Blockchain-Based Security for Organ Donation Health Records in IoMT

C. Gethara Gowri[1], M. Amanullah[2] and J. Lakshmikanth [3]

[1]Research Scholar - CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India and Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, India
gowri.smak@gmail.com
[2]Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India
amanhaniya12@gmail.com
[3] Faculty of Computer Science and Business Systems, Rajalakshmi Institute of Technology, Chennai, India. lakshmikanthj10@gmail.com

Abstract: Organ donation is a crucial aspect of healthcare, offering life-saving opportunities to those in need. However, flaws in the existing system have contributed to the rise of organ trafficking. The recent development of the Internet of Medical Things (IoMT) presents a transformative solution by leveraging a variety of bio-sensors, both invasive and non-invasive, to collect health-monitoring data. For IoMT applications, ensuring secure sensitive health records between connected devices and remote servers is essential to enable efficient analysis and decision-making across distributed networks. Our research explores how quantum blockchain technology can bolster the security of health records associated with organ donation and transplantation in IoMT systems. We propose an innovative platform aimed at enabling secure and transparent organ matching among healthcare providers, donors, and recipients, with an emphasis on preventing organ trafficking. This platform can also be adapted for other critical applications, such as plasma donation and medical distribution, which are particularly important in light of the ongoing pandemic. To accomplish this, we introduce the Quantum Key Distribution Blockchain Scheduling (QKBDS) approach, which combines blockchain technology for scheduling local sensor data and health records with quantum blockchain for remote scheduling through key distribution. Simulation result indicates that QKDBS surpasses current blockchain and quantum methods in efficiently managing IoMT applications, including organ donation and health record security, across distributed network nodes

Keywords: *Organ Donation, Blockchain, Interoperability, Internet of Medical Things (Iomt), QKD, Hyperledger Fabric, Decentralized, QB-IMD*

I. INTRODUCTION

Organ donation is a life-saving act that enables individuals to offer the gift of life to others, However, the process is accompanied by concerns such as the risk of transmitting infectious diseases, and allergens, and the possibility of organ rejections. To guarantee the safety and transparency of organ donation, rigorous regulations, and storage of organs. Organ transplantation refers to the complex surgical process of removing an organ from a donor and implanting it into a recipient. Furthermore, allocation systems are designed to prioritize fairness and equity, ensuring the organs are distributed to those in greatest need. Utilizing blockchain technology for secure organ donation represents an innovative approach to tackling the global challenge of organ shortages. The decentralizing and transparent nature of blockchain facilitates the safe and efficient exchange of information among donors, hospitals, and transplantation teams. It safeguards the integrity of the organ donation process, minimizes the risk of fraud, and offers donors greater control over their contributions. The secure and transparent system has the potential to increase the availability of organs, saving countless lives and enhancing the overall organ transplantation process. However, a significant challenge remains in addressing the stark imbalance between the growing organ demand and the limited supply.

A new platform for organ transplant aims to minimize organ trafficking. Currently, two types of models oversee the management of organ donation, transportation, and transplantation processes. Centralized Models and Blockchain-based Decentralized Models are two primary approaches governing organ donation, transportation, and transplantation processes. The main challenge with centralized models is compromised data security due to third-party involvement. Additionally, a lack of transparency in the processes for stakeholders exacerbates issues such as illicit organ allocation and unethical modifications to organ waitlists, leading to a decline in trust in the system [1-3]. Furthermore, these models do not enable patients to monitor the organs allocated to them during transportation from the donor. This limitation stems from the reliance of centralized systems on third-party data management, which hinders patients’ ability to track the condition of organs throughout their journey. Moreover, centralized models are vulnerable to single points of failure [4-5]. As a result, research is increasingly moving away from centralized, data immutability, enhanced security and integrity, greater process transparency, reliability, and the creation of a more trustworthy environment. This transition also seeks to remove the need for third-party data management. However, the cost-effectiveness of the current decentralized model for managing organ donation, transportation, and transplantation remains a significant concern. Additionally, similar to existing centralized models, these decentralized models do not provide stakeholders with light intensity inside the container, as well as the container’s orientation and vibration. This lack of transparency substantially increases the risk of organ contamination during transport highlighting a crucial shortcoming in ensuring the safety of organ delivery [6-7].

Implementing a cost-effective, decentralized, secure, and reliable system for managing organ donation, transportation and transplantation is essential for building trust among both donors and patients. Such a system should ensure transparency throughout the entire process from organ donation and efficient donor-patient matching to the transportation of the organ from donor to recipient and its subsequent transplantation. It must guarantee that organ allocation is based on a fair “first come, first served” principle, without bias, and that the established organ waitlist remains unalterable. Additionally, the system should provide patients with complete transparency and allow them to monitor the condition of the allocated organ throughout its journey, ensuring its viability despite potential fluctuations in temperature and humidity. Furthermore, the framework should include safeguards for the organ container to prevent risks such as accidental opening, tilting, or falling during transport.

Internet of Things

Internet of Things (IoT) is an intelligent computing technology that wirelessly connects various physical devices [8]. A complete IoT architecture includes the perception layer, network layer, and application layer. The perception layer consists of wireless sensors that capture and preprocess information. The network layer transmits and aggregates data between different devices, while the application layer enables customized utilization of terminal device data. IoT is pervasive computing [9], and its emergency has driven rapid growth in the medical and healthcare industries. It is estimated that by 2025, AI-driven Internet of Medical Things (IoMT) technology will generate a value of 1.17 billion dollars in the medical market [10]. The emergence of IoT has significantly advanced the healthcare industry [11], particularly in addressing cardiovascular disease, which is one of major threats to human health. ECG [12] is a standard way to monitor heart activity, and its data is with temporal continuity. As an important biological signal of the human body, ECG is used for identification [13]. Arrhythmia Detection System is an IoMT-based system that stores vast amounts of heartbeat data. With high sensitivity and importance for personal privacy. To address security and sharing needs, blockchain technology provides a feasible solution for the secure storage of medical data through the concept of decentralization [14]. Combining blockchain technology with IoMT better meets the requirements for secure and efficient sharing of data.

II. BLOCKCHAIN TECHNOLOGY

Blockchain is an innovative technology that provides ownership verification, transparency, enhanced security, and privacy. By employing hash functions and public-key cryptography, it addresses data privacy, security, and integrity challenges. The technology’s potential growth could significantly impact these areas. In 2008, Satoshi Nakamoto introduced the Bitcoin white paper [18], which outline Bitcoin’s core purpose: facilitating transactions without the need for a trusted third party(TTP). Unlike traditional financial truncations that rely on institutions such as banks—which can access users’ financial data and involve lengthy processes and additional fees—Bitcoin enables secure, verified transactions between parties directly, without intermediary involvement.

Research on blockchain and cryptocurrency has been intensely focused in both industry and academia for:

Distributed storage: Blockchain transparently records data and transmits it to third parties upon receipt. A key feature of decentralized information processing is that records are stored with the data owner.
Consent: The Consensus Algorithm governs the admission, storage, and distribution of network information. Data is updated when all network participants reach a consensus on a decision.
Immutability: Modifying records is challenging. Alterations or updates to data within a single block in the chain are not permitted.
Increased Capability: Blockchain minimizes the need for intermediaries, streamlines network data authorization, and effectively safeguards patient privacy across various fundamental healthcare applications.

Subsequent transactions create new blocks, which are validated by network nodes know as miners and then added to the chain, increasing both its size and length. The hash of the preceding block acts as a tamper-evident measure. Any changes to the block alter the hash, disrupting the entire cryptographic chain and making any tempering easily detectable across the network. The standard configuration of a block in the blockchain is illustrated in Fig.1.

.

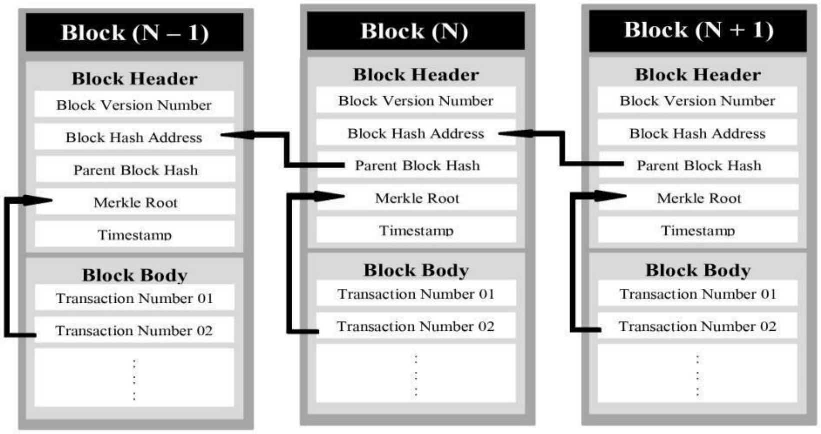

Fig. 1 Standard configuration of a block in the blockchain

Quantum Computing

Quantum computing is an emerging technology that has recently gained significant attention. Its advancements are profoundly impacting current cryptosystems and offering new perspectives on complex challenges. For instance, Shor's algorithm can efficiently solve problems related to finding hidden subgroups within infinite abelian groups, while Grover's algorithm provides a quadratic speedup for searching unordered collections [19]. This field is highly competitive and holds considerable potential for future development. From a post-quantum perspective, it is crucial to assess the security of current blockchain methods against quantum threats [20]. Quantum computers and their algorithm [21] pose a significant risk to existing public-key cryptography schemes. Predictions suggest that quantum computers could become feasible by 2026 and achieve a 59% probability of practicality by 2031 [22]. Since most blockchain systems depend heavily on public-key digital signatures and value transfers, they are particularly vulnerable to quantum attacks. Fedorov et al.[23] argue that without integrating quantum technologies, current blockchain systems may become obsolete. Although some interim solutions employ post-quantum cryptography, they are not entirely secure. Thus, it is essential to consider the impact of quantum computing on organ donation management.

Challenges in Implementing Quantum Encryption and Blockchain Integration

Implementing this model presents several challenges. First, quantum encryption necessitates substantial investment in quantum computing infrastructure and expertise. Second, integrating quantum encryption with blockchain technology requires a thorough evaluation of its potential effects on the performance and scalability of the blockchain network [24]. Lastly, the model must include robust authentication and access control mechanisms to ensure that only authorized individuals can access donor and transplant records.

Ensuring the confidentiality of critical medical data is an additional concern with quantum-safe organ donor and transplant file exchange, alongside the previously mentioned challenges [25]. While quantum cryptography can protect files from unauthorized access, it may not be sufficient to defend against cyberattacks that seek to infer sensitive information from patterns within encrypted files. Researchers are exploring ways to enhance quantum-safe patient record exchanges by integrating privacy techniques such as diverse datasets and secure multi-party computation to address these issues [26].

Despite these challenges, the quantum-safe exchange of donor and transplant records holds the potential to transform healthcare by enabling secure and efficient data interchange [27]. Distributed ledger technology and quantum cryptography could provide an unprecedented level of security and confidentiality, while also advancing clinical outcomes and scientific research.

Innovations and contributions of the QB-IMD Quantum Blockchain system

Research on the quantum blockchain is still in its initial stage. Therefore, this article designs a quantum blockchain-based system Quantum Blockchain for Internet of Medical Data (QB-IMD) for medical data processing, which is a complete idea and has good security, confidentiality, and feasibility. The innovations and contributions are listed in the following.

A Comprehensive QB-IMD scheme for organ donation and transplant processing is presented, which not only verifies new blocks but also enables blind computation for both medical and organ donation data. The system employs homomorphic encryption to achieve the required data processing results while preserving medical privacy.

A quantum blockchain data structure and an innovative algorithm called QEMR are proposed. The QEMR algorithm, integrated into the QB-IMD system, is utilized within the quantum blockchain to validate the authenticity of new diagnostic data and manage organ donation and transplant records. By leveraging quantum signatures and quantum identity authentication this algorithm mitigates the security risks associated with digital signatures and enhances the blockchain’s resilience against quantum attacks.

Quantum Key Distribution (QKD)

QKD is a method used to share encryption keys securely between two parties. It leverages the principles of quantum mechanics to ensure that any eavesdropping or interception of the key will be detected. The most common protocol used in QKD is the BB84 protocol. Key features of QKD include:
Quantum Superposition: QKD uses the properties of quantum bits (qubits), which can exist in multiple states simultaneously.
Quantum Entanglement: Two particles can be entangled so that the state of one instantly influences the state of the other, regardless of distance.
Security: Any attempt to eavesdrop on the quantum channel will alter the quantum states and can be detected.

III. Blockchain Scheduling

Blockchain scheduling refers to managing and optimizing tasks or processes within a blockchain network. It involves creating a decentralized system that enables efficient and secure management of tasks, communication, and resource allocation. This approach helps to mitigate the risks associated with centralized scheduling, such as single-point failures and data tempering. Blockchain scheduling ensures transparency, immutability, and trustworthiness, making promising solutions for industries that require secure and efficient task execution such as supply chain management, logistics, and cloud computing. Key elements include:

Decentralization: Blockchain scheduling operates on a decentralized network, eliminating the need for a central authority or intermediary. This makes it more resilient to single points of failure and reduces the risk of manipulation.

Transparency: All scheduled events, transactions, or tasks are recorded on a shared, immutable ledger visible to all participants. This transparency ensures that every participant has a clear, consistent view of the schedule.

Immutability and Security: Once a schedule or appointment is recorded on the blockchain, it cannot be altered or deleted without consensus. This feature enhances the integrity and security of the schedule, preventing tampering or unauthorized changes.

Smart Contracts: Blockchain scheduling often involves smart contracts—self-executing code with predefined conditions. For example, a smart contract could automatically trigger a task when certain conditions are met, such as time or resource availability.

Automation and Efficiency: By integrating smart contracts, tasks can be automated, reducing the need for manual intervention. This automation can streamline processes like appointment booking, supply chain logistics, or resource allocation.

Consensus Mechanisms: Protocols like Proof of Work (PoW) or Proof of Stake (PoS) are used to agree on the state of the blockchain and schedule transactions.

Transaction Ordering: Ensuring transactions are processed in the correct sequence to maintain consistency and avoid conflicts.

Combining QKD and Blockchain Scheduling

The integration of QKD with blockchain technology could enhance the security and efficiency of blockchain networks.

Enhanced Security: QKD could be used to securely distribute cryptographic keys used in blockchain networks, making it extremely difficult for unauthorized parties to access or tamper with blockchain data.

Secure Transactions: By integrating QKD with blockchain scheduling, transaction verification and scheduling could benefit from the added security of quantum cryptography, protecting against future quantum-based attacks.

Quantum-Resistant Algorithms: As quantum computers could potentially break current cryptographic methods, QKD could be part of a transition to quantum-resistant algorithms and protocols in blockchain systems.

Efficient Scheduling: Blockchain scheduling could be optimized using quantum algorithms for faster consensus or transaction processing, although this is still a theoretical area under research.

V. Proposed System QB-IMD

The system proposed is divided into three layers: 1) application layer; 2) sensing layer; and 3) cloud layer. Among them, the application layer stores the medical information obtained by the devices. The medical data is called electronic medical record (EMP) After QB-IMD, legitimated

EMR blocks are added to the chain, and EMR data can be processed blindly. The Structure diagram of our QB-IMD is in Fig, 2, The functions of each layer are described in detail below.

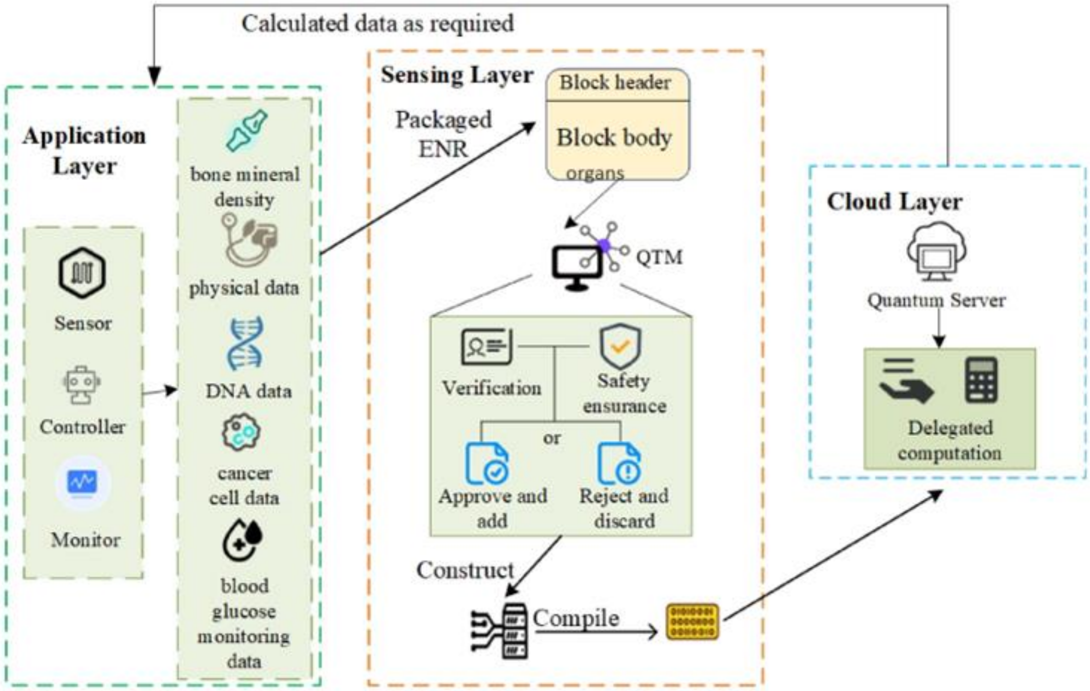

Fig. 2. Quantum blockchain-based medical data processing architecture diagram.

A. Application Layer

The application layer primarily gathers, integrates, and packages data from physical devices. As depicted in Fig. 2, the data collected from devices like sensors, controllers, and monitors are referred to as EMRs. This data includes but is not limited to, bone density, heart rate, DNA information, Cancer cell analysis, blood glucose levels, and organ details. Since this information is often considered sensitive patient data, maintaining its privacy in crucial. The package EMR data is then transmitted to the sensing layer.

B. Sensing Layer and Distributed QEMR Algorithm

The sensing layer is primarily responsible for block packaging and block additions, which is where the blockchain technology operated. The proposed distributed QEMR algorithm is also implemented within this layer, focusing on EMR block authentication. By integrating quantum signature and quantum communication technologies, the blocks are secured against attacks from malicious eavesdroppers, ensuring that each added block is trustworthy.

New EMR blocks generated by the application layer are transmitted to the sensing layer, where they are automatically packaged into a block. Over time, a continuous chain of blocks forms within the sensing layer. The designed quantum block structure is shown in Fig. 2. The block header includes the block address, Previous block address, timestamp, quantum signature, and quantum key, The block body contains the EMR information sent by the application layer,

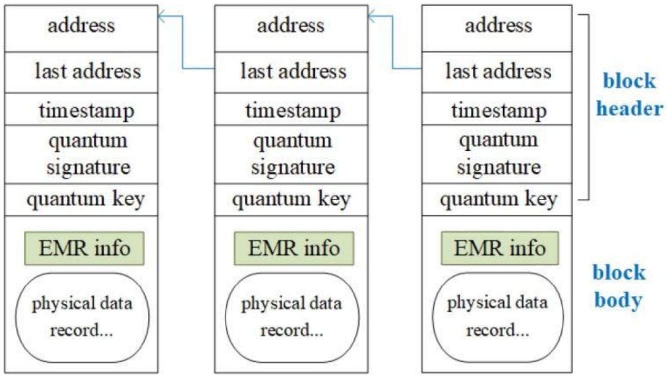

Fig. 3. New quantum blockchain structure

Table 1: Data Structure of Blockchain

Data structure	Description
Address	The specific address of the block, a string of hexadecimal has values generated by SHA256.
Last address	The address of the previous block.
Timestamp	The time when the block joined this blockchain.
Quantum signature	Signature shared by nodes
Quantum key	Key shared by nodes
EMR info	The EMR information send by the application layer

A blockchain encapsulates medical records over a specific period. The data structure of our blockchain is illustrated in Table I.

In the sensing layer, a distributed quantum EMR protocol (QEMR) is implemented to filter and validate legitimate blocks. The entire QEMR algorithm is divided into six stages, as depicted in Fig. 4. These stages are as follows:

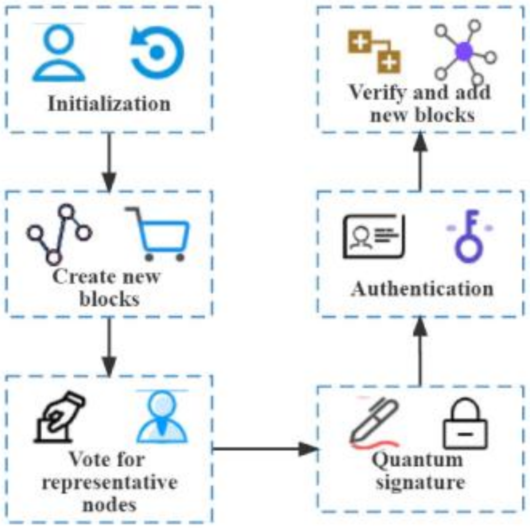

Fig. 4. Six stages of QEMR

1. **Initialization:** Within the sensing layer, EMR blocks are linked to create a distributed quantum blockchain. Each node is capable of preparing, storing, and measuring quantum states as well as exchanging quantum states and classical information with other nodes. The key strings within the quantum networks are distributed in an unconditionally secure manner by using the BB84 protocol [23].
2. **Create New Blocks:** When a new EMR is generated, the system automatically creates a new block. The block is initially assigned an address but remains unlinked to the blockchain until it undergoes authentication. It is assumed that the existing N blocks (where N is a large number) are trustworthy and have been added to the chain following the QEMR protocol. When a device from the application layer provides a block of data, a new block is generated and then authenticated by the representative node selected in the subsequent step. Only verified and legitimate blocks are allowed to join the chain.
3. **Vote for Representative Nodes:** The representative nodes is composed of main node and several backup nodes. The Bods counting method [24], [25], [26] is used to vote for these representative nodes. Nodes selected through the Borda counting method are those with relatively low error rates and strong support.
4. **Quantum Signature:** A total of M backup nodes are configured. The main node is responsible for evaluating the legality of pre-joined blocks and holds the rights to record and broadcast information. Suppose Alice is one of the backup nodes. Bob is the main node, and Charlie is a new node seeking to join the blockchain,

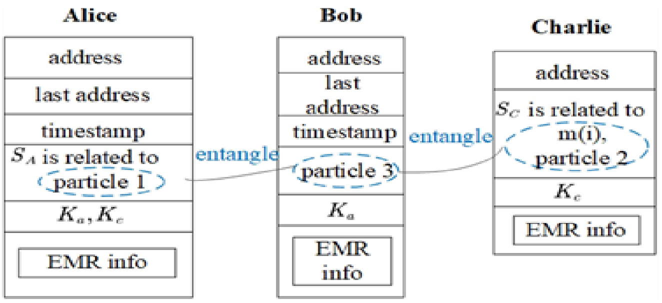

Fig. **5**. Alice, Bob, and Charlie’s blocks

Alice prepares n qubits {|0⟩,|1⟩}\{|0\rangle, |1\rangle\}{|0⟩,|1⟩} corresponding to the classical message bit mmm. These qubits are represented as as |m⟩={m1,m2,…,mn}|m\rangle = \{m_1, m_2, \dots, m_n\}|m⟩={m1,m2,…,mn}, where each qubit mim_imi is defined as mi=xi|0⟩+yi|1⟩m_i = x_i|0\rangle + y_i|1\ranglemi=xi|0⟩+yi|1⟩, with |xi|=0|x_i| = 0|xi|=0 and |yi|=1|y_i| = 1|yi|=1 or |xi|=1|x_i| = 1|xi|=1 and |yi|=0|y_i| = 0|yi|=0. One of the backup nodes, Alice, shares a quantum key KaK_aKa with the main node, Bob and a quantum key KcK_cKc with the new node, Charlie. The keys are established using the BB84 protocol [23].

5. Authentication: In this phase, Bob has to verify Alice and Charlie’s signatures. After receiving S_A and particle 3 from Alice and Charlie, Bob decrypts S_A with K_a to obtain TA and (a_i, b_i). Also, Bob decrypts S_c with Kc to obtain R_C

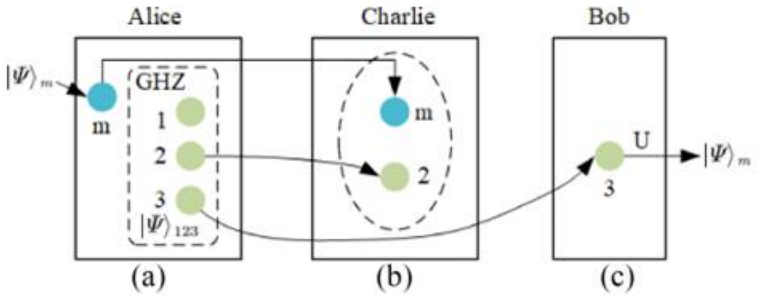

Fig. 6. Schematic diagram of particle flow in QMER.

Bob compares (xi, yi)(x_i, y_i)(xi,yi) and (xi, yi)(x_i, y_i)(xi, yi) to determine if they match. If they are equal, he can conclude that SAS_ASA and SCS_CSC are legitimate signatures. This also indicates that both the backup node and the block seeking to be added to the chain are honest and valid. In the end, the main node Bob counts the number of backup nodes that have completed authentication. A backup node that either fails to authenticate within the allotted time or experiences an interruption in its information will be deemed a faulty node off, if $M \geq 3f+1$, the main node Bob will classify the new block as legitimate. A schematic of the particle flow for signature and authentication is illustrated in Fig 6.

6. Verify and Add New Blocks: Finally, the correctness of the new block is verified by 1) ensuring the block size and the length of each field are within the specified limits; 2) confirming the accuracy of the timestamp, and 3) validating all EMR messages in the block to ensure their legitimacy. Once these checks are complete, the main node adds the block to the chain and assigns it an address, which is a string of hexadecimal hash values. The address of the new EMR is linked to the address of the previous block, ordered chronologically by timestamp.

C. Cloud Layer

The cloud layer is primarily responsible for processing EMR data without revealing any privacy. The QTM in the sensing layer compiles this information into classical bits 0 and 1 first, This system uses homomorphic encryption to process the information, which is also a delegated computing method. If the application layer wants to send encrypted messages to the QTM and the cloud layer. Fig 7 and Fig 8 show a set of universal quantum circuits for delegated computing. Specifically, X= | 0) (1| +|1)(0|.Z = |0)(0| - | 11|,H|a → -1) ^{a}|1)(1/2)(|0 +(),S|a → (e$_{i\pi}$/2)$_{a}$|a, CNOT| a|b= |a)|a +b),T |a → (e$^{i\pi/4}$)^{a}|a).a,b € {0,1}.

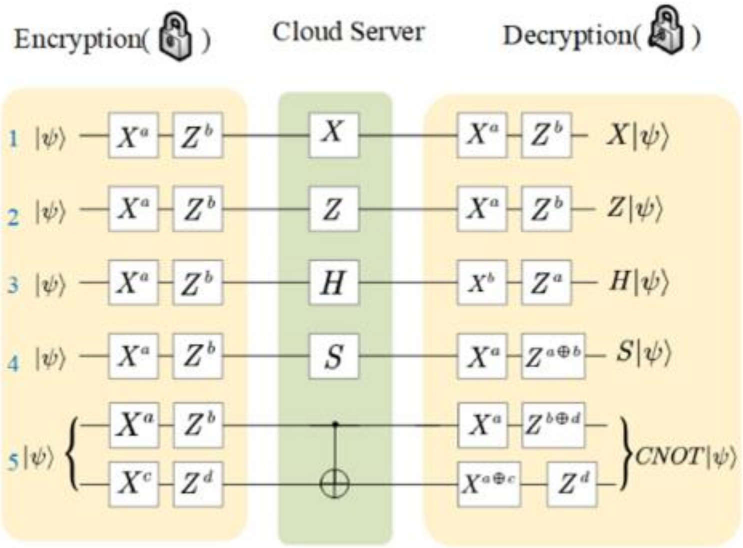

Fig.7. Universal quantum circuits {X,Z,H,S,CNOT} for delegated computing

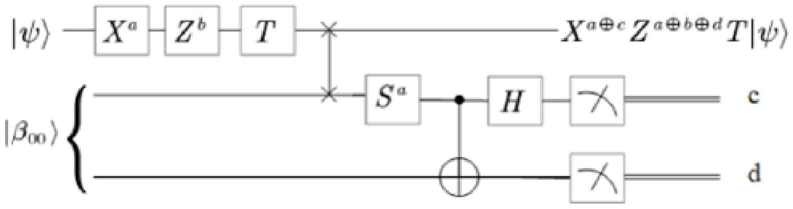

Fig. 8. Universal quantum circuit for delegated computing

There are three key entities involved in information processing: 1) the application layer, which represents the client; 2) the quantum terminal, which serves as an intermediary; and 3) the cloud layer, which performs blind information processing. The client-side information remains confidential and is not exposed to the cloud layer, while the desired processing results are still obtained. Specifically, the circuit in Fig. 9 requires the client and server to pre-share a pair of Bell states. The client encrypts the data and uploads it to the quantum server (QS). The QS applies a T-Gate to the data, and the resulting quantum state is then exchanged for its own Bell state using a swap gate, which is sent back to the client. The client performs a Bell measurement, and the results of measurements ccc and ddd are used to update the key. The server then sends the state of the first quantum bit to the client, who decrypts it to obtain.it T | ψ. The flowchart of the cloud layer for data privacy processing is shown in Fig 9.

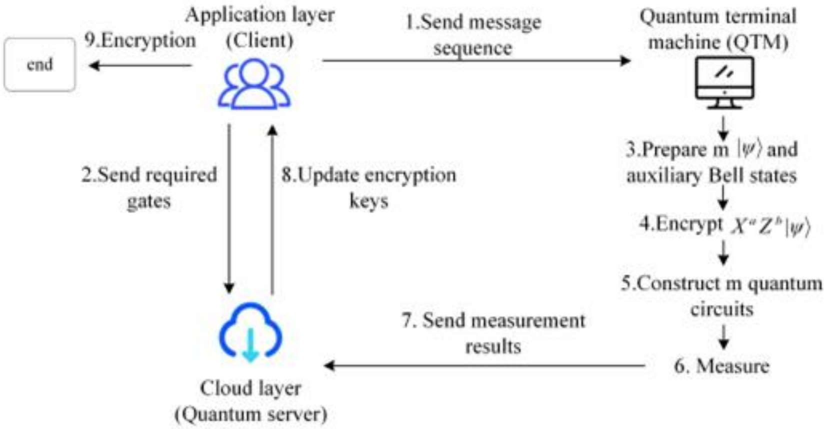

Fig. 9. Flowchart of the cloud layer for data privacy processing.

The process of delegated computing is presented as follows.

Step 1: In response to a request from the application layer, the QTM selects a block or a batch of blocks to produce a sequence of message bits. It encodes the numerical values in the medical data as digits 0 and 1.

Step 2: one of the six circuits shown in Fig 7 and 8 is selected at random to encrypt the X, Z, H, S, CNOT, and T circuits. The X, Z, H, S, and T circuits require only two classical bits each, while the CNOT circuit needs four classical bits.

Step 3: QTM prepares multiple states | ψ and sends them to the application layer. The application layer encrypts $X^a Z^b|\psi, a, b \in \{0,1\}$. If a CNOT gate is used, The encryption is $X^a Z^b \otimes X^c Z^d$. If a T-gate is used, let the application layer entangle with the cloud server via the bell states.

Step 4: The application layer informs the cloud QS which circuits to use. The QS then executes the specified gates and returns the resulting output bit sequence.

Step 5: The application layer decrypts the message using the methods outlined in Figs. 7 and 8 to obtain the desired processed data.

V. PERFORMANCE ANALYSIS

The proposed QB-IMD blockchain scheme is compared with other blockchain schemes.

A. Security Analysis of the QEMR Protocol

Intercept-Resend Attack: In this scenario, an eavesdropper named Eve attempts to intercept sensitive EMR records within the quantum channel. Her goal is to capture and then resend a falsified EMR record to another block, ultimately disrupting the QEMR protocol's integrity. However, during the security verification phase, Eve faces a critical obstacle: she cannot accurately determine whether each quantum particle is encoded in a linear or diagonal basis. This lack of knowledge results in a 50% error rate for each of Eve's the likelihood of detecting Eve's interference is high, effectively enabling early detection of any intercept-resend attack attempts on the QEMR protocol is (1/2) + (1/2) x (1/2) = (3/4). Assume that there are NMM rounds quantum state transmissions and NCM rounds security checks in the blockchain over time, $N_{MM} + N_{CM} = N$. Let c= N_{CM} /N. for N=1,2,3… , the probability that Eve will be detected is (3/4)c(1-(3/4)c)+(3/4)c(1-(3/4)c)2,… After N rounds of quantum messaging, the probability of Eve being detected is

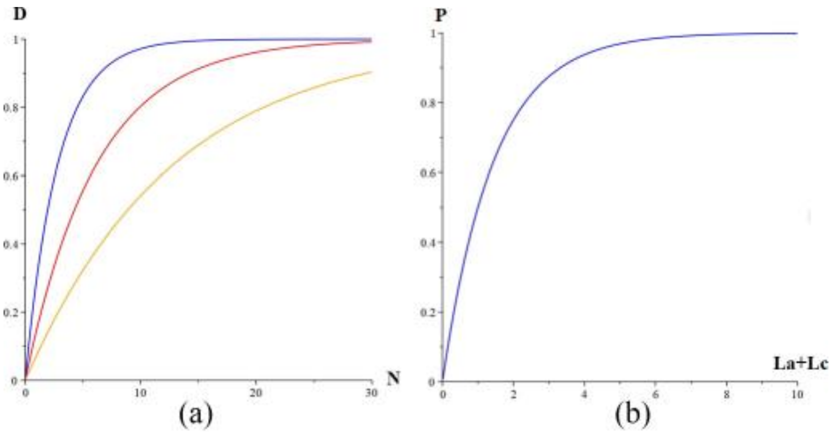

Fig. 10 Probability of EVE being detected under intercept-resend attacks

Eve's forged signature is detected. Yellow line: c=0.1; red line: c=0,2; and blue line: c=0.4. Assuming c=0.1,0.2 and 0.4, the relationship between D and N is shown in Fig 9(a). When N →∞ D→1.

2) Entangle Measure Attack: Consider that Eve attempts to carry out an entangle-measure (EM) attack to intercept the key and insert a fraudulent medical record, aiming for unauthorized duplication (Double spending). However, this approach is rendered ineffective. In the Quantum Signature phase (step 2.4), for instance, Alice retains particle 1 and send particle 2 to Charlie. To

gather information on the target qubit, Eve would try to entangle the transmitted particle with an auxiliary particle she holds, using specific unitary operations. The unitary operation in question is designed to $U|0|E=a|0|E_0+b \mid 1| E_1$, $U \mid 1|E = C|| E_2+d|1|E_{3.}$ $|E$ is the auxiliary particle of Eve and $|a|^2 =|b|^2 =|C|^2 +|d|^2=1$. $|$ E0 is orthogonal to $|E_1$, $|E_2$ is orthogonal to E_3

IV. CONCLUSION

To ensure a reliable, secure, and confidential environment for IoMT, introduces a novel quantum blockchain-based medical data processing system called QB-IMD. Within the QB-IMD framework, the sensing layer employs a distributed QEMR algorithm designed to authenticate the legitimacy of ENR data transmitted from the application layer. A Subst of representative nodes is selected using the Borda counting method to optimise the use of quantum and classical resources. Quantum signature and quantum communication technologies are utilized to safeguard the blockchain's security. In the cloud layer, the required data is encrypted and processed using quantum delegated computation schemes that remain to be tested. The concept is highly innovative and the analysis is thorough. However, the classical blockchain is susceptible to attacks from quantum computing. Their innovation is evident in the design of the QTM and the application of blockchain technology. While the solution is comprehensive, the article does not include details of the blockchain structure itself. The quantum blockchain IoMT model proposed by Qu et al.is highly feasible and introduces a new quantum blockchain structure. However, it does not address the processing system. Through decryption, the application layer can obtain the necessary computational results while keeping the EMR data confidential. Mathematical proofs, theoretical analysis, and experimental simulations demonstrate that the QEMR is resistant to attacks such as intercept-resend and signature forgery. Additionally, delegated computing in the cloud layer is proven to be secure and feasible.

Currently, due to experimental limitations, our work is primarily focused on the theoretical aspects of quantum blockchain. Given the rapid advancements in optical quantum computing technology, we are preparing to design and implement a quantum blockchain algorithm or technology utilizing optical quantum computing, aiming to enhance the feasibility and practicality of quantum blockchain technology in the future.

REFERENCES

1. Jeon,H. J., Lee, S., Oh, J., Seo, S., Cho, W., & Ahn, C. (2019). P. 163: Development of web-based e-learning educational content for organ donation and transplantation toward medical students and medical personnel. Transplantation, 103(11S), S116-S117.
2. Pfaller, L., Hansen, S. L., Adloff, F., & Schicktanz, S. (2018). 'Saying no to organ donation': an empirical typology of reluctance and rejection. Sociology of Health & Illness, 40(8), 1327-1346.
3. Brown, S. J. (2018). Autonomy, trust and ante-mortem interventions to facilitate organ donation. Clinical Ethics, 13(3), 143-150.
4. Zúñiga-Fajuri, A. (2017). The case for making organ transplant waitlists public to increase donation rates: is it possible? Rev. Bioetica & Derecho, 41, 187.

5. Zavalkoff, S., Shemie, S. D., Grimshaw, J. M., Chassé, M., Squires, J. E., Linklater, S., ...& Knoll, G. (2019). Potential organ donor identification and system accountability: expert guidance from a Canadian consensus conference. Canadian Journal of Anaesthesia, 66(4), 432.
6. Golosova, J., & Romanovs, A. (2018). The advantages and disadvantages of the blockchain technology. In 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE) (pp. 1-6). IEEE.
7. Wu, B., & Duan, T. (2019). The advantages of blockchain technology in commercial bank operation and management.In Proceedings of the 2019 4th International Conference on Machine Learning Technologies (pp. 83-87).
8. L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Inform.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
9. D. V. Dimitrov, W. He, and S. Li, "Medical internet of things and Big Data in healthcare," *Healthcare Inform. Res.*, vol. 22, no. 3, pp. 156–163, 2016.
10. S. Xu, Y. Li, R. H. Deng, Y. Zhang, X. Luo, and X. Liu, "Lightweight and expressive fine-grained access control for healthcare Internet-of-things," *IEEE Trans. Cloud Comput.*, vol. 10, no. 1, pp. 474–490, Jan.–Mar. 2022.
11. P. Tiwari, A. Lakhan, R. H. Jhaveri, and T. -M. Gronli. (2023) "Consumer-centric internet of medical things for cyborg applications based on federated reinforcement learning," *IEEE Trans. Consum. Electron.*, early access, Feb. 07, 2023, doi: 10.1109/TCE.2023.3242375.
12. L. Sun, Y. Wang, Z. Qu, and N. N. Xiong. (2022) "BeatClass: A sustainable ECG classification system in IoT-based health," *IEEE Internet of Things.*, vol.9, no. 10, pp. 7178–7195, May 2022.
13. S. Gutta and Q. Cheng, "Joint feature extraction and classifier design for ECG-based biometric recognition," *IEEE J. Biomed. Health Inform.*, vol. 30, no. 2, pp. 460–468, Mar. 2016.
14. N. Deepa et al., "A survey on blockchain for Big Data: Approaches, opportunities, and future directions," *Future Gener. Comput. Syst.*, vol. 131, no. 1, pp. 209–226, 2022.
15. O.Sattath,"Ontheinsecurityofquantumbitcoinmining,"*Int.J.Inf.Secur.*, vol. 19, no. 3, pp. 291–302, 2020.
16. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. IEEE 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.
17. L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, no. 2, 1997, Art. no. 325.
18. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, 2008
19. Rahman M, Paul G. Grover on Present: Quantum Resource Estimation. Cryptol EPrint Arch 2021.
20. Ahn J, Kwon H-Y, Ahn B, Park K, Kim T, Lee M-K, et al. Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key.
21. Ray PP, Chowhan B, Kumar N, Almogren A. BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. IEEE Internet Things J 2021. https://doi.org/10.1109/JIOT.2021.3050703
22. Baha A, Madisetti VK. A cloud-based approach for interoperable electronic health records (EHRs). IEEE J Biomed Heal Informatics 2013;17:894–906
23. Masoodi F, Alam S, Siddiqui ST. Security & Privacy Threats, Attacks and Countermeasures in Internet of Things. Int J Netw Secur Its Appl 2019;11. https://doi.org/10.5121/ijnsa.2019.11205.

24. Usman, M., & Qamar, U. (2020). Secure electronic medical records storage and sharing using blockchain technology. Procedia Computer Science,174,321–327.

22. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," 2020, *arXiv:2003.06557*.

25. Butt, G. Q., Sayed, T. A., Riaz, R., Rizvi, S. S., & Paul, A. (2022, February 23). Secure healthcare record sharing mechanism with Blockchain. MDPI.

26. Zhanb, S.,& Wang, J. (2021). A review of quantum machine learning for healthcare applications. Journal of healthcare engineering, 2021.