Cryptographic Privacy Protection in Blockchain: Analysis of Strategies and Future Directions

Chen Lin[a]
Chow Yei Ching School of Graduate Studies, City University of Hong Kong, Hong Kong, China

Keywords: Blockchain, Privacy Protection, Homomorphic Encryption, Secure Multiparty Computation.

Abstract: The growing concerns around data privacy have highlighted the need for effective privacy protection mechanisms in blockchain technology, making it a prominent research focus. This paper explores various privacy protection strategies in blockchain, particularly emphasizing the critical role of cryptographic techniques. This study examines the benefits and drawbacks of privacy-focused cryptographic methods, such as attribute-based encryption, homomorphic encryption, secure multiparty computing, and special data signatures, after analyzing advanced literature. The analysis shows that privacy issues in blockchain cannot be fully addressed at the application or contract layers alone; instead, a combination of cryptographic methods must be tailored to specific needs and scenarios. The paper further emphasizes that the practical implementation of these technologies should consider both timeliness and application relevance, carefully weighing the trade-offs between privacy and performance. In conclusion, the study highlights key challenges that must be resolved for blockchain privacy solutions to evolve, particularly in balancing transparency and confidentiality. This analysis provides insights into the future development of privacy protection in blockchain systems, urging for an integrated approach to leverage cryptographic innovations in real-world applications.

1 INTRODUCTION

With Bitcoin being the most popular decentralized digital money ever, the idea of blockchain has garnered a lot of interest. A blockchain, also known as a distributed consensus network, is a tamper-proof digital database maintained chronologically by nodes. The miners come to an agreement on the involved computations as well as the transactions. This guarantees the blockchain's decentralization, verifiability, and immutability. Because of these features, blockchain has been used in the creation of systems for supply chain financing, provenance, sharing economies, dynamic key management, and data storage, among other applications (Cai, 2017).

While the blockchain can offer a potent abstraction for distributed protocol design, it is important to consider security and privacy concerns (such as the disclosure of a user's true identity, transaction value, and balance) in order to safeguard the interests of users. Thousands of academic papers on blockchain have been published in the last five years, including twelve study reports on the privacy and security risks associated with blockchain technology. The first comprehensive explanation of Bitcoin and other cryptocurrencies was given by Joseph Bonneau et al., who also examined privacy-enhancing techniques and examined anonymity issues (Jiang et.al, 2020). Ghassan Karame reviewed and thoroughly examined the risks and assaults associated with digital currency systems similar to Bitcoin, as well as the security provisions of the blockchain in Bitcoin. Additionally, they discussed and assessed risk-reduction techniques. Mauro Conti et al. examined Bitcoin's security and privacy, pointing out any flaws that could pose a risk to various security measures when the system is put into use. Li et al. examined the security threats posed by well-known blockchain systems, examined blockchain attack examples, and examined the vulnerabilities that were used in these instances (Li et.al, 2017). The majority of research articles on blockchain security and privacy have focused on two main areas: listing some of the attacks that have been made against blockchain-based systems thus far and outlining particular strategies for implementing

[a] https://orcid.org/0009-0006-1892-0165

Lin and C.
Cryptographic Privacy Protection in Blockchain: Analysis of Strategies and Future Directions.
DOI: 10.5220/0013526900004619
In *Proceedings of the 2nd International Conference on Data Analysis and Machine Learning (DAML 2024)*, pages 494-499
ISBN: 978-989-758-754-2

cutting-edge defenses against a portion of these attacks. Nevertheless, there hasn't been much work done to provide a comprehensive analysis of the security and privacy features of blockchain technology, as well as different blockchain deployment approaches.

This paper provides a complete overview of blockchain security and privacy. It begins by explaining blockchain technology in online transactions, addressing both fundamental and advanced security and privacy attributes. A range of security techniques is explored to meet these goals. As blockchain adoption grows, understanding its security and privacy features is critical. This knowledge helps uncover the root causes of vulnerabilities and guides innovation in defense mechanisms. The review has two primary objectives: to offer a resource for non-experts to grasp blockchain security basics, and to guide specialists in exploring advanced security techniques. The study defines key security qualities, analyzes solutions to achieve these objectives, and notes outstanding issues. Furthermore, it helps domain specialists select appropriate blockchain models and methodologies for specific applications. In summary, the review outlines the current state of blockchain security, offering insights for future research and technological advancements.

2 METHODOLOGIES

2.1 Blockchain

Blockchain technology is the outcome of the combination of several technologies, including encryption, mathematics, computer networks, and others. The organic integration improves blockchain's decentralized data recording approach. The blockchain technology primarily addresses the issue of creating reliable trust records without the involvement of third-party trust institutions.

Internet finance is closely related to third-party trusted institutions. These third-party financial institutions play the role of intermediaries in electronic transactions, responsible for coordinating information between both parties involved in the transaction. Throughout the entire transaction process, third-party institutions bear the responsibility of auditing, security guarding, and maintaining the transaction. The existence of fraudulent behavior in online transactions highlights the intermediary position of third-party financial institutions, while also leading to higher transaction costs. Bitcoin is the most significant application of blockchain technology, but the application of blockchain technology is not limited to electronic currency. It can be applied to various fields of online exchange of electronic assets. This article takes Bitcoin as an example to explain the relevant principles and concepts of blockchain technology sources (Cai et.al, 2017). Bitcoin is based on cryptography technology and functions as a third-party middleman between two parties who are likely to deal. An electronic signature verifies and secures each transaction inside the designated transaction procedure (Tahir and Rajarajan, 2018). Within the Bitcoin network, the recipient's account address (such as public key) receives a transaction that has been signed by the initiator using their private key. In a gesture to sign a transaction using Bitcoin, the holder must demonstrate that they are the owner of the private key. The sender's public key is employed in the analysis of Bitcoin transactions to check the transaction signature and determine if the transaction party has the ability to use the associated Bitcoin.

Every transaction in the Bitcoin network is broadcasted to all nodes and recorded in the blockchain once it passes verification. All nodes jointly maintain these transaction records, preventing fraud, tampering, or deletion. Before a transaction is recorded, the review node ensures two things: the Bitcoin consumer possesses the required digital currency (verified by electronic signatures), and has sufficient funds (checked via the blockchain ledger). However, transactions are not broadcasted in the order they are generated; instead, each one is relayed across the network individually. To prevent double-spending, Bitcoin uses a mechanism to handle transactions broadcast out of sequence. Blockchain technology is crucial in solving the "double-spending" issue. Transactions are collected, verified, and recorded in blocks over time, which are then linked in chronological order using the hash of the block before, composing the blockchain. This creates a verifiable transaction history. However, any node can generate and broadcast new blocks, so a system is needed to decide which block to append to the chain. Bitcoin employes the Proof of Work mechanism, where nodes compete to solve a computational problem. To generate a block, nodes should find a random number namely nonce so that the hash of the block before, transaction record, and nonce is not up to a target value, ensuring that the block meets specific difficulty criteria.

However, this mathematical problem is not fixed. The Bitcoin system balances the generation time of blocks by adjusting its difficulty, resulting in an

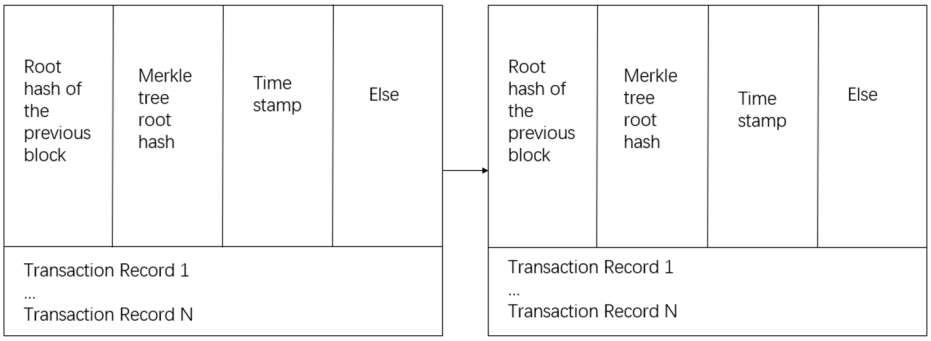

Figure 1: The specific process of implementing blockchain (Picture credit: Original).

average of 10 minutes to generate a new, accepted block within the system. In the network, nodes contribute their own computing resources to solve mathematical problems and compete to generate blocks. The node that first successfully calculates the solution to a mathematical problem will have the right to connect the block generated by this node to the end of the blockchain, be accepted by other nodes, and be awarded a certain amount of Bitcoin as a reward for contributing computing resources to it. Bitcoin calculates hash values through competition, based on POW, ensuring that new blocks are generated on average every 10 minutes, and issuing new Bitcoin through the generation of new blocks. The specific process of implementing blockchain is displayed in the Figure 1.

Collect all transaction information from network nodes over a length of time. The receiving node verifies the received transaction information and reviews whether the transaction is legal. The verified transaction records will be recorded in the entity of the new block. The hash value of the current end block of the blockchain is compared with the transaction information in the block subject at the network node to determine the hash value of the new block that satisfies the requirements. Broadcasting the newly generated block information to the rest of the network is the first node to calculate the hash value that matches the conditions. Once the newly generated block has been verified by the node, and if the review is accurate, all nodes accept it. It is considered best practice to name the recently created block as the blockchain's current terminal block. Through the above steps, all nodes in the blockchain network participate in, maintain, and review the generation process of blockchain blocks, and the blockchain network maintains the same blockchain ledger records at all nodes, ensuring the authenticity, reliability, and immutability of block records on the blockchain.

In blockchain, a block contains two pieces of information: the block header and the block body. The block body will include specific transaction information such as both parties' public key addresses, transaction quantities, signature verification, and so on, whereas the block header will have a fixed size of bytes. The hash value of a block can be used to uniquely identify it within the blockchain. Each block references the previous block's hash value field. A blockchain has been built as a chain that can keep transaction records in chronological order, ensuring that the transactions recorded on the blockchain occur in the correct order. The calculation method of the block hash value at present by virtue of introducing random numbers, Merkle tree roots, and the hash value of the block before ensures the authenticity and reliability of transaction information (Cai et.al, 2018).

2.2 Encryption

2.2.1 Asymmetric Encryption Algorithm

Asymmetric encryption algorithm is one of the most commonly used encryption algorithms in blockchain, which uses a pair of keys (public key and private key) for encryption and decryption operations. The public key is public and can be accessed by anyone; And the private key is confidential, only the holder can know. This encryption method ensures privacy protection between the communicating parties, as only those who possess the private key can decrypt the data, thereby ensuring its confidentiality.

In blockchain, asymmetric encryption algorithms are mainly used to create and verify transactions. The sender encrypts the transaction information using the receiver's public key, and then sends the encrypted transaction information to the blockchain network. The receiver decrypts the transaction information using their own private key to verify the validity of the transaction. Meanwhile, asymmetric encryption

algorithms are also used for digital signatures to verify the identity of the transaction sender and the integrity of the transaction.

2.2.2 Hash Algorithm

Hash algorithm is another important encryption algorithm in blockchain, which translates data of arbitrary length to a set length hash value, as shown in the Figure 2. Hash algorithm has collision resistance, which means that the probability of different input data obtaining the same hash value after hash algorithm is very low. This makes hash algorithms play a crucial role in blockchain.

In blockchain, each block holds the previous block's hash value, resulting in an immutable chain structure. When a new transaction is added to the blockchain, a new block is formed, and the previous block's hash value is included in the new block. This chain structure maintains the integrity and authenticity of data in the blockchain, as any modifications to the data will cause changes in the hash value, disturbing the overall chain structure (Hu et.al, 2018). In addition, hash algorithms are also used to verify the execution results of smart contracts. Smart contracts are blockchain-based algorithms that automatically execute complex transactions and business logic. After the smart contract is executed, the blockchain will generate a hash value containing the execution result and store it on the blockchain. In this way, anyone may check the validity and integrity of smart contract execution results.

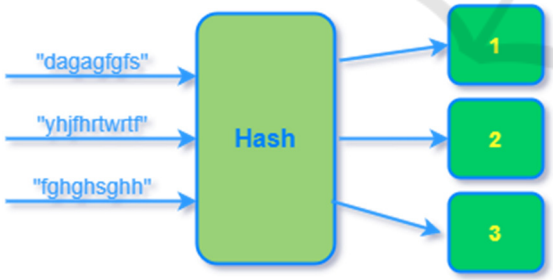

Figure 2: Hash algorithm (Picture credit: Original).

2.2.3 Digital Signature Algorithm

Digital signature algorithm is an encryption algorithm employed to check the authenticity and integrity of messages or data, as shown in the Figure 3 and Figure 4. It uses a private key to sign the message, and then verifies the validity of the signature with the corresponding public key. Digital signature algorithms play an important role in blockchain, mainly used to check the identity of transaction senders and the integrity of transactions. In blockchain, the transaction sender uses their private key to sign the transaction information before sending it to the blockchain network (Zhang et.al, 2018). The receiver verifies the signature with the sender's public key, ensuring the transaction's authenticity and integrity. This verification technique assures that blockchain transactions are worth trusting and safe.

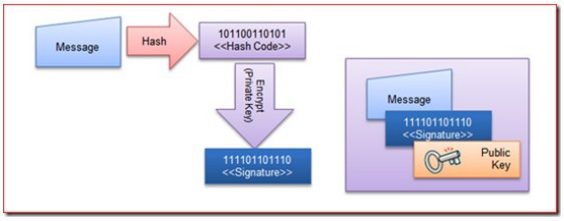

Figure 3: The signing process of digital signature (Picture credit: Original).

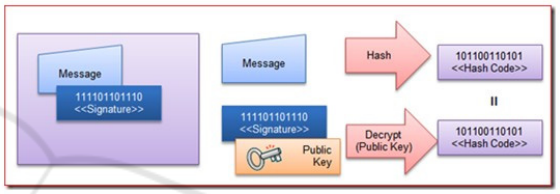

Figure 4: The verification process of digital signatures (Picture credit: Original).

3 RESULT AND DISCUSSION

3.1 Case Analysis

As for the specific application of combining the two, such as when the results returned by the Server-Sent Events (SSE) server may not be correct, how to handle it if the server maliciously returns incorrect results. In addition, if accessing private clouds, which may not share data, it is necessary to consider using blockchain to ensure security. Therefore, some researchers have pointed out the importance of storing data on public chains and innovatively constructed an SSE model using blockchain, and provided its security definition to make sure the data privacy and improve search efficiency. Based on the size of the data, consider two different scenarios and propose corresponding solutions. Among them, blockchain is responsible for storing the ciphertext of files and the index of searches, thus achieving the purpose of encryption (Chen et.al, 2019).

3.2 Discussion

With the ongoing development and extensive application of blockchain technology, the issue of privacy leaking has become more significant and is supposed be fully valued by researchers and industrial developers. Unlike traditional centralized storage systems, blockchain approaches do not rely on specific central nodes to process and store data, eliminating the risk of centralized server single point failures and data leaks. However, in a gesture to achieve consensus among nodes in a distributed system, all transaction records in the blockchain are supposed to be made available to all nodes, dramatically increasing the possibility of privacy violations. Hence, the distributed nature of blockchain differs dramatically from traditional Information Technology (IT) architecture, and large numbers of typical privacy protection measures fail to apply to blockchain applications. Therefore, assessing the privacy leaking faults of blockchain and exploring targeted privacy protection strategies are of tremendous importance.

The privacy protection objects can be classified into three categories, namely network layer privacy protection, transaction layer privacy protection, and application-level privacy protection. Privacy protection at the network layer encompasses the process of data transmission in the network, containing blockchain node establishing modes, node communication mechanisms, data transmission protocol mechanisms, and so on. The transaction layer's privacy protection extends throughout the full process of data generation, verification, storage, and use in the blockchain. The transaction layer's privacy protection is mainly focused on hiding data information and knowledge behind the data as much as possible while meeting the blockchain's basic consensus mechanism and the condition of unchanged data storage, in a gesture to prevent attackers from extracting user profiles by analyzing block data; The application layer's privacy protection scenarios include the process of blockchain data being used by external applications. The use of blockchain by external apps raises a risk of compromising transaction and identity privacy. As a result, privacy protection at the application layer focuses on boosting user security awareness and strengthening the security protection level of blockchain service providers, such as acceptable public and private key storage, and developing blockchain services free from danger (Chen et.al, 2019).

In public blockchain initiatives nowadays, all people participated have access to entire data backups, and all data is accessible to them. Anyone can make the query the on-chain data. The Bitcoin project achieves anonymity by isolating the transaction address from the address holder's real identity. Attackers can view the addresses of the sender and receiver of each transfer record, but they are unable to identify a specific person in the reality. However, attackers can still achieve their goal of stealing privacy by initiating various types of assaults at the network, transaction, and application layers (Guan et.al, 2020). Although regulatory roles with Certificate Authority (CA) properties can guarantee the reliability of access nodes for consortium chains, research based on cryptography, zero knowledge proof, and other technologies is constantly progressing if blockchain wants to take on more business, like registering real name assets in real-world scenarios, implementing concrete loan contracts by means of smart contracts, and guaranteeing that verification nodes execute contracts without knowing specific contract information. Blockchain technology can only boost traditional companies and realize its established advantages by continuously enhancing its multi-level privacy protection mechanism (Liu et.al, 2020).

4 CONCLUSIONS

Blockchain technology has made significant progress in ensuring data trustworthiness, immutability, and integrity, making it a valuable tool in various sectors. However, it remains immature in other critical areas, particularly in terms of privacy, anonymity, and security mechanisms. This paper is specifically focused on the challenges of privacy protection in blockchain systems, with a strong emphasis on the role of cryptographic methods. While blockchain's decentralized nature offers enhanced data transparency, it also raises privacy concerns, as transaction details are often accessible to all participants in the network. The study concludes that relying solely on application and smart contract layers to address these privacy concerns is insufficient. Instead, it advocates for the integration of advanced cryptographic techniques that can complement each other to meet the diverse demands of different use cases. By utilizing these cryptographic methods, blockchain systems can achieve more robust privacy protection, ensuring both security and confidentiality. Future research should focus on developing tailored privacy solutions that balance transparency with

privacy needs across various blockchain applications. In order to make blockchain technology more widely employed in sectors including supply chain management, finance, and healthcare, these obstacles must be overcome.

REFERENCES

Cai, C., Weng, J., Yuan, X., et al. 2018. Enabling reliable keyword search in encrypted decentralized storage with fairness. IEEE Transactions on Dependable and Secure Computing, 18(1), 131-144.

Cai, C., Yuan, X., Wang, C., 2017. Hardening distributed and encrypted keyword search via blockchain. IEEE Symposium on Privacy-Aware Computing, 119-128.

Cai, C., Yuan, X., Wang, C., 2017. Towards trustworthy and private keyword search in encrypted decentralized storage. IEEE International Conference on Communications, 1-7.

Chen, B., Wu, L., Wang, H., et al. 2019. A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks. IEEE Transactions on Vehicular Technology, 69(6), 5813-5825.

Chen, L., Lee, W.K., Chang, C.C., et al. 2019. Blockchain based searchable encryption for electronic health record sharing. Future generation computer systems, 95, 420-429.

Guan, Z., Wang, N., Fan, X., et al. 2020. Achieving secure search over encrypted data for e-commerce: a blockchain approach. ACM Transactions on Internet Technology (TOIT), 21(1), 1-17.

Hu, S., Cai, C., Wang, Q., et al. 2018. Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization. IEEE INFOCOM Conference on Computer Communications, 792-800.

Jiang, P., Guo, F., Liang, K., et al. 2020. Searchain: Blockchain-based private keyword search in decentralized storage. Future Generation Computer Systems, 107, 781-792.

Li, H., Zhang, F., He, J., et al. 2017. A searchable symmetric encryption scheme using blockchain. arXiv preprint :1711.01030.

Liu, S., Yu, J., Xiao, Y., et al. 2020. BC-SABE: Blockchain-aided searchable attribute-based encryption for cloud-IoT. IEEE Internet of Things Journal, 7(9), 7851-7867.

Tahir, S., Rajarajan, M., 2018. Privacy-preserving searchable encryption framework for permissioned blockchain networks. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 1628-1633.

Zhang, Y., Deng, R.H., Liu, X., et al. 2018. Outsourcing service fair payment based on blockchain and its applications in cloud computing. IEEE Transactions on Services Computing, 14(4), 1152-1166.