integrity of the health insurance network. To address this, meticulous selection and verification of the oracle service provider are imperative to maintain the system's dependability.

3. Results

3.1 The proposed blockchain-based health insurance framework

This section provides an overview of a health insurance network system that utilizes the Corda platform and incorporates the blockchain oracle. The key components of this system are presented together with an illustration of how hospitals and insurance providers can effectively share facts within the network. Additionally, the significance of a notary node is emphasized in this context. Using the Corda platform and the blockchain oracle ensures secure and transparent data sharing, facilitating an efficient and automated process for managing health insurance-related information. The role of the notary node as a trusted authority in validating and timestamping transactions adds a crucial layer of security and reliability to the overall system.

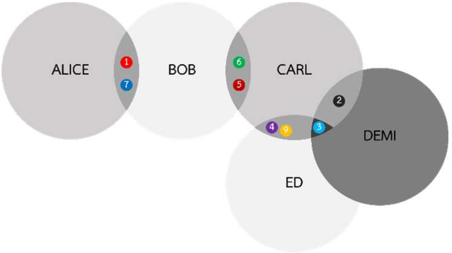

Figure 2 Example of a Corda fact-sharing diagram.

3.2 Health insurance network system overview and components

The proposed system encompasses six distinct components, as illustrated in Figure 3: 1) Patients: Individuals seeking to claim medical expenses incurred at the hospital, 2) Hospital Nodes: These signify the Corda nodes associated with the hospital party. Hospital nodes receive claim requests from the patients, 3) Insurance Nodes: These correspond to the Corda nodes affiliated with the insurance provider party. Insurance nodes collaborate with hospital nodes to validate medical expense claims in accordance with the insurance policies, 4) Blockchain Oracle: The oracle serves as an intermediary between the on-chain blockchain and the off-chain insurance database. This component facilitates the connection to the insurance database in the current case study, providing access to essential off-chain data, 5) Insurance Database: This serves as a repository for off-chain or external data accessed by the blockchain oracle to enhance the real-world business model. This entity can be implemented using any relational database, and MySQL is utilized for this case study to realize the insurance database functionality, and 6) Notary Cluster: This comprises a group of notary nodes tasked with the essential role of notarizing transactions within the health insurance network system.

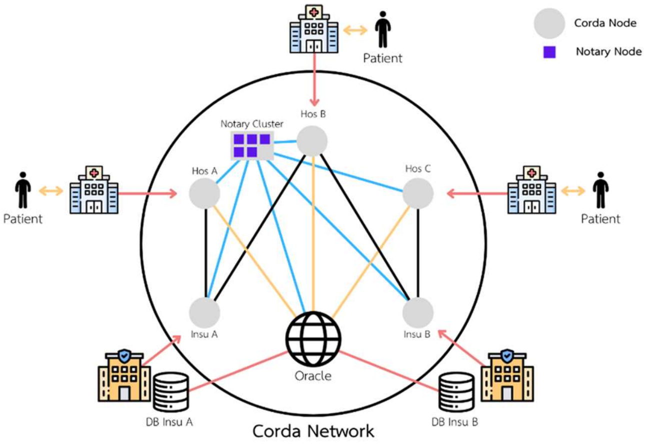

Figure 3 Overview of the health insurance network.

3.3 Shared facts model

In this case study, the sharing of fact models between hospitals and insurance providers is categorized into three distinct models: 1:1, 1:N, and N:1, as depicted in Figure 4. Firstly, the 1:1 model illustrates a scenario in which one hospital node interacts with a single insurance node, and Fact 1 is shared between both nodes, as presented in Figure 4 (A). Secondly, the 1:N model, as shown in Figure 4 (B), portrays a situation where one hospital node interacts with multiple insurance nodes. In this model, Fact 1 remains private and is exclusively shared between hospital A and insurance provider A, while Facts 2 and 3 are shared solely between specific pairs of nodes. Lastly, Figure 4 (C) exhibits the N:1 model, wherein one hospital node can interact with multiple insurance nodes. This model represents the inverse scenario of the 1:N model. All three models encompass every conceivable scenario that may arise in the interactions between hospitals and insurance providers within the health insurance network system.

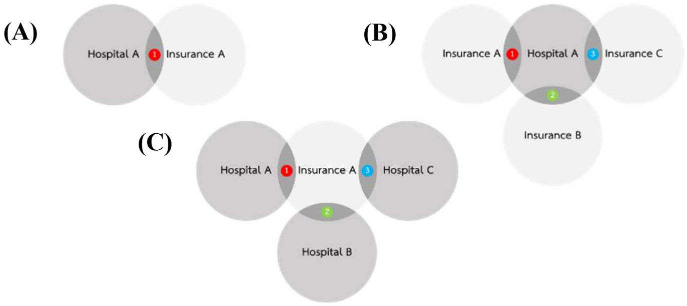

Figure 4 Shared facts use cases on the proposed system where the circle in an intersection area represents a shared fact between nodes. (A) 1:1 model, (B) 1:N model, and (C) N:1 model.

3.4 On-chain and off-chain data

In this study, the data have been classified into two distinct types: on-chain and off-chain. Within the Corda framework, facts represent on-chain data stored securely on the blockchain. Despite hospitals or insurance nodes interacting with multiple nodes, the facts are selectively shared only with the relevant node, ensuring data consistency while preserving privacy. The facts are maintained based on their paired relationships, further contributing to data consistency and confidentiality.

On the other hand, off-chain data refers to local databases maintained by insurance providers, encompassing information such as health insurance conditions and customer details. Hospital nodes have access to relevant information, as permitted by the insurance providers, ensuring the protection of customer rights and privacy. The specifics of the on-chain and off-chain data are presented in Tables 1 and 2, respectively, providing a comprehensive overview of the data classification within the health insurance network system.

Table 1 On-chain variables stored on the Corda nodes.

Variable	Description
Hospital Number	Hospital number (HN) is the number of outpatient department treatments (OPD) for a patient.
Insurance ID	Policy number of the patient.
party	Related parties on the Corda network include the hospital and insurance company.
claims	List of the claim objects.
amount	Amount claimed for each object.
count	Number of claims on the object.
Claim ID	Receipt number on the claim.
Claim Description	Additional information, such as type of illness being claimed for.

Table 2 Off-chain variables stored on the insurance database.

Variable	Description
Type	Type of health insurance.
Name	First and last name of the patient.
CID	Identification number of the patient.
Start Date Insurance	Date of start of the health insurance.
End Date Insurance	Date of expiry of the health insurance.
Gender	Gender of the patient.
Birthday	Date of birth of the patient.
Ins ID	Policy number of the patient.
Limit Cost	Claim limit.
Etc.	Additional information.

3.5 Benefits and advantages of the notary node

The notary node plays a crucial role in the system by notarizing transactions ensuring unique consensus in accordance with the Unspent Transaction Output (UTXO) model, thus mitigating the risk of double spending. Moreover, the notary node ensures the consensus validity of transactions. Before a transaction is committed to the network and the ledger is updated, the notary node validates the compliance of the transaction with the policy contract.

To maintain data confidentiality, the notary node's transaction visibility can be limited. Public keys are used to identify each party, thus restricting the data the notary node can access [19]. This mechanism enhances data privacy and security within the health insurance network.

Moreover, to enhance system performance, multiple notaries can be consolidated into a cluster. This approach offers advantages such as increased throughput and reduced latency since multiple nodes can efficiently manage the distribution workload. In this study, the proposed system is implemented using a notary cluster comprising five nodes: hospital nodes A, B, and C, and insurance nodes A and B. The collaborative configuration of diverse nodes in the notary cluster ensures the establishment of a trustless system for the health insurance network. This trustless architecture fosters a secure and reliable environment for data management and transaction validation, bolstering the overall efficacy and robustness of the health insurance network system.

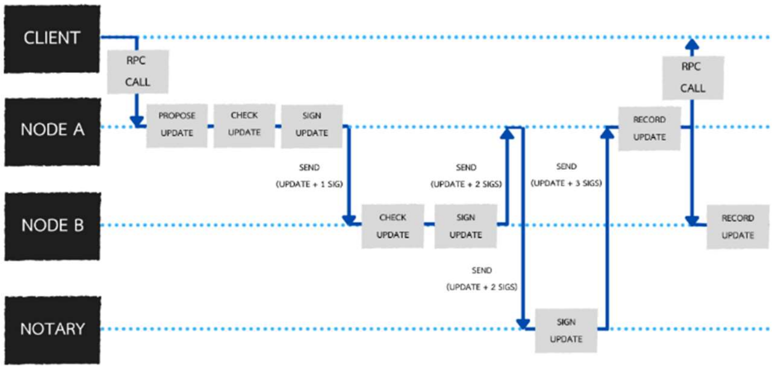

Figure 5 Example of the state flow diagram.

According to Figure 5, when a client initiates an action in the system, such as creating a claim request, the proposed transaction is sequentially sent to all nodes to collect signatures for validation in accordance with the policy contract. Upon receipt of the proposed transaction, the notary node plays a crucial role in preventing transaction fraud if the client attempts to utilize an already used state in the transaction proposal, thereby ensuring data integrity.

Following the validation process, the signed transaction is disseminated to all nodes to update the facts on each local node. Subsequently, the operation status is communicated back to the client via a remote procedure call (RPC), completing the transaction cycle and providing the client with a response regarding the outcome of the operation. This sequential process guarantees the secure and reliable execution of transactions within the health insurance network system, ensuring data consistency and trustworthiness throughout the process.

3.6 Workflow of the health insurance framework

The workflow of the health insurance network is illustrated in Figure 6. Initially, the patient initiates an insurance claim at the hospital. The hospital node then transmits the claim request to the blockchain oracle node to acquire the relevant off-chain data necessary for constructing the transactions. The blockchain oracle node thoroughly verifies the received data and responds by signing back to the hospital.

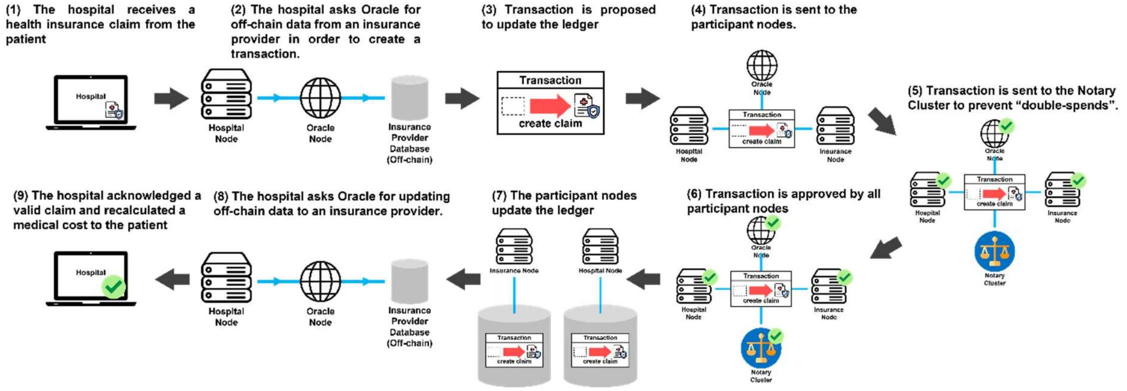
(1) The hospital receives a health insurance claim from the patient
Hospital
(2) The hospital asks Oracle for off-chain data from an insurance provider in order to create a transaction.
Hospital Node
Oracle Node
Insurance Provider Database (Off-chain)
(3) Transaction is proposed to update the ledger
Transaction
create claim
(4) Transaction is sent to the participant nodes.
Oracle Node
Hospital Node
Transaction
create claim
Insurance Node
(5) Transaction is sent to the Notary Cluster to prevent "double-spends".
Oracle Node
Hospital Node
Transaction
create claim
Insurance Node
Notary Cluster
(6) Transaction is approved by all participant nodes
Oracle Node
Hospital Node
Transaction
create claim
Insurance Node
Notary Cluster
(7) The participant nodes update the ledger
Insurance Node
Hospital Node
Transaction
create claim
Transaction
create claim
(8) The hospital asks Oracle for updating off-chain data to an insurance provider.
Hospital Node
Oracle Node
Insurance Provider Database (Off-chain)
(9) The hospital acknowledged a valid claim and recalculated a medical cost to the patient
Hospital

Figure 6 Overview of workflow for the proposed health insurance framework.

Upon receiving the proposed transaction from the hospital node, the insurance node proceeds to acknowledge and validate the transaction in accordance with the customer policy contract. If the transaction aligns with the contract criteria, the insurance node affixes its signature to the transaction and forwards it to the notary cluster. The notary cluster is responsible for providing valid consensus by meticulously assessing the transaction before committing it to the blockchain. In addition to transaction validation, the notary node plays a pivotal role in preventing "double-spends" by checking if the proposed transaction has already been claimed. In the case of any duplicity, the notary cluster can reject the transaction; otherwise, it is confirmed by the notary node.

To enhance system resilience and prevent single points of failure, a notary node can be composed of multiple nodes, referred to as a notary cluster. After the transaction has been confirmed, it is sent back to both the hospital and insurance nodes to update the facts on their respective local nodes. Subsequently, the hospital node submits a request to the blockchain oracle to update the off-chain data, finalizing the insurance claim process. This workflow ensures the secure, transparent, and efficient operation of the health insurance network, safeguarding data integrity and privacy throughout the transaction lifecycle.

The proposed transaction is approved and subsequently updated on the Corda node as on-chain data, as depicted in Figure 7. Initially, "Transaction 0" serves as the issuance or genesis point, containing an empty state as the input state and the patient's details as the output state. The patient's details encompass the information presented in Table 1. Since there is no claim request at this stage, the claims list in the "Transaction 0" output state remains empty.

Subsequently, when the patient successfully claims against their health insurance, the "Update Transaction" (Transaction 1) is employed to modify the patient's details. The input state of "Transaction 1" refers to the output state of "Transaction 0" using a hash for the transaction and its index. As a result, the output state of "Transaction 1" is updated to reflect the current state, while the output state of the previous transaction (Transaction 0) is designated as historical and cannot be accessed or used by any future transaction. This mechanism ensures a transparent and chronological record of transactions, preventing the alteration of historical data while maintaining the integrity and consistency of the on-chain data within the Corda blockchain.

In the event of a subsequent incident, such as the patient falling down and seeking to make another insurance claim at the same hospital, the health insurance claim process is executed in a similar manner as before, represented by "Transaction 2." The output state of "Transaction 2" includes the additional details of the new claim, thereby updating the claims list in the output state to accommodate the new information. Consequently, the output state of "Transaction 2" becomes the current state, recording the latest health insurance claim of the patient.

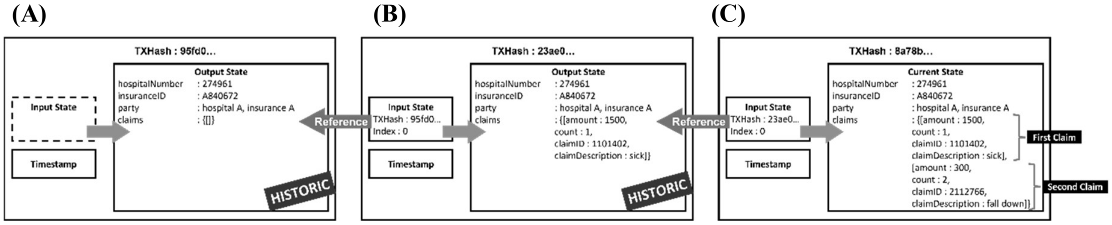

Figure 7 Transactions stored on the hospital node and the insurance node following the workflow: (A) transaction 0, (B) transaction 1, and (C) transaction 2.

In the proposed framework, the on-chain data is meticulously organized and segregated based on the insurance ID. The claim information for each patient is stored in a dedicated blockchain specific to their respective insurance provider. In essence, the patient's claim details are partitioned and distributed across various blockchains corresponding to different insurance providers based on their individual insurance IDs. This segregation ensures the structured and efficient storage of health insurance claims while preserving data privacy and security within the health insurance network. By employing this approach, the proposed framework can effectively manage and process health insurance claims from multiple patients and insurance providers in a secure and decentralized manner.

The sequence diagram illustrating the health insurance framework is presented in Figure 8, showcasing the sequential steps involved in the process:

1. The initial step in the health insurance framework involves the hospital A node requesting off-chain data from the insurance A database by sending specific queries to the blockchain oracle.
2. In response to the hospital A node's request, the blockchain oracle queries the relevant off-chain data and transmits the acquired data to the hospital's A node.
3. Upon receiving the off-chain data from the blockchain oracle, the hospital A node proceeds to construct a proposed transaction and affixes its signature to the transaction, indicating its endorsement and involvement in the process.
4. Following the creation and signing of the proposed transaction, hospital A node forwards the transaction, bearing a single signature from hospital A to the blockchain oracle. The purpose of this action is to seek acceptance and authorization from the blockchain oracle to proceed with the transaction-building process.
5. After receiving the transaction from the hospital, A node, the blockchain oracle performs essential validation to ensure accuracy and legitimacy. Upon successful validation, the blockchain oracle adds its unique signature to the transaction before sending it back to the hospital A node, fully authenticated and endorsed.
6. Upon receiving the signed transaction from the blockchain oracle, the hospital A node appends its signature, resulting in a transaction with two signatures. Subsequently, the hospital A node sends this transaction to the insurance A node for acceptance and authorization to proceed with the transaction-building process.
7. Upon receiving the transaction with dual signatures, the insurance A node validates and adds its own signature before sending it back to the hospital A node.
8. Hospital A node submits the transaction, featuring the signatures of hospital A, the blockchain oracle, and insurance A, to the notary cluster, with the primary objective of obtaining consensus on both validity and uniqueness.
9. Upon verification of the transaction, the notary cluster appends its own signature, resulting in a transaction bearing four signatures, namely from hospital A, the blockchain oracle, insurance A, and the notary cluster. The notary cluster then returns the transaction with the four signatures to the hospital A node.
10. Once all nodes have approved the transaction, the hospital and insurance nodes proceed to update the facts on their respective local nodes.
11. Following the approval of the transaction, the hospital A node initiates a request to update off-chain data on the insurance A database, utilizing the services of the blockchain oracle.
12. Upon receiving the request from the hospital, A node to update off-chain data on the insurance A database, the blockchain oracle confirms that the updating process has been successful.

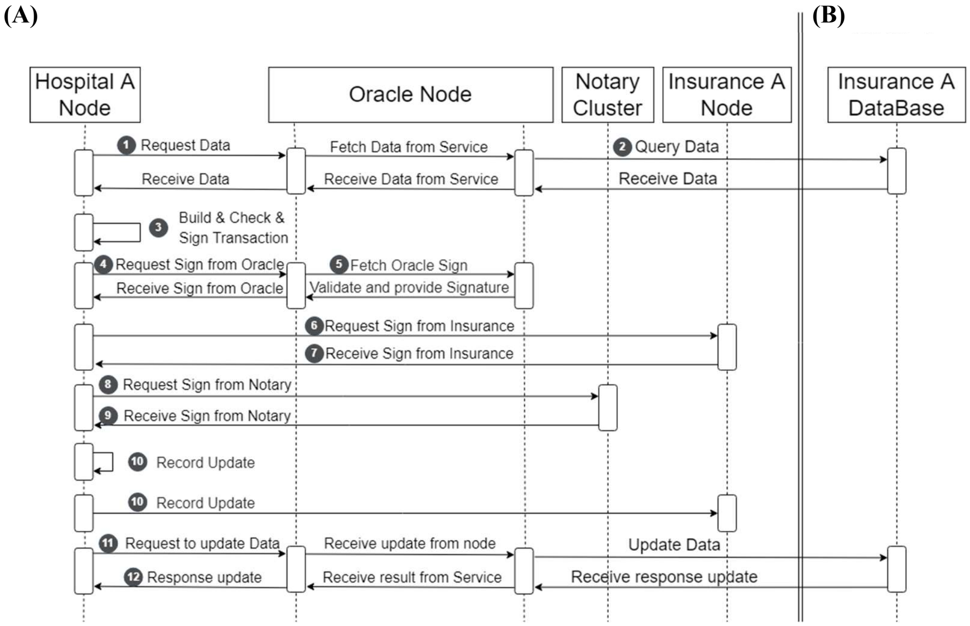

Figure 8 Sequence diagram of the proposed health insurance framework: (A) On-chain and (B) Off-chain.

After successfully updating both on-chain and off-chain data on the Corda nodes and insurance database A, respectively, the patient's claim process has been effectively completed. As a result, the patient is exempt from paying any medical expenses since the treatment condition aligns with the pre-defined health insurance policy within the smart contract on the Corda network. The proposed health insurance framework facilitates automatic claim payments, thereby avoiding the need for patients to wait for confirmation of their health insurance.

For the successful adoption of the blockchain-based health insurance network in a real-world scenario, it is essential to ensure impartiality and fairness in the governance of the proposed system. To achieve this, the Ministry of Public Health can be designated as the regulatory authority responsible for overseeing and managing the system. Regulators would then encompass crucial tasks such as establishing and maintaining the notary cluster and oracle functionalities.

Furthermore, the regulators would be tasked with setting up and maintaining the entire system, including the registration of healthcare providers, both governance hospitals and insurance providers. They would also control the participation of these entities in sharing the relevant facts within the network. By having the Ministry of Public Health as the regulatory body, the system can maintain an unbiased and neutral approach to its operations.

The collaborative efforts of these healthcare providers within the health insurance network would yield several benefits. One significant advantage would be a reduction in the time taken for claims to be processed, resulting in quicker refunds for patients. Additionally, patients would have convenient access to healthcare services provided by the governance hospitals forming part of the network. This collaborative approach would improve the overall healthcare experience for patients, offering streamlined processes and enhanced services.

4. Discussion

The proposed health insurance framework, utilizing R3 Corda and a blockchain oracle, raises several important implications worthy of discussion within the health insurance and healthcare domain. By leveraging blockchain technology's decentralized nature and smart contract capabilities, the framework aims to create a transparent and efficient ecosystem for processing health insurance claims. One notable advantage of the framework is its potential for automating and expediting the claims process, leading to reduced waiting times for customers and prompt reimbursement, thereby enhancing customer satisfaction and fostering trust in the health insurance network.

Furthermore, integrating on-chain and off-chain data addresses the challenges related to sharing sensitive health records while maintaining data privacy and security. The role of the blockchain oracle in securely interacting with off-chain databases ensures selective and secure data sharing among trusted parties, thus safeguarding patients' privacy, and sensitive medical information.

In this work, the centralized blockchain oracle introduces a significant concern, primarily in relation to the increased vulnerability for a single point of failure. In such a scenario, if the blockchain oracle relies on a single centralized service provider, any malfunction or compromise in the oracle's operation could have far-reaching consequences, disrupting the function of the entire system. Consequently, this may lead to delays in processing health insurance claims, thereby impeding the overall efficiency and reliability of the network. To address this issue, it becomes imperative to explore alternative approaches. A potential solution involves implementing a decentralized oracle network or leveraging multiple independent oracle providers. The framework can achieve redundancy and fault tolerance by adopting a decentralized oracle infrastructure.

In addition to the benefits, the adoption of blockchain in the health insurance network holds promise for enhancing fraud detection and prevention mechanisms. The immutability and transparency of blockchain records offer an auditable trail of transactions, facilitating the identification and deterrence of fraudulent activities within the healthcare industry.

Nonetheless, it is important to acknowledge that incorporating blockchain technology into large-scale healthcare networks may encounter scalability challenges due to the substantial volume of data generated and shared daily. Additionally, ensuring interoperability with existing healthcare systems and standards is crucial for a seamless integration process.

5. Conclusion

The increasing demand for trust-preserving data exchange in the healthcare network necessitates novel and improved solutions. This work explores blockchain-based solutions within the insurance claim framework. Utilizing smart contract-based databases and blockchain technology, there is potential to enhance customer satisfaction and reduce the costs involved in revenue data management. Real-time claim records can be securely shared among trusted parties, and the use of smart contracts with an off-chain oracle connector may enable automatic payouts to hospitals based on the parameters set in the original healthcare policies, eliminating the need for an intermediate authority to validate claims from the insurer. The proposed Corda fact-sharing network facilitates the management of smart contracts for multi-party transactions, such as storing the number of claims, automating bundled payments, and controlling data sharing among trusted parties. As a result, this framework aims to improve the overall experience for insurers and patients while simultaneously reducing the associated costs.

6. References

[1] Campbell SM, Roland MO, Buetow SA. Defining quality of care. Soc Sci Med. 2000;51(11):1611-1625.

[2] Liao L, Chen M, Vuong S, Lai X. A novel web-enabled healthcare solution on HealthVault system. In: Chen HH, Daneshmand M, Liu S, editors. The 5th International ICST Conference on Wireless; 2010 Mar 1-3; Singapore. New Jersey: IEEE Xplore; 2010. p. 1-6.

[3] Devadass L, Sekaran SS, Thinakaran R. Cloud computing in healthcare. Int J Students Res Technol Manag. 2017;5(1):21-25.

[4] Jaoude AJ, Saade GR. Blockchain applications-usage in different domains. IEEE Access. 2019;7:45360-45381.

[5] Hölbl M, Kompara M, Kamišalić A, Zlatolas NL. A systematic review of the use of blockchain in healthcare. Symmetry (Basel). 2018;10(10):1-22.

[6] Mendling J, Weber I, Aalst WVD, Brocke JV, Cabanillas C, Daniel F, et al. Blockchains for business process management - challenges and opportunities. ACM Trans Manag Inf Syst. 2018;9(1):1-16.

[7] R3 [Internet]. Corda. [cited 2022 May 10]. Available from: https://docs.r3.com/en/platform/corda.html.

[8] R3 [Internet]. Key concepts of ledger. [cited 2022 May 10]. Available from: https://docs.r3.com.en/platform/corda/4.8/open-source/key-concepts-ledger.html

[9] Agbo C, Mahmoud Q, Eklund J. Blockchain technology in healthcare: a systematic review. Healthcare (Basel). 2019;7(2):1-30.

[10] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. In: Awan I, Younas M, editors. The 2nd International Conference on Open and Big Data (OBD); 2016 Aug 22-24; Vienna, Austria. New Jersey: IEEE Xplore; 2016. p. 25-30.

[11] Aleksieva V, Valchanov H, Huliyan A. Smart contracts based on private and public blockchains for the purpose of insurance services. International Conference Automatics and Informatics (ICAI); 2020 Oct 1-3; Varna: Bulgaria. New Jersey: IEEE Xplore; 2020. p. 1-4.

[12] Saldamli G, Reddy V, Bojja KS, Gururaja MK, Doddaveerappa Y, Tawalbeh L. Health care insurance fraud detection using blockchain. Seventh International Conference on Software Defined Systems (SDS); 2020 Apr 20-23; Paris: France. New Jersey: IEEE Xplore; 2020. p. 145-152.

[13] Huang J, Qi YW, Asghar MR, Meads A, Tu YC. MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data. In: O'Conner L, editor. The 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE); 2019 Aug 5-8; Rotorua, New Zealand. New Jersey: IEEE Xplore; 2019. p. 594-601.

[14] Carlos Marinho SS, Filho JSC, Moreira LO, Machado JC. Using a hybrid approach to data management in relational database and blockchain: a case study on the e-health domain. In: O'Conner L, editor. IEEE International Conference on Software Architecture Companion (ICSA-C); 2020 Mar 16-20; Salvador: Brazil. New Jersey: IEEE Xplore; 2020. p. 114-121.

[15] R3 [Internet]. Key concepts of oracles. [cited 2022 May 5]. Available from: https://docs.r3.com/en.platform/corda/4.8/open-source/key-concepts-oracles.html.

[16] Caldarelli G. Understanding the blockchain oracle problem: a call for action. Information (Basel). 2020;11(11):1-19.

[17] Loukil F, Boukadi K, Hussain R, Abed M. CioSy: a collaborative blockchain-based insurance system. Electronics (Basel). 2021;10(11):1-15.

[18] Radanović I, Likić R. Opportunities for use of blockchain technology in medicine. Appl Health Econ Health Policy. 2018;16(5):583-590.

[19] R3 [Internet]. Key concepts of notaries. [cited 2022 May 10]. Available from: https://docs.r3.com/en/platform/corda/4.8/open-source/key-concepts-notaries.html.