Proceedings of the 5th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/19/20231020

Exploring and envisioning the application of blockchain technology for privacy data protection

Yuhan Gao[1,4,†], Liyuan Guo[2,†] and Tao Zhang[3,†]

[1]School of Software, Zhongyuan University of Technology, Zhengzhou, 528315, China
[2]Technical College, Zhuhai College of Science and Technology, Zhuhai, 519040, China
[3]Engineering College, Guangzhou College of Technology and Business, FoShan, 528000, China

[4]gaoq.zgtj@chinaccs.cn
[†]These authors contributed equally.

Abstract. Addressing the issue of data leakage in social networks, this paper presents a classification of users' privacy information and introduces various personal data protection schemes utilizing blockchain technology. These schemes employ timestamp data storage within the blockchain, hash function anonymization techniques, and the Rivest-Shamir-Adleman (RSA) asymmetric encryption algorithm for encrypting and digitally signing transmitted data files. This innovative blockchain-based approach effectively tackles privacy leakage concerns in social networks and sets a benchmark for research in data security and social network safety. In this article, we propose a unique blockchain-based data protection scheme, specifically designed for different types of privacy leaks. This innovative solution addresses the pervasive problem of privacy leaks in social networks. However, current methods require more computational power during data interaction, which may hinder performance. Future research will concentrate on optimizing blockchain computational efficiency, aiming to develop a more robust data privacy protection system for blockchain-based social networks. By enhancing the efficiency and effectiveness of these privacy protection schemes, we hope to create a more secure environment for users to interact and share information on social platforms, ultimately fostering trust and confidence in digital social networks.

Keywords: blockchain, zero-knowledge, homomorphic encryption.

1. Introduction

Blockchain technology is a distributed ledger characterized by decentralization, trustlessness, collective maintenance, reliable databases, and immutability. This technology enables participants to conduct transactions without revealing their identities, thereby ensuring data privacy protection through the implementation of smart contracts and consensus mechanisms during data transactions [1]. Blockchain technology promotes data security through a series of mechanisms that comprehensively support data privacy protection [2].

DOI: 10.54254/2755-2721/19/20231020

In the era of big data, blockchain offers a secure, reliable, efficient, and cost-effective platform for data storage and transmission [3]. This technology transforms the information security model during data transmission in traditional internet processes, making it an effective solution for addressing personal privacy protection issues [4]. As individuals benefit from the conveniences brought by technological advancements in the big data era, they also face risks associated with data security and privacy breaches [5].

This paper presents a comprehensive review of the current research status of blockchain technology in data privacy protection and envisions future research directions. The aim is to provide a valuable reference for the development of data privacy protection systems based on blockchain technology [6]. By analyzing the strengths and limitations of existing solutions, this work contributes to the ongoing efforts to enhance privacy and security in the digital landscape.

In the Internet era, the security of user data has attracted widespread attention from society. The networking and transparency of personal data has become an unstoppable megatrend. The advent of Internet crawlers, human flesh searches and other means has put people's lives under various microscopes; All kinds of promotions or harassing calls are annoying; Reports of economic fraud due to information leakage are also common [7]. In the absence of effective protection, data abuse and misappropriation make the problem of personal privacy leakage increasingly serious, and even breed illegal activities, and for users, the awareness of data privacy protection is also increasing. How to protect personal privacy has become one of the most concerned topics of the public [8].

2. Privacy protection and blockchain

In the internet era, user data security has garnered widespread attention from society. The interconnectedness and transparency of personal data have become an unstoppable trend. The emergence of web crawlers, doxxing, and other methods have placed people's lives under various microscopes; incessant promotions or nuisance calls are irritating; reports of financial fraud due to information leaks are also commonplace [9]. In the absence of effective protection, data misuse and misappropriation exacerbate the issue of personal privacy breaches, and may even facilitate illegal activities. Simultaneously, users are becoming increasingly aware of the importance of data privacy protection. Consequently, protecting personal privacy has emerged as one of the most pressing concerns for the public [10].

3. Traditional privacy protection

3.1. Traditional privacy protection technologies

3.1.1. Access Control List(ACL). An access control list ACL is a collection of one or more rules. ACL is essentially a message filter, and the rule is the filter element of the filter. Based on these rules, the device matches packets, filters out specific packets, and allows or blocks the passage of packets based on the processing policies of the service modules to which ACLs are applied [11].

3.1.2. Homomorphic encryption. Homomorphic encryption refers to the data results obtained by directly performing the same calculation on the obtained ciphertext after the original data is homomorphic encryption, and then the calculation results are decrypted homomorphism [12].

3.1.3. Attribute-based encryption. In 1984, Adi Shamir proposed the concept of "Identity-Based Encryption (IBE), which uses identity information as the public key for encrypted messages. In 2001, Dan Boneh and Matt Franklin proposed the first identity-based encryption scheme, and in 2005, A. Sahai and Brent Waters proposed an IBE mechanism based on attribute encryption mechanism, which solved the problem of each user being uniquely identified in IBE by introducing attribute collections [13]. In the ABE mechanism, the attribute collection is equivalent to the user's identity, taking the user's attribute as the public key, and generating the user's attribute private key according to the user's attribute

DOI: 10.54254/2755-2721/19/20231020

collection. Similarly, ciphertext is not encrypted for a specific user, but is generated from a collection of attributes and encrypted to a group of users who meet certain criteria. By developing a threshold access policy, ciphertext data can be properly decrypted only if the user attribute private key meets certain requirements for access control [14].

3.2. Traditional privacy protection schemes

3.2.1. Data masking. The storage method of data desensitization is applied to blockchain nodes, nodes refer to the terminal responsible for maintaining network operation in the blockchain network, which can be mobile phones, mining machines, servers, computers, etc, which can realize the storage of blockchain data desensitization through the method of this application [15]. The channel of the blockchain refers to the private atomic broadcast channel divided and managed by the ordering nodes in the blockchain network, which is used to isolate the data in the channel with the organizations or institutions outside the channel, and the nodes that join the same channel can jointly access the data in the channel, while the nodes outside the channel cannot access the information in the channel, thereby achieving channel-level data privacy, it is worth noting that although the channel achieves channel-level data privacy, However, the existing technology cannot achieve privacy protection of sensitive data between nodes in the same channel, and the storage method of data masking realizes privacy protection of sensitive data between nodes in the same channel in this regard.

3.2.2. Data anonymization. Through data anonymization, sensitive data and potentially leaked sensitive information are released in a targeted manner on the basis of weighing the risk of privacy leakage and data accuracy, thereby reducing the risk of privacy leakage. K-anonymity, L-diversity and t-proximity are typical technical representatives of data anonymization, among which the research on k-anonymity data privacy protection methods has attracted much attention [16]. The researchers proposed that the K-anonymity algorithm can anonymize the dataset to ensure that the anonymized information is at least similar to other K–1 records. Roberto et al. proposed an improved data management strategy based on the K-anonymization algorithm, which eliminates the time-consuming sorting process and can meet the anonymization and reduce the amount of data to be disturbed.

3.2.3. Differential privacy. Differential privacy is to achieve privacy protection by perturbing the original data, so that the perturbed data meets two conditions at the same time: the attacker cannot reconstruct the real original data through the distorted data after release, and the distorted data still maintains certain properties. It is a privacy protection technology that distorts the original data by adding noise, adding or deleting specific records in the dataset will not affect the query processing results, the amount of noise added has nothing to do with the size of the dataset, and only a small amount of noise needs to be added to the large dataset to obtain a good privacy protection effect. Differential privacy is the application of data interference and noise with the goal of reducing the likelihood of external identification of user privacy information while improving the accuracy of statistical database query results [17].

Differential privacy is generally the more accurate, conservative, and secure model globally. But first of all, it doesn't apply for small data; Secondly, noise should be added, which is not suitable for high data accuracy.

3.3. Problems faced by traditional privacy protection schemes

The use of blockchain technology can provide feasible solutions to the problems faced in traditional privacy protection:

Based on the decentralized characteristics of the blockchain, a single criterion for filtering data can be created; Realize data right confirmation based on the non-tamperability and traceability characteristics of blockchain; Finally, blockchain can track all stages of the data life cycle.

DOI: 10.54254/2755-2721/19/20231020

4. Blockchain based data privacy protection technology

At present, most of the ways to use blockchain to protect privacy are to use its reliable data storage capabilities and smart contract capabilities, data owners first use smart contracts to define access rules, and publish information to the blockchain in the form of transactions, such as smart contracts, metadata, etc., at the same time, raw data can be stored in the cloud, and the system provides access to this data only to those users who meet the requirements of the regulations. Shared data encryption is usually done by the system's cryptographic algorithm, which then uploads ciphertext data to the system to ensure unauthorized access to the data.

4.1. Privacy protection for smart contracts

Zero-knowledge proofThe most prevalent zero-knowledge proofs used for privacy protection in the blockchain domain are zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs). In this proof system, the prover and verifier do not engage in two-way communication; the proof process consists solely of a single message sent from the prover to the verifier.

Under a zero-knowledge proof, the concerned party does not reveal any information about the knowledge itself while demonstrating to the verifier that they possess the corresponding knowledge. In zero-knowledge proofs, two or more parties need to establish the authenticity of an item through a series of steps. There are currently two types of zero-knowledge proofs: interactive and non-interactive.

On one hand, there is interactive proof. The prover and verifier interact several times, with the verifier eventually being convinced that the prover holds the corresponding knowledge. Throughout these interactions, the prover sends relevant content without disclosing specific information about the knowledge. The verifier then provides immediate feedback upon receiving the information, validating the knowledge based on this feedback. After multiple interactions, the verifier gains a high level of confidence in the prover's knowledge.

On the other hand, there is non-interactive proof. The verifier selects a random value, performs a secret calculation, and assumes the result is correct, indicating that the prover possesses the knowledge. In non-interactive proofs, choosing random values is crucial not only to ensure that the prover does not cheat but also to prevent an excessive proof size and to guarantee a fast verification process.

Zerocoin: In 2013, Ian Miers and colleagues proposed a Bitcoin extension protocol called Zerocoin (or Zcoin) based on zero-knowledge proofs. The Zerocoin solution conceals the input and output addresses of Bitcoin transactions, which somewhat protects against ledger analysis attacks. The Zerocoin privacy protection implementation leverages the incompatibility between Zerocoin and Bitcoin, first converting Bitcoin into Zcoin and then obfuscating the relationship between the input and output addresses of transactions using zero-knowledge proofs and Pedersen's commitment. Additionally, the transaction amount in the Zerocoin scheme is fixed and indivisible. Zerocoin disrupts the correspondence between the sender and receiver of the transaction and is not compatible with the Bitcoin system [17].

Zerocash: While hiding transaction information such as initiator, receiver, and amount, verification nodes can still confirm the transaction's correctness. Zerocash simultaneously conceals the transaction address and amount, allowing users to set the transaction amount as needed, thus enhancing privacy protection. Moreover, Zerocoin supports amount splitting and is compatible with Bitcoin. The Zerocash minting-melting process enables anonymous transactions.

4.1.1. Multi party secure computing. The multi-party calculation of safety was proposed by Yao Zhizhi in 1982. To illustrate the concept, Yao used the famous millionaire problem to illustrate. The millionaire problem refers to how 2 millionaires can be richer than anyone without revealing their true wealth without a trusted third party. Through the innovative work of many scholars, secure multi-party computing has gradually developed into an important branch of cryptography.

4.1.2. Homomorphic encryption. Homomorphic encryption concerns the security of data processing and provides the function of processing encrypted data. Homomorphic encryption principle: the data first

DOI: 10.54254/2755-2721/19/20231020

goes through homomorphic encryption, the ciphertext data is specifically calculated and processed, the calculation result is obtained, and the corresponding homomorphic decryption of the calculation result is performed, and the processing result obtained is equivalent to the direct calculation and processing of plaintext data, realizing the "invisible" of the data. This feature is of great importance for information security, and the use of homomorphic encryption technology allows the decryptor to know only the end result, but cannot get every encrypted message, which improves information security.

Creating a zero-knowledge proof requires completing the trusted setting in advance, but the cost of making trusted settings for different smart contracts is high, which increases the complexity of the zero-knowledge proof. In secure multi-party computing, there are communication costs between nodes and slow protocol speeds, so network bandwidth requirements are high. At present, homomorphic encryption technology can only realize single-bit operations, which is inefficient, and most homomorphic encryption security is based on unproven difficult problems, and the security support is still doubtful. Trusted execution environment is the easiest technology to scale up in smart contract privacy protection technology, but hardware assurance is always at risk of security vulnerabilities being attacked.

4.2. Pairs of privacy protection for transaction information mixed currency

The core idea of the mixing mechanism (address obfuscation mechanism) is to hide the transaction process from both sides of the blockchain transaction, so that attackers cannot accurately analyze the relationship between different addresses, thereby spreading unrelated merchant trading relationships.

Aiming at the various implementation technologies in the address obfuscation mechanism, three measurement indicators are proposed:

- Asset security

After the address obfuscation operation, users can retrieve their assets (minus fees) before the agreed time.

- External privacy

The relationship between the input and output addresses of users participating in mixed currency transactions, and the possibility of being associated by external attackers.

- Internal privacy

The relationship between the input and output addresses of the user participating in the mixing transaction, and the possibility of being associated by the attacker involved in the mixing process.

There are many different implementation forms of address obfuscation mechanism, which are divided into two types of technologies: centralized coin mixing and decentralized coin mixing according to the specific operators:

Centralized coin mixing

(1) Centralized coin mixing: Centralized coin mixing technology requires the participation of centralized coin mixing service providers to help coin mixing users perform coin mixing operations. Centralized coin mixing technology is convenient for users to use, but there are security risks for coin mixing service providers.

(2) Basic model: Its basic model consists of four stages, namely negotiation, input, output, and end.

Participants in mixed coin transactions hand over transaction assets, input and output addresses, etc. to centralized providers, and the providers complete the obfuscation of output addresses. This solution protects the security of users' assets to a certain extent, but cannot guarantee the credibility of the provider and cannot provide internal privacy, which may lead to the loss of users' assets and privacy leakage. In order to protect their privacy from being leaked by the platform, users will choose to mix coins on multiple platforms continuously, which will incur higher fees. As shown in Table 1.

DOI: 10.54254/2755-2721/19/20231020

Table 1. Comparison of privacy-enhancing technologies in cryptocurrencies (part 1).

mechanism	Mixcoin	Blindcoin	TumbleBit	CoinSwap
merit	Secure assets and support auditing	Enhanced internal privacy, audit-support, low risk of leakage	Enhance internal privacy	Enhance asset security
shortcoming	The cost of mixing is high, the time overhead is high, and the risk of leakage in the mixing process is high	There are mixing fees, high computational overhead,	Costs are high and assets can be misappropriated	High fees and low mixing efficiency

Valenta et al. proposed the Blindcoin mixing mechanism based on blind signature technology. The mechanism adopts blind signature technology to ensure anonymity in the transaction process, hides the correlation between input and output addresses, and solves the problem that the input and output addresses of participants in the Mixcoin mixing mechanism are visible to third-party mixing service providers. In order to maintain the auditable nature of the MixCoin protocol, the protocol also needs to record the content of blind signatures and blind signatures in the public ledger to achieve the effect of timestamp authentication. However, this mixing mechanism still does not prevent centralized providers from abandoning their reputation and committing violations [18].

Heilmen et al. proposed the TumbleBit mixing mechanism, using Tumbler nodes to establish payment channels for mixed currency transactions, Tumbler nodes cannot obtain anonymous users' identities and transaction information, ensuring the privacy of mixed currency transaction participants, and solving the defect that centralized mixing transactions cannot guarantee internal privacy, but participants need to pay high fees, and there are also user assets embezzled [19].

CoinSwap is a centralized mixing mechanism based on hash time-locked contracts in the blockchain system, by introducing third-party users as the medium of both parties to the transaction, and at the same time limiting third-party users to steal the assets of participants with the help of hashing time-locked contracts, the two parties to the transaction can achieve the confusion of input and output addresses in a trustless environment, but the scheme needs to initiate multiple transactions to complete the mixing process, which brings additional gas fees, and the assets of both parties to the transaction take longer to unlock. This results in inefficient mixing transactions risk [20].

Decentralized currency mixing

(1) Decentralized coin mixing technology is more secure, but it requires users to find coin mixing companions and interact with other coin mixing users to construct mixed currency transactions, which is inconvenient to use.

(2) Basic model: negotiation, confusion, confirmation, and conclusion

In view of the shortcomings of the centralized mixing mechanism, Maxwell proposed the Coinjoin decentralized mixing mechanism, the main idea is to encapsulate the traditional multiple one-to-one transactions in the blockchain into a many-to-many transaction, thereby hiding the correlation between the input and output addresses of the two parties to the transaction, and fundamentally eliminating the problem of cheating by third-party providers in the centralized mixing mechanism. The CoinJoin mechanism provides a strong guarantee for the anonymity of all user transactions. This mixing mechanism, which does not rely on third-party nodes, can solve the problems of fund theft and mixing fees in centralized mixing schemes from the root. However, there is a problem that it is vulnerable to denial-of-service attacks or the privacy of other nodes is leaked.

Proposed a decentralized mixing mechanism CoinShuffle, which improves the input and output address transmission process in mixed currency transactions, and hides the association relationship of input and output addresses through multi-layer encryption to ensure internal privacy in the transaction process. As shown in Table 2. On the basis of CoinJoin, a mechanism for shuffling the output address has been added, so that mixed participants cannot obtain transaction address associations other than

DOI: 10.54254/2755-2721/19/20231020

themselves. This solution provides internal privacy and inherits the external privacy of the Coinjoin mechanism, but it also leads to large computing power consumption and low efficiency.

Table 2. Comparison of privacy-enhancing technologies in cryptocurrencies (part 2).

Mechanism	Coinjoin	CoinShuffle	Coinparty	Monero
merit	Enhanced external privacy, no cost, no risk of theft	Enhanced internal privacy, no fee, no risk of theft	Enhanced internal privacy, no fee, no risk of theft,	Enhanced internal privacy, no fee, no risk of theft, low risk of denial of service
shortcoming	The risk of denial of service is high and there is a certain risk of privacy leakage	Denial of service is risky and requires participants to be online at the same time	There is a certain risk of refusal of service and the length of the transaction	Ring signatures incur additional computational overhead

Ziegeldorf et al. proposed the Coinparty mixing mechanism in 2015, which adopts secure multi-party computing technology to protect the input and output addresses of participants in mixed currency transactions, and realizes secure and anonymous address confusion between participants by simulating a trusted third party. In CoinParty, trusted third parties are simulated by secure multi-party computing, and the mixing process is still valid even if some of the mixed coins participate in the malicious operation or invalidation of the nodes. The obfuscation mechanism does not require obfuscation fees, but the increase in computation results in more mixing transaction times.

Monero's mixing mechanism adopts ring encryption and anonymity technology, so that mixed-currency participants do not need to communicate with other participating nodes and can participate in hashing themselves, providing effective defenses against common denial-of-service attacks in decentralized hashing mechanisms and information leakage through user hashing.

4.3. Lightning network technology

Private data encryption authorizes accessTraditional blockchains have the following shortcomings:

(1) The transaction is transparent and visible to any user.

(2) The block size is small, which is not suitable for storing a large amount of data on the chain.

(3) The use of traditional symmetric encryption can only support one-to-one secure transmission.

In view of the above shortcomings, scholars propose to use attribute encryption to store data to achieve one-to-many secure transmission of data. It can solve the problem of key leakage, and there are already multiple implementations of it.

In terms of traceability, Liu and Cao proposed the black box traceable CP-ABE system, which for the first time achieved adaptive security at the same time, and the system's achievement in traceability has reached the current best level.

In addition, Zhou and Cao realized multi-level privacy protection of encrypted electronic medical records, and produced a multi-institution attribute base secret scheme that meets both the traceability and disseminable properties of white boxes.

Ledger segregation： In order to ensure the data privacy security of the network layer, the researchers propose a channel mechanism to achieve ledger data isolation. Channel isolation is implemented in the permissionless chain, and transactions are moved off-chain. For the permission chain, channel isolation is mainly used in the consortium chain, where different consortium members belong to different channels, and the channel isolation technology makes the data only visible to the nodes in the channel.

Traditional Bitcoin transactions require high transaction fees and long transaction times, are not suitable for high-frequency micropayments, and are easy to leak transaction information. Hence the development of Lightning Network technology. The Lightning Network runs under the blockchain chain and can realize high-frequency micropayments, and transaction information is not recorded on the blockchain. When making a transaction, first create a new transaction, open a two-way payment channel, record the ledger on the channel between the two parties, and update the ledger in time when assets change. After the transaction is over, both parties to the transaction need to sign the transaction with the private key to send the balance of both parties to the blockchain. This process is a single-channel payment, where both parties to the transaction transact directly through the channel. The off-chain transaction scheme of Lightning Network technology realizes high-frequency micro-transactions, which not only ensures the privacy of users, but also reduces transaction pressure and enhances the scalability of the blockchain.

5. Conclusion

There are still some flaws in the mixing mechanism of blockchain. While blockchain technology continues to develop, further research on the mixing mechanism is needed. It is important to ensure the safety of mixing coins by adopting cryptographic algorithms, such as zero-knowledge proof mechanisms and homomorphic encryption mechanisms. In future research, a more secure and efficient cryptographic scheme is needed to ensure the application of the blending mechanism. The coin mixing mechanism protected by cryptographic algorithms needs to fully consider the shortcomings of the blockchain server in computing performance and storage performance, and also need to focus on how to avoid or reduce the modification of the underlying protocol of the blockchain, so that the safe and efficient coin mixing mechanism is easier to implement and promote.

For blockchain technology, cryptographic security technology provides the necessary prerequisites, if the cryptographic technology used by the system is cracked, the security and privacy of the system based on it will be challenged, so more reliable cryptographic security technology is needed; To achieve large-scale application of blockchain technology, mature cross-chain technology is required as a bridge between different blockchain platforms, and more efficient privacy protection algorithms are required. The degree of supervision of blockchain technology by government departments will directly affect its development prospects, and only by finding the right balance between technology and government regulatory standards can we promote technological development and practical landing.

References

[1] Zyskind, G., Nathan, O., Pentland, A., et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of IEEE Symposium on Security and Privacy (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27

[2] Ibraimi, L., Tang, Q., Hartel, P. H., et al. (2009). Efficient and provable secure ciphertext-policy attribute-based encryption schemes. In Information Security Practice and Experience-ISPEC 2009 (pp. 1-12). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-00843-6_1

[3] Bethencourt, J., Sahai, A., Waters, B., et al. (2007). Ciphertext-policy attribute-based encryption. In Proceedings of IEEE Symposium on Security and Privacy (pp. 321-334). IEEE. https://doi.org/10.1109/SP.2007.11

[4] Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Advances in Cryptology-EUROCRYPT 2005 (pp. 457-473). Springer Berlin Heidelberg. https://doi.org/10.1007/11426639_27

[5] Pirretti, M., Traynor, P., McDaniel, P., et al. (2010). Secure attribute-based systems. Journal of Computer Security, 18(5), 799-837. https://doi.org/10.3233/JCS-2009-0383

[6] Wu, X., Jiang, R., Bhargava, B., et al. (2017). On the security of data access control for multiauthority cloud storage systems. IEEE Transactions on Services Computing, 10(2), 258-272. https://doi.org/10.1109/TSC.2015.2441698

[7] Zhu, L. H., Dong, H., & Shen, M. (2018). Privacy protection mechanism for blockchain

transaction data. Big Data Research, 4(1), 46-56.

[8] Abe, R. (2019). Blockchain Storage Load Balancing Among DHT Clustered Nodes [Dissertation, Keio University]. arXiv:1902.02174.

[9] Sethia, D., Saran, H., Gupta, D., et al. (2018). CP-ABE for selective access with scalable revocation: A case study for mobile-based health folder. International Journal of Network Security, 20(4), 689-701. https://doi.org/10.6633/IJNS.201807.20(4).11

[10] Stoica, I., Morris, R., Liben-Nowell, D., et al. (2003). Chord: A scalable peer-to-peer lookup protocol for Internet applications. IEEE/ACM Transactions on Networking, 11(1), 17-32. https://doi.org/10.1109/TNET.2002.808407

[11] Hassanzadeh-Nazarabadi, Y., Kupcu, A., Ozkasap, O., et al. (2019). LightChain: A DHT-based blockchain for resource-constrained environments. arXiv: Distributed, Parallel, and Cluster Computing. https://doi.org/10.13140/RG.2.2.34796.6208

[12] Liu, Z., Chan, A., Guo, Y., et al. (2018). A survey on blockchain: Techniques, applications, and future research directions. IEEE Access, 6, 62093-62110. https://doi.org/10.1109/ACCESS.2018.2872774

[13] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. In Principles of Security and Trust (pp. 164-186). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54455-6_8

[14] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

[15] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

[16] Miers, I., Garman, C., Green, M., et al. (2013). Zerocoin: Anonymous distributed e-cash from Bitcoin. In 2013 IEEE Symposium on Security and Privacy (pp. 397-411). IEEE. https://doi.org/10.1109/SP.2013.34

[17] Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). Zerocoin: Anonymous distributed e-cash from bitcoin. In 2013 IEEE Symposium on Security and Privacy (pp. 397-411). IEEE.

[18] Valenta, L., & Rowan, B. (2015). Blindcoin: Blinded, accountable mixes for bitcoin. In Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers (pp. 112-126). Springer Berlin Heidelberg.

[19] Glaeser N, Maffei M, Malavolta G, et al. Foundations of coin mixing services[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 1259-1273.

[20] Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084-2123.