Biomedical Signal Processing and Control 102 (2025) 107411

Contents lists available at ScienceDirect

Biomedical Signal Processing and Control

journal homepage: www.elsevier.com/locate/bspc

Lightweight blockchain mechanism for secure data transmission in healthcare system

Murari Kumar Singh [a,b,*], Sanjeev Kumar Pippal [c], Vishnu Sharma [d]

[a] Department of CSE, Dr. APJ Abdul Kalam Technical University, Lucknow, U.P, India
[b] SET, Sharda University, Greater Noida, U.P, India
[c] GL Bajaj Institute of Technology and Management, Greater Noida, U.P, India
[d] Department of CSE, ITS College of Engineering, Greater Noida, U.P., India

ARTICLE INFO

Keywords:
Blockchain
Healthcare networks
Lightweight proof of hybrid security-based minor solutions
Consensus algorithms
Remote healthcare monitoring

ABSTRACT

Healthcare Network refers to the interconnected IoT devices that are involved in exchanging medical information through different entities, like providers, patients, and devices. Medical information is significantly important, as it describes the person's medical conditions. However, storing and retrieving the medical-related information in the network system results ina complex task. Different existing models are introduced to provide security in the network system, but yet it faces different issues, like data security and privacy, interoperability issues, data integrity concerns, scalability limitations, regulatory compliance requirements, and difficulties in managing data access and control. To overcome these issues, and to securely store data in the provider, a lightweight proof of hybrid security-based minor solution is designed for Healthcare Networking Systems in which an optimized consensus algorithm is designed for data management in healthcare systems. The proposed model is designed in a blockchain framework, where the security protocol is adopted to transfer the information securely by preventing the threads from stealing the data. This algorithm integrates elements of both Proof of Work (PoW) and Proof of Stake (PoS) to achieve a balance between computational efficiency, security, and decentralization. The proposed solution provides seamless communication and efficient access to medical data across diverse healthcare entities, ultimately enhancing patient care outcomes and healthcare system efficiency. The proposed model achieved higher performance by considering the metrics, like gas usage, memory usage, receiving time, sending time, and transaction latency with the value of 0.69, 712.92Kbps, 0.56 ms, 0.61 ms, and 0.50msrespectively.

1. Introduction

The use of Electronic Health Records (EHRs) allows for easy and secure storage of patient's diagnostic and treatment information, leading to more efficient and coordinated care. Specifically,EHR comprises the complete health information of the patients such as medical image, health analysis, and medical records [1]. By securely sharing electronic information, EHRs ensure accurate and up-to-date patient records are accessible at the point of care [2-5]. Blockchain technology in healthcare provides a decentralized and secure way to maintain records of network devices, allowing for the identification of critical errors in the medical field [6]. This technology enhances performance, security, and transparency in the sharing of medical data among healthcare institutions. This technology is widely applied in numerous applications, such as managing patient records, drug supply systems, medical insurance, clinical trials, equipment usage and supply, medical board approvals, and government monitoring systems [7].

The utilization of this framework allows for examination, understanding, safe transfer, and prompt delivery of information to patients and physicians. Furthermore, these records have advantages for future examination and subsequent medical care. By merging traditional healthcare systems with decentralized blockchain technology, the problems concerning security, privacy, and reliability in IoT are successfully solved [8,10]. To protect their privacy and harness the benefits of blockchain technology, organizations can adopt the Proof of Authority model. The incorporation guarantees that medical information maintains its trustworthiness and reliability, offering a secure and accessible platform for managing electronic health records in a way that

* Corresponding author at: Department of CSE, Dr. APJ Abdul Kalam Technical University, Lucknow, U.P, India and SET, Sharda University, Greater Noida, U.P, India.
E-mail addresses: mksinghjamia@gmail.com (M.K. Singh), sanpippalin@gmail.com (S.K. Pippal), vishnu.sharma@its.edu.in (V. Sharma).

https://doi.org/10.1016/j.bspc.2024.107411
Received 27 February 2024; Received in revised form 22 October 2024; Accepted 17 December 2024
Available online 24 December 2024

is efficient and dependable. Proof of authority (PoA) is a consensus algorithm in blockchain networks that offers an effective and efficient solution for ensuring data privacy [9]. The PoA algorithm relies on the trustworthiness of subjectively selected nodes, utilizing their identities to enforce security. This algorithm is highly scalable as it depends on a limited number of validators who verify blocks and transactions, acting as moderators of the system [7].

Traditional gathering, processing, and storage of EHR used various centralized approaches that pose numerous risks and lean schemes compromise the availability of data towards the amount of information breaches[40].To securely share medical data between organizations, Attribute-based Encryption (ABE) technology is employed to encrypt electronic health records (EHRs) and store them in cloud-based systems. More specifically, CP-ABE is a suitable approach for overseeing data access [11,12]. In CP-ABE, the encryption process associates the cipher text with an access control structure, while users' private keys are linked to attribute sets during the creation of secret keys. While these encryption techniques provide explicit control over EHR access, cloud servers are generally moderately trusted and may either perform actions on behalf of users or have a vested interest in their personal information. Hence, if the cloud servers are susceptible to specific attacks or lack proper supervision, the integrity of the EHRs may be compromised, manipulated, or obliterated [13,14,15].

Practical Byzantine Fault Tolerance (PBFT) is commonly utilized in most healthcare applications based on blockchain. Nevertheless, certain aspects of PBFT consensus require enhancement. These include the need to ensure the dependability of participating nodes, penalize malicious nodes, improve scalability, and minimize frequent network communication [16,17]. One approach to address these concerns is to utilize a Verifiable Random Function (VRF), a pseudo-random function commonly applied in different blockchain consensus algorithms such as DPoS and PoS, to assign nodes for consensus tasks [18]. Although VRF enhances network security by randomly selecting nodes, there may still be instances where the reliability of the chosen nodes cannot be assured. The application of blockchain technology can be effectively employed in IoT. Nevertheless, traditional blockchain algorithms for consensus formation are unsuitable for IoT devices due to their resource-intensive nature, which conflicts with the limited resources of IoT devices [19]. Additionally, scalability and efficiency are crucial factors for IoT systems, but blockchain consensus creates a hindrance to achieving these goals [20,21]. This consensus mechanism plays a vital role in ensuring the proper functioning of a blockchain and guaranteeing uniform adoption of the blockchain by everyone [22,23]. It is imperative for every transaction to undergo scrutiny and for every node to audit the blockchain when adding new items to it. In the absence of effective consensus mechanisms, blockchain become susceptible to various attacks [24,25].

This research designs a security protocol in blockchain framework for effective data transmission in a secure way. The IoT nodes placed in the network environment collect input data, which is the ECG signal that is transmitted to the organization through the blockchain framework. To transfer the data securely it is mandatory to design a secure routing protocol in blockchain that enables the user to send and receive the data securely. A lightweight protocol is designed in this research that merges POW and PoS mechanisms to enhance security and efficiency in healthcare data management systems. By integrating lightweight cryptographic protocols and smart contracts, the solution ensures transparent data sharing while preserving integrity and confidentiality. Addressing scalability challenges, it facilitates seamless communication and access to medical data, thereby improving patient care and healthcare system efficiency.

- ***Lightweight Proof of Hybrid Security-based Minor Solutions:*** A lightweight proof of hybrid security-based minor solutions represents a groundbreaking advancement in the field of blockchain technology. The benefit of using this model is that it integrates trust factor calculation with a hybrid consensus model combining PoW and PoS, presenting a comprehensive solution to the pressing challenges faced by blockchain networks. It effectively balances the computation efficiency and solves the computational complexity issues. Furthermore, the fusion of PoW and PoS mechanisms not only fortifies security but also introduces powerful incentives for active participation in the network, fostering a more robust and decentralized blockchain ecosystem.

The manuscript demonstrates a remarkable structure, with Section 2 solely focusing on ongoing projects and providing detailed information about their strategies and challenges. Section 3 explores the effective strategy for Lightweight blockchain consensus mechanisms in healthcare systems. Finally, Section 4 shows the results of the proposed method. Ultimately, Section 5 offers a concise overview of the research.

2. Motivation

The motivation behind researching a secure consensus algorithm based on blockchain with scalability for healthcare systems stems from the urgent need to enhance data security, privacy, and efficiency in managing sensitive patient information. A blockchain framework is introduced in the mechanism to allow secure data transfer with encryption and decryption in the healthcare system. It provides features like encryption, immutability, and transparent data sharing, healthcare systems can ensure the integrity of medical records while improving interoperability and reducing administrative overhead. Scalability is essential to accommodate the increasing volume of healthcare data and ensure the system's ability to handle future growth [41]. Ultimately, this research aims to foster trust among patients and healthcare providers, streamline processes, and reduce costs, thereby advancing the effectiveness and affordability of healthcare delivery.

2.1. Literature review

A wearable kidney system was developed by Daniel-Jesus Munoz et al. [2] incorporating Healthcare 4.0 processes and utilizing blockchain technology. This integration allows for simplified regulation and monitoring of artificial medical automated body parts. They conducted statistical analysis to demonstrate the minimal risk of a majority attack in this system. Additional research is required to completely evaluate the incorporation of blockchain technology into Healthcare 4.0 operations. Zou, R. et al. [26] suggested SPChain, a blockchain-based medical data sharing and privacy-preserving eHealth scheme to attain safe information transmission and recovery confidentially. SPChain confidentially accomplished medical information transmission through the proxy re-encryption systems. The suggested method reached high throughput with low overhead of storage and achieved minimum complexity of time. However, the SPChain required more computations to gather the scores of reputation and the communication overhead of patients was high. Pawan Hegde and Praveen Kumar Reddy Maddikunta [27] introduced a new e-health system that aims to improve patient care and advance disease treatments by securely sharing data in a collaborative and scalable manner. The system achieves improved performance by eliminating malicious nodes while maintaining overall security. However, the system still requires testing in a real-time environment to ensure its effectiveness in actual transactions. Similarly, Zhen Pang [28] proposed a patient-controlled method utilizing both cloud computing and blockchain technology to facilitate the sharing of Electronic Health Records. Experimental findings showed that the proposed algorithm had superior handling capabilities and reduced consensus latency. Nevertheless, there is still room for improvement in the consensus algorithm that was proposed.

Yaroslav Meshcharya Kov [5] examines the potential use of blockchain technology for safeguarding data from IoT devices that have restrictions. The investigation primarily concentrated on identifying a

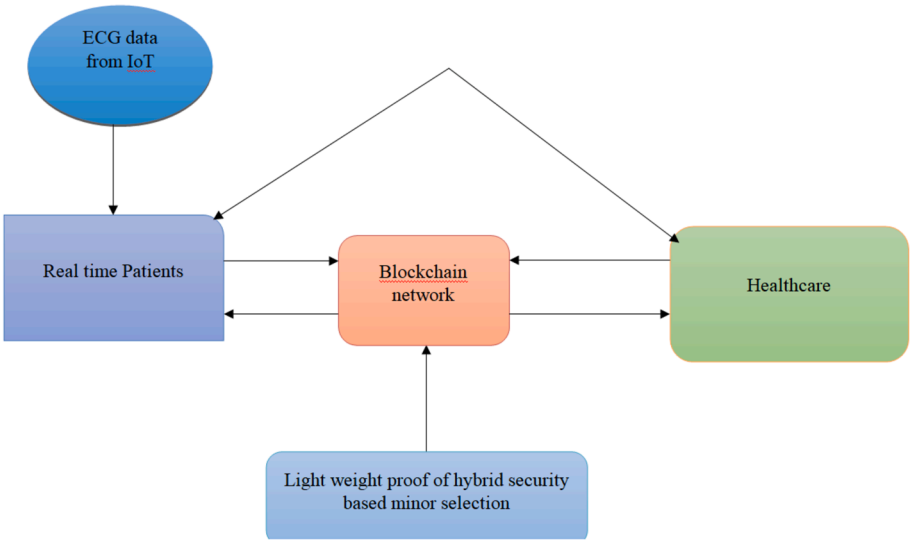


Fig. 1. Architecture of proposed Lightweight blockchain security model.

consensus algorithm that can be effectively utilized on these devices. To fully evaluate the findings, a network infrastructure using real-constrained devices was implemented during the research. The analysis focused on establishing the correlation between the number of blocks committed, block size, data generation interval, and latency in processing data packets. Alaa Awad Abdellatif [29] presented a groundbreaking e-health system designed to establish effective and cooperative platforms for providing exceptional patient care and enhancing disease treatments by securely exchanging data. The system guarantees prompt responses, adaptability, and secure transfer of medical information. However, it is important to improve certain aspects of blockchain, such as the size of blocks, the size of transactions, and the number of blockchain channels. Nafiz Al Azad [30] presented a technology that allows for permissioned data sharing in healthcare while ensuring privacy and control for data owners. The system aims to maintain interoperability, privacy, and security by using a decentralized and secure Health Information Sharing system. However, there are still challenges in implementing this system. On the other hand, Partha Pratim Ray [31] presented an improved IoT-based blockchain framework called IoB Health for managing e-healthcare EHR data. This framework provides a higher level of trust, security, transparency, and efficiency, resulting in reduced maintenance expenses, enhanced compatibility, widespread accessibility, and strong credibility. Despite these benefits, there are still complexities to address during the implementation of this model.Abbas, A. et al. [32] introduced a blockchain-assisted secure data management framework (BSDMF) to securely transmit patient's medical information and to improve the scalability and information availability. The suggested BSDMF offered safe information handling among the implantable medical systems and private servers and between the server of cloud and personal. The developed BSDMF approach achieved a low response and delay ratio. However, the BSDMF achieved a low accuracy rate that limited the performance. Lee, J.S. et al. [1] introduced Medical blockchain, which combined the concept of smart contract and blockchain to construct a medical data-sharing system. The immutableness and secrecy of blockchain were utilized to protect the privacy of the patients and retain the exact health information of the patients. The suggested Medical blockchain approach resisted the attack of potential internet through the replicated formal authentication. Therefore, there was no data leakage occurred, however, Medical blockchain was not feasible for managing the information.

The drawbacks faced by the existing methods are focused on and solved by employing a security framework in the blockchain network. The blockchain provides a secure framework in the network scenario by employing a security mechanism to encrypt and decrypt the credentials. It allows authorized users to access the data efficiently by accomplishing the trust factors. The complexity of handling electronic health records is optimally solved through the incorporation of a hybrid mechanism that allows to exchange the of information between IoT-simulated nodes and healthcare providers in s secure way.

2.2. *Challenges*

- Due to the increasing time needed for consensus to reach the node that is broadcasted in the network, this system faces issues in transaction rate [31]
- The limited computational power, resources, and storage capacity of IoT devices powered by batteries create numerous challenges when combining blockchain with IoT [27].
- To add or remove the credentials of users dynamically from the service provider in this network poses a critical task, and it failed to consider any security mechanism for data transmission [28].

3. Proposed lightweight proof of hybrid security based minor selection model in the healthcare system

This research intends to design a security framework to enhance the effectiveness of Lightweight blockchain consensus mechanisms within healthcare systems. However, the proposed model works based on bolstering security, privacy, scalability, and interoperability. The ultimate aim is to guarantee a dependable Blockchain network and foster trust within a distributed computing environment, even among unfamiliar participants. The initial stage involves using ECG signal data collected from IoT as input in real-time patient data. The integration of this data with the hospital's electronic health records allows for the use of extensive data streams to enhance patient health by employing algorithms and making informed decisions. To access patient-related data, real-time patients send a request to the blockchain network. The patient data then goes through a chain of blocks and access is granted. These data are stored on the blockchain for future reference. An important aspect of the healthcare system is the Multimodal Encrypted Authentication Scheme. This scheme enhances security during the transmission and reception of information between patients and healthcare professionals. In the healthcare industry, the incorporation of blockchain technology guarantees the implementation of enhanced security measures by healthcare professionals and doctors. By encrypting patient data and facilitating secure privacy, safety, and accessibility of

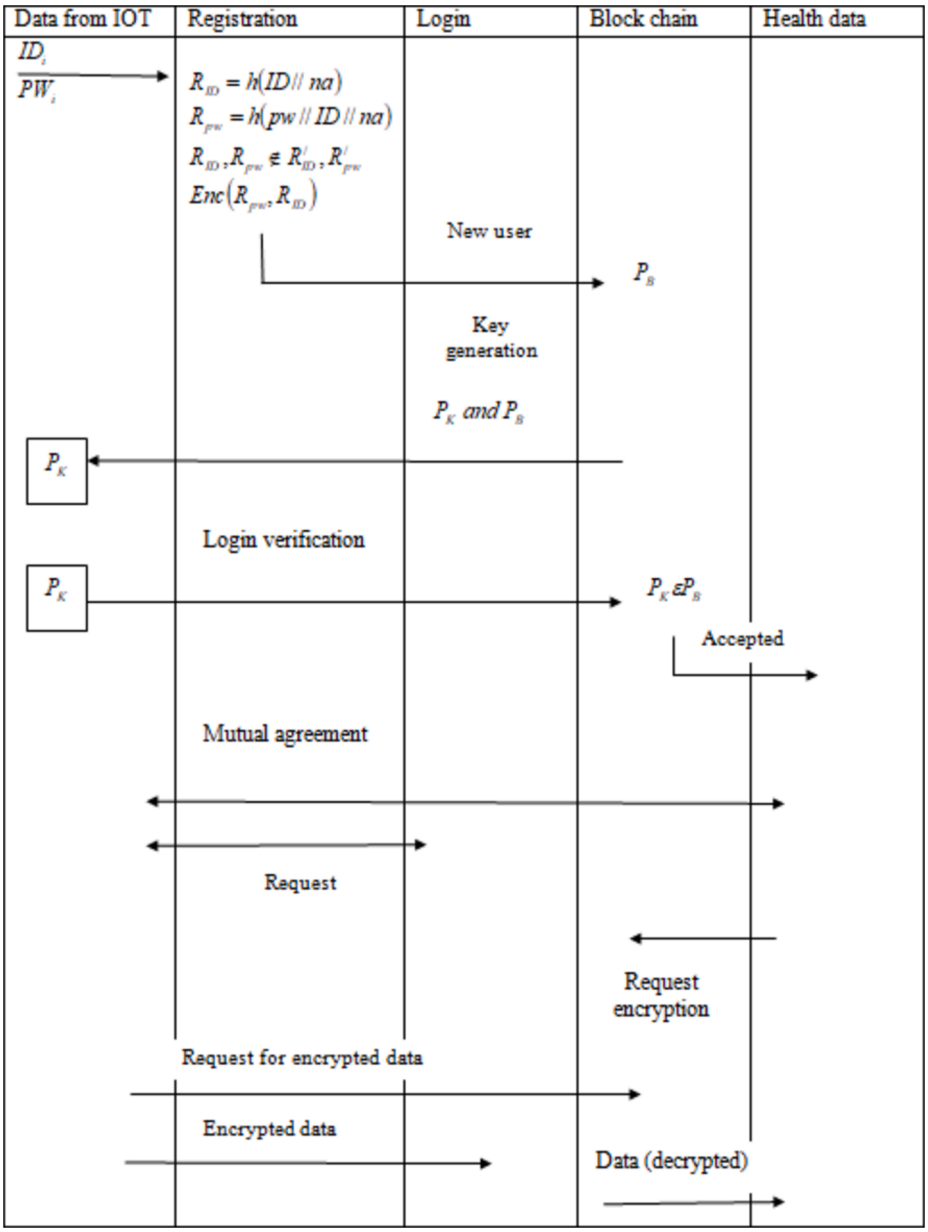


Fig. 2. Illustrative representation of the registration and the login phase.

electronic health record (EHR) information, blockchain technology safeguards the protection of sensitive healthcare data. The encrypted data is then sent to the healthcare system via the blockchain network. Storing healthcare data on the blockchain guarantees its safety even in the event of natural disasters or the collapse of medical facilities, as the data is duplicated in multiple locations, avoiding a single point of failure. The Lightweight Blockchain Security Model proposed in this study combines trust management, privacy preservation through blockchain, and attack detection mechanisms. Before reaching a consensus, the nodes in the network participate based on each node's status. Through voting, the primary node is selected, and the consensus process is completed using an enhanced PBFT consensus mechanism. The benefit of employing this proposed mechanism is that it is more scalable and secure in data transmission with the blockchain framework. Here, different entities are considered in data exchange and only authorized users can enter the system directly with their credentials. This makes the system more optimal and secure in a way that the hybrid mechanism adopted optimally achieves effective performance. The methodological framework is illustrated in Fig. 1.

3.1. Registration phase

At this phase, the user registers their credentials to the service provider with username and password values. Initially,the input utilized for the health care system is derived from sources [33]**.** Remediate $\{U_1, \ldots. \ldots U_i, U_j, \ldots U_n\}$ communication with health care by harnessing blockchain. Firstly, users fill in the fields of username and password, and each unique – account or user registration field is passed as input to the system. In turn, this information is required by a database that checks if an aspiring user already exists within its records. If the user is a new or first-time user, they have a private–public key pair generated for him by the system automatically hence this gives another layer of security not only the phone verification process. This cryptographic key pair forms the user's identifier and provides secure communication across data transmission about this system. Significantly, the user's public key is recorded on a blockchain utilizing its decentralized and unmodifiable quality to guarantee the integrity of identification information.

The registration ID is generated as,

$$R_{ID} = h(ID//na) \tag{1}$$

The password to register a user is created as,

$$R_{pw} = h(pw//ID//na) \tag{2}$$

Ensure R_{ID} and R_{pw} are not equal to previous values. Encrypt Registration Password with Registration Identifier $\left(Enc\left(R_{pw}, R_{ID}\right)\right)$.

Let ID_i be the i^{th} user ID and PW_i the i^{th} user password.$ID_iPW_i \rightarrow R_{ID}, R_{PW} \varepsilon R_{ID}/, R_{PW}/$ (i.e.) database check. If yes already registered goes to the login phase, if no, for new users private and public keys are generated. Here, the private key P_k given to the user, $P_B \rightarrow$ public key is stored in the blockchain. Fig. 2 depicts the representation of the registration and login phases.

Here random number is denoted as na, P_K is denoted as private key, and P_B is denoted as public key.

3.2. Login phase

After registering the user credentials, the next phase is the login phase, where the user directly updates the information by logging into the system with their respective username and password. The login phase mainly considers ensuring secure access and takes into account rigorous authentication with the use of harsh controls. This is made possible by requiring authenticity from the registered users in conjunction with their customized username and password. The user's identity is confirmed through this initial verification system should serve as the only way in which such an identification would be possible. Nevertheless, to enhance security further the system employs a lightweight proof of hybrid mechanism which may require validation through an appropriately chosen lightweight minor. This further security measure can be characterized as secondary-level authentication and it increases the general standard of the login process. Finally, the authenticated users who pass both stages of authentication are allowed in the system, this secures using the medical data and ensures secured privacy. The terms also become restricted to act upon via an account with necessary permission registered on a valid genuine ID.

3.2.1. Lightweight security model

The Lightweight Proof of Hybrid Security minor mechanism designed in the research is intended to improve security and efficiency by achieving a better selection strategy for minors within a network. However, the process of secure communication achieved through the lightweight model is accomplished in the blockchain framework. To achieve this, the system leverages lightweight algorithms and protocols that aim to maintain efficiency while simultaneously reducing computational complexity. This algorithm guarantees scalability and applies to resource-limited settings, like IoT networks. After the process of mining, the minors are subjected to validation and verification within the blockchain network, where factors that determine an individual's trust level as well as their credentials need to be reviewed. Blockchain verification thus ensures greater transparency, accountability, and trust in the mining selection procedure which contributes to strengthening the security as well as the integrity of a blockchain network. Here's an explanation of how it works:

i) Trust computation

In the system, there are many choices of minors from a network each having varied computational resources and functions. Factors computed for each minor may include the historical performance and reliability of nodes computing power among others which includes network participation. The trust factor is a metric used for software evaluation of the credibility and dependability of each dredger to take part in securing as well as maintaining honesty within the blockchain network. However, it determines the trustworthiness of each entity that engaged in the data transmission process, as the trust factor does not allow the malicious entity to enter into the communication framework.

To qualify a node c as an authority node (AN), it is required to meet the predetermined honesty threshold, Q_L, set by the blockchain network.

$$Q_c > Q_L \tag{3}$$

The honesty of a node depends on the effectiveness of the task it performs. If the node produces an accurate solution, its honesty level goes up by a positive amount f_l, but if the solution is incorrect, its honesty level decreases H_l.To calculate the overall positive value of honesty q_f for a node c after completing a total of b works, the following formula can be used:

$$Q_c = \sum_{a=1}^{a=b} f_l(a) \tag{4}$$

Node c is calculated for its negative honesty value, Q_x using the same approach.

$$Q_x = \sum_{1=1}^{a=b} S_l(a) \tag{5}$$

To summarize, the honesty level Q_c of the node can be ascertained through the execution of the subsequent calculation.

$$Q_c = Q_f - Q_L \tag{6}$$

ii) Consensus algorithm

To maintain consistency in the ledger among all nodes in a distributed and decentralized blockchain network, it is crucial to employ a consensus algorithm. The classification of this algorithm can be either "Proof-based" or "Voting-based." For proof-based algorithms, each node must provide evidence of its credibility to make changes to the existing ledger, which must be accepted by all other nodes. On the other hand, voting-based algorithms involve all nodes in the network voting, and an agreement is reached based on these votes. Voting-based algorithms are mostly used in closed architectures such as ledger Fabric, where the participating nodes are predetermined and known in advance. Such a system can lead to the concentration of power within the network and the establishment of a monopoly. Hence, proof-based algorithms are important as they allow us to maintain the decentralized nature of the network and ensure equal value for every node. Proof-based algorithms can be divided into three main types: a) PoW, b) PoS, and c) Hybrid algorithms that combine both PoW and PoS.

4. Hybrid Security- Proof of Work + Proof of Stake

The minors' selection procedure is a hybrid security model that operates under the consensus mechanisms of PoW and PoS. Proof of Work demands minors to solve complex cryptographic riddles at the end stage this is measured as directing transactions and insertion blocks for that blockchain hence by computation power. Proof of Stake means that minors can contribute to the validation process according to as much cryptocurrency they hold or offer it as commitment, creating an additional security layer and stimulating network participation.

By employing both PoW and PoS mechanisms in a hybrid fashion, the deficiencies of each consensus are addressed. Such a hybrid approach incorporates both PoW and PoS as consensus algorithms within the blockchain network, aiming to bridge gaps and establish a more harmonized system. The objective of Hybrid PoW/PoS is to enhance blockchain security by combining the features of both mechanisms. In the PoW mechanism, complex problems are solved to facilitate the addition of transactions to the blockchain, necessitating substantial computational power. On the other hand, PoS operates by requiring

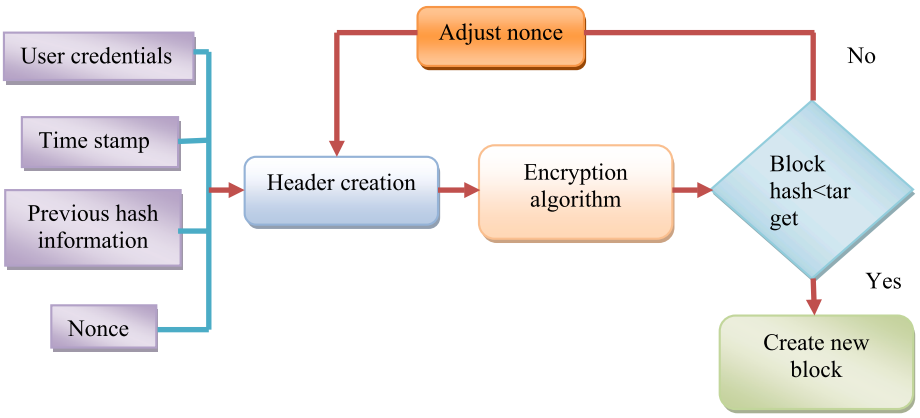


Fig. 3. Schematic representation of PoW algorithm.

users in the blockchain network to possess a certain amount of cryptocurrencies. While PoW enables minors to mine and append blocks to the chain, PoS allowsminors to validate transactions and blocks. The Hybrid PoW/PoS approach encourages minors to possess significant processing capabilities and actively contribute to the network, thereby ensuring a heightened level of blockchain security.

a) Proof of Work consensus

To ensure consistency in the ledger of nodes, it is vital to identify a reliable node as each node in the network strives to broadcast its block containing verified transactions. However, if nodes broadcast their blocks at different time intervals, discrepancies may arise. To overcome this issue and establish agreement, PoW requires every node to solve a difficult hash problem, a process also known as mining. The PoW algorithm builds upon the Hash cash algorithm, which was originally developed to combat spam The node that correctly solves the problem first gains the authority to add its block to the main chain, which is then adopted by all other nodes. The network automatically adjusts the difficulty of the hash problem based on specific criteria. In the case of Bitcoin, the difficulty is recalibrated every two weeks (or after every 2016 blocks) using the formula mentioned below:

$$E(new) = E(old)^{*}\frac{T(2weeks(ms))}{T(\text{mine}2016blocks(ms))} \tag{7}$$

In the Bitcoin network, the difficulty and time functions $E()$ and $T()$ are utilized to regulate the mining of coins. This process occurs every two weeks and ensures the difficulty level is adjusted accordingly. If it takes longer than two weeks to mine 2016 blocks, the difficulty decreases, and if it takes less time, the difficulty increases. This approach maintains a balance, neither making the process too easy nor too challenging. To initiate the process of mining, the validating nodes need to collect confirmed transactions, the hash of the previous block, and the timestamp of the new block. They aim to solve a challenging cryptographic puzzle by making educated guesses on a confidential value known as a nonce. It is even possible for multiple minors to discover the correct nonce value simultaneously, although this is quite rare. These issues can arise because individual nodes are unaware of each other's discoveries. Consequently, nodes persist in sharing their blocks, resulting in multiple blocks being received by other nodes and causing forks in the network. Satoshi presented a blockchain system in which minors continuously mine new blocks on separate branches until one branch surpasses the others in length. The shorter branch, known as the orphan chain, has its remaining transactions verified later. This element contributes to the challenge of ensuring definite transaction times in any network that is blockchain-oriented. Fig. 3 shows the schematic representation of the PoW algorithm.

b) Proof of stake algorithm

To overcome the limitations of the PoW system, Next Coin adopts an alternative approach called the PoS consensus algorithm. This algorithm selects the node responsible for adding a new block to the chain based on its stake in the network. For instance, if a node, referred to as y possesses c coins out of t total coins in the network, the probability of the node y being chosen to add a new block is c/t. Once a node is granted permission to add a block, it undertakes various tasks such as verifying transactions, collecting tasks into a block, transmitting information to

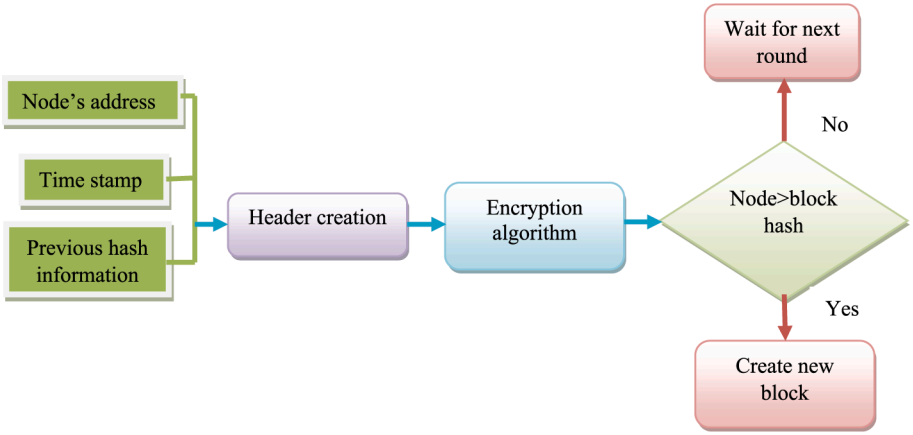


Fig. 4. Schematic representation of PoS algorithm.

other nodes, and earning fees for these actions. The primary objective of the PoS system is to eliminate the extensive computational effort required in PoW mining. Instead, PoS relies on a trust-based system, where nodes with a substantial stake are deemed reliable. This reliability is attributed to the fact that nodes with a significant stake have little incentive to launch attacks due to the low rewards and high risks involved.If a stakeholder is discovered to be behaving maliciously, all of their assets will be locked and shared among the other nodes in the network. Creating PoS-based blockchain networks from the beginning is impractical since it necessitates distributing assets or coins among the network. Therefore, PoS is usually deployed in an established PoW network. Fig. 4 represents the diagrammatic representation of the PoS algorithm.

c) Hybrid PoW and PoS

Despite being widely implemented, both PoW and PoS have their limitations. The 51 % attack is a significant worry in PoW-based networks, as it involves a malevolent entity acquiring dominance over more than half of the network's computational capabilities. By rapidly creating chains of blocks on top of honest nodes, they can gradually replace the honest chain using the longest chain rule. Additionally, the high computation power required for PoW prevents regular nodes from having a fair chance at mining. This mining process also leads to excessive energy consumption. For example, in Bitcoin, the increasing difficulty has led to the use of specialized mining hardware like application-specific integrated circuits (ASIC). To tackle these problems, mining pools have been established so that each node can participate and be rewarded by jointly solving a shared puzzle. The rewards are then divided among the nodes depending on the number of almost-perfect hash values they discover. These four mining pools – F2Pool, Pooling, Ant Pool, and BTC.com – control roughly 50 % of the entire Bitcoin network and can collaborate to carry out a 51 % attack. Likewise, networks that use PoS face similar vulnerabilities. This scenario leads to a concentration of power since stakeholders with larger holdings have a higher probability of adding blocks. These factors have prompted individuals to shift towards hybrid consensus algorithms that combine elements of both PoW and PoS.

Let us assume that n represents the total number of nodes in the network and T_s is the stake of the node s, as well as P_s the hash power of the node s, E_s the reward collected by the node, and RT the total reward to be distributed among nodes. The probability of being proposed as the node in a hybrid PoS/PoW system depends on a weighted ratio of stake and hash power which can be represented as follows:

$$P_s = W.\frac{T_S}{\sum_{t=1}^{n} T_t} + (1 - W).\frac{P_s}{\sum_{t=1}^{n} P_t} \tag{8}$$

For node that is identified as P_s being chosen to give a new block, and used W as the weighting factor which helps determine the effects of stake over hash power on the selection process. W could be tailored to suit the requirements of network specifications and parameters. Nodes can then be compensated in proportion to their contributions to the network which will lead to the accumulation of a reward by these nodes. For example, O_s the reward for a node s can be calculated as:

$$O_s = \frac{P_s.RT}{\sum_{t=1}^{n} S_t} \tag{9}$$

Hence, it ensures that the big stake nodes and greater hash power have a higher chance of being selected for proposing blocks and getting a share of the gains, but still, the participation from nodes with smaller stakes but high hash power is allowed, and vice versa.

4.1. Mutual agreement phase

The next phase is the mutual agreement phase, where the mutual contract is carried out between the IoT devices and healthcare data providers. In the Mutual Agreement Phase, a transparent and accountable framework for data sharing is created by employing smart contracts which are prioritized by the system. This streamlines the process because the smart contracts would eliminate the need for agreements between a set user and some healthcare database. In these contracts one can see certain terms relating to data sharing and access; both parties can have a mutual understanding as well as agreement. Importantly, smart contracts are automated and executed on a track of predetermined arrangements and hence the enforcement is automatic ensuring that agreed-upon terms are without human intervention.

Let F be the contract for data sharing. F has particular terms and conditions and G is agreed upon by all the parties.

$$F = \left\{G_{user}, G_{healthcare\ provider}\right\} \tag{10}$$

4.2. Data request and access

After the completion of the mutual agreement phase, the next phase is to be processed in the data request and access phase, where the request to access the data is done between the user and IoT devices. During the data Request and access phase, the system permits unhindered communication to users and providers of health care ensuring easy retrieval of ECG Data. Using its decentralized infrastructure, users can request ECG data from IoT devices via the blockchain transparent and auditable transactions. When an address makes a request, the healthcare provider responds by sending a code that is encrypted on the blockchain thereby protecting any sensitive medical information. The blockchain subsequently authenticates the request and authorizes access to requested data, using its immutable ledger authentication. Then, as soon as the access is granted user gets to know of it and retrieves data that will help them in carrying out successful healthcare needs. This streamlined process not only improves access to essential medical data but also provides compliance with regulations on privacy whereby trust and reliability are built into healthcare data management. Let Y, therefore denote a data demand from users. Let Z interpret the data. The blockchain grants access Z upon verification that the request Y fits already defined criteria.

$$Z = Verification\ by\ block\ chain(Y) \tag{11}$$

4.3. Data transfer

The final phase of the proposed method is the data transfer phase, where the user-requested data is accessed from the blockchain network. During the Data Transfer phase, they also focus most on preserving ECG data confidentiality and integrity throughout transmission. This is highly crucial in implementation and calls for encryption as the key. AES algorithm is used to encrypt the ECG data before it begins transmission. AES encryption guarantees a higher level of security through which data gets incomprehensible during transfer for unauthorized people. For ensuring the authorized access to encrypted data a key exchange facility is provided. The user uses the previously generated private key to decrypt, once he obtains it. This guarantees that only authorized users, holding the appropriate private key, can decode and make sense of sensitive data held within ECG information. Blockchain technology is a key player in ensuring that encrypted data proceeds smoothly from one party to another without the possibility of an endangered transmission. Private information is transferred using the distributed characteristic enabled by the blockchain's immutable feature to ensure its security without intermediaries or central management. The blocks are themselves cryptographically sealed, they group transactions into unalterable chain records. This guarantees the maintained quality of transmitted data throughout the transfer procedure and also reduces security risks primarily related to illicit access or tapped individually. In addition, the blockchain offers an enclosing environment up to a point providing end-

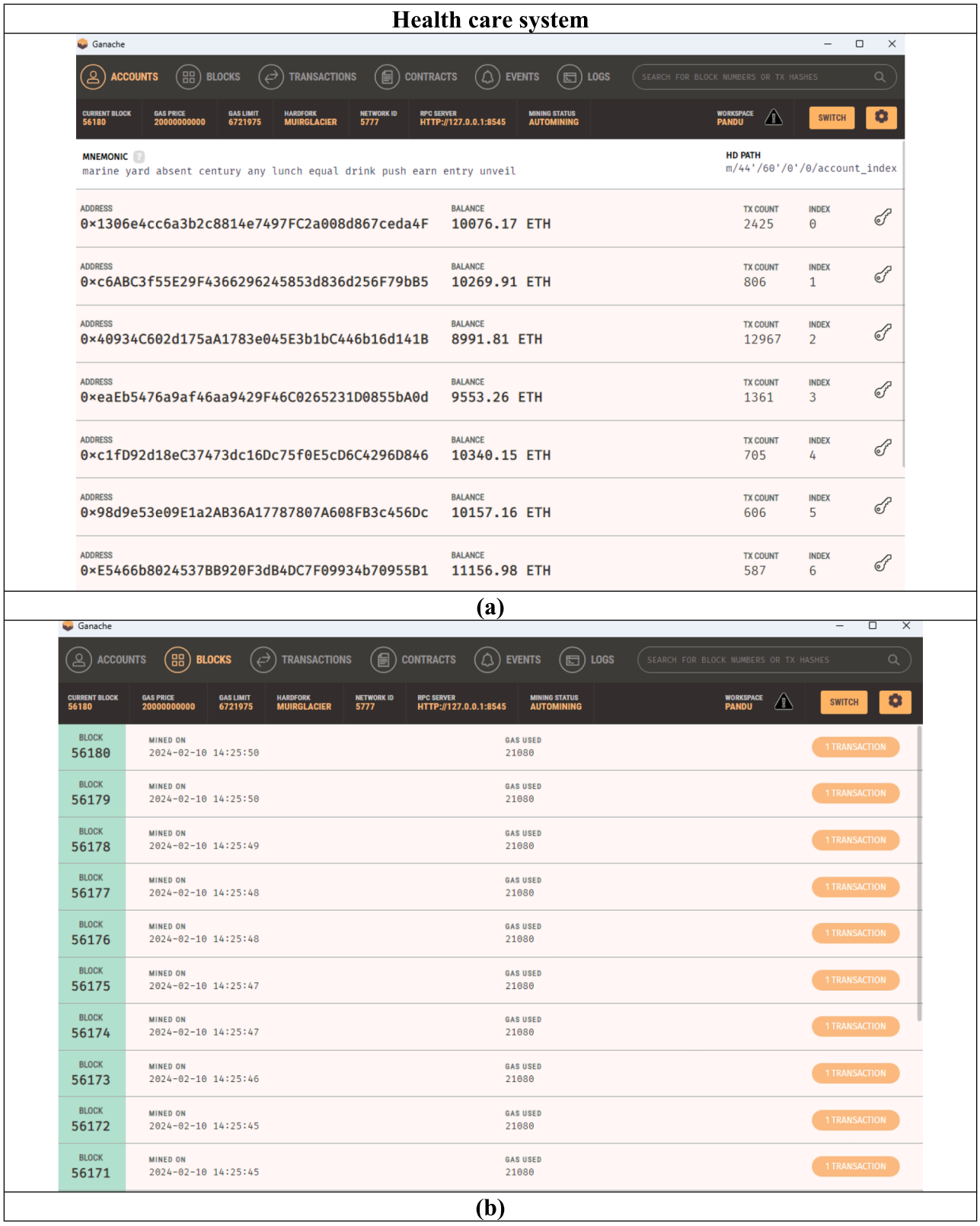
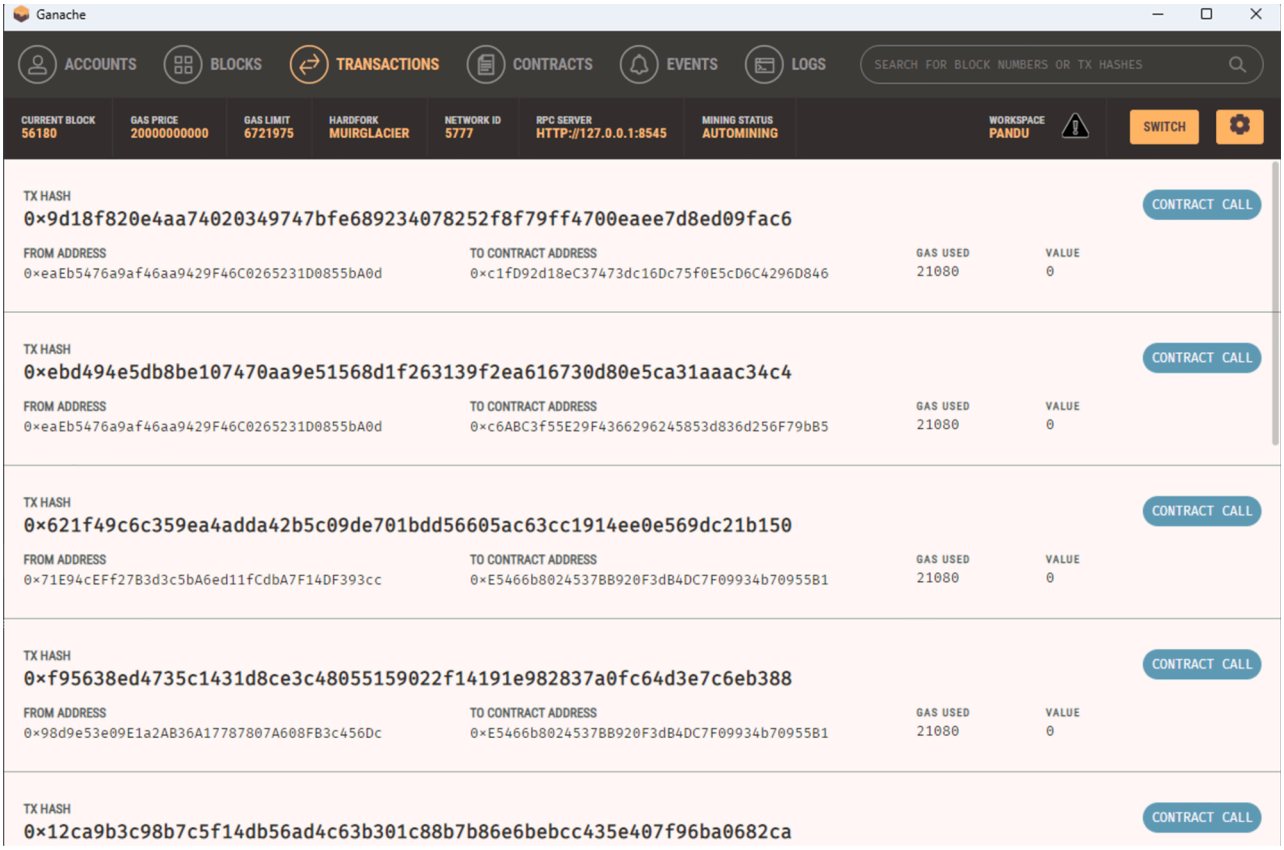


Fig. 5. Image results obtained using the lightweight HPoS-based minor solution.

to-end security as it establishes an auditable and traceable chain of data usage. From the encryption process through to decryption, every stage in the data sharing is time-stamped on a blockchain making it possible for any stakeholder to track and validate the integrity of coordinated or modified shared information at any time. This strengthens trust towards the ECG data security, deepening the integrity of the healthcare ecosystem as a whole. In this case, W symbolizes the data encryption procedure which uses the AES algorithm and F designates the key



(c)

Fig. 5. (*continued*).

exchange channel.

The AES algorithm operates on blocks that have a length of 128 bits, and the key can be 128, 192, or 256 bits long. The encryption process begins with the Add Round Key step. In each round, except for the final round, four operations are performed: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. However, in the final round, only Sub Bytes, Shift Rows, and Round Key operations are carried out. The AES algorithm applies these operations to a two-dimensional array of bytes known as the state. The Sub Bytes operation involves finding the multiplicative inverse of the input byte by $GF(2^8)$ using the polynomial $p(y) = y^8 + y^4 + y^3 + y + 1$ followed by applying an affine transformation. The affine transformation is accomplished by multiplying the byte with an 8×8 binary matrix and executing an EXOR operation with a constant value of 63H. During the Shift Rows step, the rows of the state array are shifted cyclically to the left. The first row remains unchanged, the second row shifts one byte to the left, the third row shifts two bytes to the left, and the fourth row shifts three bytes to the left. This process does not require any mathematical calculations. In the Mix Columns step, the columns of the state are treated as polynomials over $GF(2^8)$ and are multiplied modulo $(y^4 + 1)$ using a predetermined polynomial $d(y)$.

$$d(y) = \{03\}y^3 \oplus \{01\}y^2 \oplus \{0,1\}y \oplus \{02\} \tag{12}$$

Here, $GF(2^8)$ is utilized for performing the multiplications, employing the irreducible polynomial $y^8 + y^4 + y^3 + y + 1$. During the Add Round Key step, the state and round key are combined by performing a straightforward bitwise EXOR operation. To generate the necessary round keys for a 128-bit key size and 10 rounds, the cipher key is processed through the key expansion algorithm. It should be noted that the key schedule involves performing the Sub Bytes transformation, shifting a 32-bit word by one byte in a cyclic manner, adding a 32-bit constant called $RCON_i$, and performing 32-bit EXOR operations. The decryption process in the direct decryption structure differs from that of encryption. Nonetheless, there is a decryption algorithm that mirrors the structure of the encryption algorithm. Swapping the order of Inv Sub Bytes and InvShiftRows does not affect decryption, but it requires the round keys to undergo Inv Mix Columns to generate the Mix Round Key for decryption. In Inv Sub Bytes, the input byte undergoes an inverse affine transformation and is then multiplied by its multiplicative inverse $GF(2^8)$. In the process of InvMixColumns, a specific polynomial is used to multiply each column modulo $(y^4 + 1)$ to bring about its transformation.

$$d(y) = \{0b\}y^3 \oplus \{0d\}y^3 \oplus \{09\}y \oplus \{0e\} \tag{13}$$

The AddMixRoundKey transformation closely resembles the forward Add Round Key transformation because both utilize the EXOR operation. The round keys, which are required for each round, are derived from the cipher key in a manner akin to the process of encryption.

$$Data\ encrypted = W(ECG\ data) \tag{14}$$

$$Decrypted\ key = F(Private\ key\ by\ the\ user) \tag{15}$$

5. Result and discussion

The main objective of the study is to evaluate the effectiveness of the lightweight HPoS-based minor solution at key as compared to other currently employed techniques, to establish its efficiency.

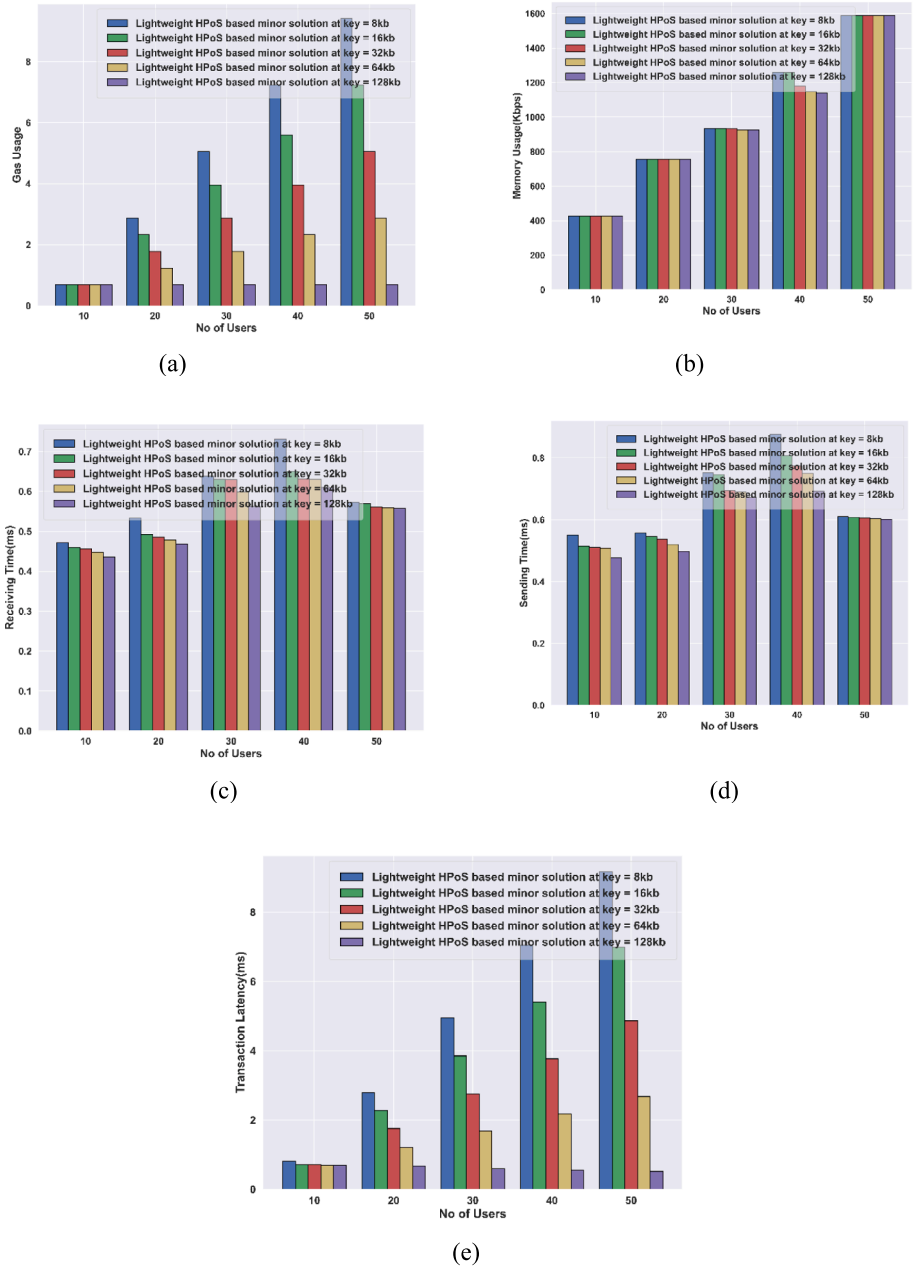


Fig. 6. Performance analysis based on user analysis, a) gas usage, b) memory usage, c) receiving time, d) sending time, e) transaction latency.

5.1. Experimental setup

The key objective of the experiment was implementing inMATLAB which had a pre-installed memory of 8 GB and was functioning on Windows 10.

5.2. Dataset description

The dataset used for the experimentation process is the ECG dataset [33] whichcontains 21,799 medical 12-lead ECG records that have a duration of 10 s. These records pertain to 18,869 individuals, where males account for 52 % and females for 48 %. The age of the patients ranges from 0 to 95 years, with a median age of 62 and a spread of 22 years between the lower and upper quartiles. The dataset is valuable because it contains a diverse collection of various diseases and also includes a significant number of healthy control samples. The diagnoses are categorized into superclasses for simplicity.

5.3. Experimental results

The data collected on blockchain address, balances, transaction number, and index indicate the result as what we have shown. The analysis demonstrated that these entries were mainly financial and operational transaction records within the healthcare system with the provision of different aspects concerning transactions and account balances such as patient data and interactions that can be seen in Fig. 5a), Fig. 5b), and Fig. 5c).

5.4. Performance analysis based on user analysis

The data presented in Fig. 6 illustrates how the lightweight HPoS-based minor solution at the key model performs in terms of gas usage, memory usage, receiving time, sending time, and transaction latency. Fig. 6 a) depicts the representation of gas usage. For 50 users, the proposed model attained gas value by varying the key size 8 kb, 16 kb, 32

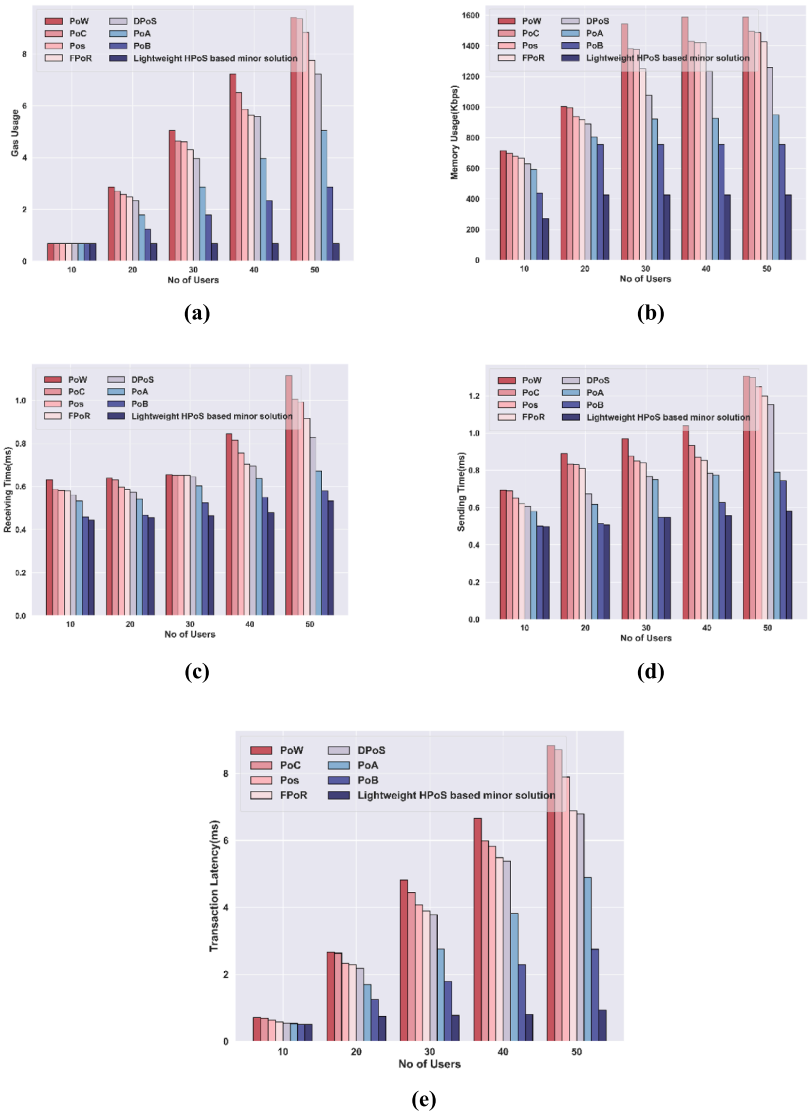


Fig. 7. Comparative analysis based on user analysis, a) gas usage, b) memory usage, c) receiving time, d) sending time, e) transaction latency.

kb, 64 kb, and 128 kb is 9.42, 7.24, 5.05, 2.87, and 0.69. Fig. 6b) displays the results of memory usage. The lightweight HPoS-based minor solution used the memory sizes, 1588.47Kbps, 1588.45 Kbps, 1588.16 Kbps, 1588.07 Kbps, and 1587.99 Kbps for the key sizes of 8 kb, 16 kb, 32 kb, 64 kb, and 128 kb respectively. Moreover, Fig. 6c) indicates the receiving time factor. The lightweight HPoS-based minor solution obtained a receiving time of 0.573 ms, 0.570 ms, 0.561 ms, 0.558 ms, and 0.557 ms by varying the key size from 8 to 128 kb with 50 users. Likewise, Fig. 6d) reveals different sending times. The developed method uses the sending time as, 0.611 ms, 0.607 ms, 0.606 ms, 0.602 ms, and 0.601 ms for 50 users for various key sizes. The outcome of transaction latency using the lightweight HPoS-based minor solution at the key model isshown in Fig. 6e). The values obtained for transaction latency are 9.18 ms, 7.00 ms, 4.86 ms, 2.68 ms, and 0.525msfor 50 users.

5.5. Comparative methods

The efficacy of the lightweight HPoS-based minor solution at a key model is illustrated by incorporating several existing models like Proof of Work (PoW) [34], Proof of Concept (PoC) [35], Proof of Stake (PoS) [36], Fair Proof of Reputation (FPoR) [37] Delegated Proof of Stake (DPoS) [38], Proof of Authority (PoA) [39], and Proof of Burn (PoB) [40].

5.5.1. Comparative analysis based on user analysis

Fig. 7a) represents the gas usage analysis. For 50 users, the proposed scheme attained gas usage of 0.69 which is reduced over existing PoW [34], PoC [35], PoS [36], FPoR [37] DPoS [38], PoA [39], and PoB [40] methods by 8.72 Kb, 8.68 Kb, 8.14 Kb, 7.06 Kb, 6.54 Kb, 4.36 Kb, and 2.18 Kb respectively. Fig. 7b) illustrates the analysis of memory usage. With 50 users, the memory utilized by the proposedHPoSmodel is 427.46Kbpswhich shows it is lower than the existing PoW by 1160.7Kbps, PoC by 1066.5Kbps, PoS by 1060.03Kbps, FPoR by 999.94Kbps, DPoS by 832.89Kbps, PoA by 521.14Kbps, PoB by 326.89Kbps. Fig. 7c) depicts the analysis based on receiving time. By considering 50 users, the receiving time computed by the proposedHpoS model is 0.53 ms, which is decreased by 0.581 ms for PoW, 0.474 ms for PoC, 0.459 ms for PoS, 0.382 ms for FPoR, 0.294 ms for DPoS, 0.138 ms for PoA, and 0.046 ms for PoB. The analysis done based on sending time is depicted in Fig. 7d). With 50 users, the sending time measured for the proposed HPoSmethod is 0.58 ms, which shows 0.722 ms, 0.716 ms, 0.666 ms, 0.616 ms, 0.570 ms, 0.208 ms, 0.162 ms lower than the

Table 1
Comparative discussion.

Models	Gas usage (Kb)	Memory usage (Kbps)	Receiving time (ms)	Sending time (ms)	Transaction latency (ms)
PoW	9.41	1588.16	1.11	1.30	8.83
PoC	9.37	1493.97	1.00	1.29	8.70
PoS	8.83	1487.49	0.99	1.24	7.89
FPoR	7.75	1427.40	0.91	1.19	6.88
DPoS	7.23	1260.35	0.82	1.15	6.78
PoA	5.05	948.60	0.67	0.79	4.88
PoB	2.87	754.35	0.57	0.74	2.74
Lightweight HPoS-based minor solution at key	0.69	427.46	0.53	0.58	0.93

existing methodsPoW, PoC, PoS, FPoR, DPoS, PoA, and PoB methods respectively. Fig. 7e) exhibits the analysis of transaction latency. With 50 users, the transaction latency obtained by the proposed HPoS model is 0.93 ms, which is reduced over existing PoW, PoC, PoS, FPoR, DPoS, PoA, and PoB methods by 7.89 ms, 7.76 ms, 6.95 ms, 5.94 ms, 5.84 ms, 3.95 ms, and 1.81 ms respectively.

5.6. Comparative discussion

Table 1 shows the comparative discussion of the proposed model. The lightweight HPoS-based minor solution model performs better than current analogs giving the performance and security with low energy expenses and the sophisticated design. Through uniting the upsides of the PoW and PoS mechanisms, HPoS leads blockchain security in the direction of improvement while mastering scalability. Its highly efficient algorithms and protocols mean that it can work well even in conditions such as scarce resources like IoT networks. As HPoS chooses reputable minors in the beginning, the blockchain network keeps its well-being strong through this implementation. To demonstrate its superior performance, a lightweight HPoS-based minor solution is compared to existing models at the main model. This comparison involves evaluating metrics using several users of 50. The findings indicate that for 50 users, the models achieve significant reductions in gas usage, memory usage, receiving time, sending time, and transaction latency. Specifically, they achieve scores of 0.69 kb, 427.46Kbps, 0.53 ms, 0.58 ms, and 0.93 ms respectively, compared to the existing models.

6. Conclusion

A lightweight proof for a hybrid security-based minor solution is developed in this research to provide security in the blockchain framework, which considers a distributed mechanism to generate and update data. It ensures security in the data accessing and transmission process and provides a great solution in the security framework. The proposed model effectively solves the issues, like computational complexity, and latency faced by the existing data security approaches in the blockchain framework by employing a secure model. The lightweight model designed is based on trust factors and considers optimization algorithms to provide a scalable and secure framework in the blockchain network Moreover, it concentrates on minimizing computation costs and the trust factor shows the security strategy efficiently. The hybrid model consisting of PoW/PoS by concentrating on the computational costs and trust regarding minor selection, presented decision renders upscale scalability improving with security features together from governance support. In addition, the union between PoW and PoS ensures a high incentive to actively participate in networking; thus, forging a robust and decentralized blockchain system. With the development of blockchain technology, this study's findings will form a strong pillar in creating solid and versatile blockchain either that are applied to several sectors or utilized for different applications thereby leading our path towards a better digital future. The proposed model achieves significant reductions in gas usage, memory usage, receiving time, sending time, and transaction latency. Specifically, the proposed model achieves scores of 0.69 kb, 427.46Kbps, 0.53 ms, 0.58 ms, and 0.93 ms respectively. The future direction of research would consider a hybrid optimization algorithm for generating key parameters, in addition to that encrypt and decrypt mechanism will also be included at the data provider entity to further increase the security and scalable performance.

CRediT authorship contribution statement

Murari Kumar Singh: Data curation. **Sanjeev Pippal:** Data curation. **Vishnu Sharma:** Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

References

[1] J.S. Lee, C.J. Chew, J.Y. Liu, Y.C. Chen, K.Y. Tsai, Medical blockchain: data sharing and privacy preserving of EHR based on smart contract, J. Inform. Security Appl. 65 (2022) 103117.
[2] T.P. Raptis, A. Passarella, M. Conti, Distributed data access in industrial edge networks, IEEE J. Sel. Areas Commun. 38 (5) (2020) 915–927.
[3] H. Elhoone, T. Zhang, M. Anwar, S. Desai, Cyber-based design for additive manufacturing using artificial neural networks for industry 4.0, Int. J. Prod. Res. 58 (9) (2020) 2841–2861.
[4] R. Colomo-Palacios, M. Sánchez-Gordón, D. Arias-Aranda, A critical review on blockchain assessment initiatives: a technology evolution viewpoint, J. Softw., Evol. Process 32 (11) (2020).
[5] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, Y. Koucheryavy, On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices, *IEEE Access* 9 (2021) 80559–80570.
[6] P. Arul, S. Renuka, Blockchain Technology Using Consensus Mechanism for IoT-Based e-Healthcare System 1055 (2021) 012106.
[7] A. Kumar, D.K. Sharma, A. Nayyar, S. Singh, B. Yoon, Lightweight proof of game (lpog): a proof of work (pow)'s extended lightweight consensus algorithm for wearable kidneys, *Sensors* 20 (10) (2020) 2868.
[8] Y. Dodis, A. Yampolskiy, A verifiable random function with short proofs and keys, in: Proceedings of the Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005, pp. 416–431.
[9] J. Chen, S. Micali, Algorand: a secure and efficient distributed ledger, Theor. Comput. Sci. 777 (2019) 155–183 [CrossRef].
[10] J.K. Oladele, A.A. Ojugo, C.C. Odiakaose, F.U. Emordi, R.A. Abere, B. Nwozor, P. O. Ejeh, V.O. Geteloma, BEHeDaS: a blockchain electronic health data system for secure medical records exchange, J. Computing Theories Appl. 1 (3) (2024) 231–242.
[11] M. Shen, X. Tang, L. Zhu, X. Du, M. Guizani, Privacy-preservingsupport vector machine training over blockchain-based encrypted IoT data in smart cities, IEEE Internet Things J. 6 (5) (Oct 2019) 7702–7712.
[12] J. Wan, S. Tang, Q. Hua, D. Li, C. Liu, J. Lloret, Context-aware cloud robotics for material handling in cognitive industrial internet of things, IEEE Internet Things J. 5 (4) (Aug 2018) 2272–2281.
[13] S. Biswas, K. Sharif, F. Li, S. Mahajan, S.P. Mohanty, Yu. Wang, PoBT: a lightweight consensus algorithm for scalable IoT business blockchain, IEEE Internet Things J. 7 (3) (2019) 2343–2355.
[14] B.K. Mohanta, U. Satapathy, S.S. Panda, D. Jena, A novel approach to solve security and privacy issues for IoT applications using blockchain, in: Proceedings of the 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India,19–21 December 2019, pp. 394–399.
[15] B. Alamri, I.T. Javed, T. Margaria, Preserving patients' privacy in medical IoT using blockchain, in: Proceedings of the International Conference on Edge Computing, Honolulu, HI, USA, 22–26 June 2020, pp. 103–110.
[16] Uddin Moin, Muhammad Muzammal, Muhammad Khurram Hameed, Ibrahim Tariq Javed, Bandar Alamri, Noel Crespi, CBCIoT: a consensus algorithm for blockchain-based IoT applications, Appl. Sci. 11 (22) (2021).
[17] Alblooshi, Mansoor, Khaled Salah, Alhammadi Y Blockchain-based ownership Management for medical IoT (MIoT) devices, in: 2018 IEEE International Conference on innovations in Information Technology (IIT), pp 151-156.

[18] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the Internet of things: a comprehensive survey, IEEE Commun. Surveys &tutorials 21 (2) (2019) 1676–1717.
[19] S. Biswas, K. Sharif, F. Li, B. Nour, Y. Wang, A scalable blockchain framework for secure transactions in IoT, IEEE Internet Things J. 6 (3) (Jun 2019) 4650–4659.
[20] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, D. Puthal, PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE), CoRR, vol. abs/1909.06496, 2019. [Online]. Available: http://arxiv.org/abs/.
[21] Manal Mohamed Alhejazi, Mustafa A. Rami, Mohammad, Enhancing the blockchain voting process in IoT using a novel blockchain Weighted Majority Consensus Algorithm (WMCA), Inform. Security J.: Global Perspect. 31 (2) (2022) 125–143.
[22] S.L. Cichosz, M.N. Stausholm, T. Kronborg, P. Vestergaard, O. Hejlesen, How to use blockchain for diabeteshealth care data and access management: an operational concept, J. Diabetes Sci. Technol. 13 (2019) 248–253 [CrossRef] [PubMed].
[23] S. Angraal, H.M. Krumholz, W.L. Schulz, Blockchain technology: applications in health care, Circ. Cardiovasc.qual. Outcomes 10 (2017) [CrossRef] [PubMed].
[24] C. Pirtle, J. Ehrenfeld, Blockchain for healthcare: The next generation of medical records? J. Med. Syst. 172 (2018) 42 [CrossRef].
[25] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-based data preservation system for medical data, J. Med. Syst. 42 (2018) 141 [CrossRef] [PubMed].
[26] R. Zou, X. Lv, J. Zhao, SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system, Inf. Process. Manag. 58 (4) (2021) 102604.
[27] P. Hegde, P.K.R. Maddikunta, Secure PBFT consensus-based lightweight blockchain for healthcare application, *Appl. Sci.* 13 (6) (2023) 3757.
[28] Z. Pang, Y. Yao, Q. Li, X. Zhang, J. Zhang, Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm, *IEEE Access* 10 (2022) 87803–87815.
[29] Abdellatif, Alaa Awad, Abeer Z. Al-Marridi, Amr Mohamed, Aiman Erbad, Carla Fabiana Chiasserini, Ahmed Refaey, ssHealth: toward secure, blockchain-enabled healthcare systems, IEEE Network 34 (4) (2020) 312–319.
[30] Nafiz Al Asad, Md Tausif Elahi, Abdullah Al Hasan, Mohammad Abu Yousuf, Permission-based blockchain with proof of authority for secured healthcare data sharing, in: 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), IEEE, 2020, pp. 35–40.
[31] P.P. Ray, D. Dash, K. Salah, N. Kumar, Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases, *IEEE Syst. J.* 15 (1) (2020) 85–94.
[32] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, F.M. Almansour, Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things, Pers. Ubiquit. Comput. 28 (1) (2024) 59–72.
[33] ECG dataset link: https://physionet.org/content/ptb-xl/1.0.3/.
[34] B. Sriman, S. Ganesh Kumar, P. Shamili, Blockchain technology: Consensus protocol proof of work and proof of stake, in: Intelligent Computing and Applications: Proceedings of ICICA 2019, 2021, pp. 395–406.
[35] R. Ibrahim, A.A. Harby, M.S. Nashwan, A. Elhakeem, Financial contract administration in construction via cryptocurrency blockchain and smart contract: a proof of concept, *Buildings* 12 (8) (2022) 1072.
[36] M. Karpinski, L. Kovalchuk, R. Kochan, R. Oliynykov, M. Rodinko, L. Wieclaw, Blockchain technologies: Probability of double-spend attack on a proof-of-stake consensus, Sensors 21 (19) (2021) 6408.
[37] T. Zhang, Z. Huang, FPoR: Fair proof-of-reputation consensus for blockchain, ICT Express 9 (1) (2023) 45–50.
[38] Y. Chen, F. Liu, Research on improvement of DPoS consensus mechanism in collaborative governance of network public opinion, Peer-to-Peer Networking Appl. 15 (4) (2022) 1849–1861.
[39] M.M. Islam, H.P. In, Decentralized global copyright system based on consortium blockchain with proof of authority, IEEE Access 11 (2023) 43101–43115.
[40] M. Rodinko, R. Oliynykov, A. Nastenko, Decentralized Proof-of-Burn auction for secure cryptocurrency upgrade, *Blockchain: Res. Appl.* 5 (1) (2024) 100170.
[41] S.A. Ansari, A. Zafar, A fusion of dolphin swarm optimization and improved sine cosine algorithm for automatic detection and classification of objects from surveillance videos, Measurement 192 (2022) 110921.