Exploring Blockchain Privacy: Threats and Optimization Solutions

Weihang Feng

School of Software Engineering, Tongji University, Shanghai, 201804, China
2251093@tongji.edu.cn

Abstract. As information technology advances rapidly, blockchain has risen as a transformative decentralized cryptographic system, celebrated for its robust security features and immutability. This paper offers a succinct overview of the various blockchain types, articulating their structures and functions. It further identifies and explores the significant privacy and security risks associated with blockchain technology from three specific angles: data structure, identity privacy, and network privacy. The discussion extends to four principal technological strategies—decentralization, cryptographic techniques, obfuscation methods, and privacy protocols—implemented to bolster privacy within blockchain systems. This analysis methodically examines the algorithms and technologies currently utilized for privacy preservation in blockchain research, with the aim of identifying current trends and anticipating future developments. By thoroughly evaluating these strategies, the paper aims to deliver an exhaustive understanding of contemporary blockchain privacy protection techniques. This investigation not only highlights the effectiveness of existing methods but also paves the way for the advancement of more sophisticated privacy protection technologies, contributing to the ongoing evolution and maturation of blockchain technology.

Keywords: Blockchain, Identity privacy, Network privacy, Encryption technology.

1 Introduction

In the digital and information age, blockchain technology has emerged as a groundbreaking decentralized ledger system, capturing global attention for its immutability, transparency, and security. However, as the deployment of blockchain technology expands rapidly, privacy leaks have increasingly become a significant barrier to its widespread adoption. The inherent public and transparent nature of public blockchains means that while the true identities of transaction participants are encrypted, all transaction information remains openly accessible on the network. This accessibility makes transaction behaviors easy to trace, presenting substantial challenges to privacy protection.

Given these concerns, privacy protection has risen to prominence in blockchain research, with numerous technologies proposed to bolster the confidentiality of blockchain systems. This paper provides an extensive review of these privacy

Y. Wang (ed.), *Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024)*, Advances in Computer Science Research 115,
https://doi.org/10.2991/978-94-6463-540-9_29

protection technologies, examining their technical principles, implementation methods, and the advantages and disadvantages associated with each. Furthermore, it analyzes the trajectory and potential future developments of blockchain privacy protection technologies. This comprehensive exploration aims to elucidate the current landscape and forecast emerging trends in the domain of blockchain privacy, offering insights into how these advancements could shape the next generation of blockchain applications.

2 Research Background

Blockchain, a distributed ledger technology, harnesses cryptography to maintain a transaction ledger, providing a decentralized, transparent, and secure framework. Recognized as a pivotal technology of the 21st century, it has been integral to the development of cryptocurrencies and has found applications across diverse sectors, profoundly transforming various aspects of life [1]. These transformations are evident in multiple fields including Blockchain and the Internet, Blockchain in Healthcare, Blockchain in Energy Management, Blockchain in Automotive Manufacturing, and Blockchain in Data Security [2, 3]. The expansive adoption of blockchain in these innovative areas underscores its development as an inevitable trend, highlighting its potential to reshape numerous industries profoundly.

2.1 Overview of Blockchain Types

Blockchain technology can be broadly categorized into the following three types.

Public Blockchain. These are open networks where anyone has the capability to read, conduct transactions, and participate in the verification process. They are completely decentralized, with Bitcoin and Ethereum being well-known examples of public blockchains.

Private Blockchain. Also referred to as permissioned blockchains, these networks impose restrictions on their participants. Only authorized nodes possess the rights to read data, initiate transactions, and engage in the verification process. Private blockchains are predominantly utilized within businesses and organizations for managing and operating internal data with Hyperledger Fabric and Corda being some of the most commonly used permissioned blockchains.

Consortium Blockchain. This form of blockchain is maintained collaboratively by multiple organizations. In such systems, a select group of nodes play roles in the consensus process. Consortium blockchains are most apt for scenarios involving business partners, such as inter-bank transactions.

Each of these blockchain architectures offers its own distinct advantages and fields of application. Public blockchains provide the highest levels of transparency and openness, private blockchains offer increased privacy and efficiency for specific organizations, while consortium blockchains sit in between, providing relatively high efficiency and control, and addressing certain privacy and trust issues.

2.2 The Architectural Model of Blockchain

From a logical and functional perspective, the architecture of a blockchain can be divided into six layers, which, from the bottom to the top layer, are as follows: the data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [4]. However, the evolution of modern blockchains has led to the weakening or omission of certain module functions. For example, consortium blockchains and public blockchains have eliminated the incentive layer function. Based on the distinctive features of modules and development trends, modern blockchain technology can be segmented into three levels [5]. The structure is illustrated in the Fig.1.

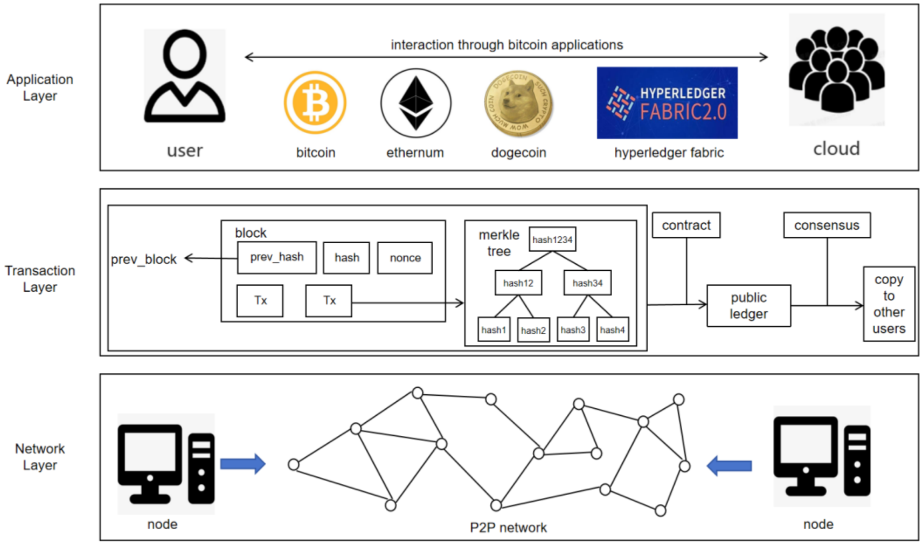

Fig. 1. Simplified blockchain structure.

Network Layer. The primary function of the network layer is to ensure effective communication between blockchain nodes via a peer-to-peer (P2P) network infrastructure. This includes the networking methods of the blockchain and the communication mechanisms between nodes. Each user serves as a node within the blockchain, with nodes interconnected directly through a distributed architecture, forming a P2P network protocol that reduces the risk of single points of failure. Whenever a node's information is updated, it is efficiently broadcasted throughout the entire network via the P2P structure, thereby maintaining synchronicity of information across the network.

Transaction Layer. The transaction layer primarily facilitates the core transactional activities of users within the blockchain, merging what were formerly the distinct data and consensus layers. This layer contains fundamental blockchain components, including block headers, verified transaction records, and sequentially arranged chains of data blocks. Cryptographic techniques are employed to ensure data integrity and immutability, while consensus mechanisms are in place to secure the consistency and safety of the blockchain system, examples of which include common protocols such as Proof-of-Work (PoW) and Proof-of-Stake (PoS).

Application Layer. The application layer caters to user interaction, providing interfaces and smart contract functionalities that enable users to effortlessly create and use decentralized applications (DApps). Cryptocurrencies represent the earliest and most widely adopted application within this layer. Users are able to transact online using encrypted virtual currencies to purchase goods and services as needed.

Another crucial role of the application layer is secure data storage. The blockchain's global ledger is immutable and highly resistant to attacks, making it particularly suitable for storing important data, such as intellectual property documents and financial transaction records. Recent applications developed include a medical information sharing system by Chen's team and financial reporting audit system created by Lu based on blockchain technology [6, 7].

3 Challenges in Ensuring Privacy Security in Blockchain

3.1 Data Structure Concerns

Compared to traditional application scenarios such as the Internet of Things (IoT), the internet, and mobile communications, the transaction data and block data dynamically generated in blockchain networks, along with the ledger data distributed across various nodes, exhibit the following characteristics:

Limited data capacity. Considering storage costs and efficiency requirements, data storage in permissioned blockchain environments can be categorized into on-chain storage and hybrid storage, which involves cooperation between on-chain and off-chain systems [8]. With on-chain storage, all data is saved within the underlying blockchain database. In contrast, for hybrid storage, full datasets are generally centralized in other nodes—often conventional servers—with metadata retained in the blockchain database. Therefore, the volume of on-chain data is not substantial. In permissionless blockchain systems like Bitcoin and Ethereum, which are dominated by cryptocurrency, the amount of ledger data is merely at the gigabyte scale, relatively small when compared to the capacities demanded by current big data technologies.

Slower growth rate. Whether permissioned or permissionless chains, the size and generation speed of transaction and block data are subject to certain constraints, resulting in a relatively slow growth rate of ledger capacity.

Relatively fixed data structure. Currently, the internet environment presents a complex array of structured, semi-structured, and unstructured data, making it challenging to form relatively unified and standardized data norms. In blockchain systems, despite some variation in underlying data structures across different application scenarios, the main functional fields remain largely consistent, contributing to a relatively unified overall structure.

Relatively centralized data storage. Transaction data is packaged into blocks, and each node involved in the blockchain maintains the same ledger. The ledgers across different nodes are completely synchronized; therefore, accessing the data from any node implies obtaining information from the entire system. The analysis of blockchain data and storage characteristics suggests that it is comparatively easy to acquire data privacy within blockchain, yet privacy protection poses a greater challenge. Furthermore, relative to privacy attacks in other systems, the most significant privacy threat within blockchain systems stems from linkage attacks. Attackers can conduct correlative analyses by collating publicly available data from other platforms (such as forums, microblogs, takeaway services, etc.) with data fetched from the blockchain, hence deducing private information. For instance, even though blockchain systems use pseudonymity to obscure the links between blockchain addresses and real-world users, correlating blockchain transaction addresses with network IP addresses and platform purchase histories can easily compromise user privacy.

3.2 Data and Privacy Concerns in Blockchain

Blockchain technology, as a form of distributed database, has garnered considerable attention regarding data protection and privacy concerns. Even though blockchain itself provides a level of anonymity and security, issues surrounding data privacy remain complex and require further resolution.

Firstly, all transaction records on public blockchains are disclosed and stored across the network, allowing visibility into the transactional activities of participants. This transparency could increase data clarity, but it also poses a risk of personal information disclosure. For example, Wang's analysis on blockchain mixing techniques for transaction amounts reveals vulnerabilities associated with anonymous multi-output scripts, which could be exploited by attackers [9].

Secondly, while blockchain employs cryptographic measures to safeguard data, this encryption is not infallible. A leaked key equates to all the data stored on the blockchain being laid bare. Furthermore, the transparency of smart contract codes means that anyone can inspect and possibly alter this code. Should there be any flaws or malicious code present, there is a risk of personal information leakage.

Lastly, issues of data ownership within blockchain are notable concerns. In traditional databases, the ownership and usage rights of data are clear. In contrast, blockchain's distributed and decentralized nature means users can only access their account information via keys and digital signatures. Once a user's private key is exposed, it is akin to revealing their account credentials, leading to potential financial losses. Therefore, how to manage data effectively while safeguarding user privacy remains a significant challenge faced by current blockchain technology.

3.3 Network Privacy Issues

The blockchain P2P network operates independently of a single central authority and is instead maintained and verified through the collaboration of multiple nodes within the network. Furthermore, the blockchain network is subject to dynamic changes, allowing new nodes to join and existing ones to leave at any time, enhancing its resilience. Given this network structure, current threat models can be categorized into two types: probing attacks and topology attacks.

Probing Attacks. Attackers can deploy a significant number of probe nodes within the network to collect transaction data from the blockchain. Subsequently, they may discover patterns in the data transmission and pinpoint specific user groups, hence inferring their transaction activities and the flow of funds. With access to such information, attackers could execute disruptive attacks on the network.

There are three primary methods for probing blockchain network nodes: broadcast-based node detection, reverse Domain Name System (DNS) lookups, and port scanning. Broadcast-based node detection is a foundational and direct method where attackers broadcast messages within the network to identify responding nodes. Reverse DNS lookups involve attackers conducting DNS queries within the Bitcoin network to locate corresponding IP addresses and hostnames. Port scanning is a technique used to determine the position of nodes in the Bitcoin network by scanning their ports. Attackers can employ commonly used port scanning tools to gather positional information about the nodes. Koshy et al expand on these detection methods to analyze the propagation patterns of Bitcoin transactions, proposing four modes of blockchain information dissemination to identify the originator [10].

Topology Attacks. Attackers can monitor node connections and data transmissions within the blockchain network to gain insight into the network's topological structure. Having acquired this information, they could exploit it to launch destructive attacks on the network, such as Denial of Service (DoS) attacks or selective data tampering. These conventional network attacks primarily consist of DoS assaults, which involve a large number of service requests or other means to occupy a system's resources, causing legitimate users to be isolated from the main network and preventing them from receiving normal services. Common types of DoS attacks include bandwidth flooding, packet flooding, Synchronize Sequence Numbers (SYN) flooding, DNS amplification, and Internet Control Message Protocol (ICMP) flooding attacks.

4 Existing Privacy Protection Mechanisms in Blockchain

Blockchain data storage is founded on decentralized, distributed ledger technology, a stark contrast to conventional data storage systems that typically rely on a central authority for data management. Consequently, blockchain privacy protection schemes represent a novel domain distinct from traditional privacy protection technologies. From a technological perspective, this article categorizes the existing privacy protection mechanisms within blockchain into several broad types, providing a detailed explanation of each and discussing the current mainstream technological solutions.

4.1 Decentralized Identity Authentication

Blockchain technology facilitates decentralized identity authentication through the use of smart contracts. These automated contracts, executed on the blockchain, possess predefined conditions and rules. Smart contracts enable users to verify their identities without disclosing personal information. Specifically, a user can register a digital identity on the blockchain and link it with other identifying information. For authentication purposes, the user submits their public key and digital signature to the smart contract as proof of identity. The smart contract then authenticates the user's identity based on the established rules and key information and retrieves corresponding permissions from the blockchain to grant to the user. This entire process operates independently of third-party data storage, thereby enhancing the security of users' information.

Merkle Tree. Optimizing data structures is an effective method to enhance blockchain performance in decentralized settings. The Shrubs Merkle Tree is a variant of the incremental Merkle tree. This Merkle tree variant selects a node from each level and collects these chosen nodes as a "root set" ensuring that every leaf node can be indexed. This design permits the insertion of a leaf node with O (1) complexity but requires more complex Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (ZK-SNARK) proofs to verify the presence of the leaf node within the tree, resulting in a performance that is inferior compared to traditional Merkle trees. The team led by Zhang applied decentralized identity authentication on the blockchain and zero-knowledge proof encryption algorithms, proposing the Z-Shrubs Merkle Tree structure, which creates a final root through hashing the original Merkle tree roots, thus removing the layer restrictions of the Merkle tree and improving performance and efficiency over previous algorithms [11].

Federated Learning. Federated learning is an effective scheme for information sharing without breaching privacy in decentralized contexts. The federated system facilitates parameter exchange through encryption mechanisms, establishing a shared virtual model while complying with data privacy laws. This model is designed to serve local objectives within its regional context. Under such a federated mechanism, the identity and status of each participant are equalized, enabling decentralized data management and application. Researchers have demonstrated how deep gradient leakage, model inversion, and membership inference attacks pose threats to node privacy security. Building upon these security concerns, Hou's team proposed a blockchain-based Trustworthy Blockwise Training Slice Aggregation (BBTSA) strategy and the Federated Attribution (FedAom) algorithm, mitigating the Non independent identically distributed (Non-IID) issue of federated nodes' local data [12, 13]. These solutions can conceal the clients' privacy parameters and ensure comprehensive monitoring and privacy security during the training process without compromising accuracy.

4.2 Advanced Encryption Techniques

Blockchain technology ensures the security of data through cryptographic algorithms. Within the blockchain, all transaction information is encrypted and unique encrypted hash values are generated using hash functions. This encryption secures the immutability of the data, as any unauthorized alteration made to a single node by hackers would result in inconsistencies across the nodes within the blockchain, thereby rendering the altered content ineffective.

Homomorphic Encryption Techniques. Homomorphic encryption is a category of encryption methods endowed with unique natural properties, which allow for direct computation on encrypted data without the need for decryption keys. The Fig.2 illustrates the computational flow utilizing homomorphic encryption technology, where operators can directly process data on its encrypted form. Upon receipt, the data owner can decrypt the processed data to retrieve the original information. Since the computation of ciphertexts does not require keys, it reduces communication costs and allows the offloading of computational tasks, thus balancing the computational expenses across different parties. The application of homomorphic encryption technology ensures that the party decrypting the data only learns the final result and cannot access the messages within each ciphertext, thereby significantly enhancing the security of the information.

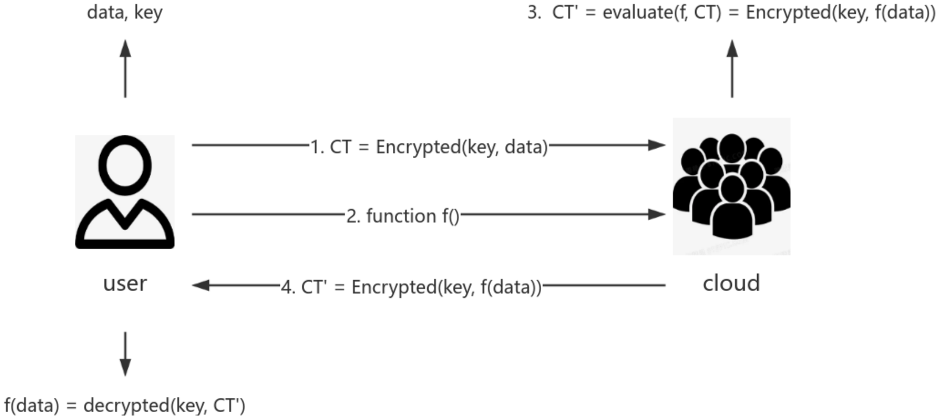
data, key
3. CT' = evaluate(f, CT) = Encrypted(key, f(data))
1. CT = Encrypted(key, data)
2. function f()
user
4. CT' = Encrypted(key, f(data))
cloud
f(data) = decrypted(key, CT')

Fig. 2. Homomorphic encryption workflow.

Homomorphic encryption technology can be categorized into fully homomorphic encryption and partially homomorphic encryption. Partially Homomorphic Encryption (PHE) supports computation in an encrypted form to a limited extent—for instance, supporting only addition or multiplication operations—and is classified further into additive or multiplicative homomorphic encryption algorithms. Notable examples of multiplicative homomorphic encryption include RSA and ElGamal algorithms, while Paillier algorithm is a well-established example of additive homomorphic encryption.

Fully Homomorphic Encryption (FHE) enables unlimited types of homomorphic operations on ciphertexts any number of times. In theory, any function can be computed homomorphically. FHE schemes include four algorithmic components: key generation, encryption, decryption, and an additional evaluation algorithm. FHE is more versatile compared to PHE, suitable for a broader range of application scenarios, and capable of performing more complex computational tasks. However, existing FHE algorithms are challenged by significant computational and storage overheads. The NTRU-based multi-key scheme proposed in 2020 is designed to optimize the problems faced by FHE [14].

Zero-Knowledge Proofs. Introduced by Goldwasser in 1989, zero-knowledge proofs enable one to assert the validity of a statement to a verifier without revealing any additional information. In the blockchain context, zero-knowledge proofs are used to verify the legitimacy of transactions by allowing verifiers to believe in the correctness of the prover's claim with high probability after several iterations of the transaction assertion.

Zero-knowledge proofs have a wide range of applications in cryptography and privacy, playing an important role in identity verification, encrypted communication, and the privacy protection of digital currencies. They allow participants to prove their claims during interactive processes while protecting their privacy and ensuring the security of their information. Current optimization efforts focus on improving verification efficiency, such as Deng’s work on constructing a novel non-interactive zero-knowledge proof scheme based on the Bulletproofs protocol, which enhances user privacy while increasing verification efficiency [15].

4.3 Confusion Techniques

Confusion techniques, by mixing transactions from different users, obscure the origins and destinations of transactions, enhancing their anonymity and making them less traceable. Blockchain confusion techniques typically employ transaction mixing services or mixers, also known as coin mixing technologies. These services collect transaction requests from several users, blend them together, and redistribute them to different addresses at random, creating a degree of disassociation between original and final transactions.

The most common coin mixing technique in blockchain is CoinJoin, which essentially severs the link between the input and output addresses of transactions, making the source and destination untraceable to protect privacy. CoinJoin allows multiple users to initiate a single transaction collectively, blending it together before broadcasting it to the blockchain network. This blending reduces the traceability of individual transactions due to the intermixing of contributions from various users.

Gui's team addressed the time-consuming nature of executing mixing transactions in the CoinShuffle scheme by proposing a ring signature-based mixing protocol [16]. Users announce their input and output addresses for coin mixing. The final user publishes the collection of addresses to the network. Each user then confirms their output address is in the collection before initiating a mixing transaction and signing it. This process is repeated until the final user signs, and the transaction is published. Experiments indicate that this scheme has significantly improved efficiency over existing mixing schemes.

Yan's team proposed a decentralized blockchain mixing mechanism based on multiple xor-encryption, named MXShuffle [17]. In this mechanism, a proxy node is randomly selected among participants, and other nodes generate encryption keys through multiple xor encryptions. Once the proxy node has received all data, it decrypts and distributes the data in sequence. This approach not only ensures the privacy of participants but also reduces the chances of malicious nodes intercepting mixing relationships and diminishes the impact of denial-of-service attacks.

4.4 Privacy Agreement

Secure Multi-Party Computation. Secure Multi-Party Computation (SMC) is a technological framework that allows parties to collaboratively share and process data in a manner that secures each participant's private information while enabling the completion of specific computing tasks. This process involves multiple parties, each with their own input data, who wish to keep this information confidential from the other participants. SMC protocols enable the collaborative computation of a function that depends on all participants' input without revealing their private data. The general flow of information sharing in this process is depicted in the Fig.3.

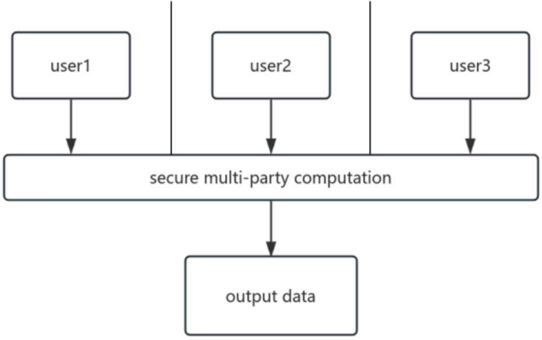

Fig. 3. SMC information sharing process.

Within blockchain contexts, SMC is primarily utilized for cryptographic currency validations, execution of smart contracts, and similar applications. In the case of permissioned blockchains, where participants are authorized and authenticated, SMC allows multiple entities to verify each other's actions and reach consensus, thereby ensuring the authenticity and integrity of data on the blockchain. It also safeguards sensitive information such as identity details and transaction records, enhancing privacy protection and mitigating the risk of data leaks. In permissionless blockchains, the identity and permissions of each participant do not require approval or authorization from others; rather, cryptographic protocols ensure the security of data and transactions within the network. However, SMC requires all users to adhere to the computational protocols of the blockchain. The presence of malicious actors not abiding by these protocols can pose a serious threat to the security and privacy of information. Yin proposed an outsourced secure multi-party statistical computation solution that delegates computational tasks to blockchain smart contracts to manage user node privacy [18]. Nevertheless, due to the mix of connectivity and anonymity mechanisms in SMC processes, members can't receive feedback on their contributions to the blockchain, thus hindering the development of incentive mechanisms.

Differential Privacy. Differential Privacy is predicated on the concept of deliberately adding random noise to query results or datasets, ensuring that even if external observers have knowledge of all other information except for a particular piece of data, they cannot ascertain whether that data exists in the original database. In other words, given an algorithm's output, an attacker's confidence level in determining whether an individual is part of the data set is significantly limited. Employing differential privacy in blockchain applications can effectively thwart analytical attacks on specific user behaviors, as any modification in the database does not impact the results accessed by final users, hence precluding attackers from pinpointing specific individuals and in principle reducing the risk of DoS-type attacks.

Yang's study moved differential privacy to the smart contract layer, enabling automatic noise addition to user-uploaded data and thus securing data storage; it also proposed a permissioned blockchain Reusable-noise Response Answer Protocol (RRAP), which matches queries and noise responses, addressing issues related to the reduction in privacy protection levels due to excessive data responses [19]. Dong's team introduced the DPstacking algorithm, which maintains data privacy while providing superior predictive performance and mitigating the issue of single homogenous ensemble learning algorithms' heightened sensitivity to noise [20].

5 Comparative Analysis of Privacy Protection Technologies

This article analyzes existing optimization algorithms in terms of security, performance, and risk factors. Security analysis includes traditional and contemporary algorithms focusing on three aspects: hiding transaction content, hiding transaction addresses, and privacy protection performance. Performance is analyzed through a comparative study of state-of-the-art algorithms versus established algorithms. Finally, by analyzing each algorithm in turn, potential risks inherent in each methodology are identified and discussed. As show in Table 1.

Table 1. Summary of privacy protection methods.

Protection Technique	Short Description	Hide Content	Hide Address	protection performance	Computing efficiency	Risks & Drawbacks	Latest Technology
Merkle tree	Optimizing performance through tree storage	Y	Y	medium	high	Fragile storage structure	Z-Shrubs Merkle Tree
Federated learning	Establish a virtual shared model, Users obtain operation results locally	N	Y	strong	medium	Low execution efficiency	BBTS, FedAom
Homomorphic encryption	Data can be processed directly without decryption	Y	N	strong	low	Large consumption on computing and storage	NTRU
Zero-knowledge proof	Repeated declaration of transactions to enhance credibility	Y	Y	strong	medium	Redundant data transmission and long time on verification	Non-interactive scheme
CoinJoin	Mixing transactions and transmit randomly	Y	Y	medium	low	Consuming much time in completing exhausting	Ring signature technology, MXShuffle
SMC	Collaborate to calculate a function, each user manage their own parts	Y	Y	strong	medium	Severe results on violating consensus, Difficult to join incentive mechanism	multi-party statistical calculation
Differential privacy	Adding noise to user data to protect privacy	Y	Y	strong	medium	Misreporting and privacy leakage risks	RRAP, DPstacking

Based on the analysis presented in the Tab.1, it is observed that aside from the specialized optimization of data storage efficiency via the Merkle tree algorithm, other technologies still require improvement regarding computational performance while protecting user privacy. Recent optimization techniques fall into two categories: those aimed at enhancing system performance and those focused on bolstering user privacy security. Most research dedicated to maintaining privacy security is predicated on sustaining or enhancing system performance. Modern blockchain technology increasingly emphasizes performance and efficiency enhancements alongside the protection of user privacy.

With the progress of computer technology, the study of quantum computing plays a significant role in computational performance. Traditional blockchain systems typically employ cryptographic techniques such as encryption algorithms based on mathematical challenges and digital signature technology to ensure the security and privacy of the blockchain. However, these encryption methods could potentially be compromised by high-performance computing systems. For instance, large integer encryption used by RSA is no longer viable in the current field of information security. Hence, these encryption algorithms are susceptible to being breached as computing power advances.

Regarding identity privacy, with the continuous refinement of zero-knowledge proofs and homomorphic encryption techniques, users' identity information during blockchain transactions can be effectively concealed, safeguarding their personal privacy. Furthermore, in network privacy, secure multiparty computation, federated learning, and other technologies are implemented for collaborative data sharing, ensuring that data transfers and processing across organizations are well-protected. Future developments in blockchain privacy protection will focus more on the integrity of privacy preservation and data security, advancing the establishment and enactment of decentralized privacy protection standards. As privacy regulations continue to improve and incidents of data breaches become more frequent, blockchain privacy protection technology will gradually mature, offering users a more secure and private environment for digital finance and data exchange.

6 Conclusion

In the era of the digital economy, enhancing the protection and management of personal privacy data is becoming an essential trend in technological advancement. Blockchain technology, renowned for its decentralization, data immutability, and trustworthiness, has found extensive application across various sectors. Nonetheless, the inherent transparency and decentralization of blockchain pose significant challenges to effectively safeguarding user privacy, making privacy protection within blockchain a critical area of research. This paper begins by elucidating the fundamental characteristics of blockchain technology, the theoretical concepts related to privacy within blockchain, and the privacy threats it faces. It proceeds to provide a comprehensive summary and analysis of the optimization algorithms that have been developed in recent years to address privacy issues in blockchain. Additionally, the paper reviews the current state of blockchain privacy challenges and anticipates future trends, thereby offering valuable insights and guidance for researchers focused on this evolving field.

References

1. Johar, S., Ahmad, N., Asher, W., et al.: Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey. Applied Sciences-Basel 11(14), 6252 (2021).

2. Yang, J.: Research on the optimization of industrial internet resource allocation integrating edge computing and blockchain. Network Security and Informatization 2024(02), 71-73 (2024).
3. Liang, C. X., Liao, J.: Design of an internet-based remote medical system using blockchain. Electronic Technology 53(02), 61-63 (2024).
4. Yuan, Y., Wang, F. Y.: The current status and prospects of blockchain technology development. Acta Automatica Sinica 42(4), 481-494 (2016).
5. Zhu, L. H., Gao, F., Shen, M., et al.: A survey of blockchain privacy protection research. Journal of Computer Research and Development 54(10), 2170-2186 (2017).
6. Chen, J. L., Ma, Z. Q., Lan, Y. J., et al.: A review of medical information sharing based on blockchain technology. Computer Applications Research 1-14 (2024).
7. Lu, W. Q.: The application of blockchain technology in the audit work of financial reporting. Accounting Learning 2024(09), 109-111 (2024).
8. Wang, Q., Li, F. J., Ni, X. L., et al.: Blockchain data formation and privacy threats. Computer Engineering 49(08), 1-12 (2023).
9. Sun, G. Z., Wan, M. F., Wang, Y., et al.: Analysis of transaction privacy protection in blockchain. Journal of Nanjing University of Posts and Telecommunications (Natural Science) 1-20 (2024).
10. Zhu, X., Xu, H., Zhao, Z., et al.: An Environmental Intrusion Detection Technology Based on WiFi. Wireless Personal Communications 119(2), 1425-1436 (2021).
11. Zhang, Y., Mo, X. L.: An identity authentication mechanism based on blockchain and zero-knowledge proofs. Journal of Tianjin University of Technology 1-7 (2024).
12. Ge, L., Li, H., Wang, X., et al.: A review of secure federated learning: privacy leakage threats, protection technologies, challenges and future directions. Neurocomputing 126897 (2023).
13. Hou, Z., Dong, J.: Privacy-preserving federated learning optimization method in decentralized scenarios. Computer Application Research 1-9 (2024).
14. Che, X. L., Zhou, T. P., Li, N. B., et al.: Optimization of NTRU-type Multi-key Fully Homomorphic Encryption Scheme. Engineering Science and Technology 52(05), 186-193 (2020).
15. Deng, C.: Optimization of zero-knowledge proofs and their application in identity authentication. Hangzhou Dianzi University (2023).
16. Gui, K. Y., Li, S. E.: RSCoinJoin: A coin mixing scheme based on ring signatures. Computer Applications and Software 41(03), 109-116 (2024).
17. Yan, Y., Li, J. J., Liu, Q.: A blockchain coin mixing mechanism based on multiple XOR encryption. Computer Application Research 40(11), 3235-3240 (2023).
18. Yin, Z. J.: Research on privacy-preserving techniques for secure multi-party computation based on blockchain. University of Electronic Science and Technology of China (2023).
19. Yang, W. H.: Study on blockchain data privacy protection algorithms based on differential privacy. Xi'an University of Technology (2024).
20. Dong, Y. L., Zhang, S. F., Xu, J. C., et al.: Research on differential privacy protection for the Stacking algorithm. Computer Engineering and Science 46(02), 244-252 (2024).