A randomized blockchain consensus algorithm for enhancing security in health insurance

Najah Al-Sarayrah, Nidal Turab, Abdelrahman Hussien
Department of Networks and Cyber Security, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan

Article Info

Article history:

Received Feb 18, 2024
Revised Feb 25, 2024
Accepted Feb 26, 2024

Keywords:

Blockchain
Consensus algorithm
Fraud
Health insurance system
Random consensus algorithm

ABSTRACT

Health insurance fraud is a significant problem affecting insurance providers and policyholders. To address the rising problem of fraudulent activities in the health insurance sector, this paper proposes a pioneering blockchain-based system aimed at increasing transparency and security. Utilizing a hybrid blockchain architecture, the system incorporates a consensus algorithm influenced by practical byzantine fault tolerance (PBFT) and proof of activity (PoA) to ensure reliability and efficiency in distributing mining power. Developed using Python, extensive testing confirms the system's performance and security metrics. Results show that a block size containing one transaction is 1.63 KB, with 1.2 KB for data and 0.43 KB for identification and hashing. Operational tests demonstrate that a single participant can upload 850 transactions to the transaction pool, with validation completed in just 7.49 seconds. Block appending time for these transactions is a swift 10 seconds. Notably, the system exhibits resilience against data tampering, detecting unauthorized changes within 881.3 milliseconds across 10,000 blocks and identifying irregularities in the transaction pool within 8.78 seconds. Additionally, to enhance data privacy, patient information is accessible only through a unique QR code, providing an extra layer of security; this research represents a significant advancement in combatting fraud and safeguarding data privacy.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Nidal Turab
Department of Networks and Cyber Security, Faculty of Information Technology
Al-Ahliyya Amman University
Amman, Jordan
Email: n.turab@ammanu.edu.jo

1. INTRODUCTION

The health insurance industry ensures that individuals and communities access essential healthcare services while mitigating financial burdens. However, this industry faces significant challenges related to security and trust. Data breaches, fraudulent activities, and a lack of transparency threaten health insurance systems' confidentiality, integrity, and effectiveness. Therefore, there is an urgent need to explore innovative solutions to enhance security and address these challenges effectively. Health insurance fraud is a significant problem affecting insurance providers and policyholders. According to the National Health Care Anti-Fraud Association, healthcare fraud costs the United States approximately $300 billion annually [1]. Health insurance fraud includes various activities, such as submitting false claims, providing unnecessary medical services, and stealing identities. These activities result in financial losses and compromise the quality of healthcare services. Blockchain (BC) technology has emerged as a potential solution to prevent health insurance fraud and enhance security. BC is a decentralized and immutable ledger that provides transparency, safety, and traceability; the properties above make BC suitable for enhancing health insurance security.

By utilizing BC technology, it is possible to create a tamper-proof record of all healthcare transactions, which can be accessed and audited by authorized parties [2]. This paper presents a robust framework leveraging BC technology to enhance security in health insurance. It introduces a novel consensus algorithm focused on randomization to bolster system security and scalability. Additionally, smart contracts automate claims management and payment processing, offering potential benefits such as fraud prevention, cost reduction, and improved healthcare service quality.

2. RELATED WORK

Karmakar and colleagues proposed an "Ethereum-blockchain based framework" as well as "smart-contracts" to address the problem of a single point of failure as well as human interference in healthcare, as well as to provide an automated, tamper-resistant, transparent, and expandable system that addresses all of the primary operating blocks in an insurance coverage environment [3]. Dulan and Hannan [4] proposed a representation of medical data combining BC technology and artificial intelligence (AI). The proposed structure was divided into four layers: healthcare participants, BC layers, artificial intelligence layers, and decentralized storage layers. Those four layers work with the smart contract, a crypto contract, to make decisions and preserve accessibility throughout the healthcare system. Ali *et al.* [5] presented a "multi-user-extended -secure searchable encryption (SSE)" that allows parties to inquire about the distributed ledger against desired keyword searches safely. From the outset, the patient protects the information by encryption and uploads it to the BC. Rupa *et al.* [6] suggested knowledge system made up of several parts: clients, specialists, users, expertise engineers, entered agents in addition to expert systems, inference agents, and intelligent agents. Knowledge engineering phases are considered when designing and implementing the suggested decentralized blockchain application (DApp) for official health record production and management. Jain *et al.* [7], proposed architecture for BC innovation in e-health-records (EHR) and safe digital records capabilities by defining precise access controls for the client of the present scheme. The suggested framework had been evaluated with BC for adaptability, security, and other structural support. Kapadiya *et al.* [8] suggested integrating BC with AI to detect and avoid fraud in health insurance; data obtained from wearables and smartphone healthcare apps were used. Omar *et al.* [9] created a smart-contract-based architecture to improve the health service in smart cities to be safer, more trustworthy, and resilient to willful errors. They also used a BC mechanism to boost the model's transparency.

Based on BC, a novel architecture and consensus algorithm are proposed by Alhasan and colleagues in [10] technology to avoid forgery in health insurance by limiting duplication in medicare claims. Used first-in-first-out (FIFO), POW, and POS techniques. Saeedi *et al.* [11] created a BC application the replaced a third-party intermediary previously used to transport original bills between insurance companies and healthcare providers. The second one demonstrated design choices while creating a BC application with references to software architecture-introduced BC application design methodologies. Saldamli *et al.* [12] proposed a blockchain-based approach by combining data with building a system for efficiently administering and tracking insurance activities from all insurance firms to detect health insurance counterfeiting. They used BigChainDB, which is open-source and available through Amazon Web Services (AWS), to develop a distributed database akin to Ethereum. To ensure that the system was working correctly.

Raikwar *et al.* [13] developed a distributed platform that BC can use as a system service to facilitate the execution of transactions in insurance operations. In the imaginary BC network, client C wants a transaction from agent A. The smart contract method and client attributes required for method execution are included in the request, and agent A signs the transaction, which the smart contract signatories also support. After confirming the transaction, agent A presents it to the ordering nodes for chronological ordering. Once the fundamental consensus routine has been completed with all received transactions, the peer nodes append the new records to the BC. Linag and colleagues in [14] proposed a solution to prevent counterfeiting; BC technology has been proposed for shared and integrated patient activities. The Merkle tree was employed in that system's validation to ensure the data was error-free. That system was graded according to the average duration for authenticity proof formation and the time taken for authenticity proof verification. Vian *et al.* [15] proposed an intelligent health profile; that profile offers the groundwork for rethinking how personal health and financial information is accessible across various platforms and applications using BC features such as tokens, wallets, smart contracts, and oracle services.

3. THE PROPOSED SYSTEM

This sectiont demonstrate the functionality of the suggested system. The emphasis will be on the utilization of the random consensus algorithm within the healthcare system, with an in-depth examination of each component comprising the proposed system's layers. Detailed information about each component will be provided.

3.1. System overview and proposed framework for health insurance system

The proposed BC-based framework uses a hybrid BC type and contains four major parts: HIP, HSP, HIS, and MOH. The proposed solution focuses on several objectives, such as increased transparency, security, efficiency, and fraud detection and prevention in health insurance. For security reasons, these transactions are signed and hashed; the data is signed using a private key for the sender to guarantee authentication and prevent generating claims from unknown parties. The proposed framework will be divided into five layers see in Figure 1. The proposed framework for healthcare system security comprises five layers, each fortified with specific techniques to prevent penetration and tampering. If one layer is breached, the next layer applies corresponding techniques, iteratively escalating defense until the fifth and final layer is reached [16]–[19]. Flowchart for proposed system as shown in Figure 2.

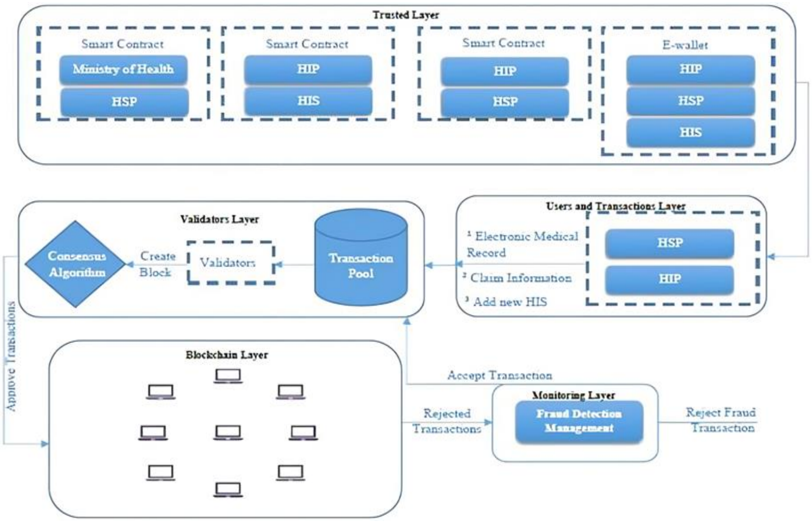


Figure 1. The proposed framework

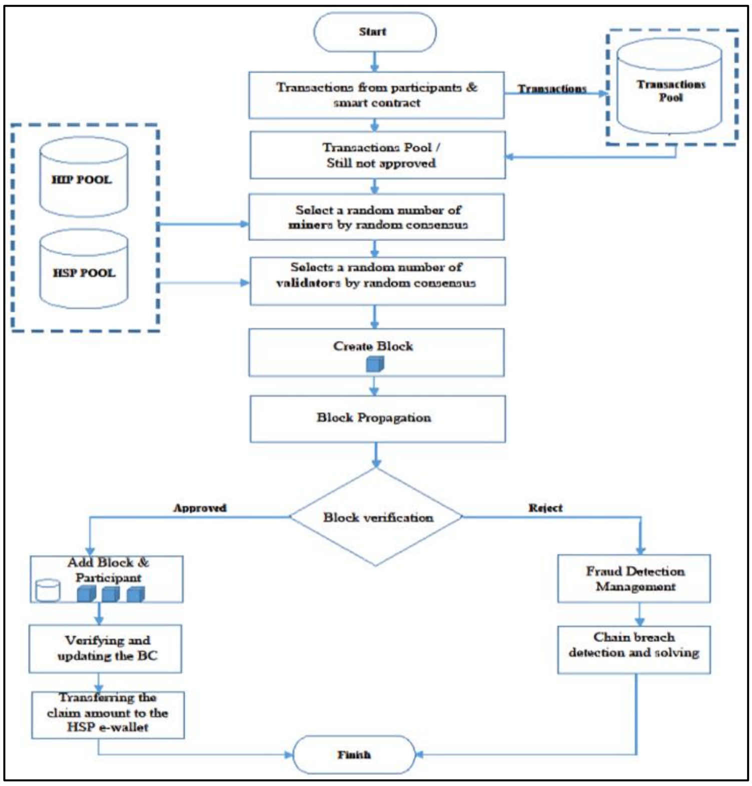

Start
Transactions from participants & smart contract
Transactions
Transactions Pool
Transactions Pool / Still not approved
HIP POOL
HSP POOL
Select a random number of miners by random consensus
Selects a random number of validators by random consensus
Create Block
Block Propagation
Approved
Block verification
Reject
Add Block & Participant
Verifying and updating the BC
Transferring the claim amount to the HSP e-wallet
Fraud Detection Management
Chain breach detection and solving
Finish

Figure 2. Flowchart for proposed system

3.2. The trusted layer

This layer consists of smart contracts and e_wallets that have been built and stored on the BC network, which has thus become a trusted reference for all transactions that will be audited. In addition, it will create a smart contract between each:

- Ministry of health and HSP for approving new HSP.
- Ministry of health and HIP for supporting new HIP.
- HIP and HIS, in which the terms of the contract and the fees per capita for the cost of treatment in and out of the hospital are specified. Also, the percentage of self-pay amount medical examinations and treatment costs is specified. HIP and HSP will decide on the price lists.

Each participant (HIP, HSP, HIS) in the proposed framework creates an e-wallet with a private key and public key; the main objective of this wallet is:

- Transfer the percentage of the self-pay amount from the e-wallet to the HSP and transfer the claim amount from the HIP to the HSP after validating the transaction.
- To avoid sybil attack, where the attacker uses multiple fake identities or nodes on the network to take control and modify the BC's transactions. Here, the contract cost with the insurance company will be transferred when the process is completed, making it difficult for the attacker to request many applications for participation in health insurance because he will directly pay the cost of this contract by activating it.

3.3. Users and transactions layer

The following are the participants of the proposed system:

a. HIP: The insurance companies oversee creating new insurance for patients, create smart contracts with HSP, and participate in creating a new block after validating the transaction in transaction_pool, and validate the created block before broadcasting to the BC network
b. HSP: The health service provider adds the following transaction to the Transactions pool: new transactions about the patient's disease code and the treatment procedures followed:
   - Fill in the medical treatment application (treatment_id, HIS_ID, HSP_ID, HIP_ID, disease code, diagnosis, procedures, medicines, medical examinations, x-rays, timestamp, transactions type).
   - claim for patients (treatment_id, HIS_ID, HSP_ID, HIP_ID, timestamp, transactions type, total amount).

Also, it participates in creating a new block after validating the transaction in transaction_pool and validating the created block before broadcasting to the BC network.

a. HIS: The patient cannot add a new transaction to the transaction_pool or validate a new block created.
b. MOH is responsible for approving new HIP and HSP.

In a public key cryptography system, private and public keys are generated and used to authenticate and verify transactions. The private key is a secret key kept by the owner and used to sign transactions, while the public key is widely known and used to verify the signature. To verify the authenticity of a transaction using a private key, the following steps are typically taken:

a. The sender (HIP or HSP) generates and signs a transaction using their private key.
b. The transaction is there sent to the Transactions Pool.
c. The miners verify the transaction using the sender's public key to decrypt the signature and compare it to the transaction details. If the signature is valid, the transaction is considered authentic.

Using private keys for authentication and verification provides high security in BC systems, as only the private key owner can sign a transaction and prove their identity. This helps to prevent fraudulent transactions and ensures the integrity of the BC ledger.

3.4. Validator's layer

Transaction-pool: a transaction pool is a temporary storage place for awaiting transactions in a BC network; when a HIP and HSP commence a transaction. It is sent to the transaction pool in the ministry of health. The transaction pool is crucial to a BC network's overall security and efficiency. The proposed consensus technique aids nodes in validating new transactions and including them in a block without waiting for confirmation from all nodes in the network by keeping unconfirmed transactions in the transaction pool; this speeds up transaction processing and helps avoid double-spending attacks.

Miners and validators pools: the users in the network are divided into three pools: one for HIS, the second for HIP, and the last one for HSP. The miners and validators in the network choose from the HIP pool and HSP pool see in Figure 3. Consensus algorithm: supply a new consensus algorithm based on randomization for the proposed framework. Randomization is a technique that can be used to improve security in various systems. It adds an element of unpredictability to the system, making it more difficult for attackers to predict or manipulate the outcome of a security process successfully. Randomization can also add variability to system processes, making it more difficult for attackers to detect patterns or weaknesses in the system [20]–[22].

Therefore, this thesis will combine two algorithms to produce a more robust and random algorithm than the earlier two. The PBFT algorithm chooses random miners, and the PoA consensus algorithm chooses random validators [23]–[25]. However, based on this number from user pools, the proposed algorithm will choose the random number first and then the miners and validators. The consensus algorithm is divided into two steps see in Figure 4:

a. The first step selects a random number of miners. If the number is odd, add one, then divide it by two to ensure equality between parties with conflicting aims, the first half of nodes from HIP_Pool and the second half from HSP_Pool.
b. The second step selects a random number of validators. If the number is odd, add one, then divide the number by two to
c. ensure equality between parties with conflicting aims, the first half of nodes from HIP_Pool and the second half from HSP_Pool.

The random number of miners between 2 and (NO of participants in HIP_Pool+ NO of participants in HSP_Pool)/2), because there is no need for more than 50% of participants to share in the mining and validation processes and at least two miners. The random number of validators between 3 and (number of participants in HIP_Pool+ number of participants in HSP_Pool); because the number of nodes allowed in the mining and verification process within the proposed framework is small, it may not exceed 100 nodes; there is no problem that all nodes take part in the verification process. Therefore, the number of participating nodes ranges from three to the total number of nodes.

The pre-selected “Miners” will confirm the transactions in the “pool transaction” before adding them to the BC network and creating an entirely new block on the BC network with the secured transactions. The validation procedure will include the following steps:

- Verifying the existence of a valid contract between the HSP and the patient’s HIP. Verifying the existence of a valid contract between the HIS and the patient’s HIP.
- A unique number is given for each treatment process (treatment_id), and all treatment procedures are entered and used to decide the number of treatment times allowed for each insured.
- Hash function: each block in the chain will be given a unique identification. Before adding a block to the chain, it will be contented and hashed using a cryptographic hash function, such as SHA-256, in the proposed approach.
- Add block: the miners collect the accepted transactions in a block and connect this block with the earlier block by the earlier hash to add to the chain.
- Add participant information from smart contract transactions to the specific pool.
- Block propagation: after adding this block to the chain, the miner broadcasts this block to all Participants to validate the created block, then adds it to their distributed ledger to ensure synchronization.
- Block verification: each node from the preselected in steps 1 and 2 from the consensus algorithm verifies the validity of the newly created block. This includes checking that all the transactions in the block are valid and that the block was created according to the rules of the BC.

3.5. BC layer

BC layer will verify and update the BC; once a new block has been added to the BC, nodes in the network will verify its validity and update their copy of the BC accordingly. Nodes will also check to ensure the new block references the correct earlier block in the chain.

- The consensus process ensures that all nodes in the network have an up-to-date and correct copy of the BC, which helps to ensure the" security and integrity” of the network.
- After that, the percentage of the patient’s Self-Pay amount is transferred from his e-wallet to the HSP, and the claim amount from the HIP to the HSP.
- Add a new block created to the BC network.
- Once a block is added to the BC, it becomes a permanent part of the ledger, and its contents cannot be altered without changing all earlier blocks. This makes the BC highly secure and resistant to tampering.

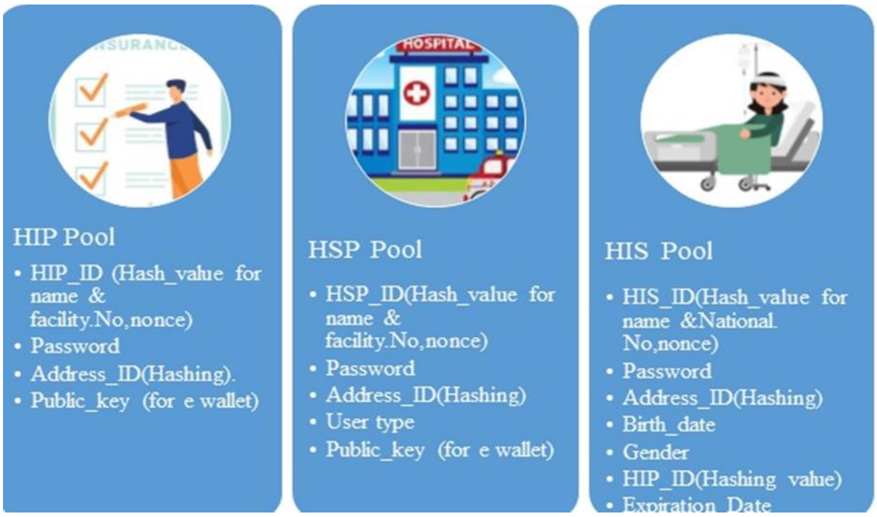


Figure 3. Participants' pool structure

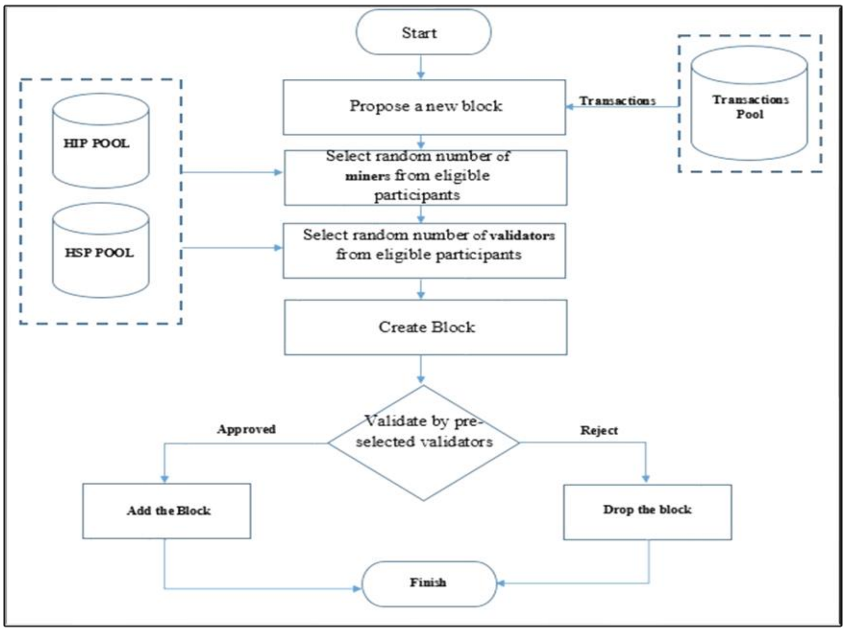

Start
Propose a new block
Transactions
Transactions Pool
HIP POOL
HSP POOL
Select random number of miners from eligible participants
Select random number of validators from eligible participants
Create Block
Validate by pre-selected validators
Approved
Reject
Add the Block
Drop the block
Finish

Figure 4. Proposed consensus algorithm

3.6. Monitoring layer

Responsible for chain breach detection and solving; to know if splits happened in the chain, then solve the problem by adopting the longest branch from the chain, and any transactions on the other branch are considered invalid, and nodes will stop adding new blocks to it. The transactions in the discarded branch will be returned to the transaction pool, and validators must resend transactions to be included in the new valid chain. On the other hand, if the transaction is not valid after the validation process, it is sent to the fraud detection management (FDM) at MOH.

3.7. Transaction structure

Indeed, the transactions in the blockchain system for health insurance will encompass critical data about patient information, healthcare service details, and financial aspects. This data will include unique identifiers for transactions and individuals, relevant medical diagnosis and treatment information, and comprehensive financial breakdowns of the associated healthcare costs. The structure of transactions in our suggested system is illustrated in Figure 5.

3.8. Block structure

In the proposed framework, as depicted in Figure 6, each block is uniquely identified by a block ID. The timestamp indicates the moment the block was initially generated, while the 'previous hash' refers to the hash code of the preceding block. The 'transactions' serve as the data within the block. The current block's hash code is represented by 'hash,' and the ID of the stakeholder who created the block is denoted by 'creator ID.' The 'signature' is also derived from hashing the creator's keys.

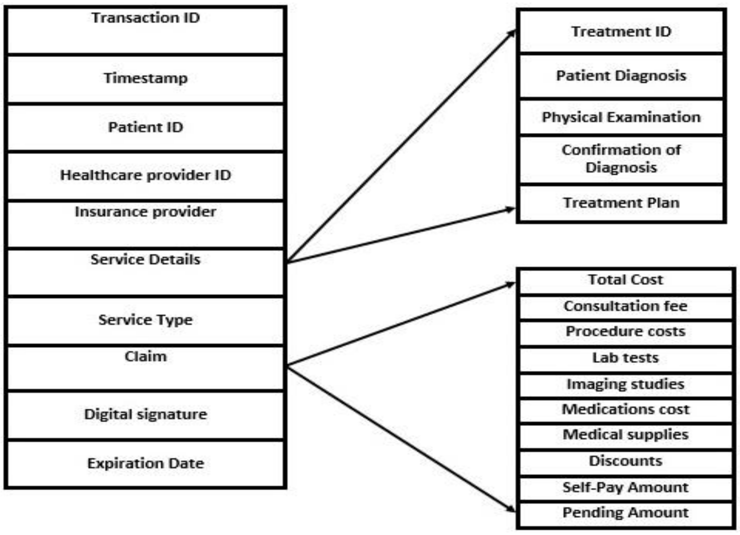


Figure 5. Transaction structure

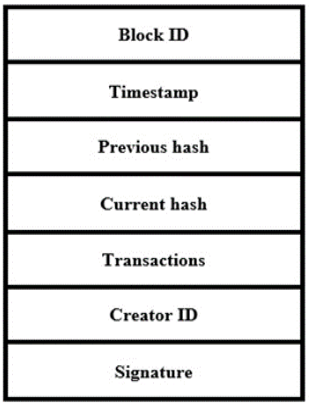


Figure 6. Block structure

4. RESULTS AND DISCUSSION

4.1. Block structure analysis

The block's dimensions are contingent upon the quantity of transactions housed within each block, denoted as Transactions_Pool. Every vested party is tasked with crafting a block containing numerous transactions. Represented as a JSON entity. The magnitude of a block housing a solitary transaction, with Transactions_Pool set to one, amounts to 1.63 KB, as demonstrated in Table 1. In contrast, a block comprising five transactions spans 6.46 KB, signifying an augmentation of almost 1.2 KB per transaction, accompanied by 0.43 KB designated for block identification and hashing particulars.

Table 1. Number of transactions T_POOL and block size relationship

Number of transactions	Block size (KB)
1	1.63
5	6.46
10	12.4
20	24.4
40	48.4

4.2. Transactions upload time into the transactions pool with validation time

The validation process on the blockchain verifies transactions for their validity. Increasing transaction count leads to longer verification times, but results show efficient validation, with the optimal block size being 850 transactions. The duration needed for this verification is graphically represented in Figure 7. Another experiment shows all four nodes uploading transactions successfully, with variations in upload times due to node complexities, indicating overall efficient system performance. Figure 8 illustrates differences in the upload times between the nodes.

4.3. The time needed to append block into BC

The experiment mined blocks with varying transaction numbers from a Kaggle dataset to calculate throughput. Four nodes were used consistently across experiments. The results, as shown in Figure 9, show that as the block size increases, the time to reach consensus also increases, influenced by the consensus algorithm's dependency on network response messages and throughput.

4.4. Data integrity test

The system ensures data integrity by detecting unauthorized changes in transactions and the distributed ledger. It introduces a novel framework and consensus algorithm tailored for fraud prevention in healthcare insurance. Through blockchain technology, data transparency and security are enhanced across healthcare entities. Rigorous evaluations against data manipulation attacks confirm the system's integrity. As demonstrated in Figure 10, tampering was detected within just 881.3 milliseconds for a chain of 10,000 blocks. Figure 11 showcases the transaction pool monitoring system's efficacy in a blockchain network, detailing detection rates and processing times for different transaction volumes. The system consistently detects and terminates malicious transactions, maintaining high performance as transaction numbers increase. Detection times scale linearly with transaction volume, demonstrating scalability.

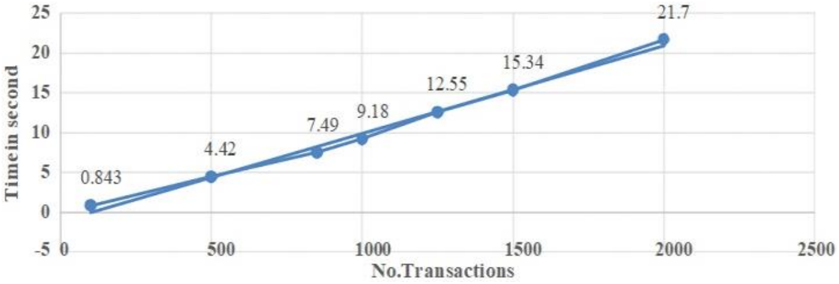


Figure 7. Upload transactions into transaction-pool with validation time

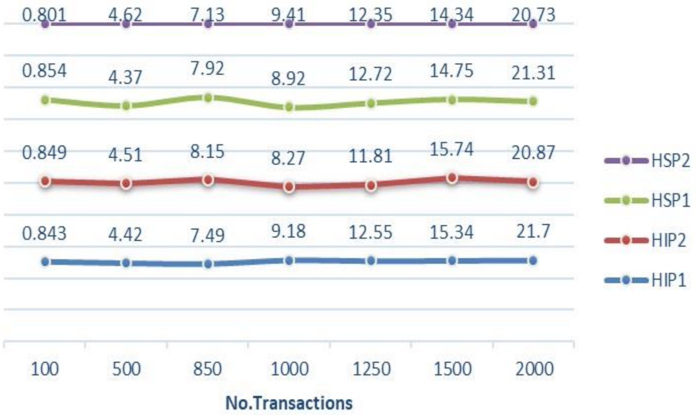


Figure 8. Time in seconds needed to upload transactions

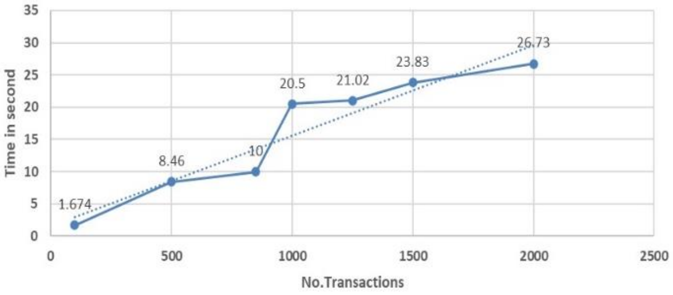


Figure 9. The time needed to append block into BC

4.5. Response time for a read patient's medical history records

Users access a patient's medical history by scanning a QR code and entering the patient's ID. The system searches the blockchain to compile a detailed report, including transaction records, a creator's signature, and a report hash for digital integrity. Experiments with various blockchain sizes, as shown in Figure 12, show that as the blockchain grows, the time to retrieve a patient's history increases. Local machine capabilities, such as CPU and memory usage, also influence response time.

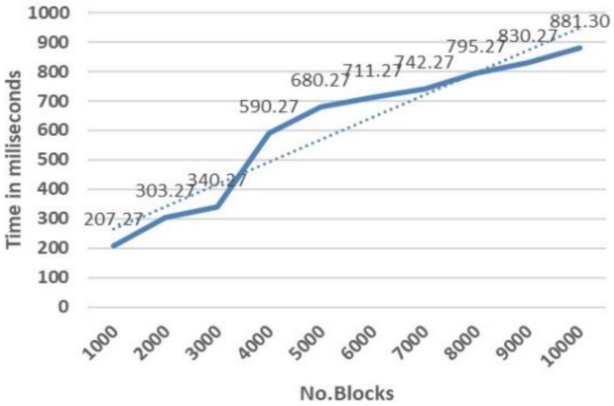
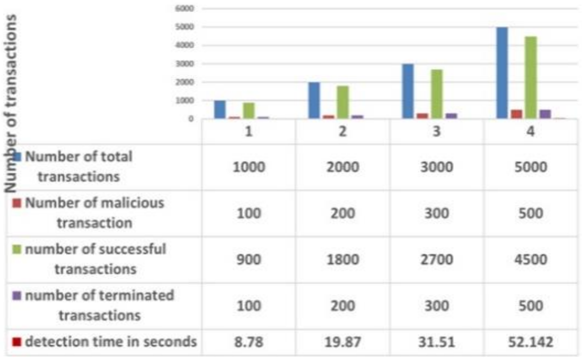


Figure 10. The time needed to detect attacks on BC



	1	2	3	4
🟦 Number of total transactions	1000	2000	3000	5000
🟥 Number of malicious transaction	100	200	300	500
🟩 number of successful transactions	900	1800	2700	4500
🟪 number of terminated transactions	100	200	300	500
🟥 detection time in seconds	8.78	19.87	31.51	52.142

Figure 11. The time needed to detect attacks on the transactions pool

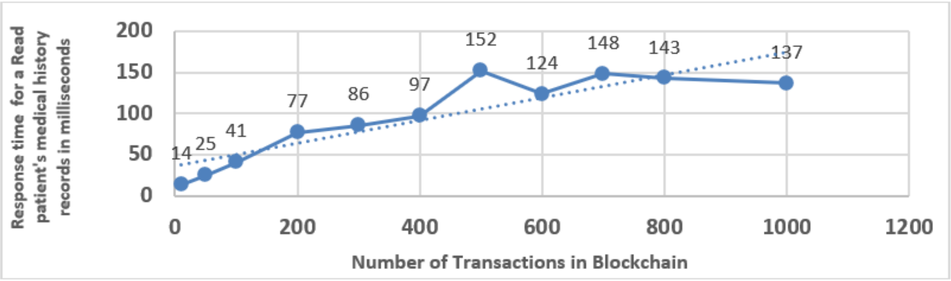


Figure 12. Relationship between BC size and time required for read response

5. CONCLUSION

This paper presents a secure and efficient health insurance data management system leveraging BC technology to combat fraudulent activities in the sector. The proposed system integrates a hybrid BC architecture with a consensus algorithm inspired by PBFT and PoA, ensuring equitable mining power distribution. Extensive testing confirms the system's efficiency, latency, security, and privacy, demonstrating robustness through various experiments. Utilizing QR codes and advanced security measures like SHA-256 hashing algorithms and digital signatures enhances data security. The system's novel consensus algorithm surpasses traditional approaches in power consumption and efficiency. Overall, this research offers a pioneering blockchain-based solution tailored for the health insurance sector, validated through empirical data, marking a significant step in combating fraud and ensuring data security and privacy in healthcare.

REFERENCES

[1] C. A. I. Fraud, "Insurance fraud costs the U . S . $ 308 . 6 Billion Annually," 2022. https://www.conroysimberg.com/blog/insurance-fraud-costs-the-u-s-308-billion-annually/ (accessed Apr. 29, 2023).

[2] J. Golosova and A. Romanovs, "Overview of the blockchain technology cases," *59th International Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2018 - Proceedings*, 2018, doi: 10.1109/ITMS.2018.8552978.

[3] A. Karmakar, P. Ghosh, P. S. Banerjee, and D. De, "ChainSure: agent free insurance system using blockchain for healthcare 4.0," *Intelligent Systems with Applications*, vol. 17, p. 200177, Feb. 2023, doi: 10.1016/j.iswa.2023.200177.

[4] J. Dulan and S. A. Hannan, "Challenges of blockchain technology using artificial intelligence in healthcare system," *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET) | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal* | ||, vol. 12, no. 1, p. 64, 2023, doi: 10.15680/IJIRSET.2023.1201010.

[5] A. Ali *et al.*, "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: a novel approach to cryptography," *Sensors*, vol. 22, no. 2, 2022, doi: 10.3390/s22020528.

[6] C. Rupa, D. MidhunChakkarvarthy, R. Patan, A. B. Prakash, and G. G. S. Pradeep, "Knowledge engineering–based DApp using blockchain technology for protract medical certificates privacy," *IET Communications*, vol. 16, no. 15, pp. 1853–1864, 2022, doi: 10.1049/cmu2.12439.

[7] M. Jain, D. Pandey, and K. K. Sharma, "A granular access-based blockchain system to prevent fraudulent activities in medical health records," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 106, pp. 635–645, 2022, doi: 10.1007/978-981-16-8403-6_58.

[8] K. Kapadiya *et al.*, "Blockchain and ai-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects," *IEEE Access*, vol. 10, pp. 79606–79627, 2022, doi: 10.1109/ACCESS.2022.3194569.

[9] A. Al Omar *et al.*, "A transparent and privacy-preserving healthcare platform with novel smart contract for smart cities," *IEEE Access*, vol. 9, pp. 90738–90749, 2021, doi: 10.1109/ACCESS.2021.3089601.

[10] B. Alhasan, M. Qatawneh, and W. Almobaideen, "Blockchain technology for preventing counterfeit in health insurance," *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, pp. 935–941, 2021, doi: 10.1109/ICIT52682.2021.9491664.

[11] K. Saeedi *et al.*, "Building a blockchain application: a show case for healthcare providers and insurance companies," *Advances in Intelligent Systems and Computing*, vol. 1069, pp. 785–801, 2020, doi: 10.1007/978-3-030-32520-6_57.

[12] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, and L. Tawalbeh, "Health care insurance fraud detection using blockchain," *2020 7th International Conference on Software Defined Systems, SDS 2020*, pp. 145–152, 2020, doi: 10.1109/SDS49854.2020.9143900.

[13] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K. Y. Lam, "A blockchain framework for insurance processes," *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, vol. 2018-January, pp. 1–4, 2018, doi: 10.1109/NTMS.2018.8328731.

[14] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, vol. 2017-October, pp. 1–5, 2017, doi: 10.1109/PIMRC.2017.8292361.

[15] K. Vian, A. Voto, and K. Haynes-Sanstead, "Institute for the future a blockchain profile for medicaid applicants and recipients institute for the future blockchain futures lab 1," *Institute for the Future August 8*, pp. 1–10, 2016, [Online]. Available: http://www.iftf.org/blockchainfutureslab/.

[16] M. D. Markee, C. Ascencio, L. Brugger, R. Jonas, and H. Matsuo, "Perceptions of the healthcare system among stakeholders," *Patient Experience Journal*, vol. 8, no. 3, pp. 79–87, 2021, doi: 10.35680/2372-0247.1561.

[17] J. B. Barber, K. E. Koch, D. Parente, J. Mark, and K. M. Davis, "Evolution of an integrated health system: a life cycle framework," *Journal of Healthcare Management*, vol. 43, no. 4, pp. 359–377, 1998, doi: 10.1097/00115514-199807000-00011.

[18] H. Rosery and T. Schönfelder, "Healthcare system stakeholders," *White Paper on Joint Replacement: Status of Hip and Knee Arthroplasty Care in Germany*, pp. 91–104, 2017, doi: 10.1007/978-3-662-55918-5_4.

[19] T. M. Cheung, "A conceptual framework of defence innovation," *Journal of Strategic Studies*, vol. 44, no. 6, pp. 775–801, 2021, doi: 10.1080/01402390.2021.1939689.

[20] V. Sudha and R. Kalaiselvi, "A survey on slight barriers to using blockchain in healthcare," *Sustainable Digital Technologies for Smart Cities: Healthcare, Communication, and Transportation*, pp. 207–212, 2023, doi: 10.1201/9781003307716-20.

[21] P. D. F. Pdf, "Network security private communication in a public world pdf.pdf," *Pearson Education India*, pp. 1–4, 2012.

[22] G. M. Perez, S. Tiwari, M. C. Trivedi, and K. K. Mishra, "Ambient communications and computer systems: RACCCS 2017," *Springer*, 2018.

[23] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, "Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning," *Journal of Network and Computer Applications*, vol. 224, 2024, doi: 10.1016/j.jnca.2024.103834.

[24] M. U. Tariq, "Revolutionizing health data management with blockchain technology," pp. 153–175, 2024, doi: 10.4018/979-8-3693-1214-8.ch008.

[25] R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, "Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 1, 2024, doi: 10.1002/ett.4884.

BIOGRAPHIES OF AUTHORS

Najah AL-Sarayrah received her B.Sc. In E Bachelor's in Computer Information Systems from Mutah University in 2018. Received her M.Sc. student at Cyber Security, Al-Ahliyya Amman University, Jordan. She can be contacted by email at nsarayrah@ssc.gov.jo.

Nidal Turab Ph.D. in computer science Professor at the Networks and Cyber Security Department, Al-Ahliyya Amman University, Jordan. His research interests include WLAN security, computer networks security and cloud computing security, e-learning, and IoT. He can be contacted by this email: N.turab@ammanu.edu.jo.

Abdelrahman Hussein Ph.D. in computer science Professor at the Networks and Cyber Security Department, Al-Ahliyya Amman University, Jordan. His research interests include mobile ad-hoc networks, database management system, wireless networking. He can be contacted at email: a.husein@ammanu.edu.jo.