Interdisciplinary Research in Medical Sciences Specialty
ISSN: 3062-4401
2021, Volume 1, Issue 1, Page No: 100-110

Available online at: www.galaxypub.co/page/journals

Galaxy Publication

AI-Enhanced Secure and Efficient Information Exchange in Medical IoT Using DAG-Based Blockchain

Lukas Schneider[1], Martin Keller[1], Johannes Braun[1]*

[1]Department of Medical Informatics, Faculty of Medicine, Heidelberg University, Heidelberg, Germany.

***E-mail** ✉ johannes.braun.med@hotmail.com

Received: 19 February 2021; **Revised:** 21 April 2021; **Accepted:** 23 May 2021

ABSTRACT

Advances in artificial intelligence (AI)–driven medical Internet of Things (IoT) systems have greatly simplified the acquisition and sharing of clinical data. Nevertheless, issues related to confidentiality, protection of sensitive information, and communication performance have become increasingly urgent. Although numerous studies apply AI and blockchain frameworks to mitigate these concerns, limited attention has been given to how the inherently slow consensus procedures of traditional blockchain designs restrict exchange efficiency. To address this, we introduce an AI-assisted information exchange model built on a DAG-based blockchain architecture, aiming to deliver a secure and high-performance data-sharing environment for the medical IoT. Furthermore, a new tip-selection mechanism is presented to shorten consensus latency, enabling quicker access to reliable blockchain-based information. Simulation outcomes confirm that, relative to existing DAG-oriented blockchain strategies, the method described in this work offers superior information exchange efficiency.

Keywords: Information exchange, DAG-Enabled blockchain, Medical IoT, AI

How to Cite This Article: Schneider L, Keller M, Braun J. AI-Enhanced Secure and Efficient Information Exchange in Medical IoT Using DAG-Based Blockchain. Interdiscip Res Med Sci Spec. 2021;1(1):100-10. https://doi.org/10.51847/2v8zK0sCQt

Introduction

With the emergence of smart healthcare, automated farming, intelligent home technologies, and self-driving systems, societal development has significantly improved everyday life. In particular, IoT-driven medical systems have shown substantial advantages He, Shi, Liu, Guo, Chen and Shi [1]. Sensors in IoT environments continuously track physiological indicators—including heart rate, blood pressure, and glucose readings—and transmit these data to clinicians, enabling rapid medical responses AlSelek, Alcaraz-Calero and Wang [2] Cheng, Wu, Wang, Yin, Li, Chen and Chen [3]. Analyzing the extensive datasets generated by these devices allows practitioners to design individualized therapeutic strategies for patients Saraswat, Bhattacharya, Verma, Prasad, Tanwar, Sharma, Bokoro and Sharma [4]. ML tools also support the detection of health patterns and risk elements, facilitating preventive care. IoT platforms further encourage patients to participate in their daily health routines by offering immediate feedback and personalized guidance, improving engagement and adherence Taimoor and Rehman [5] Kalakoti, Bahsi and Nõmm [6].

Blockchain technology has gained prominence because of its decentralized nature, tamper-resistant design, and auditability. Dave *et al*. Dave, Rastogi, Miglani, Saharan and Goyal [7] developed a privacy-preserving smart-home video monitoring framework using distributed fog nodes, incorporating a private blockchain for system integrity, fuzzy-key handling, and controlled video access. Rana *et al*. Rana, Sharma, Nisar, Ibrahim, Dhawan, Chowdhry, Hussain and Goyal [8] introduced a blockchain-supported model that strengthens accountability, privacy, and data availability while uncovering hidden patterns. In contrast to prior work relying on private blockchains or focusing solely on privacy protection, this study integrates AI with a DAG-enabled blockchain to support medical IoT information sharing.

Despite its benefits, secure and efficient communication among interconnected devices still faces considerable obstacles involving privacy, protection, and latency. Attackers frequently target weak IoT components to launch diverse cyberattacks Shah, Koundal, Sai and Rani [9] Rai, Shukla, Tightiz and Padmanaban [10]. AI-driven security frameworks can defend confidential medical data, Martínez and Galmés [11], as AI models can learn baseline user and network behaviors, detect anomalies in real time, and reveal possible threats. Through ML-based pattern recognition, AI can identify attack signatures and vulnerabilities, enabling proactive defense strategies Sankaran, Kim and Renjith [12]. ML techniques can also help differentiate uncompromised information, which smart contracts can then commit to a DAG-enabled blockchain, ensuring immutability and integrity Reddy, Satish, Prakash, Babu, Kumar and Devi [13] Phatak, Patil, Arshad, Jitkar, Patil and Patil [14]. Smart contracts—automated protocols encoded on the blockchain—allow reliable operations without intermediaries, executing predefined actions such as fund transfers, asset swaps, or data recording once preset conditions are fulfilled Shen, Li, Huang, Gao, Li, Li and Lei [15] Shrivastav and Sadasivan [16].

However, the slow consensus procedure used in conventional blockchain platforms greatly limits the immediacy of accessing newly recorded information. For instance, the Bitcoin network produces roughly one block every 10 min, meaning that at least 10 min must pass before any data receives final confirmation. In comparison, Ethereum creates a block about every 12 s, offering a quicker confirmation rate than Bitcoin, yet still failing to satisfy the near–real-time requirements expected in medical IoT environments Cullen, Ferraro, Sanders, Vigneri and Shorten [17]. A DAG-enabled blockchain adopts a different ledger structure than linear blockchains Popov [18]. Instead of arranging transactions sequentially in a chain, DAG systems link each transaction to earlier ones via directed edges, forming a directed acyclic graph Zhao, Vigneri, Cullen, Sanders, Ferraro and Shorten [19]. This architecture enhances scalability and throughput because each new transaction validates several previous ones rather than waiting for an entire block to be verified. Nonetheless, the commonly adopted Markov Chain Monte Carlo (MCMC) tip-selection process in traditional DAG frameworks often requires numerous computation rounds to stabilize, slowing confirmation times and restricting performance. Consequently, a more efficient tip-selection mechanism is needed to overcome MCMC-related limitations and create a faster, more secure medical IoT information-exchange environment.

To mitigate these concerns, this study presents an AI-assisted information-exchange framework built on a DAG-enabled blockchain to deliver a protected medical-data sharing environment. Additionally, a disease-category-driven tip selection strategy is introduced to accelerate consensus formation, thereby offering quicker access to trustworthy information. The key contributions are outlined below.

- We introduce an AI-supported DAG-enabled blockchain information-exchange model designed to provide a safe and reliable communication environment for the medical IoT.
- We propose a tip-selection mechanism based on disease classification to shorten consensus time, allowing information to be added to the ledger more rapidly and improving exchange efficiency.
- Experimental simulations show that, relative to prior approaches, the method described in this work achieves superior security and information-exchange performance for medical IoT systems.

Overall, the AI-driven DAG-enabled blockchain information-exchange framework developed in this paper refines the consensus procedure, reduces confirmation latency, and aims to offer a faster and more secure data-exchange environment for the medical IoT. The remainder of this article is structured as follows. Section 2 presents related research. Section 3 outlines the information-exchange scheme. Section 4 introduces the disease-category-based tip-selection algorithm. Section 5 provides performance evaluations. Section 6 concludes the study.

Related work

As the medical IoT expands rapidly, challenges related to protecting medical data and ensuring efficient communication have become more prominent. Centralized approaches create vulnerability risks, whereas blockchain technology offers a decentralized alternative to enhance dependability. When combined with AI, these systems can process, analyze, and exchange medical information more intelligently. Thus, this paper explores an efficient AI- and DAG-enabled blockchain method for medical IoT information exchange. Because both AI and blockchain bring complementary strengths, research on their integration within medical IoT settings has grown steadily.

Edward *et al*. Alrubei, Ball and Rigelsford [20] proposed a framework merging edge computing, AI, IoT sensing devices, and blockchain. The system performs environmental monitoring, data collection, analysis, and AI-based inference, then publishes results to a public blockchain. Subhi *et al*. Alrubei, Ball and Rigelsford [21] developed

a similar architecture combining edge resources, AI methods, and blockchain to support rapid, secure, and intelligent data handling and distribution. Gautam *et al*. Selvarajan, Srivastava, Khadidos, Khadidos, Baza, Alshehri and Lin [22] designed a lightweight AI-driven blockchain security model that safeguards privacy in IoT systems, particularly those relying on cloud or edge processing. Charles *et al*. Charles, Emrouznejad and Gherman [23] surveyed the integration of blockchain and AI across supply-chain applications, summarizing current implementations and identifying future research avenues. Meng *et al*. Shen, Gu, Kang, Tang, Lin, Zhu and Niyato [24] explored why blockchain is useful for AI-of-Things systems, reviewed existing solutions in terms of efficiency, privacy, trust, incentives, and security, and discussed ongoing challenges and prospective research directions.

Besides, Quan *et al*. Quan, Yao, Chen, Fang, Zhu, Si and Li [25] designed a blockchain-oriented scheme for trusted sharing of medical data within an edge-computing setting. Their model uses an edge-based consortium blockchain to realize fine-grained authorization of medical records. Liu *et al*. Liu, Guan, Bai, Qin, Chen and Liu [26] explored a medical information diagnostic platform by incorporating swarm algorithms and evolutionary computation. They examined the current progress of diagnosis platforms built on chat-based pre-trained converters and IoT systems, followed by an in-depth comparison of the strengths and limitations of swarm and evolutionary techniques in such platforms. Sankaran *et al*. Sankaran, Kim and Renjith [12] introduced a Secure M-Trust Privacy Protocol (SMP) to counter related challenges. SMP merges trust evaluation, cryptographic protection, and machine learning to offer confidentiality and privacy during data transmission. It is designed to operate alongside smart health-monitoring infrastructures, supplying an isolated and secure communication route among devices. However, the approach suffers from drawbacks, including reduced efficiency of its cryptographic scheme when many devices and large patient datasets are involved, as well as dependence on a centralized trust entity for key distribution. Panchal *et al*. Panchal, Parmar, Rathod, Jadav, Gupta and Tanwar [27] proposed an AI-driven and blockchain-supported mechanism to secure medical IoT traffic. Several ML classifiers are leveraged to distinguish normal medical IoT data from attack-related data, after which an IPFS-backed blockchain is used to ensure transparency and protection. Nevertheless, the study does not address how slow blockchain consensus impacts message-exchange performance.

As outlined above, although the fusion of AI and blockchain has drawn extensive interest in medical IoT research, only a small number of studies have examined how slow consensus mechanisms influence these solutions. Thus, this work presents an AI-enhanced medical IoT information-exchange model using a DAG-enabled blockchain. By introducing a new tip-selection mechanism, the goal is to shorten consensus latency and improve overall information-exchange efficiency.

Information exchange approach

The AI-assisted DAG-enabled blockchain information-exchange framework proposed in this study aims to establish a secure and high-performance communication environment for medical IoT systems. Owing to its decentralized nature, blockchain ensures immutability and strong protection of stored data Sharma, Kumar, Bhushan, Goyal and Iyer [28]. Additionally, DAG-enabled blockchain, through parallel verification and fast confirmation, significantly reduces delays and processing overhead, thereby providing more efficient information dissemination. To further reduce consensus time and boost exchange efficiency, this work incorporates a disease-category-oriented tip-selection strategy. The algorithm intelligently ranks and filters medical data according to category, improving resource utilization and lowering system congestion. The architecture is presented in **Figure 1** and consists of three layers: the perception layer, the AI-and-blockchain layer, and the application layer. The perception layer collects information in real time; the AI-and-blockchain layer applies decentralized methods and intelligent algorithms to ensure secure, private, and efficient data flow; and the application layer delivers healthcare services and supports user-side interactions. By integrating AI and blockchain, the proposed system not only preserves data integrity and confidentiality but also noticeably enhances the responsiveness and reliability of information exchange across the medical IoT.

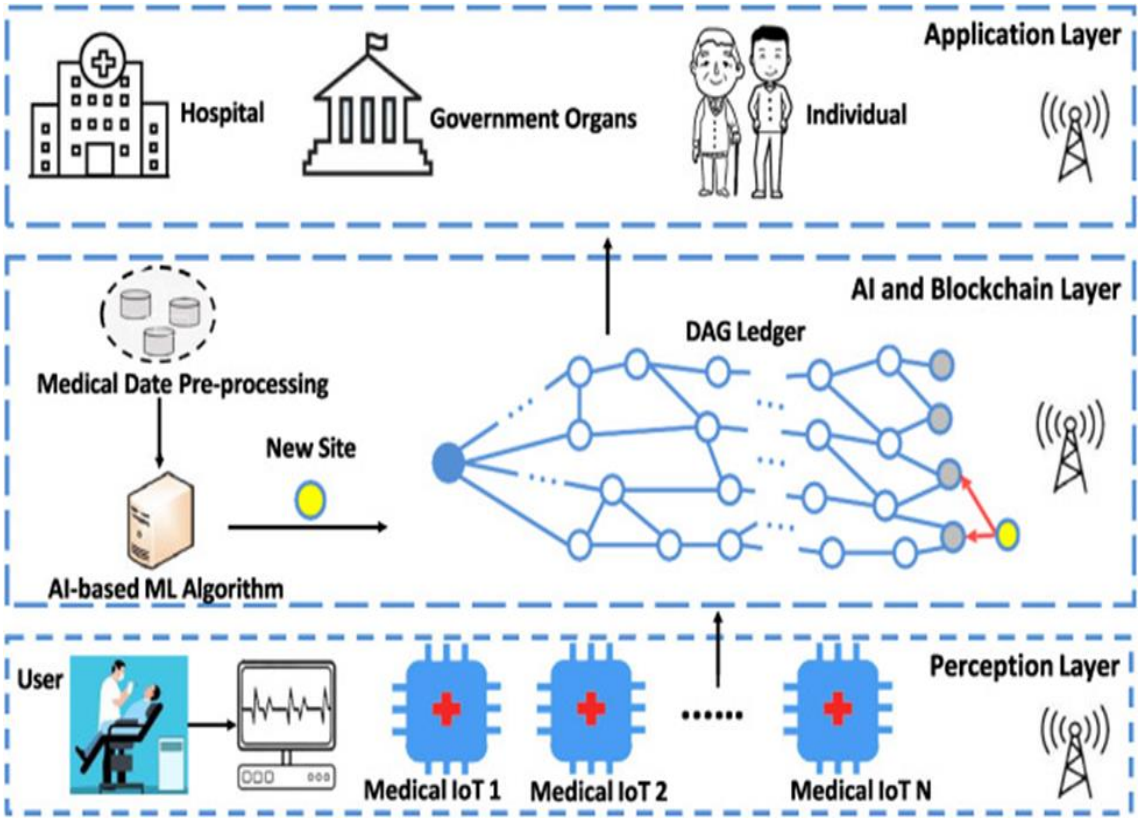

Figure 1. Information exchange approach.

The perception layer

As modern medical technology evolves, IoT, Augmented Reality (AR), Virtual Reality (VR), and other intelligent tools have become indispensable in healthcare. The broad deployment of medical sensors and wearable devices enables more precise and continuous monitoring of patients' physiological indicators. These smart systems offer medical personnel instant access to patient data, providing essential input for clinical decisions. Simultaneously, patients gain improved control over personal health management, supporting personalized healthcare services. Thus, the growth of medical IoT continues to bring significant convenience to healthcare delivery. This layer is composed of various sensing devices that forward collected information to the AI-and-blockchain layer.

A critical requirement is ensuring that IoT devices possess adequate computational resources and reliable connectivity to support blockchain participation. Blockchain operations demand specific levels of storage, processing capability, and built-in security to maintain transparency, tamper resistance, and data integrity. Stable network connections are equally important because blockchain relies on timely data propagation and synchronization. Therefore, we assume that participating IoT devices involved in information exchange are capable of running blockchain-related processes.

The AI and blockchain layer

Within medical IoT systems, protecting data confidentiality and safeguarding patient privacy are crucial requirements. To prevent unauthorized modification or access to health-related information, hashing methods and encryption schemes are routinely integrated into both the transmission and storage workflows. Hash functions are applied before the encryption of sensitive data to generate a fixed-size digest, enabling the receiver to determine whether any alterations occurred while the data was in transit. Encryption methods, by contrast, ensure that only validated users can view the content.

When information is being transmitted, the sender begins by encrypting the sensitive data using an appropriate cryptographic technique (for example, symmetric or asymmetric encryption). Under asymmetric encryption, the sender makes use of the recipient's public key to encrypt the message, and only the corresponding private key can decrypt it. After receiving the ciphertext, the recipient applies the private key to recover the original content, thereby preserving both confidentiality and integrity. It is also standard practice for the recipient to recheck data integrity with a hash function: the hash they compute is compared with the sender's hash to confirm that the

message was not modified during delivery. To strengthen protection measures further, the recipient must verify authorization to ensure that data is accessed or processed only when proper consent exists. This may be implemented through digital signatures or identity-verification procedures so that data usage remains compliant with required privacy and consent standards. Consequently, when hashing and encryption are coupled with machine-learning–based anomaly detection in medical IoT environments, they collectively prevent unauthorized disclosure or alteration of information, while also preserving its accuracy, dependability, and regulatory compliance—ultimately reinforcing the security posture of healthcare infrastructures.

In the information pre-processing stage, AI-driven methods are widely applied to refine, reformat, and standardize raw data, making it more suitable for downstream machine learning tasks. Initially, data-cleaning operations remove duplicated records, missing items, and abnormal values. Subsequently, data-transformation steps are used for feature extraction, dimensionality minimization, and encoding. Lastly, normalization procedures are applied to adjust values into a unified range or consistent distribution, such as:

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

where *x* denotes the unprocessed data values, and *min(x)* and *max(x)* correspond to the lowest and highest values observed in the dataset, respectively. Following this data preparation step, various ML classification models are employed to identify and categorize atypical data points. Frequently adopted methods for anomaly detection include Support Vector Machines, Random Forest classifiers, and different types of Neural Networks. As an illustration, neural models used in anomaly detection can capture intricate data relationships to flag unusual observations. The decision function of a neural network can be formulated as:

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

where σ denotes the chosen activation operation (e.g., Sigmoid, ReLU), W represents the matrix of trainable weights, and b indicates the associated bias terms.

After abnormal data entries are identified, the AI model proceeds to tag and filter out these irregular records, producing a refined dataset that includes only standard data points. This cleaning step can be expressed through the following relation:

$$Clean\ Information = xi | yi = Normal, i = 1,2,\ldots,N \tag{3}$$

where xi denotes the i-th data instance, yi specifies its associated class label (normal or abnormal), and N represents the total number of samples in the dataset.

By following the above procedures, the AI module processes the data, filters out corrupted entries via machine learning models, and then commits the sanitized dataset to the blockchain. This workflow upholds the permanence and openness of medical IoT data, thereby strengthening both its reliability and protection. As a result, incorporating blockchain into medical data exchange becomes highly significant. Storing medical records on the ledger allows both data confidentiality and privacy safeguards to be achieved. In addition, the anti-tamper and distributed attributes of blockchain reduce exposure to illicit modification or data leakage, reinforcing confidence among patients and healthcare providers and promoting safer data sharing and use. Smart contracts—an integral element of blockchain—can autonomously trigger predetermined rules and procedures. Within medical data administration, these contracts ensure accuracy and completeness while lowering mistakes and vulnerabilities tied to manual handling. This automated mechanism provides substantial support for the orderly and effective administration of medical information.

To enhance the performance of blockchain consensus, we incorporate a DAG-based ledger design and introduce a tip-selection method guided by disease categories. This methodology improves transaction validation and throughput, enabling more rapid confirmation and storage of records. After data is securely written to the blockchain, users can readily obtain the required information at the application layer, promoting smoother access and exchange of medical data. A detailed discussion of the disease-category-driven tip selection algorithm is provided in Section 4.

Application layer

To preserve confidentiality, the individuals permitted at this layer are limited to those directly involved in the patient's care—namely the patient, authorized relatives, and the attending medical staff. Through the verified data supplied by the AI and blockchain layers, users can promptly gain insight into the patient's status and take timely actions to maintain their health. Additionally, due to the traceable nature of blockchain, clinicians can review and evaluate earlier medical records, enabling more precise and tailored treatment plans.

The combined use of AI and blockchain for healthcare data exchange not only fortifies patient privacy but also contributes major improvements to clinical practice. AI enables rapid access to current patient data, supporting evidence-based decision-making and individualized therapy. Blockchain ensures data consistency and prevents manipulation or abuse, providing a solid foundation for trustworthy medical information management. Moreover, with the proposed tip-selection strategy, the consensus latency in the DAG-enabled blockchain is shortened, reducing the waiting time for obtaining validated information and improving the throughput of medical IoT data exchange.

Extensive literature explores the use of blockchain in IoT-related data transmission. For example, Bhattacharjee *et al*. Bhattacharjee, Gangwar, Kumar, Saini, Saini, Chauhan, Pandey, and Goyal [29] introduced a blockchain-oriented IoT model aimed at strengthening data protection in transmission scenarios. Qi *et al*. Qi, Chiaro, Giampaolo, and Piccialli [30] developed DON-B-STRESSED, a framework merging deep learning, blockchain, and medical IoT to offer early stress detection for users with predictive wearable devices. Distinct from these works, the AI-supported, DAG-based blockchain exchange model in this study specifically emphasizes improving the speed and efficiency of information flow within medical IoT systems.

Disease category-based tip selection algorithm

A tip selection algorithm functions within a DAG-structured blockchain to determine which block should be referenced next. Unlike conventional blockchains, which rely on a linear arrangement where each block points to a single ancestor, a DAG-enabled scheme allows a block to reference multiple predecessors, thus forming a directed acyclic graph. Under defined policies, the tip selection mechanism chooses two unconfirmed blocks so that the new site can be attached to the DAG within the prescribed time window. This maintains balanced network expansion and preserves both safety and scalability.

In standard DAG-enabled blockchain designs, the likelihood of selecting a tip is governed by biased random walk processes, typically implemented via the MCMC approach. The probability of moving from site x to tip y can be formulated as:

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

where $\kappa > 0$ is a tunable parameter, and $\mathbb{T}$ denotes the set of active tips in the DAG ledger. CW represents the cumulative weight assigned to these tips. In addition, the algorithm must backtrack through the previous M sites (with M referred to as the particle depth (PD), typically chosen to be large; see Popov [18]). However, during medical data exchange, the choice and confirmation of tips depend on disease categories. Thus, relying only on cumulative weight to verify tips results in insufficient accuracy. Furthermore, because the DAG structure distributes data across many branches, information retrieval becomes more complex and less efficient.

To enhance tip selection precision and strengthen connections among medically related records, we introduce a disease-associated parameter, termed the disease category indicator I. This indicator may represent a single feature—such as a numeric class label—or a union of multiple attributes. By integrating the indicator I into the tip-selection probability, the revised selection rule for intelligent nodes can be written as

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

where α and β are adjustable positive weighting coefficients. $CW_{s_1{}^1}$ and $CW_{s_2{}^1}$ denote the cumulative weights of the two sites referenced by tip y. Ix and Iy represent the disease category indicators associated with sites x and y, respectively.

This disease-aware tip selection strategy supports the formation of a more unified and domain-focused information exchange network. By giving priority to tips that align with the same disease category, sites develop stronger interconnections, which promotes, the sharing and transmission of information within a specific medical field.

Such increased relevance elevates both the precision and speed of data exchange, helping to generate more meaningful advancements in medical IoT applications and research. Moreover, this adaptive selection method strengthens the reliability of data used for clinical decisions, thereby improving the overall quality and operational efficiency of healthcare delivery.

To assess how well the proposed tip selection algorithm performs, we contrast it with the conventional MCMC-based approach employed in typical DAG-structured blockchain platforms. The comparative experimental analysis is presented in detail in Section 5.

Performance evaluation

We examine the performance of the introduced AI-supported DAG blockchain in terms of ledger convergence, time required for tip selection, and delay in confirming a site. The principal configuration parameters are summarized in **Table 1**.

Table 1. Main parameters.

Parameter	Value / Setting
Number of IoT devices	20
Contention window (CW) per site	1
Cryptographic hash function	SHA-256
α	1
β	1
Transaction weight distribution	Uniform: Uni(40, 50)
Transaction arrival process	Poisson: Poi($\lambda = 100$)
Transaction size distribution	Normal: Nor($\mu = 80$, $\sigma = 0$)

Ledger convergence

Ledger convergence plays a vital role in ensuring that a DAG-based blockchain operates correctly. In such systems, convergence implies that all nodes eventually agree on transaction validity and ordering, thereby maintaining overall network integrity and dependability. Thus, any modification to the tip selection mechanism must still guarantee this convergence property.

To thoroughly assess convergence behavior, we simulated fluctuations in the number of tips when site arrivals followed three distributions: Uniform, Poisson, and Normal. To further test stability under varying initial conditions, two starting sizes were used—one small (20 initial sites) and one large (800 initial sites). As long as the total number of sites levels off at a steady value regardless of the starting point, the ledger can be considered convergent.

As illustrated in **Figure 2**, when sites are generated according to a Uniform distribution, tip count variations remain minimal once the network reaches steady state. Under a Poisson distribution, tip count oscillations are more pronounced after stabilization but still progress toward a stable pattern. For the Normal distribution scenario, the degree of fluctuation falls between the preceding two cases. These observations confirm that the proposed tip selection method maintains ledger convergence in a DAG environment.

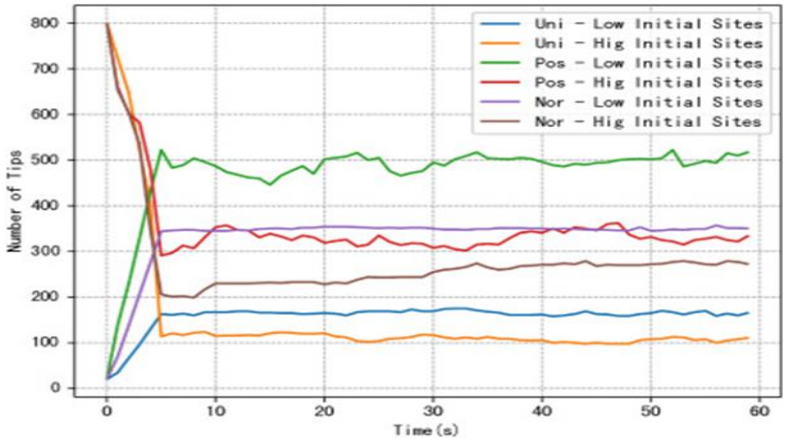

Figure 2. Ledger convergence.

Tip selection delay

Tip selection delay describes how long a newly created site requires to identify suitable tips before being appended to the DAG structure. In our selection algorithm, the disease category indicator is incorporated so that new sites preferentially attach to tips sharing similar indicators. This design not only speeds up the selection process but also strengthens contextual relevance in the appended information.

We benchmarked our approach against the MCMC-based tip selection, measuring the time needed for new sites to choose tips when PD was set to 50, 100, and 150.

As shown in **Figure 3**, experiments reveal that our algorithm achieves shorter selection times than the MCMC approach. Reduced selection latency helps lower overall confirmation delays and increases network throughput, thereby improving the system's ability to support timely information exchange and rapid data transmission in medical IoT settings. The improved responsiveness is especially significant for emergency-driven healthcare scenarios, enhancing both reliability and system robustness.

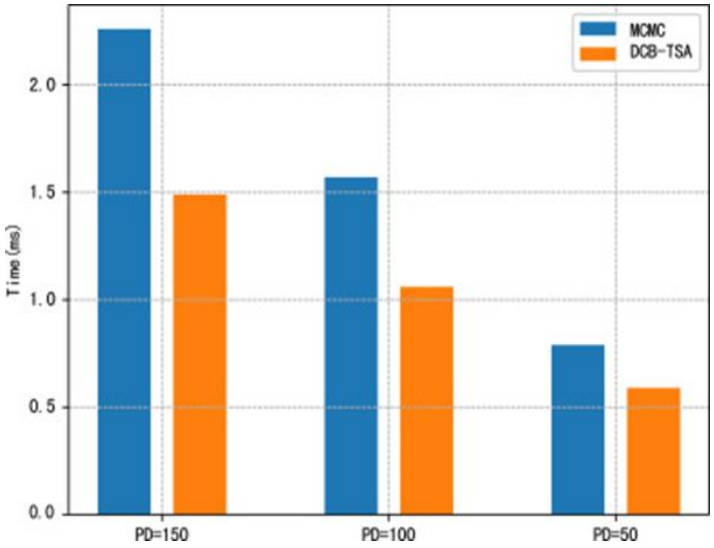

Figure 3. Tip selection delay.

Site confirmation delay

Confirmation delay denotes the time needed for a site to accumulate a target cumulative weight. Based on Popov [18], during the adaptation phase, benign sites gain cumulative weight at an accelerating pace; once adaptation ends, weight grows at the rate λW. Since each site is assigned a weight of 1, cumulative weight growth depends solely on the rate λ. Thus, we examined confirmation delays under varying λ values. Comparisons for different cumulative weight thresholds using both our algorithm and the MCMC method are displayed in **Figure 4**.

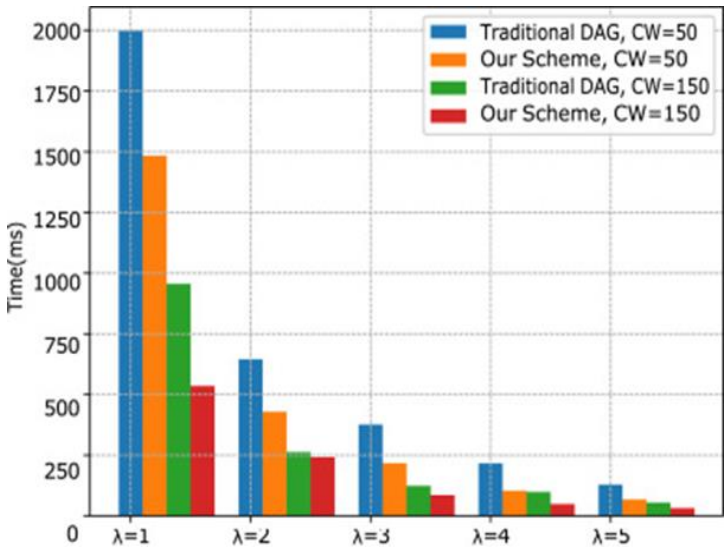

Figure 4. Site confirmation delay.

The findings show that, for identical weight thresholds, our method results in shorter confirmation delays than the MCMC strategy. This improvement supports faster and more dependable transmission of critical and real-time medical IoT information, enabling quicker clinical response and elevating the overall effectiveness of healthcare services. Additionally, by decreasing confirmation time, the proposed algorithm provides a more reliable exchange environment, reinforcing the protection and consistency of medical records.

Conclusion

This work introduces an optimized medical IoT information exchange framework built on AI and DAG-enabled blockchain. To overcome the slow consensus limitations of traditional blockchain architectures, we integrate AI-assisted preprocessing with a redesigned DAG tip selection algorithm to accelerate data incorporation. Both security evaluation and simulation outcomes demonstrate that the proposed model improves information exchange performance within medical IoT networks. Future work will aim at lowering redundant data and reducing communication overhead to further enhance consensus speed and support better scalability of the blockchain system.

Acknowledgments: 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).

Conflict of Interest: None

Financial Support: None

Ethics Statement: None

References

1. He S, Shi K, Liu C, Guo B, Chen J, Shi Z. Collaborative sensing in internet of things: a comprehensive survey. IEEE Commun Surv Tutor. 2022;24:1435–74. doi:10.1109/COMST.2022.3187138
2. AlSelek M, Alcaraz-Calero JM, Wang Q. Dynamic AI-IoT: enabling updatable AI models in ultra-low-power 5G IoT devices. IEEE Internet Things J. 2023;1–1. doi:10.1109/JIOT.2023.3340858

3. Cheng N, Wu S, Wang X, Yin Z, Li C, Chen W, et al. AI for UAV-assisted IoT applications: a comprehensive review. IEEE Internet Things J. 2023;10:14438–14461. doi:10.1109/JIOT.2023.3268316
4. Saraswat D, Bhattacharya P, Verma A, Prasad VK, Tanwar S, Sharma G, et al. Explainable AI for healthcare 5.0: opportunities and challenges. IEEE Access. 2022;10:84486–517. doi:10.1109/ACCESS.2022.3197671
5. Taimoor N, Rehman S. Reliable and resilient AI and IoT-based personalised healthcare services: a survey. IEEE Access. 2022;10:535–63. doi:10.1109/ACCESS.2021.3137364
6. Kalakoti R, Bahsi H, Nõmm S. Improving IoT security with explainable AI: quantitative evaluation for IoT botnet detection. IEEE Internet Things J. 2024;1–1. doi:10.1109/JIOT.2024.3360626
7. Dave M, Rastogi V, Miglani M, Saharan P, Goyal N, Sharma R. Smart fog-based video surveillance with privacy preservation based on blockchain. Wirel Pers Commun. 2022;124.
8. Rana A, Sharma S, Nisar K, Ibrahim AAA, Dhawan S, Chowdhry B, et al. The rise of blockchain Internet of Things (BIoT): secured device-to-device architecture and simulation scenarios. Appl Sci. 2022;12:7694. doi:10.3390/app12157694
9. Shah SHA, Koundal D, Sai V, Rani S. Guest editorial: special section on 5G edge computing-enabled internet of medical things. IEEE Trans Ind Inf. 2022;18:8860–3. doi:10.1109/TII.2022.3193708
10. Rai HM, Shukla KK, Tightiz L, Padmanaban S. Enhancing data security and privacy in energy applications: integrating IoT and blockchain technologies. Heliyon. 2024;e38917. doi:10.1016/j.heliyon.2024.e38917
11. Martínez CJ, Galmés S. Analysis of primary attacks on IoMT communication protocols. In: 2022 IEEE World AI IoT Congress (AIIoT); 2022. p. 1–7. doi:10.1109/AIIoT54504.2022.9817252
12. Sankaran KS, Kim TH, Renjith PN. An improved AI-based secure m-trust privacy protocol for medical IoT. IEEE Internet Things J. 2023;10:18477–85. doi:10.1109/JIOT.2023.3280592
13. Reddy KP, Satish M, Prakash A, Babu S, Kumar P, Devi BS. Machine learning revolution in early disease detection. In: 2023 IEEE ICCCMLA; 2023. p. 638–643. doi:10.1109/ICCCMLA58983.2023.10346963
14. Phatak SS, Patil HS, Arshad MW, Jitkar B, Patil S, Patil J. Advanced face detection using machine learning. In: 2022 IEEE IC3I; 2022. p. 1111–1116. doi:10.1109/IC3I56241.2022.10072527
15. Shen P, Li S, Huang M, Gao H, Li L, Li J, et al. A survey on blockchain regulation and ecology. In: 2022 IEEE Blockchain Conference; 2022. p. 494–499. doi:10.1109/Blockchain55522.2022.00076
16. Shrivastav P, Sadasivan M. Blockchain-based secure cloud data sharing using machine learning. In: 2023 ICIDCA; 2023. p. 1078–1084. doi:10.1109/ICIDCA56705.2023.10099950
17. Cullen A, Ferraro P, Sanders W, Vigneri L, Shorten R. Access control for distributed ledgers in IoT. IEEE Internet Things J. 2022;9:2277–92. doi:10.1109/JIOT.2021.3096129
18. Popov S. The Tangle. White Paper. 2018.
19. Zhao L, Vigneri L, Cullen A, Sanders W, Ferraro P, Shorten R. Secure access control for DAG-based distributed ledgers. IEEE Internet Things J. 2022;9:10792–806. doi:10.1109/JIOT.2021.3128025
20. Alrubei SM, Ball E, Rigelsford JM. A secure blockchain platform for AI-enabled IoT at edge layer. IEEE Access. 2022;10:18583–95. doi:10.1109/ACCESS.2022.3151370
21. Alrubei S, Ball E, Rigelsford J. A secure distributed blockchain platform for AI-enabled IoT. In: 2020 IEEE Cloud Summit; 2020. p. 85–90. doi:10.1109/IEEECloudSummit48914.2020.00019
22. Selvarajan S, Srivastava G, Khadidos AO, Baza M, Alshehri A, Lin JCW. AI lightweight blockchain security model for IIoT. J Cloud Comput. 2023;12:38.
23. Charles V, Emrouznejad A, Gherman T. Integration of blockchain and AI in supply chain: a critical analysis. Ann Oper Res. 2023:1–41.
24. Shen M, Gu A, Kang J, Tang X, Lin X, Zhu L, et al. Blockchains for AI of things: a comprehensive survey. IEEE Internet Things J. 2023;10:14483–506. doi:10.1109/JIOT.2023.3268705
25. Quan G, Yao Z, Chen L, Fang Y, Zhu W, Si X, et al. Trusted medical data sharing framework using blockchain. Heliyon. 2023;e22542.
26. Liu H, Guan X, Bai R, Qin T, Chen Y, Liu T. Medical information diagnosis platform with IoT integration. Heliyon. 2024;e25390.
27. Panchal B, Parmar S, Rathod T, Jadav NK, Gupta R, Tanwar S. AI and blockchain-based secure message exchange framework for medical IoT. In: 2023 NMITCON; 2023. p. 1–6. doi:10.1109/NMITCON58196.2023.10275950
28. Sharma S, Kumar A, Bhushan M, Goyal N, Iyer SS. Is blockchain technology secure to work on? IGI Global; 2021. doi:10.4018/978-1-7998-6694-7.ch005

29. Bhattacharjee S, Gangwar S, Kumar M, Saini K, Saini R, Chauhan S, et al. Secure data transmission using blockchain in IoT. J Auton Intell. 2024;7.
30. Qi P, Chiaro D, Giampaolo F, Piccialli F. Blockchain-based IoMT framework for stress detection. Inf Sci. 2023;628:377–90. doi:10.1016/j.ins.2023.01.123