Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Efficient information exchange approach for medical IoT based on AI and DAG-enabled blockchain

Shanqin Wang [a], Gangxin Du [b], Shufan Dai [a,*], Mengjun Miao [a,c], Miao Zhang [a]

[a] *School of Information Engineering, Chuzhou Polytechnic, Chuzhou, 239000, Anhui, China*
[b] *Sany Energy Equipment Co., Ltd, Zhuzhou, 412000, Hunan, China*
[c] *School of Computer, Qinghai Normal University, Haihu Avenue Chengbei District, Xining, 810008, Qinghai, China*

ARTICLE INFO

Keywords:
Information exchange
DAG-Enabled blockchain
Medical IoT
AI

ABSTRACT

The development of artificial intelligence (AI) based medical Internet of Things (IoT) technology plays a crucial role in making the collection and exchange of medical information more convenient. However, security, privacy, and efficiency issues during information exchange have become pressing challenges. While many scholars have proposed solutions based on AI and blockchain to address these issues, few have focused on the impact of the slow consensus algorithm of blockchain on the efficiency of information exchange. To improve the efficiency of information exchange, we propose an information exchange approach based on AI and DAG-enabled blockchain, providing a secure and efficient environment for information exchange in the medical IoT. Additionally, to enhance the efficiency of information exchange in the medical IoT, a novel tip selection algorithm is introduced to reduce the time delay in reaching consensus, thereby enabling faster acquisition of trusted information via blockchain. Simulation results demonstrate that compared to methods based on traditional DAG-enabled blockchain, the approach proposed in this paper improves the efficiency of information exchange.

1. Introduction

With the development of society and various technological advancements such as smart healthcare, smart agriculture, smart home systems, and autonomous vehicles, people's lives have been greatly facilitated. Particularly, the application of IoT in the field of healthcare has brought significant benefitsHe, Shi, Liu, Guo, Chen and Shi [1]. IoT devices can monitor patients' physiological parameters in real time, such as heart rate, blood pressure, and blood glucose levels, and send these information to healthcare professionals, enabling them to provide timely medical interventions AlSelek, Alcaraz-Calero and Wang [2] Cheng, Wu, Wang, Yin, Li, Chen and Chen [3]. By analyzing the large amount of health information collected from IoT devices, doctors can develop more personalized treatment plans for each patient Saraswat, Bhattacharya, Verma, Prasad, Tanwar, Sharma, Bokoro and Sharma [4]. In addition, machine learning (ML) algorithms can help identify patients' health trends and risk factors, thus enabling early disease prevention. IoT technology empowers patients to actively participate in their own health management, providing them with real-time feedback and health advice through smart devices. This sense of involvement and control contributes to improving patient satisfaction and treatment compliance Taimoor and Rehman [5] Kalakoti, Bahsi and Nõmm [6].

* Corresponding author.
E-mail addresses: wangshanqin@chzc.edu.cn (S. Wang), gangxin.du@163.com (G. Du), daishufan@chzc.edu.cn (S. Dai), miaomj@stu.qhnu.edu.cn (M. Miao).

https://doi.org/10.1016/j.heliyon.2024.e41617
Received 25 June 2024; Received in revised form 28 December 2024; Accepted 31 December 2024
Available online 31 December 2024

Blockchain has received significant attention due to its characteristics such as decentralization, immutability, and traceability. Dave et al. Dave, Rastogi, Miglani, Saharan and Goyal [7] proposed a video surveillance system based on distributed edge fog nodes for smart home environments to protect personal privacy. The system is integrated with a private blockchain network embedded in the surveillance system. This transformation of the surveillance system can be used to check and maintain integrity, manage fuzzy keys, and provide authorized access to video information. Rana et al. Rana, Sharma, Nisar, Ibrahim, Dhawan, Chowdhry, Hussain and Goyal [8] proposed a new solution combining blockchain to ensure information accountability, enhance information privacy and accessibility, and extract hidden patterns and available knowledge. Unlike the use of private blockchain mentioned above, or applying blockchain in areas such as information privacy, this paper uses DAG-enabled blockchain combined with AI for information exchange in the medical IoT.

However, in the process of exchanging information among all connected devices, privacy, security, and efficiency face significant challenges. Attackers exploit the security vulnerabilities of IoT devices to execute various network attacks Shah, Koundal, Sai and Rani [9] Rai, Shukla, Tightiz and Padmanaban [10]. AI based cybersecurity solutions can protect sensitive medical information against attacks Martínez and Galmés [11]. For instance, AI systems can learn normal network traffic and user behavior patterns, enabling real-time monitoring and identification of abnormal behaviors or potential security threats. By utilizing ML algorithms, AI systems can identify potential attack patterns and vulnerabilities, taking preemptive defensive measures Sankaran, Kim and Renjith [12]. By using ML methods to distinguish information that has not been attacked, smart contracts can store this untouched information in a DAG-enabled blockchain to ensure its security and immutability Reddy, Satish, Prakash, Babu, Kumar and Devi [13] Phatak, Patil, Arshad, Jitkar, Patil and Patil [14]. Smart contracts are computer protocols that automatically enforce contract terms, allowing for trusted transactions without the need for third-party intermediaries. The terms of these contracts are written in code on the blockchain, and when the specified conditions are met, the smart contract automatically executes relevant operations, such as fund transfers, asset exchanges, or information recording Shen, Li, Huang, Gao, Li, Li and Lei [15] Shrivastav and Sadasivan [16].

However, the slow consensus process of traditional blockchain seriously affects the timeliness of information viewing. For example, the Bitcoin system generates approximately one block every 10 min, implying that a minimum of 10 min is required to obtain final confirmation when recording information. On the other hand, the Ethereum system produces an average of one block every 12 s. While Ethereum's confirmation speed is faster compared to the Bitcoin system, it still falls short of meeting the real-time information viewing requirements in the field of medical IoT Cullen, Ferraro, Sanders, Vigneri and Shorten [17]. DAG-enabled blockchain is a distributed ledger technology that differs from traditional blockchain structures Popov [18]. In DAG-enabled blockchain, transactions are not linearly arranged in order on a blockchain but are connected to previous transactions through directed edges, forming a directed graph structure Zhao, Vigneri, Cullen, Sanders, Ferraro and Shorten [19]. This design can improve network throughput and scalability because in DAG, each new transaction confirms multiple previous transactions before being confirmed, rather than waiting for the entire block to be confirmed. However, the Markov Chain Monte Carlo (MCMC) algorithm commonly used in traditional DAG-enabled blockchain typically requires multiple iterations and computations to reach a stable state, leading to slower transaction confirmation speeds and limiting overall throughput. Therefore, there is a need to design a more efficient tip selection algorithm to compensate for the shortcomings of the MCMC algorithm, providing a more secure and efficient environment for information exchange in the field of medical IoT.

To address the aforementioned issues, this paper introduces an information exchange approach based on AI and DAG-enabled blockchain to establish a secure environment for exchanging medical information within the medical IoT. Furthermore, a new tip selection algorithm based on disease categories is proposed to expedite the consensus process, enabling quicker access to secure and reliable information. The main contributions are summarized as follows.

- We propose an information exchange approach based on AI and DAG-enabled blockchain to provide a secure and trustworthy environment for information exchange within the medical IoT.
- We introduce a disease category based tip selection algorithm to reduce the time required for the blockchain system to reach consensus, aiming to decrease the time for information to enter the blockchain and thus enhance the efficiency of information exchange.
- Simulation results demonstrate that compared to existing methods, the approach presented in this paper excels in terms of security and efficiency of information exchange in medical IoT.

In summary, the information exchange approach based on AI and DAG-enabled blockchain proposed in this paper optimizes the consensus algorithm, thereby reducing the time required to reach consensus within the blockchain system, with the goal of providing a more efficient and secure information exchange environment for the medical IoT. The remainder of this paper is organized as follows. We introduce the related work in Section 2. Section 3 describes the information exchange approach. The disease category based tip selection algorithm is proposed in Section 4. Performance evaluation is shown in Section 5. Finally, Section 6 concludes the paper.

2. Related work

With the rapid development of the medical IoT, the issues of medical information security and efficient exchange are increasingly prominent. Traditional centralized management poses risks, while blockchain technology offers a new approach to addressing this challenge. By combining AI technology, intelligent processing and efficient exchange of medical information can be achieved. Therefore, this paper aims to explore an efficient information exchange method for the medical IoT based on AI and DAG-enabled blockchain. Given the advantages of blockchain and AI, the research on AI and blockchain in the field of medical IoT has drawn significant attention from scholars.

Edward et al. Alrubei, Ball and Rigelsford [20] proposed an architecture that integrates the advantages of edge computing, AI, IoT terminal devices, and blockchain. This architecture is capable of monitoring the environment, collecting information, analyzing information, processing it using an AI expert engine, providing predictive and actionable results, and ultimately sharing them on a public blockchain platform. Subhi et al. Alrubei, Ball and Rigelsford [21] proposed an architecture that combines the advantages of edge computing, AI, and blockchain technology to provide a robust, secure, and intelligent solution for secure and rapid information processing and sharing. Gautam et al. Selvarajan, Srivastava, Khadidos, Khadidos, Baza, Alshehri and Lin [22] proposed a lightweight blockchain security model based on AI to ensure the privacy and security of IoT systems. This model is designed to address security and privacy issues that may arise when dealing with cloud-based IoT systems, which process information on devices in the cloud or at the network edge. Charles et al. Charles, Emrouznejad and Gherman [23] conducted a recent review of blockchain and AI in the field of supply chain, including current research on the integration of blockchain and AI in the supply chain, existing use cases of blockchain and AI in the supply chain, and potential research directions for the future integration of blockchain and AI. Meng et al. Shen, Gu, Kang, Tang, Lin, Zhu and Niyato [24] discussed the motivation for using blockchain in AI of things and its characteristics, and comprehensively reviewed existing blockchain solutions for AI of things systems from the perspectives of efficiency, security, privacy, trust, and incentives. The review also covered the challenges faced and future research directions in this area.

Besides, Quan et al. Quan, Yao, Chen, Fang, Zhu, Si and Li [25] proposed a blockchain based framework for trusted medical information sharing in the edge computing environment. This framework utilizes the edge blockchain of medical alliances to achieve fine-grained access control of medical information. Liu et al. Liu, Guan, Bai, Qin, Chen and Liu [26] studied a medical information diagnosis platform by applying swarm algorithm and evolutionary algorithm. They first analyzed the current development status of medical information diagnosis platforms based on chat generated pre trained converters and IoT technology, and then comprehensively explored the advantages and disadvantages of swarm algorithms and evolutionary algorithms in medical information diagnosis platforms. Sankaran et al. Sankaran, Kim and Renjith [27] proposed a secure M-Trust Privacy Protocol (SMP) to address these issues. The SMP protocol combines trust, encryption, and machine learning technologies to provide security and privacy for information in transit. The SMP protocol has been designed to work in conjunction with intelligent healthcare monitoring systems, providing a secure and dedicated communication channel between devices within the system. However, there are some drawbacks in this work, such as the cryptographic algorithm becoming inefficient when there are a large number of devices and a substantial amount of patient information. Additionally, it has centralized trust responsible for key distribution. Panchal et al. Panchal, Parmar, Rathod, Jadav, Gupta and Tanwar [28] proposed a solution supported by AI and blockchain to provide network security for medical IoT messages. Different ML classifiers are used to categorize medical IoT information into attack and normal classes. Subsequently, a blockchain network based on IPFS is employed to ensure security and transparency for medical IoT messages. However, the article did not consider the impact of the slow consensus process of blockchain on message exchange efficiency.

As mentioned above, the combination of AI and blockchain has received significant attention in the field of medical IoT. However, few scholars have paid attention to the impact of the slow consensus process of blockchain on the proposed models. Therefore, this paper presents a medical IoT information exchange approach based on AI and DAG-enabled blockchain, aiming to reduce the time

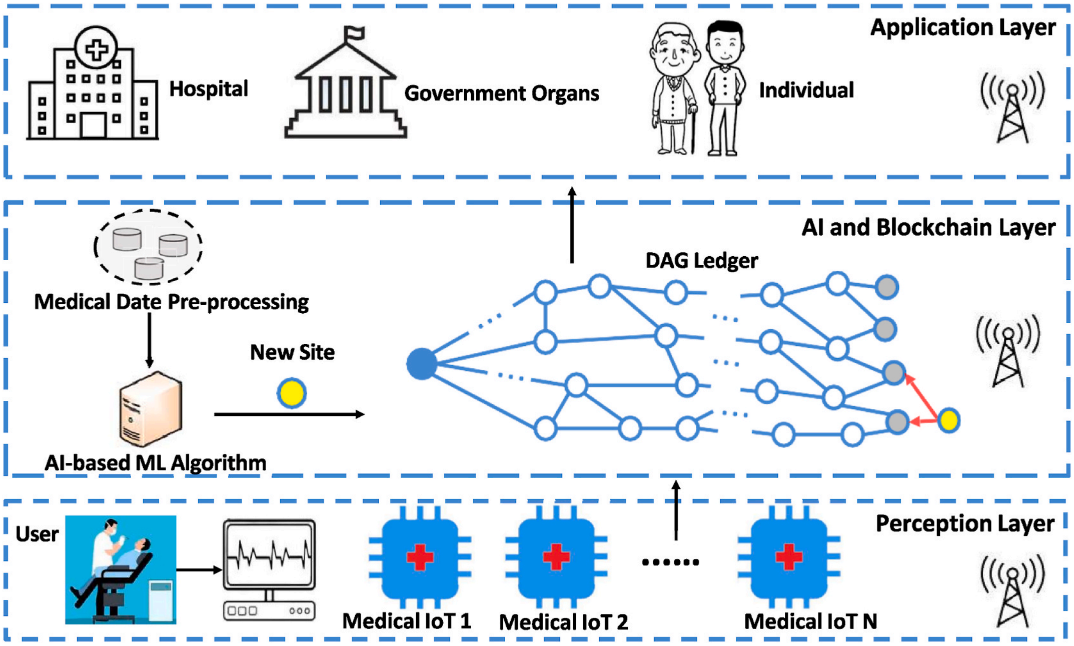

Fig. 1. Information exchange approach.

required for blockchain systems to reach consensus by designing a new tip selection algorithm, thereby improving the efficiency of information exchange.

3. Information exchange approach

The information exchange framework based on AI and DAG-enabled blockchain proposed in this paper is designed to provide a secure and efficient information exchange environment for the Medical IoT. Blockchain technology, with its decentralized architecture, guarantees information immutability and robust security Sharma, Kumar, Bhushan, Goyal and Iyer [29]. Additionally, the DAG-enabled blockchain, due to its parallel validation and

rapid confirmation mechanisms, significantly mitigates latency and processing time in information exchange, thereby enhancing information transfer efficiency. To further optimize consensus time within the DAG-enabled blockchain and improve information exchange efficiency, this paper introduces a disease category based tip selection algorithm. This algorithm intelligently filters and prioritizes the processing of medical information from specific categories, thereby optimizing resource allocation and reducing network load. Fig. 1 illustrates the architecture of the proposed approach, which is structured into three distinct layers: the perception layer, the AI and blockchain layer, and the application layer. The perception layer is responsible for real-time information acquisition, while the AI and blockchain layer employs advanced algorithms and decentralized technologies to ensure the security, privacy, and efficient transmission of information. The application layer delivers specific medical services and facilitates user interaction. By integrating AI and blockchain technologies, this approach not only ensures the integrity and security of information but also significantly enhances the availability and responsiveness of information exchange within the medical IoT ecosystem.

3.1. The perception layer

With the continuous development of medical technology, IoT, Augmented Reality (AR), Virtual Reality (VR), and other intelligent technologies are becoming crucial pillars in the healthcare industry. The widespread use of various medical sensors and wearable devices makes it more convenient and precise to monitor patients' physiological parameters. Through these smart devices, healthcare professionals can access real-time health information of patients, providing important references for diagnosis and treatment.

At the same time, patients can better manage their own health conditions, promoting the realization of personalized medical services. The application of medical IoT technology will bring more convenience and benefits to the healthcare sector. This layer consists of various medical IoT sensor devices that transmit sensed information to the AI and blockchain layers.

An important aspect of this process is ensuring that these devices possess sufficient computational power and network connectivity to effectively support blockchain operations. Specifically, blockchain technology requires devices to have certain storage capacity, processing power, and security features to ensure information transparency, immutability, and integrity. Additionally, the network connectivity of the devices is a crucial factor, as blockchain operations require a stable network environment to ensure the timely transmission and synchronization of information. Therefore, we assume that the IoT devices involved in information exchange have the capabilities to run the blockchain.

3.2. The AI and blockchain layer

In the field of medical IoT, ensuring information security and privacy protection is of paramount importance. To safeguard patient health information from unauthorized access or tampering, hash algorithms and encryption technologies are widely employed in both information transmission and storage processes. Hash algorithms are used for integrity checks prior to encrypting sensitive information, transforming the information into a fixed-length hash value. This allows the recipient to verify whether the information has been altered during transmission. Encryption technologies, on the other hand, protect the confidentiality of the information content, ensuring that only authorized recipients can decrypt and read the information.

During information transmission, the sender first encrypts the sensitive information using encryption algorithms (such as symmetric or asymmetric encryption). In the case of asymmetric encryption, the sender encrypts the information using the recipient's public key, and only the recipient's private key can decrypt the information. Upon receiving the encrypted information, the recipient decrypts it using the private key, ensuring both the integrity and confidentiality of the information. Additionally, the recipient typically verifies the integrity of the information using a hash algorithm after receiving the encrypted information. This process involves comparing the received hash value with the hash value provided by the sender, ensuring that the information has not been tampered with during transmission. To further enhance information security, the recipient must also perform authorization checks to ensure that information is accessed or processed only when explicit consent has been granted. This can be achieved through digital signatures or identity authentication mechanisms, ensuring that information usage complies with relevant privacy protection and consent regulations. Therefore, the application of hash and encryption technologies in healthcare IoT, combined with machine learning-based anomaly detection algorithms, not only effectively prevents information breaches and tampering but also ensures the quality, reliability, and legality of the information, thereby enhancing the security and trustworthiness of healthcare systems.

During the information pre-processing stage, AI techniques are commonly employed to clean, transform, and normalize raw information, thereby enabling more efficient handling by subsequent machine learning algorithms. First, information cleansing is performed to eliminate duplicate entries, missing values, and outliers. Next, information transformation techniques are applied for tasks such as feature extraction, dimensionality reduction, and encoding. Finally, information normalization is carried out to scale the information to a consistent range or distribution, such as

$$x_{norm} = \frac{x - min(x)}{max(x) - min(x)} \tag{1}$$

where x represents the raw information, while min(x) and max(x) denote the minimum and maximum values of the information, respectively.

After the information pre-processing stage, ML classifiers are applied to the dataset to detect and classify anomalous information points. Commonly used anomaly detection algorithms include Support Vector Machines, Random Forests, and Neural Networks. For example, in anomaly detection tasks, neural networks can learn complex patterns in the information to identify anomalous instances. The classification function of a neural network can be represented as

$$f(x) = \sigma\left(\boldsymbol{W}^T x + \boldsymbol{b}\right) \tag{2}$$

where σ is the activation function (such as Sigmoid, ReLU, etc.), **W** is the weight matrix, and **b** is the bias vector.

Once anomalous information is detected, the AI algorithm will automatically label and remove these information, returning a cleaned dataset comprising only normal information. This process can be represented by the following formula

$$\text{Clean Information} = x_i | y_i = \text{Normal}, i = 1, 2, \ldots, N \tag{3}$$

where x_i represents the i-th information sample, y_i is its corresponding label (normal or anomalous), and N is the size of the dataset.

Through the aforementioned steps, AI pre-processes the information, removes any compromised information using machine learning classifiers, and subsequently records the cleaned information onto the blockchain. This process ensures the immutability and transparency of medical IoT information, thereby enhancing its credibility and security. Consequently, the integration of blockchain technology in medical information exchange is of paramount importance. By storing medical information on the blockchain, both information security and privacy protection can be effectively ensured. Furthermore, the tamper-resistant and decentralized characteristics of blockchain make medical information less vulnerable to unauthorized alterations or theft. This enhances trust among patients and healthcare institutions, facilitating more secure sharing and utilization of medical information. As a key component of blockchain technology, smart contracts are capable of automatically executing predefined conditions and operations. In the context of medical information management, smart contracts help maintain information accuracy and integrity, while minimizing errors and risks associated with human intervention. This mechanism provides strong support for the

efficient management and use of medical information.

To improve the efficiency of blockchain consensus, we introduce a DAG-enabled blockchain system and propose a disease category-based tip selection algorithm. This approach optimizes transaction processing and verification mechanisms, enabling faster and more efficient information confirmation and storage. Once information is securely stored on the blockchain, users can seamlessly access and retrieve the necessary information at the application layer, thereby facilitating the sharing and utilization of medical information. A detailed explanation of the disease category-based tip selection algorithm will be provided in Section 4.

3.3. The application layer

To protect patient privacy, the users of this layer only include individuals closely related to the patient's condition, such as the patient, their family members, and attending physicians. At the application layer, by receiving trustworthy information transmitted through AI and blockchain layers, users can promptly understand the relevant situation of the patient and take necessary actions to safeguard the patient's health and well-being. Furthermore, leveraging the traceability provided by blockchain, healthcare professionals can extract and analyze the past medical records of patients, enabling more targeted treatment approaches.

This integration of AI and blockchain technologies in the healthcare information exchange system not only effectively safeguards patient privacy but also brings significant advancements to the healthcare sector. With the assistance of AI, medical personnel can rapidly and accurately access the latest patient information, facilitating scientific decision-making and personalized treatment plan development. The introduction of blockchain technology ensures the security and integrity of medical information, preventing tampering and misuse, thereby providing robust support for the integrity building in the healthcare industry. Moreover, with the proposed tip selection algorithm, the consensus-reaching time in the DAG-enabled blockchain system can be reduced, decreasing the time for users to obtain trustworthy information from the DAG-enabled blockchain and enhancing the efficiency of medical IoT information exchange.

Many scholars have conducted extensive research on the integration of blockchain in areas such as IoT information transmission. For instance, Bhattacharjee et al. Bhattacharjee, Gangwar, Kumar, Saini, Saini, Chauhan, Pandey and Goyal [30] proposed a blockchain-based IoT system framework that uses blockchain for secure information transmission, with a primary focus on enhancing information security. Qi et al. Qi, Chiaro, Giampaolo and Piccialli [31] proposed DON-B-STRESSED, an innovative framework that integrates deep learning, blockchain, and medical IoT technologies to provide an early stress detection method for users wearing predictive IoT devices. In contrast, the AI and DAG-enabled blockchain information exchange approach for medical IoT presented in this paper focuses on improving the efficiency of information exchange within the medical IoT ecosystem.

4. The disease category based tip selection algorithm

Tip selection algorithm is an algorithm used in DAG-enabled blockchain to select the next block that should be added to the blockchain. In traditional blockchain, a chain-like structure is used where each block has only one predecessor. However, in DAG-enabled blockchain, blocks can have multiple predecessors, forming a directed acyclic graph structure. The tip selection algorithm is based on specific rules and strategies, selecting two blocks from numerous unconfirmed blocks to add the newly generated site to the DAG-enabled blockchain within a given time. This ensures that the entire DAG structure can maintain reasonable growth and guarantees the security and scalability of the network.

In traditional DAG-enabled blockchain system, the tip selection probability depends on biased random walks, i.e., the MCMC algorithm. The selection probability from site x to tip y can be represented as

$$P_{xy} = \frac{exp\{-\kappa(CW_x - CW_y)\}}{\sum_{z\in\mathbb{T}} \exp\{-\kappa(CW_x - CW_z)\}} \tag{4}$$

where $\kappa > 0$ is a parameter to be chosen, and $\mathbb{T}$ represents the collection of current tips of the DAG ledger. CW is the cumulative weight of the tips. Moreover, the algorithm has to trace the previous M sites (M is called particle deep (PD) and is large Popov [18]). However, in the process of exchanging medical information, the selection and validation of tips are related to disease categories. It is inaccurate to solely use cumulative weights to validate tips. Additionally, due to the graph-like structure of DAG-enabled blockchain, stored information is relatively scattered, which hinders information retrieval on the blockchain.

Therefore, to improve the accuracy of tip selection and the relevance of similar information, we have defined a parameter related to disease categories, namely the disease category indicator, denoted as I. It can be a single attribute, such as a category number, or a combination of several attributes. Therefore, combining the disease category indicator I into the selection probability of intelligent vehicles can be expressed as

$$P_{xy} = \frac{exp\left\{-\alpha\left(CW_{s_1^1} - CW_{s_2^1}\right) - \beta(I_x - I_y)^2\right\}}{\sum_{z\in\mathbb{T}} \exp\left\{-\alpha\left(CW_{s_1^z} - CW_{s_2^z}\right) - \beta(I_x - I_z)^2\right\}} \tag{5}$$

$^{\mathrm{w}}$here α and β are both positive weight parameters to be chosen. $CW_{s_1^1}$ and $CW_{s_2^1}$ are cumulative weights of two sites approved by tip y. I_x and I_y are the corresponding disease category indicator of sites x and y.

This tip selection algorithm based on disease category indicator contributes to the establishment of a more cohesive and specialized information exchange network. By prioritizing tips that are relevant to their own disease category, sites establish closer connections, facilitating the exchange and sharing of information within the same domain. This enhanced relevance improves the efficiency and accuracy of information exchange, aiding in achieving more significant outcomes in the field of medical IoT research and applications. Additionally, this intelligent tip selection mechanism provides more reliable information support for medical decisions, thereby enhancing the quality and efficiency of healthcare services.

To evaluate the performance of the proposed tip selection algorithm, we compared it with the traditional MCMC algorithm used in conventional DAG-enabled blockchain systems. The experimental comparison results will be elaborated in detail in Section 5.

5. Performance evaluation

We evaluate the performance of the proposed AI and DAG-enabled blockchain on ledger convergence, tip selection delay, and site confirmation delay in the following details. The main parameters are shown in Table 1.

5.1. The ledger convergence

Ledger convergence is crucial for the proper functioning of a DAG-enabled blockchain. In a DAG-enabled blockchain, ledger convergence means that nodes across the entire network can achieve consensus on the validity and ordering of transactions, ensuring the security and reliability of the network. Therefore, it is essential to ensure ledger convergence whenever the tip selection algorithm is modified.

In order to comprehensively evaluate ledger convergence, we simulated the changes in the number of tips when site generation follows Uniform distribution, Poisson distribution, and Normal distribution. To verify the convergence of the ledger under different

Table 1
The main parameters.

Parameters	Values
Device number	20
CW of each site	1
Hash algorithm	SHA-256
α	1
β	1
Uniform distribution	Uni in (40, 50)
Poisson distribution	Poi with $\gamma = 100$
Normal distribution	Nor with $\mu = 80$, $\sigma = 0$

initial states, we provided two different initial values for the number of sites (e.g., low initial sites equal to 20, high initial sites equal to 800). Regardless of the initial values of the sites, as long as the total number of sites in the ledger stabilizes around a certain value, it can be demonstrated that the ledger has converged.

As shown in Fig. 2, when the generation of sites follows a Uniform distribution, the fluctuation in the number of tips is minimal once the blockchain system stabilizes. When the site generation follows a Poisson distribution, although the fluctuation in the number of tips is maximal after the blockchain system stabilizes, it still tends towards

stability. In the case where site generation follows a Normal distribution, the fluctuation in the number of tips tends to be between the two aforementioned scenarios. This demonstrates that the proposed tip selection algorithm can ensure the convergence of the DAG ledger.

5.2. The tip selection delay

Tip selection delay refers to the time taken by a site to choose a tip for appending when joining the DAG-enabled blockchain. In the tip selection algorithm used in this paper, we consider the disease category indicator, and newly generated sites prioritize selecting tips that are similar in disease category indicator. This approach not only enables quick tip selection but also increases the relevance of the information being added to the chain. We compared the algorithm proposed in this paper with the MCMC algorithm. We contrasted the time taken for tip selection for newly generated sites in the two algorithms when the parameter PD takes values of 50, 100, and 150, respectively.

As shown in Fig. 3, experimental results demonstrate that the algorithm proposed in this paper exhibits lower tip selection latency compared to the MCMC algorithm. This reduction in latency contributes to minimizing site confirmation delays. Furthermore, it enhances overall network throughput, promoting efficient information exchange and real-time information transmission within medical IoT systems. Additionally, the reduction in tip selection latency

improves the system's responsiveness to emergency situations, thereby strengthening the security and reliability of medical IoT systems.

5.3. The site confirmation delay

Confirmation delay refers to the time taken for a specific site to reach a certain cumulative weight. According to reference Popov [18], during the adaptation period, the cumulative weight of benign sites grows with increasing speed. After the adaptation period, the cumulative weight increases with the rate λW. We set the weight of each site to 1, so the growth of the cumulative weight is only related to the rate λ. Therefore, we considered the impact of different rates λ on confirmation delay. Comparisons of the DAG-enabled blockchain using our proposed algorithm and the MCMC algorithm under different cumulative weight threshold settings are shown in Fig. 4.

The results indicate that, when the cumulative weight threshold is the same, our proposed algorithm exhibits a shorter confirmation delay compared to using the MCMC algorithm, thereby enhancing the efficiency of information exchange in medical IoT. This will enable medical IoT systems to transmit critical medical information and real-time monitoring information more rapidly and reliably, accelerating healthcare professionals' response to patients' conditions and contributing to the improvement of the quality and efficiency of healthcare services. Simultaneously, by reducing confirmation delay, our algorithm provides a more stable and reliable information exchange environment for medical IoT systems, contributing to ensuring the security and integrity of medical information.

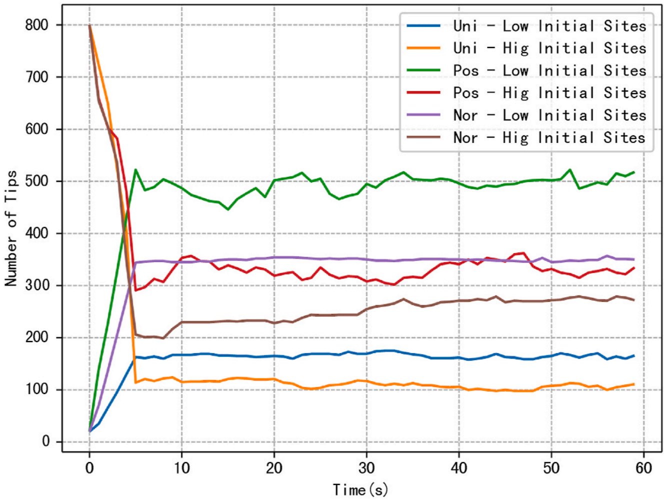

Fig. 2. Ledger convergence.

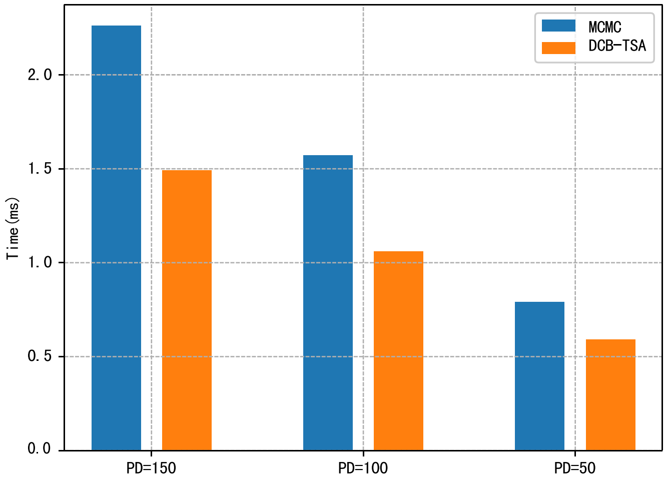

Fig. 3. Tip selection delay.

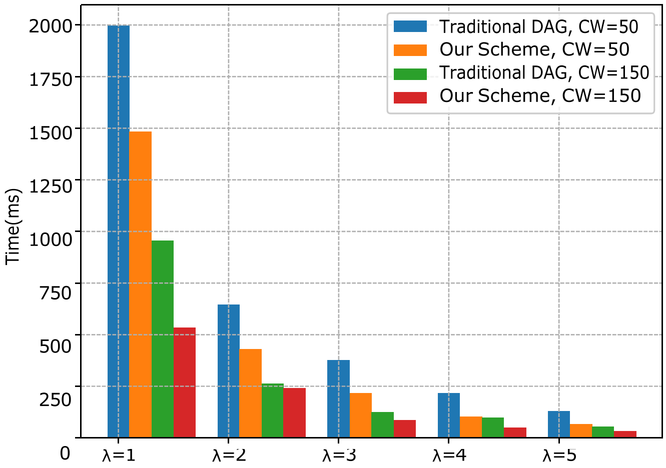

Fig. 4. Site confirmation delay.

6. Conclusion

In this paper, we propose an efficient information exchange approach based on AI and DAG-enabled blockchain for medical IoT. To address the challenge posed by the slow consensus process of traditional blockchains, which hinders the rapid incorporation of information, we introduce a novel method that combines AI with DAG-enabled blockchain technology and design a new tip selection algorithm to accelerate information entry into the blockchain network. Security analysis and simulation results demonstrate that the proposed approach enhances the efficiency of information exchange within medical IoT systems. Future research will focus on reducing information redundancy and minimizing communication complexity to improve consensus efficiency and further enhance blockchain scalability.

CRediT authorship contribution statement

Shanqin Wang: Writing – review & editing, Writing – original draft, Software, Methodology, Data curation. **Gangxin Du:** Writing – review & editing, Conceptualization. **Shufan Dai:** Writing – review & editing, Conceptualization. **Mengjun Miao:** Writing – review & editing. **Miao Zhang:** Writing – review & editing.

Data availability statement

The datasets generated and analyzed during the current study are available from the corresponding author upon reasonable request. Access to the data may require an appropriate data-sharing agreement to ensure compliance with ethical and legal considerations.

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.

Acknowledgements

The work was supported by Anhui Provincial Quality Engineering Project for Higher Education Institutions (2022jnds043), Chuzhou Polytechnic Campus Science and Technology Innovation Platform Project (YJP- 2023-02), Anhui Provincial Natural Science Research Project for Higher Education Institutions (2023AH053088, 2022AH040332), Chuzhou Polytechnic Campus Research Project (ZKZ-2022-02), Anhui Province Quality Improvement and Talent Cultivation Project (2022TZPY040), Anhui Province Mid-Career and Young Teachers Training Initiative - Outstanding Young Teacher Cultivation Project(YQYB2023163).

References

[1] S. He, K. Shi, C. Liu, B. Guo, J. Chen, Z. Shi, Collaborative sensing in internet of things: a comprehensive survey, IEEE Commun. Surv. Tutor. 24 (2022) 1435–1474, https://doi.org/10.1109/COMST.2022.3187138.
[2] M. AlSelek, J.M. Alcaraz-Calero, Q. Wang, Dynamic ai-iot: enabling updatable ai models in ultra-low-power 5g iot devices, IEEE Internet Things J. (2023), https://doi.org/10.1109/JIOT.2023.3340858, 1–1.
[3] N. Cheng, S. Wu, X. Wang, Z. Yin, C. Li, W. Chen, F. Chen, Ai for uav-assisted iot applications: a comprehensive review, IEEE Internet Things J. 10 (2023) 14438–14461, https://doi.org/10.1109/JIOT.2023.3268316.
[4] D. Saraswat, P. Bhattacharya, A. Verma, V.K. Prasad, S. Tanwar, G. Sharma, P.N. Bokoro, R. Sharma, Explainable ai for healthcare 5.0: opportunities and challenges, IEEE Access 10 (2022) 84486–84517, https://doi.org/10.1109/ACCESS.2022.3197671.
[5] N. Taimoor, S. Rehman, Reliable and resilient ai and iot-based personalised healthcare services: a survey, IEEE Access 10 (2022) 535–563, https://doi.org/10.1109/ACCESS.2021.3137364.
[6] R. Kalakoti, H. Bahsi, S. Nõmm, Improving iot security with explainable ai: quantitative evaluation of explainability for iot botnet detection, IEEE Internet Things J. (2024), https://doi.org/10.1109/JIOT.2024.3360626, 1–1.
[7] M. Dave, V. Rastogi, M. Miglani, P. Saharan, N. Goyal, Smart fog-based video surveillance with privacy preservation based on blockchain, Wireless Pers. Commun. 124 (2022), https://doi.org/10.1007/s11277-021-09426-8.
[8] A. Rana, S. Sharma, K. Nisar, A.A.A. Ibrahim, S. Dhawan, B. Chowdhry, S. Hussain, N. Goyal, The rise of blockchain internet of things (biot): secured, device-to-device architecture and simulation scenarios, Appl. Sci. 12 (2022), https://doi.org/10.3390/app12157694. URL: https://www.mdpi.com/2076-3417/12/15/7694.
[9] S.H.A. Shah, D. Koundal, V. Sai, S. Rani, Guest editorial: special section on 5g edge computing-enabled internet of medical things, IEEE Trans. Ind. Inf. 18 (2022) 8860–8863, https://doi.org/10.1109/TII.2022.3193708.
[10] H.M. Rai, K.K. Shukla, L. Tightiz, S. Padmanaban, Enhancing data security and privacy in energy applications: integrating iot and blockchain technologies, Heliyon 10 (2024) e38917, https://doi.org/10.1016/j.heliyon.2024.e38917.
[11] C.J. Martínez, S. Galmés, Analysis of the primary attacks on iomt internet of medical things communications protocols, in: 2022 IEEE World AI IoT Congress (AIIoT), 2022, pp. 1–7, https://doi.org/10.1109/AIIoT54504.2022.9817252.
[12] K.S. Sankaran, T.H. Kim, P.N. Renjith, An improved ai-based secure m-trust privacy protocol for medical internet of things in smart healthcare system, IEEE Internet Things J. 10 (2023) 18477–18485, https://doi.org/10.1109/JIOT.2023.3280592.
[13] K.P. Reddy, M. Satish, A. Prakash, S. Babu, P. Kumar, B.S. Devi, Machine learning revolution in early disease detection for healthcare: advancements, challenges, and future prospects, in: 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), 2023, pp. 638–643, https://doi.org/10.1109/ICCCMLA58983.2023.10346963.
[14] S.S. Phatak, H.S. Patil, M.W. Arshad, B. Jitkar, S. Patil, J. Patil, Advanced face detection using machine learning and ai-based algorithm, in: 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022, pp. 1111–1116, https://doi.org/10.1109/IC3I56241.2022.10072527.
[15] P. Shen, S. Li, M. Huang, H. Gao, L. Li, J. Li, H. Lei, A survey on safety regulation technology of blockchain application and blockchain ecology, in: 2022 IEEE International Conference on Blockchain (Blockchain), 2022, pp. 494–499, https://doi.org/10.1109/Blockchain55522.2022.00076.
[16] P. Shrivastav, M. Sadasivan, Blockchain-based system for secure data sharing in cloud using machine learning: current researches and challenges, in: 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), 2023, pp. 1078–1084, https://doi.org/10.1109/ICIDCA56705.2023.10099950.
[17] A. Cullen, P. Ferraro, W. Sanders, L. Vigneri, R. Shorten, Access control for distributed ledgers in the internet of things: a networking approach, IEEE Internet Things J. 9 (2022) 2277–2292, https://doi.org/10.1109/JIOT.2021.3096129.
[18] S. Popov, The tangle, White paper 1 (2018).
[19] L. Zhao, L. Vigneri, A. Cullen, W. Sanders, P. Ferraro, R. Shorten, Secure access control for dag-based distributed ledgers, IEEE Internet Things J. 9 (2022) 10792–10806, https://doi.org/10.1109/JIOT.2021.3128025.
[20] S.M. Alrubei, E. Ball, J.M. Rigelsford, A secure blockchain platform for supporting ai-enabled iot applications at the edge layer, IEEE Access 10 (2022) 18583–18595, https://doi.org/10.1109/ACCESS.2022.3151370.
[21] S. Alrubei, E. Ball, J. Rigelsford, A secure distributed blockchain platform for use in ai-enabled iot applications, in: 2020 IEEE Cloud Summit, 2020, pp. 85–90, https://doi.org/10.1109/IEEECloudSummit48914.2020.00019.
[22] S. Selvarajan, G. Srivastava, A.O. Khadidos, A.O. Khadidos, M. Baza, A. Alshehri, J.C.W. Lin, An artificial intelligence lightweight blockchain security model for security and privacy in iiot systems, J. Cloud Comput. 12 (2023) 38.
[23] V. Charles, A. Emrouznejad, T. Gherman, A critical analysis of the integration of blockchain and artificial intelligence for supply chain, Ann. Oper. Res. (2023) 1–41.
[24] M. Shen, A. Gu, J. Kang, X. Tang, X. Lin, L. Zhu, D. Niyato, Blockchains for artificial intelligence of things: a comprehensive survey, IEEE Internet Things J. 10 (2023) 14483–14506, https://doi.org/10.1109/JIOT.2023.3268705.
[25] G. Quan, Z. Yao, L. Chen, Y. Fang, W. Zhu, X. Si, M. Li, A trusted medical data sharing framework for edge computing leveraging blockchain and outsourced computation, Heliyon 9 (2023) e22542.
[26] H. Liu, X. Guan, R. Bai, T. Qin, Y. Chen, T. Liu, Designing a medical information diagnosis platform with iot integration, Heliyon 10 (2024) e25390.
[27] K.S. Sankaran, T.H. Kim, P.N. Renjith, An improved ai-based secure m-trust privacy protocol for medical internet of things in smart healthcare system, IEEE Internet Things J. 10 (2023) 18477–18485, https://doi.org/10.1109/JIOT.2023.3280592.

[28] B. Panchal, S. Parmar, T. Rathod, N.K. Jadav, R. Gupta, S. Tanwar, Ai and blockchain-based secure message exchange framework for medical internet of things, in: 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), 2023, pp. 1–6, https://doi.org/10.1109/NMITCON58196.2023.10275980.

[29] S. Sharma, A. Kumar, M. Bhushan, N. Goyal, S.S. Iyer, Is Blockchain Technology Secure to Work on? Igi-Global, com, 2021, https://doi.org/10.4018/978-1-7998-6694-7.ch005.

[30] S. Bhattacharjee, S. Gangwar, M. Kumar, K. Saini, R. Saini, S. Chauhan, K. Pandey, N. Goyal, An efficient framework for secure data transmission using blockchain in iot environment, J. Autonom. Intell. 7 (2024), https://doi.org/10.32629/jai.v7i2.1073.

[31] P. Qi, D. Chiaro, F. Giampaolo, F. Piccialli, A blockchain-based secure internet of medical things framework for stress detection, Inf. Sci. 628 (2023) 377–390, https://doi.org/10.1016/j.ins.2023.01.123. Elsevier.