Computer Standards & Interfaces 92 (2025) 103902

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

A consent-aware electronic medical records sharing method based on blockchain☆

Xiao Qu [a], Zhexuan Yang [a], Zeng Chen [b], Guozi Sun [a,c,*]

[a] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China
[b] Jiangsu Cancer Hospital, Nanjing, China
[c] Institute of Data Security & Compliance, Nanjing University of Posts and Telecommunications, Nanjing, China

ARTICLE INFO

Keywords:
Blockchain
Data sharing
Smart contracts
Ring signature
Privacy protection

ABSTRACT

Electronic medical records (EMRs) sharing has become a vital component of the modern health care system, which involves patients, The Medical Institution with Medical Records (MI-MR), and The Medical Institution Requiring Medical Records (MI-RMR) within this ecosystem. Currently, a substantial amount of research focuses on the security, authenticity, and privacy of the shared information. However, there is a shortage of attention on design and research that adequately reflect personal rights and interests of patients. We propose a consent-aware EMR sharing method leveraging blockchain technology, which not only preserves patients' right to be informed, but also fulfills the fundamental needs for security and privacy in EMR sharing. Furthermore, it ensures transparency and decentralization in the sharing process and incorporates on-chain verification mechanisms against malicious alteration of blockchain data. To enhance system scalability, a secure off-chain storage mechanism has been implemented. Our experimental findings underscore the practicality of our smart contract on Ethereum, along with its economic benefits, evaluated using tests conducted on a Ganache-based Ethereum blockchain network and a Remix-based Ethereum blockchain network. The performance and advantages of the proposed architecture have been corroborated through a prototype implementation using Ethereum.

1. Introduction

In the era of digital healthcare, the secure exchange of electronic medical records (EMRs) is a tangible example of how the security of personal information is critical to the protection of citizens' lives and well-being. With the rise of telemedicine and data-driven patient care, it is of paramount importance to maintain the confidentiality, integrity, and authenticity of shared medical data. While online systems have accelerated the availability and exchange of health data, they frequently are not equipped with adequate safeguards to ensure the privacy and security of patients' sensitive information. Traditional cybersecurity means often fall short in addressing the sophisticated and evolving landscape of cyber threats plaguing the digital health sector. Blockchain technology, heralded for its potential to revolutionize the sharing and storage of data, presents a novel and promising avenue for establishing secure and resilient EMR sharing frameworks [1–5].

Blockchain technology, with its decentralized nature and steady, traceable features, provides a promising solution to address data security concerns, significantly during data storage and transmission. It allows medical institutions to share and use data confidently, reducing risks of data tampering and improving disease diagnosis and prediction [6]. Wireless body area networks facilitated by implantable and wearable medical devices are used for real-time health monitoring in modern healthcare, despite having limited capacities, necessitating efficient data handling [7]. Our research focuses on securing shared electronic medical records (EMRs), emphasizing patients' rights, and privacy assurance. We propose a blockchain-based consent-aware method for EMR sharing that guarantees security, system transparency, and decentralization. This method includes on-chain verification mechanisms to prevent malicious modification of blockchain data, and a secure off-chain storage mechanism for improved scalability. The rise of digital connectivity and the Internet of Things (IoT) have increased the need for secure systems as the number of connected devices expands, potentially creating broader avenues for security attacks [8]. Responding to this, our research prioritizes the security of the EMR sharing process, focusing not only on security, authenticity, and privacy but also on protecting patients' personal rights. Our experiments on

☆ This work was supported by the National Natural Science Foundation of China (No. 62372245 & 62372250 & 62102192), the Fellowship of China Postdoctoral Science Foundation (2022M710071).

* Corresponding author at: School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China.
E-mail addresses: 1222045622@njupt.edu.cn (X. Qu), 1222045624@njupt.edu.cn (Z. Yang), chenzeng@jszlyy.com.cn (Z. Chen), sun@njupt.edu.cn (G. Sun).

https://doi.org/10.1016/j.csi.2024.103902
Received 5 June 2024; Received in revised form 15 July 2024; Accepted 26 July 2024
Available online 31 July 2024

Ethereum networks showcase the practical and economical advantages of our method, displaying performance benefits and highlighting its effectiveness in improving embedded security and medical service efficiency. Hence, our research crucially resonates with the trends and challenges in embedded security and systems design.

Blockchain's inherent properties of decentralization, transparency, and ledger immutability make it an ideal platform for creating a secure and tamper-evident repository for medical data transactions. As a decentralized system, it eliminates the risks associated with a single point of control, employing advanced consensus mechanisms and encryption to enhance data security [9,10]. A blockchain-enabled ecosystem for EMR sharing not only serves to solidify data protection but also delineates the permissions and responsibilities of all stakeholders involved in the healthcare information exchange. Although blockchain's transparent nature may raise concerns over patient privacy, strategic application of pseudonymization and encryption techniques can be utilized to address and mitigate these issues effectively. However, it is crucial to recognize that despite its robust structure, blockchain technology may face challenges like the risk of 51% attacks and potential vulnerabilities in smart contracts, calling for persistent monitoring and advancements in cryptographic defenses to counter new threats [11,12].

In the title "A Consent-Aware Electronic Medical Records Sharing Method Based on Blockchain", the phrase "Consent-Aware" mirrors the concept of "informed and consented" in the regulations of the "Personal Information Protection Law of the People's Republic of China". Taking the fourteenth article of Chapter Two of this law as an example, if the processing of personal information is based on the individual's consent, such consent must be given voluntarily and explicitly, under the prerequisite of being fully informed. If other laws or administrative regulations require obtaining individual's separate or written consent when processing personal information, then such provisions should be complied with. Therefore, "Consent-Aware" highlights the basic principle of personal information processing — the individual must be fully aware, voluntarily provide and clearly express consent. This captures the essence of legal requirements in the field of personal information handling that involves informed consent. Combined with blockchain technology, the integrity, security, and transparency of information processing can be highly guaranteed.

Our objective is to construct a blockchain-based framework tailored for the secure sharing of electronic medical records. This solution aims to fortify the rights and confidentiality of the individuals whose data is being shared, while at the same time, ensuring the process remains open and decentralized. It will also offer safeguards including proactive measures to detect and prevent malicious alterations of the blockchain ledger. Furthermore, the proposed system is designed to be highly scalable in order to accommodate the expanding nature of e-health services.

1.1. Motivation

In the healthcare sector, electronic medical information sharing stands as a critical application of personal data in today's digital age. The exchange of health records and patient information between healthcare providers seeks to improve the efficiency and accuracy of patient care. However, this digital transformation raises substantial challenges regarding the patient's privacy and the secure management of such sensitive data. Unauthorized access or leakage of this data could lead to serious ramifications, including identity theft and medical fraud [13]. Even more so, malicious parties may collaborate with storage service providers to alter patient records or directly disclose health record content to other competitors in order to gain a financial advantage [14].

Inter-institutional collaboration often necessitates the transfer of personal health information, which, despite strict regulatory frameworks, is still vulnerable to security brea-ches and misuse. Traditional centralized health data management systems are plagued by risks such as cyber attacks, opaque practices, and excessive retention of data without proper justification [15].

In summary, our work faces the following challenges. Despite the existence of strict regulatory frameworks, the cross-institutional transfer of personal health information still faces security risks. Traditional centralized health data management systems might be susceptible to issues such as cyber attacks, opaque operations, and unjustified excessive retention of data. Blockchain has the potential to revolutionize the way health data is shared and stored, providing innovative solutions for privacy and security issues[16]. The immutable nature and decentralized structure of the blockchain offer a strong defense against data tampering and fraud, but vigilance against sophisticated cyber threats, like the 51% attack, is necessary. Ensuring the authenticity and traceability of medical information within the blockchain infrastructure is crucial as it helps maintain trust and supports the long-term sustainable development of electronic medical record systems [17].

1.2. Contribution

This study aims to present a comprehensive analysis of a model designed to facilitate the secure exchange of electronic medical data at both process and data layers. The model synergizes multiple technologies without delving into overly intricate technical details. Nonetheless, we critically investigate and dissect core components such as blockchain and smart contract technologies, which are central to the improved security and automation of health data transactions [18].

Our research endeavors to solve the issues mentioned above in medical data sharing by integrating technologies such as blockchain and smart contracts. The principal achievements outlined in this paper can be encapsulated in the following points:

- Considering various perspectives on privacy protection regulations, a risk-isolation, clear accountability personal information sharing mechanism is proposed.
- Propose a blockchain-based personal information sh-aring scheme for securely sharing personal information among users.
- Utilize off chain storage mechanisms to reduce storage pressure on blockchain systems and improve scalability.
- Introduce traceable ring signatures and propose an efficient verification method for the authenticity of information on the blockchain.

In other words, firstly, we propose a risk-isolation and clear accountability personal information sharing mechanism to enhance the protection of personal health information. Secondly, we propose a blockchain-based personal information sharing scheme to securely share personal information among users. Furthermore, we utilize off-chain storage mechanisms to reduce the storage pressure on blockchain systems and improve its scalability, thereby addressing complex network threats. Lastly, we introduce traceable ring signatures and propose an effective method for verifying the authenticity of information on the blockchain, ensuring the authenticity and traceability of medical information within the blockchain infrastructure. In summary, our method can protect patient privacy, ensure the integrity and traceability of data, and facilitate the sharing of electronic medical records among medical institutions.

The paper is structured as follows: Section 2 discusses the risks and related technologies in data sharing and block-chain research. Section 3 describes the proposed architecture. Section 4 details the experimental results. Section 5 presents a security analysis. Section 6 analyzes the challenges we still face in our current work. Section 7 concludes the paper and suggests future research avenues.

2. Preliminary

2.1. Legal and security aspects of electronic medical records sharing

The increasing integration of technology in healthcare has made the sharing of electronic medical records (EMRs) a vital part of medical practice. Nonetheless, this digital transformation is followed by the generation, storage, and transmission of substantial volumes of sensitive personal health information. These activities not only come with significant financial costs but also present a plethora of problems and challenges. The most notable concern is the privacy and data security [19,20] of patients' medical information. Inappropriate sharing of EMRs could lead to privacy breaches, as such delicate data might inadvertently be accessed by unauthorized entities, leading to misuse. Concurrently, the looming risks of data breaches and cyber-attacks pose significant threats to the integrity and security of these medical records [21]. These issues are major hindrances to the development of trustworthy systems for the sharing of electronic medical information.

The issues of data ownership and control related to EMRs have become increasingly relevant. Patients frequently lose control over their medical data during the exchange process, which results in a loss of transparency and controllability in the handling of this sensitive information. With EMRs being extensively utilized for diagnostics, treatment plans, medical research, and insurance purposes, the urgency to implement robust privacy and security measures is acute.

Legislation has been imposed in numerous countries and regions to safeguard the legality, security, and privacy of electronic healthcare data. The Personal Information Protection Law of the People's Republic of China, instated in 2021, defines regulations for the handling of personal information, including EMRs, that accentuate protection and introduce penalties for infractions. Prior to this, the European General Data Protection Regulation (GDPR) empowered individuals with greater authority over their data since 2018, coercing healthcare providers to comply with strict protocols, such as seeking prior consent and providing transparent disclosures, in addition to ensuring data security [22,23]. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) also enforces directives for the management of personal information in healthcare, emphasizing patient consent and the security of their records [24].

Regarding dynamic consent, Mascalzoni [25] and others have given relevant definitions: based on a strong governance and an ongoing tailored communication with participants, it aims to promote autonomy and to develop a trust-based engaged relationship with participants, also relevant for retention. Built within an online platform, the consent allows granular choices, which can be changed over time. Our work is in accordance with the characteristics of dynamic consent: patients' autonomy empowers them to decide whether or not to continue the operation, rather than passively accepting all procedures; they can dynamically adjust their consent decisions on the blockchain, reflecting the changeable choices; and all behaviors and choices of all participants, including patients, will be transparently and traceably recorded on the blockchain, ensuring continuous records.

An examination of the relevant laws and regulations worldwide indicates that dynamic consent has progressively become a trend and a focus in academic discourse [26]. Exploring solutions to consent management in healthcare through the adoption of blockchain technology is becoming a prevalent trend [27].

Our approach is in strict compliance with the legal standards decreed by the Personal Information Protection Law of the People's Republic of China concerning the management of electronic medical records. Specifically, the legal framework outlines certain scenarios under which EMRs may be processed lawfully:

- With the individual's consent (Article 13, Clause 1).
- As necessary for the execution or fulfillment of contracts where the individual is a party or for human resource management per lawful labor rules and collective agreements (Article 13, Clause 2).
- To fulfill legal obligations or duties imposed by law (Article 13, Clause 3).
- To address public health emergencies or to protect the safety of person and property in urgent situations (Article 13, Clause 4).
- For public interest activities such as journalism and public opinion supervision, provided the personal information processing is within reasonable limits (Article 13, Clause 5).
- Where the information has been made publicly available by the individual or is otherwise legally in the public domain (Article 13, Clause 6). Other circumstances as stipulated by laws and administrative regulations (Article 13, Clause 7).
- Furthermore, when consent forms the basis for processing personal information, such consent should be informed, voluntary, and explicit, with provisions for individuals to withdraw consent conveniently, without affecting the legality of any information processing undertaken before the consent was withdrawn (Articles 14, 15).

Including such stipulations underscores our compliance with legal standards for personal data handling within the scope of our research methodology, ensuring that our processes preserve the rights and safety of individual data subjects under the law.

2.2. Blockchain in personal information sharing

Studies exploring the application of blockchain tech-nologies for personal information sharing have spanned a wide range of disciplines. In the realm of digitizing government affairs [28–31], Maxat has suggested that the utilization of blockchain technology by government departments not only fortifies security and reliability but also augments transparency and efficiency of public digital platforms, thereby fostering data sharing among citizens, businesses, and governments [32]. Piao et al. proposed a blockchain-based solution for government information chain services to tackle the challenges encountered by e-government systems [33].

In the healthcare sector, blockchain technology lends support to drug management and the sharing of electronic medical records [34–36]. He et al. proposed a solution for medical records, inclusive of electronic prescriptions with data anonymization, through the Hyperledger Fabric platform [37]. Wang et al. suggested a blockchain-based EHR sharing system that achieves fine-grained access control and privacy protection [38]. The aforementioned work harnesses the transparent and tamper-proof attributes of blockchain to propose a plethora of equitable and effective information management and sharing methods that safeguard personal privacy.

Existing research on privacy in data sharing primarily concentrates on regulating and tracing transactions, but often neglects the risk of forgery and tampering due to blockchain attacks, as well as the issue of how to fully exercise the rights of information owners.

Distinguished in Table 1 from previous works, our research unfolds a novel blockchain-oriented scheme tailored for the sharing of personal health records that accentuates the prerogatives of the data owner, while aligning with international legal frameworks. Built on our prior achievements in safeguarding data privacy within the burgeoning Internet of Vehicles (IoV) sphere—where a privacy-preserving construct for blockchain-facilitated data sharing was introduced within vehicular edge networks [39]—we now broaden our scope to conquer the overarching challenges inherent to EMR sharing. We tackle the hurdle of on-chain storage expenditures through the integration of distributed ledger technology for off-chain data housing, diminishing the costs and circumventing the pitfalls of centralized bottlenecks. Additionally, we implant a ring signature protocol not only validating

Table 1
Comparison of our work with other pertinent works.

Reference	Information owner centric	Authenticity	Integrity	Privacy	Off-chain storage	Cost computation	Test of execution time	Scalability
[36]	✗	✓	✓	✓	✗	✗	✗	✗
[38]	✗	✓	✓	✓	✗	✓	✓	✗
[30]	✗	✓	✓	✗	✗	✓	✓	✓
[37]	✗	✓	✓	✓	✗	✗	✗	✓
[28]	✗	✓	✓	✗	✗	✗	✓	✗
[29]	✗	✓	✓	✓	✓ (Distributed)	✓	✓	✗
[35]	✓	✓	✓	✓	✓	✗	✗	✓
[31]	✗	✓	✓	✓	✓ (Centralized)	✗	✗	✓
Our work	✓	✓	✓	✓	✓ (Distributed)	✓	✓	✓

on-chain data veracity and wholeness but also bolstering the concealment of legitimately anonymous stakeholders. This holistic strategy, deployed within a decentralized application, has been rigorously assessed through widespread testing.

2.3. Ring signature and traceable ring signature

2.3.1. Ring signature

Ring signature is a cryptographic technique used to achieve anonymous identity verification and signature authentication [40]. It was first proposed by Ronald L. Rivest, Adi Shamir, and Yael Tauman in 2001 [41]. Ring signatures allow a signer to sign a message using members of a key ring without the need for authorization or cooperation from other members. In a ring signature, a key ring is a collection of user public keys. When a user wants to create a ring signature, they can choose to sign on any number of public keys in the key ring. Then, by applying a series of cryptographic algorithms, the signer can generate a signature that includes the selected public key and the signer's own private key information. In this way, for the verifier, they only need to verify whether the signature is valid, and cannot determine which specific user signed it. The basic ring signature consists of three algorithmic parts $(KeyGen(), Sign(), Verify())$.

- **KeyGen():**
  The user generates a pair of keys (pk, sk), where pk is the public key and sk is the private key.
- **Sign():**
  The signer uses their own private key and the selected set of public keys $L = \{PK_1, PK_2, \ldots, PK_n\}$ to sign message M and obtain a ring signature σ.
- **Verify():**
  Input (σ, M. L), output "True" or "False".

Given its untraceable and unlinkable characteristics, it aligns with the requirements for digital currency transactions that depend on blockchain technology. In digital currency transactions, there are clear requirements to ensure anonymity, untraceability, privacy protection, decentralization, legality, and compliance. Based on these requirements, in 2013, Saberhagen et al. proposed the CryptoNote protocol [42] based on ring signature technology, which proposes two privacy characteristics that anonymous electronic cash systems need to meet, and designed protocols for these two characteristics. These two major characteristics are untraceability and unlinkability, which means that for each transaction input, all possible transaction initiators are equally possible, while for any two transaction outputs, it cannot be proven whether they were sent to the same user.

2.3.2. Traceable ring signature

The traceable ring signature is slightly different. Fujisaki et al. [43] believe that due to the anonymity of ring signatures, they are easily attacked by malicious or irresponsible signers. Therefore, they propose a ring signature scheme that limits "excessive" anonymity. Not only can it verify the validity of the signature, but it can also trace and disclose the identity of the malicious user who caused the signature failure. This process will not expose the true identity of legitimate anonymous users at all. The traceable ring signature scheme consists of four algorithms.

- **KeyGen():** Take the security parameter $k \in \mathbb{N}$ and output a public/private key pair (pk, sk).
- **Sign():** Enter key sk_i, Where $i \in \mathbb{N}$, label $L = (issue, pk_N)$, message $m \in \{0,1\}^*$, and output signature σ.
- **Verify():** Input label $L = (issue, pk_N)$, message $m \in \{0,1\}^*$ and signature σ, output "True" or "False".
- **Trace():** Input label $L = (issue, pk_N)$ and two message/signature pairs $\{(m_1, \sigma_1), (m_2, \sigma_2)\}$, output "indep", "linked" or pk.

The traceable ring signature scheme proposed by Fujisaki et al. provides the following functionalities:Public traceability, label linkability (with an additional unforgeability), anonymity and exculpatory. In view of the light weight of its algorithm and the fit with all aspects of our scheme, we integrated its algorithm into our scheme design.

3. Consent-aware framework for secure sharing of electronic medical information

This section introduces an enhanced framework for secure electronic medical information sharing. Initially, we propose a comprehensive system architecture that incorporates clear rights, responsibilities, transparency, security, and reliability. The integration of blockchain and smart contract technologies enhances its security, trustworthiness, and scalability through off-chain storage. In the subsequent stages, we use traceable ring signatures to store the associated signature data across the chain, which makes the business process transparent and protects the identity privacy of each user. Moreover, the application of ring signatures can effectively increase the difficulty of malicious tampering with the blockchain.

The framework has been designed to cater to a medical information system involving three essential stakeholder categories. It is perfectly suited for a variety of applications including, but not limited to, electronic medical records, prescription filling and medication tracking. Furthermore, the framework is equally adept for integration into e-government infrastructures that necessitate the secure processing of personal medical data. We elaborate on the unique roles and responsibilities shouldered by healthcare providers, patients, and regulatory bodies:

- The Personal Information Owner (Patient): Specifically denotes individuals possessing absolute ownership over specific personal data. The patient retains the right to dictate any operation involving their personal information, provided it does not violate the relevant regulations. The patient can facilitate certain actions by submitting their personal data or delegating its safekeeping to a specified party. More frequently than not, the patient transfers personal data generated by one or more agencies, or merely entrusted for storage, to another entity not for the purpose of completing a transaction but rather for ensuring the continuity and quality of healthcare services.

Table 2
Symbols and explanations.

Notation	Description
N	Number of doctors in one hospital system
Patient, MI-MR, MI-RMR	Personal Information Owner; Medical Institution with Medical Recordsy; Medical Institution Requiring Medical Records
P_i	The i_{th} participant
pk_i, sk_i	Public and private keys of the i_{th} participant
E_{k_i}, sk_i	Using symmetric key k_i to encrypt information M
σ	Signature results generated during the signature process
H, H', H''	Three Hashing Methods

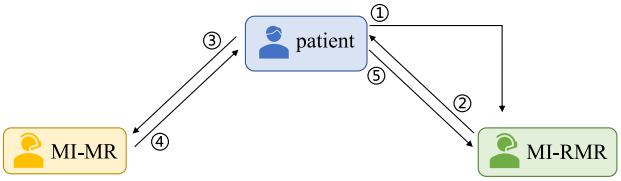

Fig. 1. Personal information data sharing based on blockchain.

- The Medical Institution with Medical Records (MI-MR): This term refers to an abstract entity, and the medical institution with medical records, hereafter referred to as MI-MR, is an organization capable of securely storing the patient's personal data. Typically, the data held by MI-MR is either commissioned by the patient or generated during the patient's treatment and interaction within the institution. It is essential to retain this data within MI-MR to ensure the smooth and ongoing delivery of healthcare services to the patient.
- The Medical Institution Requiring Medical Records (MI-RMR): The MI-RMR is an organization tasked with incorporating personal information into healthcare operations. While healthcare applications are typically initiated by the executing party, it does not mark the inception of a healthcare process. It depends on the circumstances. The healthcare executive will send the application details, along with a list of required information, to the MI-MR in order to obtain the necessary personal information to facilitate a particular healthcare service.

Some of the symbols used in this article are shown in Table 2.

3.1. Medical records sharing and privacy protection

Safeguarding the confidentiality of personal data is paramount throughout all stages of its lifecycle. Strict adherence to regulatory protocols and the enforcement of comprehensive data management principles are fundamental to controlling the access and use of personal data. This approach not only diminishes potential threats but also lessens the operational and security burdens borne by associated services. Through these measures, we strengthen our defenses against unauthorized access to data, thus bolstering the overall trust in and reliability of our services.

In the scenario illustrated in Fig. 1, we designate the following entities: The Personal Information Owner (Patient), The Medical Institution with Medical Records (MI-MR), and The Medical Institution Requiring Medical Records (MI-RMR), to build the foundational model that Fig. 1 represents. The process is initiated by the Patient, who consents to the sharing of their medical records. In response, MI-RMR requests the necessary health information from the Patient; the Patient then submits a data request to MI-MR, which maintains the records; MI-MR authenticates the Patient's identity and transfers the medical data; finally, the medical records are securely conveyed to MI-RMR through the Patient's authorization. This flow delineates the standard procedure for the secure exchange of personal health information.

In this framework, The Medical Institution with Medical Records (MI-MR) that archives information and The Medical Institution Requiring Medical Records (MI-RMR) that obtains information are entirely separated by the authorization of The Personal Information Owner (Patient). Information retrieval and transfer are two distinct actions initiated by the Patient, which signify the end of the responsibility for the MI-MR. Consequently, the transfer of information to MI-RMR does not implicate MI-MR in any further obligations.

Entities responsible for storing information, such as MI-MR, offer legally mandated inquiry services to the Patients in compliance with legislation. This enables Patients to lawfully access all of their personal medical data and to convey this information to MI-RMR in accordance with their preferences. Thus, the transfer of any personal data can be executed within the bounds of legality.

Aligned with the Personal Information Protection Law of the People's Republic of China, enacted in 2021, the philosophy of personal data protection underscores the importance of consent in the collection and usage of personal information, laying the groundwork for specific regulations safeguarding personal information. "Informed consent" is a cornerstone principle stipulated by this law, crucial for protecting individuals' rights to be aware of, and to decide on, the processing of their personal data.

As demonstrated in Fig. 1, for the Patient, each step involving data flow will be communicated explicitly. In the absence of agreement, the process is halted to maintain compliance with the "informed consent" principle. This adherence meets the specifications of the Personal Information Protection Law, amplifies the Patients' awareness of their rights, and safeguards their privacy through active consent.

3.2. Consent-aware medical records sharing architecture

Fig. 2 illustrates our proposed architecture for medical records sharing, which encompasses three roles and is also built on top of a block-chain infrastructure and distributed storage system. All participant interactions will be logged on the blockchain, and smart contracts are deployed on the chain to deliver the relevant functions. Traceable ring signatures are used to authenticate the data and preserve the integrity of the data on the chain.

Regarding user registration, it is not the focus of this study and only provides a brief explanation, without being introduced as a core function. The user's identity is assigned by the blockchain, and once assigned, it is permanently bound and stored on the blockchain. Users use this identity account to participate in personal information sharing transactions. The exact way to create and assign a unique ID is not within the current scope of work and can be determined by the relevant agency depending on the specific situation.

The general process of data sharing is as follows:

(1) Patient initiates business proactively: Patient applies for business to the target MI-RMR.
(2) Business initiation: The business executor MI-RMR responds to the patient's business application and sends the application of business application information and a list of required information to the patient.

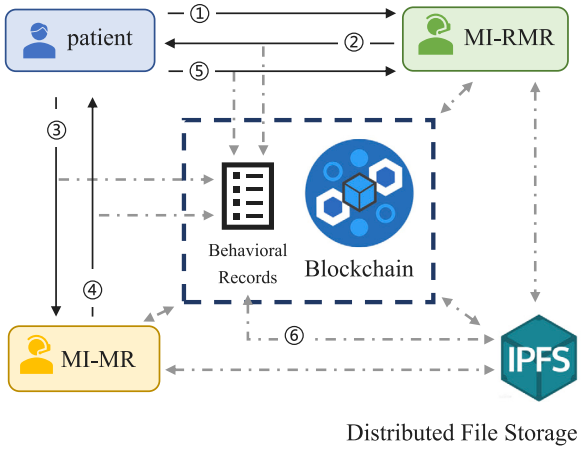

Fig. 2. Personal information sharing model based on blockchain.

(3) Patient prepares data: If the patient does not intend to continue with the business, the application to reject MI-RMR will end the process. If the patient agrees to continue with the business, relevant information m needs to be prepared according to the information list. If the patient can directly provide personal information, such as ID card number, age, gender, address, telephone number, etc., which does not need to be notarized by a professional organization, the patient can directly submit it to MI-RMR. However, in most cases, personal information management needs to handle the transfer or sharing of personal information stored by one organization to another. At this point, when the patient agrees to the application for MI-RMR, the medical institution (MI-MR) with medical records will receive the relevant information. Therefore, the acquisition of information is completely transparent to the patient, and only needs to decide whether to agree to the business process. When a patient agrees to handle the business, they will use a ring signature to sign the information needed to be transferred, and this signature, along with the corresponding action, is recorded on the blockchain.

(4) MI-MR data preparation: When receiving data request requests and information lists from the patient, the first step is to verify the identity of the patient. The simplest method is to use the blockchain infrastructure to provide a solution for identity authentication. After successful identity authentication, the MI-MR retrieves data from the database according to the information list and sends the information to the patient through symmetric encryption. When obtaining data, MI-MRs need to first obtain the hash index of the corresponding information from the blockchain, and then obtain the information from distributed storage. We use IPFS to implement distributed storage here. Similarly, MI-MR will use the ring signature algorithm to sign the information sent, recorded on the blockchain along with the action.

(5) The patient delivers personal information: After receiving encrypted information, the patient decrypts the information and then performs symmetric encryption, sending it to MI-RMR for business processing. MI-RMR decrypts information and conducts business processing, bringing a complete business process to an end. Note that, whether it is patients or other business participants, as long as there is data transfer, this data will be signed, and the generated signature with the action will be recorded on the blockchain.

(6) Initially, following any action taken by participants, the blockchain creates respective logs of their behaviors. For the convenience of storage and supervision, we have designed a business process recording smart contract.

Based on the above process, a deployment roadmap is compiled as shown in Table 3.

As can be seen in Fig. 2, all three types of roles or users involved in a certain business will have their behavior and activities recorded on the blockchain. Secondly, for the three types of roles, the reason for dividing and adopting a phased point-to-point encrypted data transmission instead of using the data access control authorized by patients, which is favored by most schemes, is because in our proposed architecture, patients have absolute decision-making power over whether to start or continue transactions both theoretically and practically, which can truly ensure patients' "informed and consent" in handling personal information sharing, being in an absolute dominant position. The Medical Institution with Medical Records (MI-MR) who saves information and the Medical Institution Requiring Medical Records (MI-RMR) who receives information are completely isolated through the patient. Information query and transfer are two independent patient user behaviors, and the obligation of the MI-MR is terminated by the patient. The business of the MI-RMR will not be associated with the MI-MR.

This strategy is heavily reliant on explicit patient authorization and blockchain technology to ensure the secure sharing of patient medical data. All data exchanges require explicit consent from patients. Leveraging blockchain technology, all transaction records are permanently stored on the blockchain, considerably enhancing the difficulty for any collusive action in accessing patient information. The assurance of security could possibly be further strengthened by additional measures, such as introducing third-party auditing mechanisms to prevent and monitor potential misbehaviors. In our future work, we plan to incorporate advanced encryption techniques like homomorphic encryption to add an extra layer of protection to patient privacy.

As previously discussed, to ensure that the patient retains absolute control throughout the entire process, we employ end-to-end encryption transmission instead of delegating access control outsourcing to a third party. This fundamentally eliminates the possible uncertainties and uncontrollable factors that may arise from a third party, reducing the risk of data being compromised. On the other hand, our current strategy does not require users to set consent preferences temporarily. However, we may consider incorporating access control management and preset preferences in future enhancements. Furthermore, regarding the use of the InterPlanetary File System (IPFS) by various parties, each time a data segment is stored in IPFS, an index pointing to this piece of data is provided. In subsequent peer-to-peer communications, the encrypted index replaces the originally needed enormous segment of medical information data. The holistic approach integrates a ring signature scheme proposed in our strategy, where the signatures derived from this information flow are uploaded onto the blockchain. These introduce tamper-resistant evidence crucial for future audits. Concurrently, electronic therapeutic data is stored within IPFS. Each of these steps is integrated systematically to ensure data compliance, without compromising on the secure and seamless exchange of information.

We chose IPFS from several distributed storage systems for its unique advantages. It has the functionality of content addressing rather than location addressing, providing a global unified namespace. Moreover, IPFS has version history functionality, which is conducive to data version management and historical review. In addition to these, IPFS also features data redundant storage and file deduplication, thereby increasing the reliability and efficiency of data storage.

We also examined other distributed storage systems like HDFS and Amazon S3. HDFS is predominantly for large-scale data processing, providing a framework suitable for large-scale data sets, but its efficiency might be lower when dealing with dynamically changing content as it relies on network location for data indexing and management. Amazon S3 is a scalable storage service based on the Internet, but its data redundancy and reliability largely depend on the user performing appropriate settings and operations. Therefore, after comparing the various distributed storage systems, we decided upon IPFS, which suited our needs better.

Table 3
Full process deployment strategy.

Function	Description	Application scenario
Patient initiates business proactively	The patient applies for business to the target MI-RMR.	In scenarios where proactive patient engagement is required.
Business initiation	The MI-RMR responds to the patient's application and sends application information and a list of required information.	When a patient must provide required information to MI-RMR for business processing.
Patient prepares data	The patient decides whether to continue with the business, and prepares the requested information, either directly or via a smart contract with MI-MR.	In situations where sensitive information must be reliably secured, such as when a patient provides personal information for a medical procedure.
MI-MR data preparation	MI-MR verifies the identity of the patient, retrieves the requested data, then sends this data to the patient in an encrypted form.	When data security and patient identity need to be verified in the medical health record application process.
The patient delivers personal information	The patient receives, decrypts, and re-encrypts their information before sending it on to MI-RMR for business processing.	When the patient's encrypted information needs to be safely transmitted and processed.
Blockchain logging and recording	The blockchain creates logs of each stage in this process.	When the behaviors of all participants need to be logged and recorded in a fail-safe and secure manner.

For data partitioning, IPFS introduces a concept known as "Content Identifier" (CID). Each time a user uploads a data object to the IPFS network, the system generates a unique CID for it. The CID serves not only as a representation of the data content but also includes the metadata of the data, such as the data format and the data hash value. In this way, each data object has its independent location in the IPFS network, thereby realizing effective data partitioning. Regarding the indexing strategy, IPFS utilizes a Distributed Hash Table (DHT). In this network, each node is responsible for storing a portion of the DHT. Given its extensible and distributed characteristics, DHT is an ideal solution for data indexing. When a user needs to search for a data object, they can simply use that object's CID to search, and the network will find the corresponding node information in the DHT mapping and obtain the data from that node. What is worth mentioning is that the index information established based on DHT can also carry more advanced queries, such as searching for data by name and attributes. This indexing strategy not only meets the needs of large-scale data retrieval but also ensures the efficiency of queries. This hybrid application has a rich range of standard functions, is flexible for different scales of data requirements, and accelerates the efficiency of data retrieval and storage.

After the research of centralized storage and distributed storage, we utilize IPFS as a distributed storage for our data. The advantage of centralized storage is its extremely high performance, high throughput, high IO, and low latency, as well as good data consistency and disaster recovery solutions. Many enterprises choose centralized storage as their primary storage architecture for security and performance considerations, to carry critical businesses, especially in industries with high data compliance such as government, finance, and healthcare. However, some limitations faced by centralized storage cannot be ignored.

Despite its outstanding performance, centralized storage presents some challenges in terms of scalability and fault tolerance. With the growth of data scale, a single storage point may become a performance bottleneck, leading to system instability. In addition, hardware failures or unexpected events may have a serious impact on the entire system, as all data is concentrated in the same location.

In contrast, distributed storage effectively overcomes these issues by dispersing data across multiple nodes. Distributed storage systems have good scalability and can flexibly expand storage capacity according to requirements. At the same time, in the event of a node failure, the system can still maintain stable operation. This redundancy and distribution help improve the robustness of the entire system and reduce the risk of single point failures.

It is worth mentioning that for industries with high compliance requirements, the data redundancy and decentralization characteristics of distributed storage make it more in line with data security and compliance standards. The distribution of data in multiple locations reduces the potential risk of data leakage and better adapts to regulatory and legal requirements in different regions.

Therefore, considering these factors, IPFS fully meets the unique network requirements of content distribution because it is distributed, has no hard requirement for storage granularity, and has the natural advantage of tamper resistance [44], we choose distributed storage as the data storage method to achieve a better balance between performance and security. In our proposed architecture, IPFS not only serves the purpose of storing personal health information but also supports off-chain storage of blockchain information. Transferring a large amount of blockchain-stored data to distributed storage, while only storing relevant hashes and indexes on the chain, can greatly reduce the storage cost and burden of the blockchain.

Fig. 2 shows three roles, each with one subject. However, in reality, subjects may need to interact with multiple Medical Institutions with Medical Records (MI-MRs) to gather all necessary personal information for a specific business. In our scenario, dealing with multiple MI-MRs at the same time does not complicate the process. As shown in Fig. 3, personal information is directly requested from multiple MI-MRs, decrypted and integrated by the patient, and then submitted to the MI-RMR.

3.3. Scheme description

In the architectural framework tailored for electronic medical record (EMR) sharing, ring signatures emerge as a cornerstone in safeguarding patient data privacy. This technique enables patients to share their medical records with healthcare providers without disclosing their identity, epitomizing the principles of confidentiality and transparency within the healthcare sector. By embedding ring signatures into our architecture, we not only enhance the privacy of health information but also set the stage for a stringent regulatory framework. This twofold benefit secures patient anonymity whilst maintaining system openness and accountability, delicately balancing privacy concerns with compliance requirements in the digital healthcare environment.

System Initialization: Let G be the multiplication group of prime order q, and let g be a generator of G. Let $H : \{0,1\}^* \rightarrow G$, $H' : \{0,1\}^* \rightarrow G$, and $H'' : \{0,1\}^* \rightarrow \mathbb{Z}_q$ are different hash functions. Any participant P_i extract element x_i from $\mathbb{Z}_q$ and calculate $y_i = g^{x_i}$.

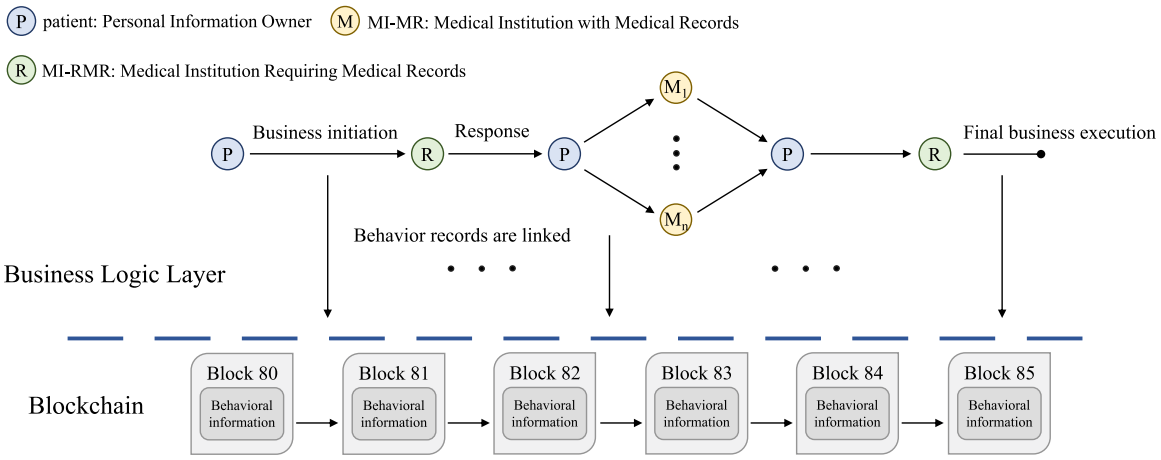

Fig. 3. Personal information sharing process with multiple information storage parties.

The public key P_i of i is $pk_i = g, y_i, G$, the corresponding key is $sk_i = \{pk_i, x_i\}$. We use $N_{all} = \{1, \ldots, n_{all}\}$ indicates that there are n_{all} users in the system at this time. Using $N_w = \{1, \ldots, n\}$ represents an ordered list of n participants in a certain business w. Set $pk_N = (pk_1, \ldots, pk_n)$ is an ordered public key list of set N.

Algorithm 1 System initialization.

Input: None
Output: Public and private key pairs, N_{all}, and N_w datasets
1: Define G as multiplication group of prime order q
2: Define g as a generator of G
3: Define hash functions H, H', H''
4: **for** each participant P_i **do**
5: Extract x_i from Z_q
6: Calculate y_i using g and x_i
7: Define public key y_i and private key sk_i
8: **end for**
9: Define N_{all} and N_w as the total number of participants and the number of participants in w, business respectively
10: Define pk_N as an ordered public key list of set N
11: **return** N_{all}, N_w

Data Generation: Assuming that patient needs to obtain personal information from an MI-MR in the business process, the following is an introduction to how to generate and store information:

When patient generates a medical record data M on an MI-MR or entrusts it to store this data, patient generates a non-public symmetric key k_i. Encrypt M and upload encryption result$EM = E_{k_i}(M)$ to IPFS and hand over the hash index HI to the MI-MR for storage. Note that due to relevant legal requirements, MI-MR have no right to refuse any reasonable requests from patient regarding medical record entrusted to them for safekeeping. Meanwhile, due to the encryption of this information, the MI-MR is unable to add, delete, modify or check the original data without authorization.

Algorithm 2 Data generation.

Input: Medical record data M
Output: Encrypted M and its hash index HI on IPFS
1: M = Patient.GenMRData()
2: k_i = Patient.GenSymmetricKey()
3: EM = Patient.Encrypt(M, k_i)
4: HI = IPFS.Upload(EM, M)
5: MI-MR.Store(HI)
6: **return** HI

Data Sharing: Taking Fig. 2 as an example, assume that patient agrees to the business. The following steps are based on a blockchain identity trusted environment. Through smart contracts, as shown in Fig. 4, $\text{MI}-\text{RMR}_k$ generate a business record structure on the chain, save the business number $issue$, and the signatures σ_i obtained by all parties using private keys and parameter A_{0i} (assuming $h = H(L)$, $A_0 = H'(L, m)$). Its structure and usage are shown in Fig. 3. This record is saved on the chain, and during the data sharing phase, all parties can use this record to verify the identity of the other party and verify the business status. At the same time, generate random non repeating business numbers for generating ring signatures. $\text{MI}-\text{RMR}_k$ transmits the required information list string **List** through the generated public and private keys, waiting for patient_i pass or reject. To verify identity, $\text{MI}-\text{RMR}_k$ needs to sign the **List** and $issue$, therefore, the actual message sent by $\text{MI}-\text{RMR}_k$ is $E_{pk_i}(\textbf{List}\|issue\|\sigma_1)$. When $\text{MI}-\text{RMR}_k$ sends information, it is necessary to set ST_1 in the business record to $(\sigma_1\|A_{01})$, and set the status of ST_1 in the business record to $standby$ for patient_i verify the business. patient_i decrypt the information to confirm identity and business information on the blockchain. After agreeing, patient_i use private key to sign the **List** and submit it to the $\text{MI}-\text{MR}_j$ holding the relevant information in the **List** sends $E_{pk_j}(\textbf{List}\|issue\|\sigma_2)$. Similarly, patient_i set ST_2 to $(\sigma_2\|A_{02})$. After decryption, identity and business confirmation, $\text{MI}-\text{MR}_j$ prepare the relevant information index HI and send $E_{pk_i}(HI\|issue\|\sigma_3)$ to patient_i, set ST_3 to $(\sigma_3\|A_{03})$.Among σ_3 is the signature for HI and $issue$. After decrypting message from $\text{MI}-\text{MR}_j$ and verifying the correctness of the signature and transaction information, patient_i obtain information M from IPFS, encrypt it with a temporary key k', and upload it again to IPFS to obtain a new index HI'. patient_i also sign and encrypt, and send $E_{pk_k}(HI'\|k'\|\sigma_4)$ to $\text{MI}-\text{RMR}_k$. Set ST_4 to $(\sigma_4\|A_{04})$. $\text{MI}-\text{RMR}_k$ decrypt and verify that the signature is correct for the business, obtain σ_5 through sign H' under label $L_{all} = \left(pk_{N_{all}}\right)$. Set ST_5 to $(\sigma_5\|A_{05})$. patient_i can verify that $\text{MI}-\text{RMR}_k$ is known successfully decrypted the information, and the data sharing process ends here. The business records are encapsulated and recorded on the blockchain.

In our design, the user's re-encryption is a must for two main reasons. Firstly, re-encryption provides an additional layer of security to ensure the safety of data during its transmission. When the patient obtains the information M from IPFS, they re-encrypt it with a temporary key, k', for the sake of safe transmission towards the MI-RMR process. This can prevent potential risks like cyber-attacks, sensitive information theft or data tampering that can occur during data transmission. Secondly, re-encryption permits the shift of data ownership and control among the participants. The data owner (patient) through re-encrypting their data can directly govern which entities can access their data — thereby ensuring both data privacy and data usability.

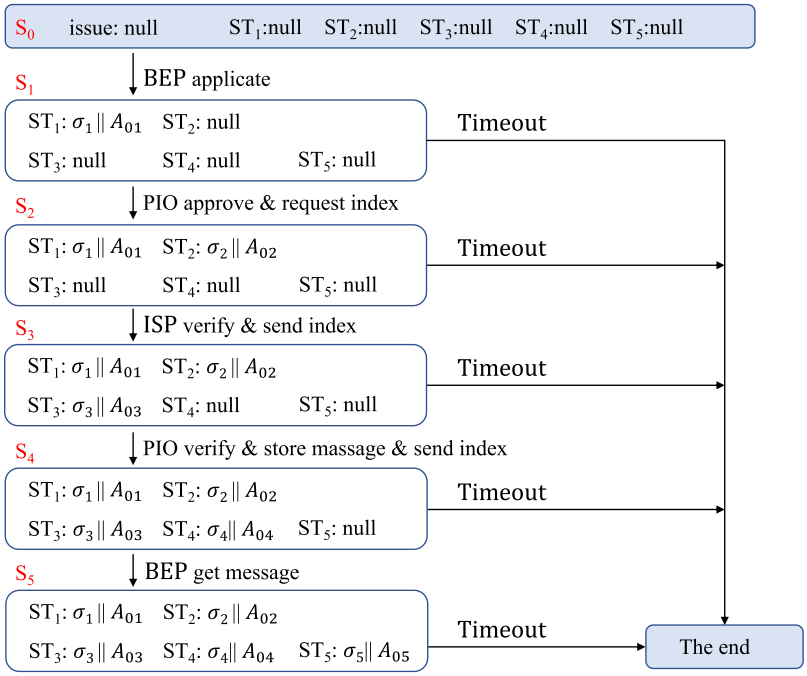

Fig. 4. Smart contract implementation business record structure.

The process of re-encryption allows that the MI-RMR can only ascertain these data after receiving the newly generated Index HI', evidently enhancing the data owner's control over their data.

Algorithm 3 Data sharing.

Input: The business number issue B, signature σ_i, and parameter A_{0i}
Output: Business information BI on blockchain, new index HI' on IPFS

Let BI = generate_record(B), and store B and σ_i
R = generate_ring_signatures(BI)
Transmit L = required_info_list(BI), wait for response
if patient verifies and agrees **then**
    S = sign_list(L) and submit to $MI - RMR_j$
end if
HI = prepare_index($MI - RMR_j$) and send to patient
$M = (D, V)$ = decrypt_verify(HI)
Re-Encrypt M with temporary key k', re-upload to IPFS
Sends new index HI' and encrypted data M' to $MI - RMR_k$
$MI - RMR_k$ decrypt_verifie($MI - RMR_k$, M')
If successful, patient knows that $MI - RMR_k$ successfully decrypted info
return HI'

Signature Tracking: In this scheme, various business participants ensure the authenticity and correctness of data sources through multiple verification methods, including traceable ring signature verification and on-chain and off-chain signature data comparison verification. Once a problem is discovered after the completion of a business, it can be traced through encapsulated business records to verify the signers of each signature in the encapsulated information. When tracing, there is no need to obtain the original data for signature: Verifying σ is actually verifying the relationship between (m, σ_i) and (m', σ_i') for the same pk_N, where $\sigma = (A_1, c_N, z_N)$, $\sigma' = (A_1', c_N', z_N')$. The original data m transmitted by both parties during data sharing is currently invisible. m' can be any data, specified here as the business number $issue$ of the target business, and σ_i' is the signature used for verifying the issue. Let L be $(issue, pk_N)$. Let $h = H(L)$, obtain A_0, and calculate $\sigma_i = A_0 A_1^i \in G$ for all $i \in G$. Do the same thing for σ' and search for σ_i' for all $i \in N$. For all $i \in N$, if $\sigma' = \sigma_i'$, pk_i is stored in **TList**, **TList** is initially an empty list. If pk is the only entry in **TList**, output pk; If **TList** = pk_N. Then it is "linked"; Otherwise, it is "indep" (i.e. **TList** = ∅ or $1 <$ **TList** $< n$). Considering that there is no signature for the issue in the normal business process, the first scenario will not occur; If the output result is "linked", it can be proven that the target signature and the signer of the verification signature are the same person; If the output result is "indep", it indicates that the signature to be verified and the assumed signer are not the same person, indicating that there is an issue with the recorded information during encapsulation, and the related business will also be suspected.

4. Experiment results and discussion

In this section, we delve into the empirical analysis to validate the usability, scalability, and tamper-resistance of our proposed framework for on-chain data management. To this end, we have orchestrated a series of simulation experiments focusing on the smart contract infrastructure, the comprehensive information sharing mechanism, and the ring signature protocols delineated in our study. These simulations were meticulously conducted on a robust experimental setup, comprising an i7-12700H processor clocked at 2.30 GHz and 16.0 GB of RAM, all operating under the Windows 11 OS. This configuration was selected for its relevance to a high-performance computing environment, which is essential for assessing the real-world applicability of our scheme in handling extensive datasets and complex cryptographic operations with efficiency and reliability.

4.1. Computation of cost for smart contracts

To ascertain the real-world viability of the smart contract articulated in our proposed framework, we have initiated deployment and rigorous testing phases. Our implementation leverages the Ethereum platform, renowned for its open-source, public blockchain network

Algorithm 4 Signature tracking.

Input: m, m', σ, σ'
Output: pk_N, verification of the consistency of σ and σ' for m and m'
$\sigma = [A1, c_N, z_N]$, $\sigma' = [A1', c'_N, z'_N]$)
Define L as $(issue, pk_N)$
Get $h = H(L)$
Obtain A_0
$\sigma_i = A_0 A_1^i \in G$ for all $i \in G$
Do the same thing with σ', and look for σ_i for all $i \in N$
for all $i \in N$ **do**
  if $\sigma = \sigma'$ **then**
    add pk_i to $TList$
  end if
  if pk is the only entry in $TList$ **then**
    output pk
  end if
  if $TList$ equals pk_N array **then**
    output $\varepsilon linked \varepsilon$
  end if
  output $\varepsilon indep \varepsilon$
  $T = T \cup PosSample(c)$
end for
return pk_N, verification

that specializes in the deployment of smart contracts. These smart contracts unlock a plethora of functionalities for decentralized applications, setting the stage for innovative use cases. Our experimental setup is bolstered by the utilization of Ganache, a suite of tools designed for creating personal blockchain networks for Ethereum development testing, and the Remix Integrated Development Environment (IDE), which serves as a sophisticated compiler for smart contracts. Within this environment, we meticulously implemented the core components of a smart contract—variables, modifiers, state variables, and events—using the Solidity programming language. Remix IDE played a crucial role, offering a versatile platform for the development and testing of smart contracts, ensuring their seamless integration both locally and within the broader blockchain ecosystem. This comprehensive approach not only demonstrates the practicality of our smart contract but also showcases the flexibility and robustness of Ethereum as a platform for fostering the development of distributed applications.

To bolster the security and availability of the decentralized peer-to-peer (P2P) network, the blockchain ecosystem incentivizes miners by rewarding them for the critical tasks of transaction verification and new block mining. In the context of Ethereum, this reward system is intricately linked to the computational prowess involved in the process of transaction verification. Miners are compensated in 'gas' by the transaction initiators, a unique feature of the Ethereum network. This concept of gas translates to a mandatory fee required for executing transactions on the Ethereum blockchain.

A pivotal aspect of this study is the evaluation of gas consumption, an essential factor in determining the economic sustainability of decentralized applications (DApps). It is crucial to meticulously compute the cost associated with executing smart contracts and their key functions, as these costs directly impact the feasibility and efficiency of DApps in a real-world setting. Our proposed methodology was rigorously tested on a Ganache-based Ethereum blockchain network and analyzed using the Remix platform, with a specific focus on assessing the gas consumption associated with various operations. This approach not only provides insights into the economic implications of deploying smart contracts but also underscores the importance of optimizing such contracts for minimal gas expenditure, thereby enhancing the overall viability and user adoption of DApps in the Ethereum ecosystem.

Fig. 5 provides a detailed examination of gas consumption patterns across a comprehensive business process, utilizing two pivotal Ethereum blockchain platforms: Remix and Ganache. This analysis reveals a direct correlation between the scale of the blockchain architecture and the gas expenditure associated with the application in question. Specifically, as the blockchain accrues more blocks, signifying an expansion in its ledger, the gas costs incurred by the application escalate in tandem with the growth in user participation. This dynamic indicates that with an increase in the number of users engaging with the blockchain, there is a corresponding rise in the demand for computational resources, thereby elevating the gas fees on both platforms. However, it is noteworthy that despite these variations, the overall cost of gas tends to stabilize and maintain a relatively constant threshold over time. This observation underscores the inherent scalability challenges and economic considerations in the Ethereum ecosystem, highlighting the need for efficient management of gas costs to sustain the economic viability of decentralized applications (DApps) as they scale.

Fig. 6 elucidates the gas consumption dynamics as the number of users engaging with the smart contract increases, specifically during processes of business initialization and data viewing. This figure clearly illustrates that the gas required for initializing transactions on both Remix and Ganache platforms escalates as more users participate in the network. However, a notable distinction is observed in the behavior of querying operations within the Ganache testing environment, where such activities do not incur any gas consumption.

This discrepancy highlights a crucial aspect of block-chain platform functionalities and their implications on the efficiency and cost-effectiveness of executing smart contracts. While the initiation of business processes demands a proportional increase in gas fees with user participation, reflecting the computational effort required, the absence of gas costs for queries in Ganache points to an optimization in data retrieval operations that could significantly reduce the operational expenses associated with DApps. This observation suggests potential pathways for optimizing smart contract design and execution to balance between operational efficiency and economic sustainability in decentralized applications.

Given that the sharing of personal information within decentralized applications is not time-sensitive, it is feasible to set the gas price at a minimal threshold of 1 GWEI. This strategic adjustment significantly lowers the operational costs associated with the development and execution of the application, thereby enhancing its economic viability. By adopting this approach, developers can optimize resource utilization and minimize transaction fees without compromising the functionality or security of the application. This tactic not only makes the deployment of decentralized applications more affordable but also encourages broader adoption by reducing the financial barriers for users and developers alike. Furthermore, this cost-effective strategy underscores the potential for blockchain technology to be implemented in a wide range of applications where the immediacy of transaction confirmation is less critical, thereby providing a direction worth considering for innovation and accessibility in the digital ecosystem.

4.2. Execution time to share personal information

Network latency represents a critical performance indicator for blockchain-based infrastructures. To evaluate this aspect, we conducted simulation tests within a Ethereum environment, focusing on the data-sharing process across several stages. These stages encompass: (1) patient applies for business processing from MI-RMR, (2) MI-RMR applies for relevant information from patient, (3) patient asks for relevant information from MI-MR, (4) MI-MR submits IPFS index to patient, and (5) patient uploads the information to IPFS and provides the temporary index to MI-RMR.

The goal of our experimental framework was to assess the transaction timeline, from initiation to completion, across various pending transactions which ranged from 0 to 200. These transactions incorporated user group sizes of various scales, with scenarios that included

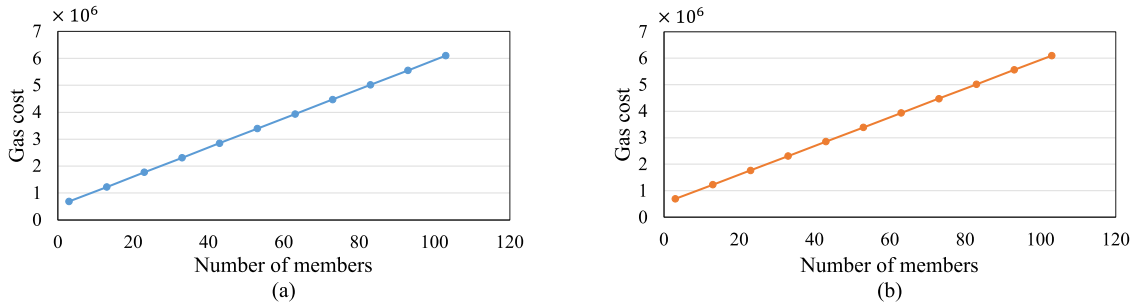

Fig. 5. Platform wise gas cost for business.

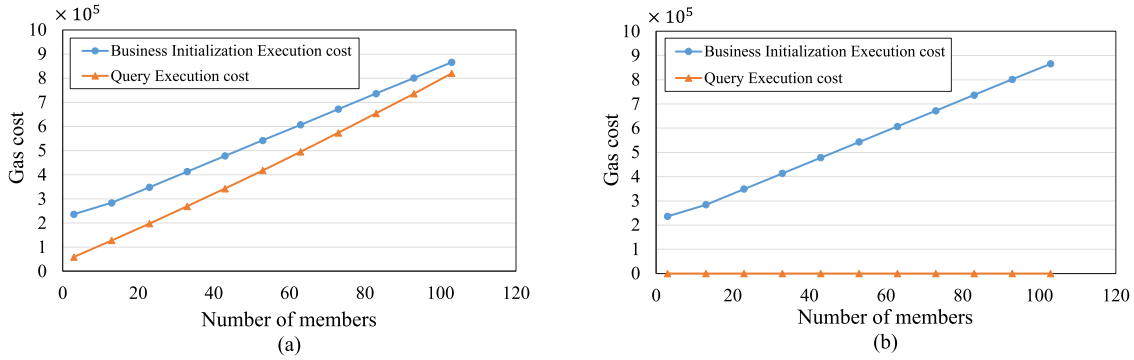

Fig. 6. Platform wise gas cost for business initial & query.

groups of 3, 5, 10, 15, and 20 users. In this section of the experiments, we transmitted the same medical records as those in the comparative trial, with sizes ranging from 400 to 1000 bytes. As depicted in Fig. 7, the results provide a comprehensive view of the network's efficiency and capabilities under different load conditions. This analysis sheds light on system scalability and responsiveness, as well as how blockchain operations can be optimized for improved performance and reliability. The comprehensive scalability analysis conducted in our study, which included stress tests with a spectrum of user group sizes, transaction sizes, and data volumes, provides deeper insights into the dynamics and possible bottlenecks of blockchain-based systems, which could foster more robust and efficient decentralized application designs. This research is imperative for real-world healthcare data sharing scenarios. Empirical evidence equips us with a valuable perspective on potential issues that a blockchain infrastructure might encounter when handling real-world data. All of these are clearly demonstrated in Fig. 7, presenting an unabridged view of the network's responses under varying load conditions.

In the realm of blockchain research, the proposed work is compared with related works such as BinDaaS [45], data allocation frameworks within blockchain contexts [46], distributed hospital networks [47], and IoT-driven healthcare systems [48]. This comparative scrutiny hinges on evaluating the performance metrics and operational efficiencies of our approach vis-à-vis the established frameworks in the field.

Illustrated in Fig. 8 is an analytical breakdown focusing primarily on the latency metrics of the entire data-sharing protocol within our proposed system, benchmarked against the latency figures reported in the aforementioned studies. Here, latency is meticulously defined as the temporal gap between the initiation of a transaction by a user and the ultimate inclusion of said transaction as a new block within the blockchain ledger. A notable point of differentiation arises with BinDaaS, which incurs additional latency due to its predictive modeling processes for medical documents.

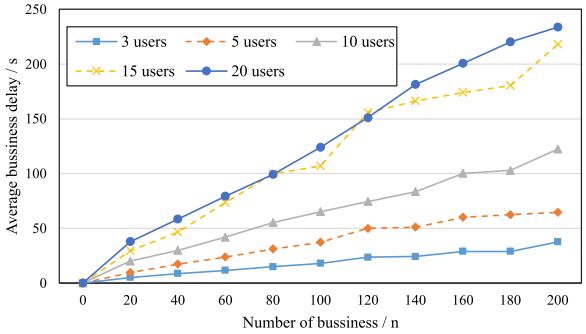

Fig. 7. Latency of the proposed work.

This comparative analysis is not merely an exercise in benchmarking but serves as a critical lens through which the nuanced efficiencies and potential bottlenecks of our proposed system can be discerned against the backdrop of existing blockchain implementations. It is through such rigorous evaluations that we can ascertain the relative merits and demerits of our approach, thereby contributing to the broader discourse on blockchain's applicability and scalability, particularly in the context of healthcare and data sharing paradigms.

In juxtaposition, distributed hospital network architectures necessitate augmented latency relative to BinDaaS and blockchain-based data allocation frameworks, attributed primarily to the incorporation of intricate authentication mechanisms. Consequently, such existing methodologies entail a heightened latency period for document processing. In comparison, IoT-based healthcare models exhibit a diminished latency interval for data handling, owing to their streamlined operational protocols.

In addition to latency considerations, it is vital to delve deeper into the cost implications of different healthcare data management systems

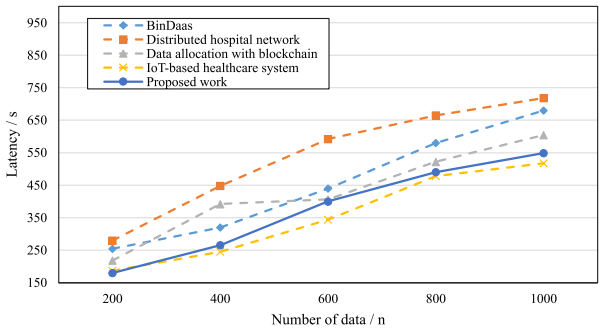

Fig. 8. Latency comparison among the proposed work and other works.

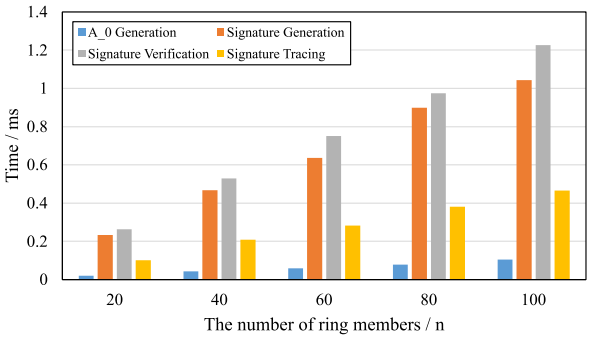

Fig. 9. Time consumption for each step.

to provide a comprehensive analysis. Distributed hospital network architectures introduce notable cost factors in terms of implementation and maintenance. The intricate authentication mechanisms integrated into these systems require significant investment in both technology and human resources, resulting in higher operational expenses compared to other solutions.

On the contrary, IoT-based healthcare models offer a more cost-effective approach to data management. The streamlined operational protocols of IoT systems streamline processes, reducing the need for complex and costly infrastructure. This ultimately translates to lower initial setup costs and ongoing maintenance expenses, making IoT a more financially viable option for healthcare organizations looking to modernize their data management practices without incurring substantial costs.

In our work, while similarly embracing distributed storage solutions to alleviate the demands on on-chain storage and communication overheads, places a heightened emphasis on the prerogatives of information proprietors and adherence to data sharing regulations. This approach, inherently, renders the process more laborious and protracted than that observed in IoT-based healthcare frameworks. This deliberate complexity, although potentially contributing to increased latency, is instrumental in fortifying the security and compliance aspects of data sharing within blockchain networks.

By meticulously balancing the trade-offs between efficiency and compliance, our work endeavors to chart a course towards a more nuanced and secure framework for blockchain-based data sharing. This not only seeks to tackle the immediate challenges of data latency and system scalability but also aims to contribute to the integration of rigorous data governance mechanisms into the blockchain domain, with the hope of offering useful insights for future research and development in the field.

4.3. Execution of ring signature

To substantiate the reliability and authenticity of the on-chain data upheld by our proposed framework, an evaluation of the adopted ring signature mechanism was undertaken. This analysis was carried out within the Pycharm integrated development environment, leveraging Python version 3.6. Within this context, the notation T_E is employed to denote the time consumed by exponential operations within the groups G_T or G, T_P signifies the time taken by bilinear pairing operations, T_M represents the duration of multiplication operations, and T_H corresponds to the time required for hash-to-group operations. Table 4 elucidates the semantic and temporal attributes of the symbols integral to our framework.

The efficiency of various phases within our scheme is delineated as follows: the signature generation phase necessitates $(n+6)T_E + 3T_H + (n)T_M$, the signature verification phase demands $5nT_E + 3T_H + 2T_M$, and the signature tracking phase requires $nT_E + 2T_H + nT_M$.

Drawing upon the operational timings delineated in Table 4 and the intricate steps of our framework, we conducted simulations to

Table 4
Running time consumption.

Symbol	Description	Time/10^{-5}_s
T_E	Exponential calculation time	8.52
T_M	Multiplication time	0.27
T_P	Bilinear pair operation time	33.18
T_H	Hash to group operation time	11.44

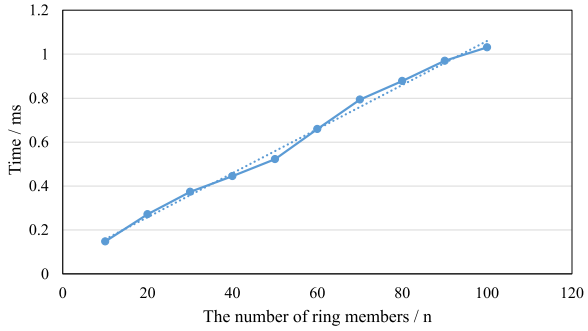

Fig. 10. Signature tracing.

gauge the temporal expenditure across four distinct phases within a scheme, accommodating a varying ring member count n spanning from 20 to 100. These simulations are graphically represented in Figs. 9 and 10, offering a comprehensive visualization of the temporal dynamics associated with each phase of the scheme. This meticulous analysis not only underscores the operational efficiency of our proposed scheme but also lays the groundwork for future enhancements and optimizations in the realm of blockchain-based data integrity and authentication protocols.

Table 5 presents a comparative analysis of the temporal efficiency across four distinct ring signature frameworks during the critical processes of signature generation, verification, and tracking. Notably, the algorithm we use distinguishes itself by eschewing the utilization of bilinear mappings. This strategic omission simplifies the algorithmic complexity and, consequently, reduces the computational demand during the signature generation phase relative to competing frameworks. Similarly, the computational load during the tracking phase is also minimized in comparison to alternatives as documented in prior studies [49–51]. It is pertinent to note that the scheme presented in [51] operates within the standard model and lacks a tracking functionality, thereby exempting it from consideration in this context. This streamlined computational framework we adopt not only enhances the operational efficiency of our scheme but also underscores its approach to minimizing computational overhead without compromising on security or functionality.

In our study, we delved into the temporal dynamics involved in executing three pivotal stages of a ring signature framework, with the

Table 5
Comparison of computational costs of different algorithms.

Algorithm	Signature generation	Signature verification	Tracing
[49]	$(5n-1)T_M$	$nT_E + 2T_P$	$(2+2n)T_P + (4n-1)T_M$
[50]	$6nT_P + 4nT_E$	$nT_E + 2nT_P$	$(6+2n)T_P + 9nT_M + 3nT_E$
[51]	$4nT_M + 2nT_E$	$(n+1)T_P$	$Not\ \ applicable$
Ours	$(n+6)T_E + 3T_H + (n)T_M$	$5nT_E + 3T_H + 2T_M$	$nT_E + 2T_H + nT_M$

number of loop members (n) varying from 20 to 100. The ring signature mechanism employed within this framework is notably founded on straightforward algebraic operations for the generation of G, with its complexity contingent upon the prime number utilized for generating G (for which we persist in employing the Sophie Germain prime number). The empirical evidence gleaned from our experiments unequivocally demonstrates that the time expenditure required for loop generation and ancillary processes is significantly lesser in comparison to that necessitated by signature schemes that rely on curve-generated loops. These experimental findings are encapsulated in Fig. 9.

A discernible trend from Fig. 9 is the linear escalation in time consumption corresponding to each procedural step as the number of loop members increases. Furthermore, it becomes apparent that the temporal investment for signature tracing within this specific signature scheme does not surpass half of the time required for signature verification. This observation underscores the efficiency of the trace principle, enabling the validation of signature authenticity on blockchain data with a substantially reduced time footprint compared to conventional signature verification methodologies. Fig. 10 further illustrates that the time allocation for the algorithm's traceability component is directly proportional to the loop members' count.

Overall, the ring signature framework deployed in this context demonstrates an adept capability in affirming the integrity of facial data with a minimal time expenditure. This efficiency not only solidifies the framework's suitability for blockchain applications but also highlights its potential for facilitating enhanced data verification processes with reduced computational demands.

5. Security analysis of the implementation

5.1. Security of scheme

Our innovative medical record sharing framework leverages a blockchain ledger, establishing a paradigm of public transparency, irrefutability, and elevated trust. In a departure from traditional practices, our system obviates the need for parties to exchange plaintext or ciphertext of raw data directly. Instead, we opt for the encryption of data by the personal information owner (patient) and its subsequent storage within the InterPlanetary File System (IPFS), while the corresponding indices are signed and encrypted for transmission purposes. These indices, relayed from the patient to the business execution providers (MI-RMR), facilitate the temporary upload of information, conferring upon the patient sole decryption rights to the raw data.

The utilization of the IPFS system is a strategic move that significantly slashes data storage costs and bolsters security measures. Furthermore, the transmission of merely the IPFS index dramatically lowers the costs associated with data transfer and mitigates the risk of original data ciphertext leakage during transit. The implementation of temporary IPFS storage serves to create a commercial buffer between the information storage providers (MI-MR) and the MI-RMR, effectively severing any direct link to the raw data and thereby enhancing data privacy and security.

Grounded in blockchain technology, our scheme ensures the veracity of participant identities, reinforcing the integrity of the data exchange process. Additionally, we integrate ring signatures to authenticate identities reliably during the transmission of off-chain information. This feature not only fosters an audit trail but also enables all involved parties to validate business statuses and facilitate identity verification, thereby enriching the ecosystem with a robust structure for business record-keeping and accountability. This comprehensive approach not only secures personal information of medical record but also paves the way for a more efficient and secure digital exchange landscape.

Our proposed scheme has the security property that can resist at least the following attack means:

Conspiracy Attack: In every business process, the involvement of information subjects is mandatory, thwarting attempts by other participants to engage in collusion attacks. When the information subject does not have informed consent, the business process cannot proceed. A collusion attack here is when multiple commercial participants engage in unauthorized operations on a piece of data by bypassing a certain information subject and engaging in unauthorized operations on information belonging to that individual. Therefore, to prevent collusion attacks, information agents are only allowed to conduct business related to themselves with their knowledge and consent.

Phishing Attack: When an attacker or malicious user obtains a user's personal or sensitive information (such as user ID, login credentials, etc.), a phishing attack occurs, and the attacker uses the user's authorization data to exploit the application's services. In the proposed scheme, the blockchain network uses a blockchain structure to store the detailed information of all users in the form of hash values. When a user sends an access request to a distributed application, it checks the information using a blockchain structure and verifies the user details using the requested documents. Therefore, an attacker or a malicious user cannot obtain the details of the user, as all the details are stored in the blockchain structure using a hash algorithm.

Masquerade Attack: Masquerade attack allows unauthorized users to access the system using false credentials or information. This solution requires registering a blockchain platform account first to prevent disguised attacks. In the proposed plan, all users need to register an account and log in successfully before they can participate in the business. Therefore, unauthorized or malicious users cannot use fake identities to access recommended application services.

51% Attack: 51% attack is also known as majority attack. This situation occurs when an individual or group controls over 50% of the blockchain network's mining computing power. Therefore, attackers may stop transactions or payments between certain users in the blockchain network. In the proposed scheme, the blockchain adopts the PoW algorithm, which requires more energy to mine blocks in the blockchain network. Therefore, attackers require a significant amount of power and hardware resources to control over 50% of the nodes in the proposed blockchain network, which is almost impossible to achieve.

5.2. Security of signature

The traceable ring signature scheme cited in this article has been proven to have the following security requirements:

Public traceability: For the same token L, anyone who creates two signatures for different messages can be tracked, where tracking can only be achieved through paired message/signature pairs and tokens.

Mark Linkability: Every two signatures generated by the same signer for the same mark are linked.

Anonymity: As long as the signer does not have the same tag and signs on two different messages, the signer's identity cannot be distinguished from any possible ring members.

Exculpability: Honest ring members cannot be accused of signing the same label twice, as opponents cannot generate traceable ring signatures to specify the target member together with the ring signature generated by the target in the presence of a publicly traceable mechanism. The attacker cannot destroy all ring members except the target.

In our scheme, it is very difficult to forge an untraceable signature. Before proving this conclusion, we have demonstrated the following useful lemmas. We consider adversary A against our signature scheme above. A is given 1^k and allowed to access the random oracles, H' and H'', at most $q_{H'}$ and $q_{H''}$ times, respectively. Here it is not necessary that A is polynomial-time bounded. Then, we have the following lemmas.

Lemma 5.1. *Suppose that A outputs valid pair* (L, m, σ).

1. The probability that $\sharp\left\{i \in N \mid \log_h(\sigma_i) = \log_g(y_i)\right\} < 1$ *is at most* $\frac{q_{H''}}{q}$, *whereas*

2. The probability that $\sharp\left\{i \in N \mid \log_h(\sigma_i) = \log_g(y_i)\right\} > 1$ *is at most* $\frac{q_{H'}}{q}$,

where the probability is taken over the choice of H', H'' and the inner coin tosses of A.

Proof. Case 1 ($\sharp\left\{i \in N \mid \log_h(\sigma_i) = \log_g(y_i)\right\} < 1$): $\mathbf{Ver}(L, m, \sigma) = 1$ implies that $a_i = g^{z_i} y_i^{c_i} \in G$ and $b_i = h^{z_i}\sigma_i^{c_i} \in G$ for $i \in N$, which means that $\log_g(a_i) = z_i + c_i \cdot \log_g(y_i)$ and $\log_h(b_i) = z_i + c_i \cdot \log_h(\sigma_i)$ for $i \in N$. Note that if $\log_g(y_i) \neq \log_h(\sigma_i)$, c_i is determined. Hence, Case 1 implies that all c_i's, where $i \in N$, are uniquely determined. Since H'' is a random oracle, for any given $(L, m, A_0, A_1, a_N, b_N)$, the probability that $H''(L, m, A_0, A_1, a_N, b_N) = \sum_{i \in N} c_i (mod\, q)$, is at most q^{-1}. Therefore, for any A with at most $q_{H''}$ queries to random oracle H'', the probability of Case 1 is at most $\frac{q_{H''}}{q}$.

Case 2 ($\sharp\left\{i \in N \mid \log_h(\sigma_i) = \log_g(y_i)\right\} > 1$): Since $\sigma_i = A_0 A_1^i \in G$ for $i \in N$, every point $(i, \log_h(\sigma_i))$, $i \in N$, is on line $y = \log_h(A_1)\, x + \log_h(A_0)$. Case 2 implies that at least two points, $(i, \log_g(y_i))$'s, are on the line, which means, when pk_N are fixed, the line is determined, so $\log_h(A_0)$ and $\log_h(A_1)$ are determined. However, we also need $\log_h(A_0) = \log_h\left(H'(L(issue, pk_N), m)\right)$, where $H'(L, m)$ is determined independently of the above line, because H' is a random oracle. Actually, the probability that $\log_h\left(H'(L, m)\right) = \log_h(A_0)$ is at most q^{-1} for given (L, m). Hence, for any adversary A with at most q'_H number of queries to random oracle H', the probability of Case 2 is at most $\frac{q_{H'}}{q}$.

Lemma 5.2. *Suppose that A defined above and it outputs* $(L, m^{(1)}, \sigma^{(1)})$ *and* $(L, m^{(2)}, \sigma^{(2)})$, *such that* $\mathbf{Trace}(L, m^{(1)}, \sigma^{(1)}, m^{(2)}, \sigma^{(2)}) = \varepsilon indep\varepsilon$. *Let* ***TList*** *be the list defined above in our tracing protocol. Then, the probability that* $1 < \sharp\mathbf{TList}$ *is* $\frac{q_{H'}^2}{2q}$, *where the probability is taken over the choices of* H' *and the inner coin tosses of A.*

Proof. By $1 < \sharp\mathbf{TList}$, the line defined by $\sigma^{(1)}$ intersects with the line defined by $\sigma^{(2)}$ at least at two points, which means that the two lines coincide. Hence, $A_0^{(1)} = H'(L, m^{(1)})$ and $A_0^{(2)} = H'(L, m^{(2)})$, because $\log_h\left(A_0^{(1)}\right) = \log_h\left(A_0^{(2)}\right)$ where $h = H(L)$. Therefore, the advantage of A is bounded by the probability that A can find a collision of outputs of H', which is $\frac{q_{H'}^2}{2q}$.

Theorem 5.3 (*Tag-Linkability*). *This scheme is tag-linkable in the random oracle model.*

Proof. Suppose for contradiction that there is adversary F that takes 1^k and successfully outputs tag $L = (issue, pk_N)$ and $\left\{(m^{(1)}, \sigma^{(1)}), \ldots, (m^{(n+1)}, \sigma^{(n+1)})\right\}$.

Based on Lemma 5.2, $\mathbf{Trace}(L, m^{(i)}, \sigma^{(i)}), (m^{(j)}, \sigma^{(j)}) =$ "indep", for all i, j, means that, (with over whelming i.e., 1-($\frac{q_{H'}^2}{2q}$) probability), $\sigma_k^{(i)} \neq \sigma_k^{(j)}$ holds, for all i, j, k, where $1 \leq i, j \leq n+1, i \neq j$, and $1 \leq k \leq n$. On the contrary, by Case 1 of Lemma 5.2, for every i, where $1 \leq k \leq n+1$, there exist $k \in N$ such that $\log_g(y_k) = \log_h\left(\sigma_k^{(i)}\right)$ (with at least $1 - \frac{(n+1)q_{H''}}{q}$ probability). Since $1 \leq k \leq n$, there exist i, j, k such that $\sigma_k^{(i)} = \sigma_k^{(j)}$, which contradicts the assumption (if the advantage of F exceeds $\max(\frac{q_{H'}^2}{2q}, \frac{(n+1)q_{H''}}{q})$).

Therefore, the probability that F can forge the Proposed scheme above is at most $\max(\frac{q_{H'}^2}{2q}, \frac{(n+1)q_{H''}}{q})$, where $q_{H'}$ and $q_{H''}$ denotes the number of queries of F to random oracles, H' and H'', respectively.

6. Discussions

The advent of post-quantum cryptography necessitates a reevaluation of current security applications, especially within the realm of Electronic Medical Records (EMR) sharing. The implementation of post-quantum cryptography techniques, such as those based on isogenies on elliptic curves implemented in FPGA [52], alongside key exchange protocols [53], underscores the importance of developing future-proof security mechanisms in healthcare systems. This is further supported by advancements in NTT-based polynomial multiplication accelerators [54] and cryptographic accelerators for digital signatures [55], which play a pivotal role in safeguarding EMR sharing processes against emergent cryptographic threats.

With the increasingly important role of Electronic Medical Records (EMR) sharing in modern healthcare systems, the issue of security cannot be overlooked. Side-channel attacks, which exploit information leaked during the execution of cryptographic procedures, pose potential threats to the security and privacy of EMR sharing. Moreover, in scenarios involving massive data processing of medical records, lightweight cryptographic protocols have significant advantages. While ensuring robust security, they can reduce computational overhead and energy consumption. The Advanced Encryption Standard (AES), as a widely adopted encryption approach, has in some cases been proven susceptible to side-channel attack threats [56]. We recognize these potential security issues as pressing topics that require in-depth study and resolution in this field. Therefore, though our research has made certain achievements in technology used for EMR sharing, we continue to explore additional potential security challenges and technical solutions. These include measures to prevent side-channel attacks and the application of cryptographic methods such as lightweight cryptography and AES, which will be the focus of our future work.

There is not a strict standard to classify encryption algorithms as lightweight. Lightweight encryption algorithms primarily refer to those that can still provide effective security protection in resource-limited environments (such as embedded systems, low-power devices, Internet of Things devices, etc.). They usually need to run under limited computational capabilities, storage space, and energy consumption restrictions, therefore they require as little resource consumption as possible while ensuring security. The term 'lightweight' does not indicate that the security of the encryption algorithm is weak, but rather that there is a higher demand for algorithm efficiency and resource consumption. Lightweight and ultra-lightweight ciphers typically provide security ranging from 80 to 128 bits [57]. It is generally deemed that 80-bit security suffices for constrained devices, such as 4-bit microcontrollers and RFID tags [58], whereas 128-bit security is commonly utilized for mainstream applications [59].

In addition, considering the lightweight cryptographic protocols' suitability for massive data processing of medical records due to their efficiency in resource-constrained environments, our future efforts will focus on integrating such protocols that offer a balance between robust security and minimal resource consumption [56–59]. The emphasis on lightweight cryptography is prompted by the dual necessity of ensuring the security of EMR sharing while addressing the vulnerabilities associated with widely adopted encryption methods, such as AES, to side-channel attacks.

Furthermore, the ring signature scheme utilized in our current design exemplifies the feasibility of achieving light-weight yet secure encryption; however, its potential for further optimization suggests a dual-path strategy for future research: enhancing algorithm efficiency through optimization while exploring high-efficiency algorithms to maintain or improve lightweight characteristics without compromising security.

The exploration of blockchain technology as a backbone for secure EMR sharing introduces a novel paradigm for data access control. Inspired by Maesa et al.'s work [60], transforming access control policies into smart contracts offers a distributed and secure mechanism that enhances patient privacy and data integrity. This blockchain-centric approach, while promising, presents challenges, including attribute privacy and smart contract limitations, which necessitate further research to refine and implement such strategies effectively.

The consent-aware EMR sharing method proposed, leveraging blockchain technology, not only aligns with the current focus on security and privacy but also underscores the importance of patient consent and transparency in medical data sharing. This approach, demonstrated through our prototype implementation, offers a scalable and decentralized system that incorporates on-chain verification mechanisms to combat malicious alterations. By incorporating advanced encryption techniques, such as homomorphic encryption, in our future work, we aim to further fortify patient privacy against the looming threat of post-quantum cryptography.

In conclusion, our discussion navigates through the complexities of securing EMR sharing in a future-facing healthcare ecosystem. By acknowledging the emerging cryptographic challenges and integrating lightweight, blockchain-based, and consent-aware strategies, our research endeavors to contribute to the resilient and ethical sharing of medical data, thus safeguarding patient privacy and security in the era of post-quantum cryptography.

7. Conclusion

In this paper, we elaborate on a consent-aware approach for the secure and compliant sharing of personal health information via electronic means, leveraging blockchain technology and traceable ring signatures. Initially, we present a model for sharing personal health information, steered by its proprietor, that isolates risks and delineates clear rights and responsibilities. This model thoroughly embodies the individual's "informed consent" regarding the handling of pertinent health data. Utilizing blockchain technology and amalgamating both on-chain and off-chain business processing techniques enable the effective validation of user identity authenticity, along with the authenticity and integrity of the information. This dual approach enhances the transparency and oversight of personal health information sharing. Furthermore, the incorporation of the ring signature algorithm serves as a robust defense against malicious alterations and forgeries of block information on the blockchain. Given the extensive volume of personal health information, reliance on a distributed storage system significantly alleviates the strain on blockchain data processing and storage. It also circumvents the need for multiple transmissions of original data, substantially mitigating the risk of surveillance and interception of personal health data. The ring signature algorithm employed herein has been deemed provably secure through verification, and a subsequent security analysis confirms that our proposed scheme exhibits pronounced security and anonymity characteristics.

To fully flesh out the value of our existing model and enhance the efficacy of medical data sharing further, we will focus on addressing several key facets of improving medical data sharing. Our research priorities will include developing a mechanism for selective data disclosure that allows patients to share data as necessary, exploring designs for fine-grained access control that provide in-depth protection for medical information, and implementing privacy-preserving identity verification methods to enhance data security while ensuring user anonymity.

Compliance with ethical standards

This article does not contain any studies with human participants or animals performed by any of the authors.

CRediT authorship contribution statement

Xiao Qu: Writing – review & editing, Writing – original draft, Software, Investigation, Conceptualization. **Zhexuan Yang:** Validation, Project administration, Investigation, Conceptualization. **Zeng Chen:** Supervision, Investigation, Formal analysis, Conceptualization. **Guozi Sun:** Writing – review & editing, Supervision, Resources, Methodology, Funding acquisition.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Guozi Sun reports financial support was provided by National Natural Science Foundation of China. Guozi Sun reports financial support was provided by Fellowship of China Postdoctoral Science Foundation. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

The authors would like to thank the anonymous reviewers for their elaborate reviews and feedback. We acknowledge the support received from the National Natural Science Foundation of China (No. 62372245 & 62372250 & 62102192), and the Fellowship of China Postdoctoral Science Foundation (2022M710071).

Appendix. Appendix of traceable ring signature algorithm

Signature tracking:

Let G be a multiplicative group of prime order q, and let g be a generator of G. Let $H : \{0,1\}^* \to G$, $H' : \{0,1\}^* \to G$, and $H'' : \{0,1\}^* \to \mathbb{Z}_q$ be distinct hash functions. The above are public parameters.

Key generation:

Participant P_i extracts element x_i from $\mathbb{Z}_q$ and calculates $y_i = g^{x_i}$. The public key of P_i is $pk_i = \{g, y_i, G\}$, and the corresponding secret key is $sk_i = \{pk_i, x_i\}$. We denote the ordered list of n participants as $N = \{1, \ldots, n\}$. Let $pk_N = (pk_1, \ldots, pk_n)$ be the ordered list of public keys for the set N.

Signature generation:

Sign the message $m \in \{0,1\}^*$ with respect to the label $L = (\text{issue}, pk_N)$ using the key sk_i according to the following algorithm:

(1) Calculate $h = H(L)$ and $\sigma_i = h^{x_i}$ using $x_i \in \mathbb{Z}_q$.

(2) Let $A_0 = H'(L, m)$, and $A_1 = \left(\frac{\sigma_i}{A_0}\right)^{\frac{1}{i}}$.

(3) Compute $\sigma_j = A_0 A_1^j \in G$, where $j \neq i$. Note, each $(j, \log_h(\sigma_j))$ lies on the line defined by $(0, \log_h(A_0))$ and (i, x_i), where $x_i = \log_h(\sigma_i)$.

(4) A non-interactive zero-knowledge proof based on knowledge of relations derived from language, generating a signature (c_N, z_N) on L, m, where $L \triangleq \{(L, h, \sigma_i) | \exists i' \in \mathbb{N}$ such that $\log_g(y_{i'}) = \log_h(\sigma_{i'})\}$.
Here, $\sigma_N = (\sigma_1, \ldots, \sigma_n)$, and:

(a) Select random w_i from Z_q and set $a_i = g^{w_i}$, $b_i = h^{w_i} \in G$.
(b) Select random z_j, c_j from Z_q and for $j \neq i$, set $a_j = g^{z_j} y_i^{c_j}$, $b_j = h^{z_j} \in G$.
(c) Let $c = H''(L, A_0, A_1, a_N, b_N)$, where $a_N = (a_1, \ldots, a_n)$ and $b_N = (b_1, \ldots, b_n)$.
(d) Let $c_i = c - \sum_{j \neq i} c_j mod q$, $z_i = w_i - c_i x_i mod q$. Return (c_N, z_N) as the proof for L, where $c_N = (c_1, \ldots, c_n)$ and $z_N = (z_1, \ldots, z_n)$.
$L = \left(issue, pk_N\right)$

(5) Output $\sigma = (A_1, c_N, z_N)$ as the signature for (L, m).

Signature verification:

Verify the signature $\sigma = (A_1, c_N, z_N)$ on the message m regarding L using the following algorithm:

(1) Parse L as (issue, pk_N). For all $i \in N$, check $g, A_1 \in G$, $c_i, z_i \in \mathbb{Z}_q$, and $y_i \in G$. Let $h = H(L)$, $A_0 = H'(L, m)$, and for all $i \in N$, compute $\sigma_i = A_0, A_1^i \in G$.
(2) Compute for all $i \in N$ the $a_i = g^{z_i} y_i^{c_i}$ and $b_i = h^{z_i} \sigma_i^{c_i}$.
(3) Check if $H''(L, m, A_0, A_1, a_N, b_N) \equiv \sum_{i \in N} c_i \mod q$, where $a_N = (a_1, \ldots, a_n)$ and $b_N = (b_1, \ldots, b_n)$.
(4) If all of the above checks are successfully completed, then accept, otherwise reject.

Signature tracking:

Verify the relationship between (m, σ) and (m', σ') for the same pk_N, where $\sigma = (A_1, c_N, z_N)$ and $\sigma' = (A_1', c_N', z_N')$, according to the following algorithm.

(1) Parse L as (issue, pk_N). Let $h = H(L)$, $A_0 = H'(L, m)$, and compute $\sigma_i = A_0 A_1^i \in G$ for all $i \in N$. Do the same thing for σ', and retrieve σ_i' for all $i \in N$.
(2) For all $i \in N$, if $\sigma_i = \sigma_i'$, store pk_i in TList, where TList is initially an empty list.
(3) If pk is the only entry in TList, then output pk; if TList equals pk_N, then output 'linked'; otherwise, output 'indep' (i.e., TList equals $\emptyset$ or the number of entries in TList is between 1 and n).

References

[1] K. Gai, Y. She, L. Zhu, K.-K.R. Choo, Z. Wan, A blockchain-based access control scheme for zero trust cross-organizational data sharing, ACM Trans. Internet Technol. 23 (3) (2023) 1–25.
[2] L. Campanile, M. Iacono, F. Marulli, M. Mastroianni, Designing a GDPR compliant blockchain-based IoV distributed information tracking system, Inf. Process. Manage. 58 (3) (2021) 102511.
[3] Y. Liu, D. He, M.S. Obaidat, N. Kumar, M.K. Khan, K.-K.R. Choo, Blockchain-based identity management systems: A review, J. Netw. Comput. Appl. 166 (2020) 102731.
[4] J. Li, J. Wu, G. Jiang, T. Srikanthan, Blockchain-based public auditing for big data in cloud storage, Inf. Process. Manage. 57 (6) (2020) 102382.
[5] S. Rai, B.K. Chaurasia, R. Gupta, S. Verma, Blockchain-based NFT for healthcare system, in: 2023 IEEE 12th International Conference on Communication Systems and Network Technologies, CSNT, IEEE, 2023, pp. 700–704.
[6] M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, N.K. Jha, Systematic poisoning attacks on and defenses for machine learning in healthcare, IEEE J. Biomed. Health Inform. 19 (6) (2014) 1893–1905.
[7] A.M. Nia, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, N.K. Jha, Energy-efficient long-term continuous personal health monitoring, IEEE Trans. Multi-Scale Comput. Syst. 1 (2) (2015) 85–98.
[8] M.M. Kermani, M. Zhang, A. Raghunathan, N.K. Jha, Emerging frontiers in embedded security, in: 2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems, IEEE, 2013, pp. 203–208.
[9] Ö.F. Görçün, D. Pamucar, S. Biswas, The blockchain technology selection in the logistics industry using a novel MCDM framework based on Fermatean fuzzy sets and Dombi aggregation, Inform. Sci. 635 (2023) 345–374.
[10] H. Guo, X. Yu, A survey on blockchain technology and its security, Blockchain Res Appl. 3 (2) (2022) 100067.
[11] J. Kolb, M. AbdelBaky, R.H. Katz, D.E. Culler, Core concepts, challenges, and future directions in blockchain: A centralized tutorial, ACM Comput. Surv. 53 (1) (2020) 1–39.
[12] B. Wen, Y. Wang, Y. Ding, H. Zheng, B. Qin, C. Yang, Security and privacy protection technologies in securing blockchain applications, Inform. Sci. (2023) 119322.
[13] E.D. Frauenstein, S. Flowerday, S. Mishi, M. Warkentin, Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model, Inform. Manag. 60 (7) (2023) 103858.
[14] B.K. Chaurasia, Blockchain enabled MediVault for healthcare system, Multimedia Tools Appl. (2024) 1–21.
[15] P. Sharma, S. Namasudra, R.G. Crespo, J. Parra-Fuente, M.C. Trivedi, EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain, Inform. Sci. 629 (2023) 703–718.
[16] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, J. Tazelaar, A distributed ledger for supply chain physical distribution visibility, Information 8 (4) (2017) 137.
[17] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. 21 (1) (2018) 858–880.
[18] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, An overview on smart contracts: Challenges, advances and platforms, Future Gener. Comput. Syst. 105 (2020) 475–491.
[19] S. Sicari, A. Rizzardi, A. Coen-Porisini, Security&privacy issues and challenges in NoSQL databases, Comput. Netw. 206 (2022) 108828.
[20] K.-K.R. Choo, Z. Yan, W. Meng, Blockchain in industrial IoT applications: Security and privacy advances, challenges, and opportunities, IEEE Trans. Ind. Inform. 16 (6) (2020) 4119–4121.
[21] L. Thomas, I. Gondal, T. Oseni, S.S. Firmin, A framework for data privacy and security accountability in data breach communications, Comput. Secur. 116 (2022) 102657.
[22] D.S. Guamán, D. Rodriguez, J.M. del Alamo, J. Such, Automated GDPR compliance assessment for cross-border personal data transfers in android applications, Comput. Secur. 130 (2023) 103262.
[23] A. Xiang, W. Pei, C. Yue, PolicyChecker: Analyzing the GDPR completeness of mobile apps' privacy policies, in: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2023, pp. 3373–3387.
[24] A. Aljeraisy, M. Barati, O. Rana, C. Perera, Privacy laws and privacy by design schemes for the internet of things: A developer's perspective, ACM Comput. Surv. 54 (5) (2021) 1–38.
[25] D. Mascalzoni, R. Melotti, C. Pattaro, P.P. Pramstaller, M. Gögele, A. De Grandi, R. Biasiotto, Ten years of dynamic consent in the CHRIS study: informed consent as a dynamic process, Eur. J. Human Genet. 30 (12) (2022) 1391–1397.
[26] S. Daoudagh, E. Marchetti, V. Savarino, R. Di Bernardo, M. Alessi, How to improve the GDPR compliance through consent management and access control, in: ICISSP, 2021, pp. 534–541.
[27] A. Hasselgren, K. Kralevska, D. Gligoroski, S.A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences—A scoping review, Int. J. Med. Inform. 134 (2020) 104040.
[28] L. Feng, L. Zhang, J. Wang, J. Feng, How to promote the participation of enterprises using open government data? Evolutionary game analysis by applying dynamic measures, Expert Syst. Appl. 238 (2024) 122348.
[29] J. Xue, S. Luo, Q. Deng, L. Shi, X. Zhang, H. Wang, KA: Keyword-based auditing with frequency hiding and retrieval reliability for smart government, J. Syst. Archit. 138 (2023) 102856.
[30] D. Geneiatakis, Y. Soupionis, G. Steri, I. Kounelis, R. Neisse, I. Nai-Fovino, Blockchain performance analysis for supporting cross-border E-government services, IEEE Trans. Eng. Manage. 67 (4) (2020) 1310–1322.
[31] Y. Hao, C. Piao, Y. Zhao, X. Jiang, Privacy preserving government data sharing based on hyperledger blockchain, in: Advances in E-Business Engineering for Ubiquitous Computing: Proceedings of the 16th International Conference on E-Business Engineering, ICEBE 2019, Springer, 2020, pp. 373–388.
[32] M. Kassen, Blockchain and e-government innovation: Automation of public information processes, Inf. Syst. 103 (2022) 101862.
[33] C. Piao, Y. Hao, J. Yan, X. Jiang, Privacy preserving in blockchain-based government data sharing: A service-on-chain (SOC) approach, Inf. Process. Manage. 58 (5) (2021) 102651.
[34] O. Oksuz, A system for storing anonymous patient healthcare data using blockchain and its applications, Comput. J. 67 (1) (2024) 18–30.
[35] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P.S. Zambani, A. Swaminathan, M.M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, et al., ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care, J. Med. Internet Res. 22 (8) (2020) e13598.
[36] P. Li, S.D. Nelson, B.A. Malin, Y. Chen, DMMS: A decentralized blockchain ledger for the management of medication histories, Blockchain Healthc. Today 2 (2019).
[37] M. He, X. Han, F. Jiang, R. Zhang, X. Liu, X. Liu, BlockMeds: A blockchain-based online prescription system with privacy protection, in: Service-Oriented Computing–ICSOC 2019 Workshops: WESOACS, ASOCA, ISYCC, TBCE, and STRAPS, Toulouse, France, October 28–31, 2019, Revised Selected Papers 17, Springer, 2020, pp. 299–303.

[38] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, X. Jia, MedShare: A privacy-preserving medical data sharing system by using blockchain, IEEE Trans. Serv. Comput. (2021).
[39] P. Hao, T. Pan, R. Han, X. Qu, Z. Yang, G. Sun, A privacy-preserving data sharing scheme based on blockchain for vehicular edge networks, in: GLOBECOM 2023-2023 IEEE Global Communications Conference, IEEE, 2023, pp. 5116–5121.
[40] J. Odoom, X. Huang, Z. Zhou, S. Danso, J. Zheng, Y. Xiang, Linked or unlinked: A systematic review of linkable ring signature schemes, J. Syst. Archit. 134 (2023) 102786.
[41] R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings, Vol. 7, Springer, 2001, pp. 552–565.
[42] S. Noether, S. Noether, A. Mackenzie, A note on chain reactions in traceability in cryptonote 2.0, in: Research Bulletin MRL-0001, Vol. 1, Monero Research Lab, 2014, pp. 1–8.
[43] E. Fujisaki, K. Suzuki, Traceable ring signature, in: International Workshop on Public Key Cryptography, Springer, 2007, pp. 181–200.
[44] Y. Li, Y. Yu, X. Wang, Three-tier storage framework based on TBchain and IPFS for protecting IoT security and privacy, ACM Trans. Internet Technol. 23 (3) (2023) 1–28.
[45] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, N. Kumar, Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications, IEEE Trans. Netw. Sci. Eng. 8 (2) (2019) 1242–1255.
[46] W. Yánez, R. Mahmud, R. Bahsoon, Y. Zhang, R. Buyya, Data allocation mechanism for Internet-of-Things systems with blockchain, IEEE Internet Things J. 7 (4) (2020) 3509–3522.
[47] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, K.-K.R. Choo, M. Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inform. 24 (8) (2020) 2146–2156.
[48] P. Sharma, S. Namasudra, N. Chilamkurti, B.-G. Kim, R. Gonzalez Crespo, Blockchain-based privacy preservation for IoT-enabled healthcare system, ACM Trans. Sensor Netw. 19 (3) (2023) 1–17.
[49] D.-W. Huang, X.-Y. Yang, H.-B. Chen, Ring signature scheme with revocable anonymity, Jisuanji Gongcheng yu Yingyong (Comput. Eng. Appl.) 46 (24) (2010).
[50] X. Cheng, R. Guo, Y. Cheng, Construction of efficient ring signature scheme with revocation of anonymity, Commun. Eng. Des. Mag. 36 (4) (2015) 857–861.
[51] Y. Zhang, H. Li, Y. Wang, Identity-based ring signature scheme under standard model, J. Commun. 29 (4) (2008) 40–44.
[52] B. Koziel, R. Azarderakhsh, M.M. Kermani, D. Jao, Post-quantum cryptography on FPGA based on isogenies on elliptic curves, IEEE Trans. Circuits Syst. I. Regul. Pap. 64 (1) (2016) 86–99.
[53] B. Koziel, A. Jalali, R. Azarderakhsh, D. Jao, M. Mozaffari-Kermani, NEON-SIDH: Efficient implementation of supersingular isogeny Diffie-Hellman key exchange protocol on ARM, in: Cryptology and Network Security: 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings 15, Springer, 2016, pp. 88–103.
[54] M. Bisheh-Niasar, R. Azarderakhsh, M. Mozaffari-Kermani, High-speed NTT-based polynomial multiplication accelerator for post-quantum cryptography, in: 2021 IEEE 28th Symposium on Computer Arithmetic, ARITH, IEEE, 2021, pp. 94–101.
[55] M. Bisheh-Niasar, R. Azarderakhsh, M. Mozaffari-Kermani, Cryptographic accelerators for digital signature based on Ed25519, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 29 (7) (2021) 1297–1305.
[56] M. Renauld, F.-X. Standaert, N. Veyrat-Charvillon, Algebraic side-channel attacks on the AES: Why time also matters in DPA, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2009, pp. 97–111.
[57] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An ultra-lightweight block cipher, in: Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9, Springer, 2007, pp. 450–466.
[58] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, T. Shirai, Piccolo: an ultra-lightweight blockcipher, in: Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13, Springer, 2011, pp. 342–357.
[59] A. Moradi, A. Poschmann, S. Ling, C. Paar, H. Wang, Pushing the limits: A very compact and a threshold implementation of AES, in: Advances in Cryptology–EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings 30, Springer, 2011, pp. 69–88.
[60] D.D. Maesa, P. Mori, L. Ricci, A blockchain based approach for the definition of auditable access control systems, Comput. Secur. 84 (2019) 93–119.