Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 6196872, 7 pages
https://doi.org/10.1155/2023/6196872

Research Article

Research on Privacy Protection of Technology Service Transactions Based on Blockchain and Zero-Knowledge Proof

Jialin Zhu, Wenlong Feng, Wang Zhong, Mengxing Huang, and Siling Feng

School of Information and Communication Engineering, Hainan University, Haikou 570228, China

Correspondence should be addressed to Wenlong Feng; fwlfwl@163.com

Received 1 July 2022; Revised 3 February 2023; Accepted 6 February 2023; Published 16 February 2023

Academic Editor: Junaid Shuja

In view of the problem that the transaction privacy in the current blockchain technology service is easy to be leaked, a bulletproof alliance chain technology service transaction privacy protection mechanism is proposed. Firstly, this paper uses digital certificates as access mechanisms and stores them on the chain to ensure that the identity of technical service transactions is trusted. Secondly, the transaction data of the technical service user is hidden in the Pedersen commitment, and the Bulletproof is used to build the scope proof. Enable the verifier to conduct confidential verification of the legitimacy of the transaction without obtaining the sensitive information of the transaction, so as to ensure that the user's transaction privacy is not disclosed. Finally, the security and privacy of the proposed privacy protection scheme are analyzed, and the comparison with other zero-knowledge proof schemes shows that the scheme has the advantages of strong privacy, scalability, and low storage cost.

1. Introduction

The concept of blockchain was first proposed in *Bitcoin: A Peer-to-Peer Electronic Cash System* published by Satoshi Nakamoto in 2008 [1]. Blockchain technology is mainly composed of distributed storage, consensus mechanism, smart contract, and cryptography. It shows great promise in reducing the drawbacks of traditional centralized platforms and achieving credible data management. As an emerging technology with great potential, blockchain technology has broad application prospects in the fields of digital currency [2], medical care, Internet of Things [3], and supply chain [4].

The privacy protection of blockchain has been one of the research hotspots in recent years. In 2020, literature [5] proposed a decentralized authentication approach based on blockchain to guarantee the trustworthiness of medical data and the privacy of related users. In 2021, literature [6] proposed an anonymous identity authentication scheme to achieve privacy protection and mutual authentication between EV, charging station, and data center. In 2022, literature [7] proposed a blockchain node traceable identity privacy technology scheme based on edge computing, which ensured security and realized privacy protection. However, the above related work only discussed the identity privacy protection of blockchain, without considering the data privacy protection of transactions. Additionally, most of the existing technology service platforms are based on the centralized architecture. The authenticity and originality of the technology service data mainly depend on the trust of the system center or the third-party entities [8–10]. Once the system center is no longer trusted, the authenticity and security of the data will be difficult to be guaranteed.

Based on the above research, it is urgent to find a decentralized technology service platform that can meet the requirements of privacy security of users and confidentiality of transaction data. The technology service has high intellectual property attributes. It requires that the specific data of the transaction can be kept confidential while the transaction records are stored in the blockchain. Compared with another zero-knowledge proof technologies, bulletproof has shorter proof length and smaller time complexity. Moreover, it does not rely on trusted setup. So, it can be selected to protect the privacy of transaction data in technology services.

Therefore, this paper uses the blockchain to store digital certificates to achieve identity trustworthy management and introduces bulletproof technology to improve the confidentiality of blockchain transactions. The main contribution of the paper is as follows.

(i) A digital certificate model based on blockchain is proposed to protect the identity privacy of technology service transactions

(ii) Introducing bulletproof to realize the privacy protection of technology service transaction data

(iii) Privacy, security, and scalability are improved, and storage costs are lower

The remainder of this paper is organized as follows: the second section provides a literature review on the use of zero-knowledge proof technology to improve blockchain privacy protection. The third section presents privacy protection scheme of technology service transaction based on bulletproof. The fourth section compares the zero-knowledge proof privacy protection scheme proposed in this paper with other schemes from the perspective of security and privacy and performance. Finally, the fourth section gives the conclusion of this paper.

2. Related Work

The blockchain itself is a transparent public ledger, and the details of transactions can only be stored after verification by consensus nodes, which shows that the confidentiality of the blockchain itself is a big hidden problem. To improve the confidentiality of blockchain, adding zero-knowledge proof technology is one of the focuses of many researchers in recent years [11–13]. Literature [14] adds zero-knowledge proof to the blockchain environment to authenticate members and disclose or anonymize them through decentralized identifiers to solve the privacy problem. Literature [15] proposes an anonymous hidden transaction model based on the blockchain by modifying the original blockchain transaction script and combining with the zero-knowledge proof mechanism, which can effectively protect the transaction user information. Literature [16] designed a digital identity management system using smart contracts and zero-knowledge proof. It adopts the framework of off-chain computation and on-chain verification, which effectively prevents the exposure of ownership between user entities and attributes in distributed ledgers, and realizes privacy and security. Literature [17] achieves anonymous identity verification of electric vehicle users by applying zero-knowledge proof to blockchain. Literature [18] proposes a blockchain-based zero-knowledge proof scheme for identity verification by improving the classical zk-SNARK scheme to ensure the authenticity and privacy of uploaded data.

To sum up, most of the privacy protection studies of zero-knowledge proof are about identity anonymization. Few of them are dedicated to the privacy protection of transaction data. The comparison of the zero-knowledge proof researches of blockchain privacy protection are mentioned in Table 1. As shown in the table, bulletproof has the best comprehensive performance. Therefore, this paper selects bulletproof [19] to realize the protection of transaction privacy.

Table 1: Comparison of the zero-knowledge proof researches of blockchain privacy protection.

Papers	Method	Proof size	Time complexity	Trusted setup
[16]	zk-stark	Long	$O(n)$	No
[17]	AZTEC	Medium	$O(n \lg n)$	Yes
[18]	zk-snark	Medium	$O(n \lg n)$	Yes
[19]	Bulletproof	Short	$O(4 \lg n)$	No

3. Privacy Protection Scheme of Technology Service Transaction Based on Zero-Knowledge Proof

3.1. Design of Technology Service Architecture Based on Alliance Chain. Alliance chain refers to the blockchain used within a certain group or organization, which has certain restrictions and requirements on participating organizations and units. It not only realizes the functions of blockchain distributed ledger, consensus algorithm, and antitampering but also achieves the access mechanism. Exactly, technology service transactions are generally carried out between enterprises or schools and enterprises, and not all of them have bookkeeping rights. In the meantime, they have high property rights and high requirements for privacy and confidentiality, which are highly compatible with the alliance chain. Therefore, this paper selects the alliance chain as the underlying blockchain and uses the CA agency to review the identity information of technology service users as the access mechanism of the technology service platform to ensure the credibility of the transaction identities. It also uses the digital certificates to authenticate the identity of both parties in technology services when users conduct technology service transactions, while adding Pedersen commitment and zero-knowledge proof encrypts and verifies the specific information of the transaction.

In order to solve the problem of single point of failure in the traditional technology service-centralized system and ensure that only legitimate users have the right to use the platform functions, the distributed decentralization and high reliability of blockchain are used to manage the trusted identity authentication of the roles of technology service demander, technology service provider, and technology service platform. The identity authentication management model based on the alliance chain in this study is shown in Figure 1, which mainly consists of ordinary users, CA agency, regulator, and blockchain. First, ordinary users are divided into technology service providers and demanders and upload their respective information to the regulator, which is responsible for auditing the identity information uploaded by ordinary users. It initially verifies whether the uploaded information is complete and whether the data format is correct and then uploads the audited user information to the CA agency. Then, the CA agency conducts a second

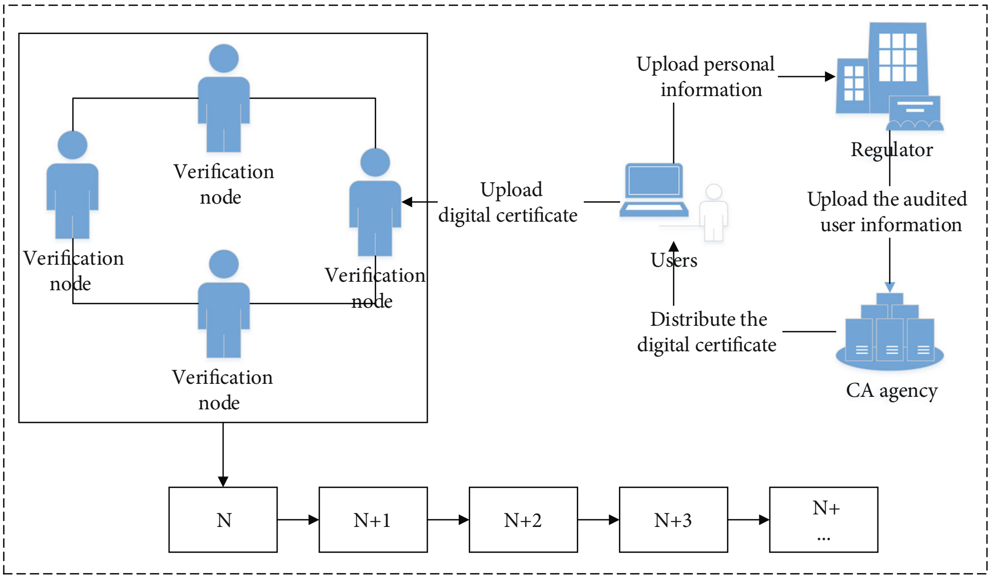
Verification node
Verification node
Verification node
Verification node
Upload digital certificate
Upload personal information
Regulator
Users
Upload the audited user information
Distribute the digital certificate
CA agency
N
N+1
N+2
N+3
N+ ...

Figure 1: Identity authentication management model based on alliance chain.

review of the user information and distributes the digital certificate to the users who have passed the review. The user uploads the digital certificate to the verification node for consensus. Finally, the consensus-certified digital certificate is packaged into a block and stored in the blockchain, which can effectively prevent the loss and tampering of the digital certificate.

3.2. Technology Service Privacy Protection Scheme. To achieve transaction security and privacy protection between the technology service provider and the technology service demander in the technology service system, this study integrates blockchain, technology service user, smart contract, and zero-knowledge proof to construct a privacy protection scheme for technology services. As shown in Figure 2, the blockchain-based zero-knowledge proof privacy protection scheme for technology services consists of CA organization, technology service demanders, technology service providers, smart contract, and blockchain. The functions are as follows:

(1) CA: issue digital certificates to users

(2) Technology service demanders: publish technology service demand

(3) Technology service providers: provide technology services and make reasonable use of the technology services they own for profit

(4) Smart contract: preset trigger conditions to judge the correctness of zero-knowledge proof

(5) Blockchain: the alliance chain is adopted to realize the trusted identity management of the technology service platform, and zero-knowledge verification of transaction information across the network using consensus algorithms to achieve transaction storage on the chain

The blockchain-based technology service privacy protection scheme is shown in Figure 2. First, the technology service platform distributes digital certificates to each successfully registered user for identity authentication, and both sides of the technology service transaction verify the authenticity of each other's identity through the digital certificates. Then, the peer-to-peer technology service transaction is carried out in the blockchain network, and the specific data of the transaction is packaged and encrypted after the transaction is completed. After that, both parties (the prover) of the technology service transaction use Pedersen promise to hide the transaction data. Then, use the bulletproof algorithm to generate zero-knowledge proof and sent it to the smart contract, which verifies the authenticity of the commitment and the legitimacy of the transaction data. Finally, if the verification is passed, the transaction is successful, and a new block is generated. Otherwise, the transaction fails.

3.3. Zero-Knowledge Proof Realizes Transaction Privacy Protection

3.3.1. Pedersen Commitment. Pedersen commitment is a perfectly hidden, computationally bound commitment protocol that meets the needs of confidential transactions (CT). When the two parties of the technology service conduct a transaction, the transaction data is replaced with the Pedersen commitment without displaying the specific information of the transaction. Other nodes cannot artificially modify the transaction data in the Pedersen commitment, because only the original value when constructing the Pedersen commitment can satisfy the mathematical operations involved. The detailed steps for hiding the transaction data of the technology services using Pedersen commitments are as follows.

(Step 1) Set the transaction data of both sides of the technology service as v; multiply it with a

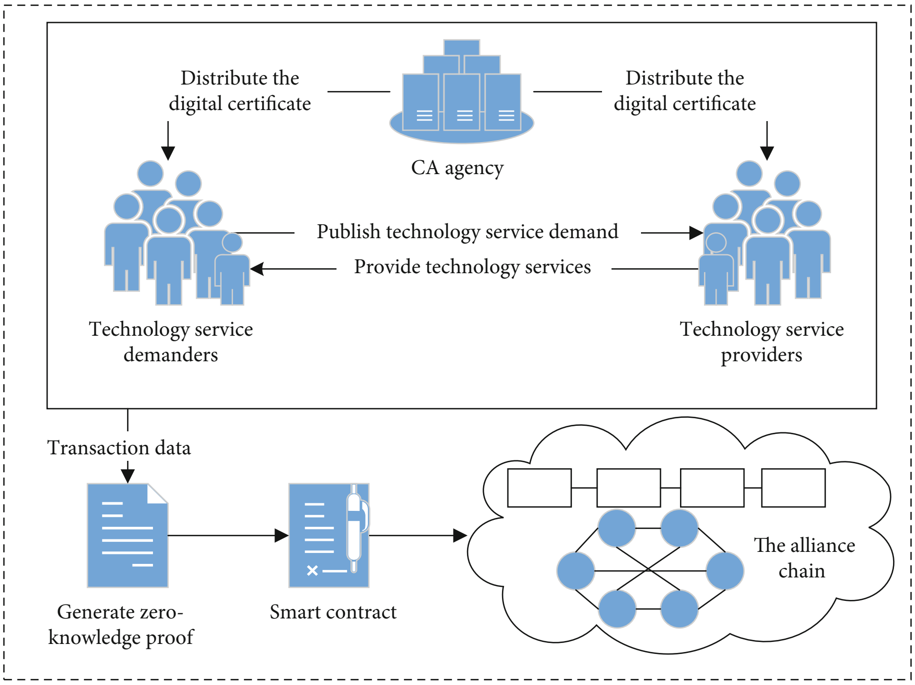
Distribute the digital certificate
CA agency
Distribute the digital certificate
Publish technology service demand
Provide technology services
Technology service demanders
Technology service providers
Transaction data
Generate zero-knowledge proof
Smart contract
The alliance chain

Figure 2: Blockchain-based privacy protection scheme for technology services.

generator point G on the additive group of the elliptic curve, denoted as $v * G$

(Step 2) Select a random number r as the blinding factor and multiply it with a random base point H on the additive group of elliptic curves, denoted as $r * H$

(Step 3) Generate a promise $\mathrm{Com} = v * G + r * H$ and send it to the validation node in the blockchain for verification, whereby the transaction data v is hidden in the promise

Pedersen commitment has two phases, commitment generation and commitment disclosure. The commitment generation process is to input a plain text value v and a random blinding factor r, and then, a commitment Com to v can be returned. The commitment verification process is to verify whether the commitment Com is truly bound to the value v it claims to be bound to. The commitment generation and verification process is shown in Figure 3.

3.3.2. Bulletproof. Pedersen commitment can only hide the transaction value without any restriction on the arithmetic result, while technology services require a nonnegative transaction result. Therefore, this paper introduces bulletproof to prove that the promised transaction data is within the allowable range without revealing any information. Bulletproof, as a relatively advanced noninteractive zero-knowledge proof technique in recent years, its biggest feature is that it provides native support for submitted values such as Pedersen commitments and public keys and can perform scope proofs in this general zero-knowledge proof framework without requiring installing large and complex elliptic curve arithmetic in it.

The zero-knowledge proof mechanism based on blockchain using bulletproof to achieve privacy of technology service transactions is shown in Figure 4, which is divided into three main parts: client, proof generation phase, and proof verification phase. The transaction is initiated by the client, and the transaction data of the tech service user is hidden using Pedersen commitment, denoted as $\mathrm{com}(r, v)$. In the meantime, adding zero-knowledge rangeproof ensures the legitimacy of transaction data. Then, the relevant promises and proofs are sent to the smart contract, which can verify the correctness of the transaction. Finally, the successfully verified transaction data are deposited into a new block for on-chain storage.

3.3.3. Realization of Technology Service Transaction Process. The realization process of technology service transaction based on blockchain and zero-knowledge proof designed in this paper is shown in Figure 5. The specific steps for the realization of technology service transactions are as follows.

(Step 1) The information m_0 consists of the Pedersen commitment $\mathrm{com}(r_0, v_0)$ of the initial amount of the technology service demander p_i and the scope proof rangeproof (v_0) generated by bulletproof. The demander of the technology service r_i initiates a transaction request with the transaction amount of v_1 from the technology service provider p_j

(Step 2) After receiving the transaction request, the technology service provider first confirms

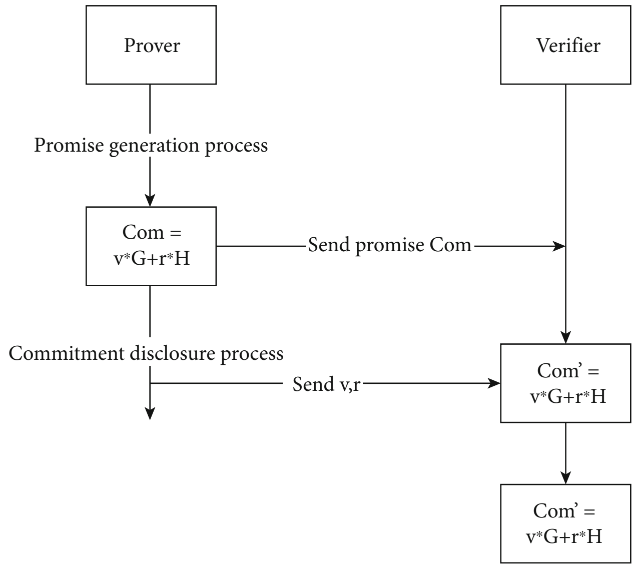

Figure 3: Pedersen commitment generation and verification process.

whether the identity of the counterparty is correct by checking the digital certificate of the demander of the technology service p_i and then generates a random number, and then, the transaction commitment then generates a random number r_1. After that, it sends the information m_1 consisting of the transaction commitment $\text{com}(r_1, v_1)$ and rangeproof (v_1) generated by bulletproof to the demander of technology services p_i

(Step 3) After receiving the reply, the demander of technology services p_i calculates the current account balance $v_2 = v_0 - v_1$ and generates a random number $r_2 = r_0 - r_1$. Then, it composes the generated Pedersen commitment $\text{com}(r_2, v_2)$ and the scope proof rangeproof (v_2) into a message m_2. Meanwhile, it sends the three parts of information input1, output1, and output2 generated by m_0 and m_1 and m_2 to the smart contract for verification

(Step 4) The smart contract checks the correctness of the transaction. It mainly includes the following aspects: whether the input is consistent with the initial balance before the account transaction; whether the range proof of the transaction output is correct; whether the sum of the input of the transaction is equal to the sum of the transaction outputs, that is, whether it is satisfied $\text{com}(r_0, v_0) = \text{com}(r_1, v_1) + \text{com}(r_2, v_2)$

(Step 5) If the smart contract checks out, it will broadcast this transaction to the whole network, and other nodes of the blockchain will conduct consensus verification. If the verification is passed, the packaged and encrypted technology service transaction data will be stored in a new block, and the transaction will be completed. Otherwise, the transaction fails

As a result, the transaction information seen by other nodes of the blockchain exists in the form of commitment proof, and no plaintext of any transaction data is disclosed in the whole process, which shows that user privacy is protected in the transaction.

4. Analysis and Evaluation

Based on the above description, this section is mainly about analysis and experiment. It mainly analyzes security and privacy. The client operating environment is Ubuntu 16.04 (64 bit), Intel Core i5-1135G7@2.40 GHz, 16 G RAM. This experiment uses the underlying platform of Hyperleger Fabric for testing and GO language for programming language.

4.1. Security and Privacy Analysis. First of all, the identity authentication mechanism of the traditional technology service platform based on centralized management has the risk of privacy leakage. In this paper, the alliance chain is used to manage the identity of technology service users by using the issuance of digital certificates as the access mechanism of the technology service platform. The digital certificates is stored on the blockchain to prevent loss and tampering, effectively avoiding the single point of failure problem in the traditional identity authentication method. Secondly, the transaction data in the scheme proposed in this paper are stored in the block in the form of committed values. Users other than both sides of the transaction will not know the specific transaction information, thus ensuring the privacy of the transaction. The Pedersen commitment used in the scheme provides the privacy of the transaction data by introducing a random blinding factor r. Even if the privacy data v remains unchanged, the final commitment Com will change with r. Moreover, since the Pedersen commitment is based on the elliptic curve discretization problem, it is almost impossible to reverse the known commitment Com and elliptic curve points G and H to solve for the data v and r, thus providing the steganography of the transaction data. Finally, the scope proof of hidden transaction information is achieved by adding bulletproof, where the verifier can verify the legitimacy of the transaction data through zero-knowledge proofs, but cannot obtain the secret value according to the commitment and known parameters.

It can be seen that the access mechanism of the alliance chain ensures that the users of technology services who join are authentic and trustworthy, thereby guaranteeing the security of transactions between the technology service users. The addition of bulletproof can hide the specific transaction information of both parties of the technology service transaction, which can effectively prevent the leakage of transaction information, thus guaranteeing the privacy of technology service transactions.

4.2. Performance Analysis. The performance of the scheme in this paper is mainly compared and analyzed with the scheme of literatures [16–18, 20–22]. Performance parameters mainly refer to literature [23]. As shown in Table 2, it

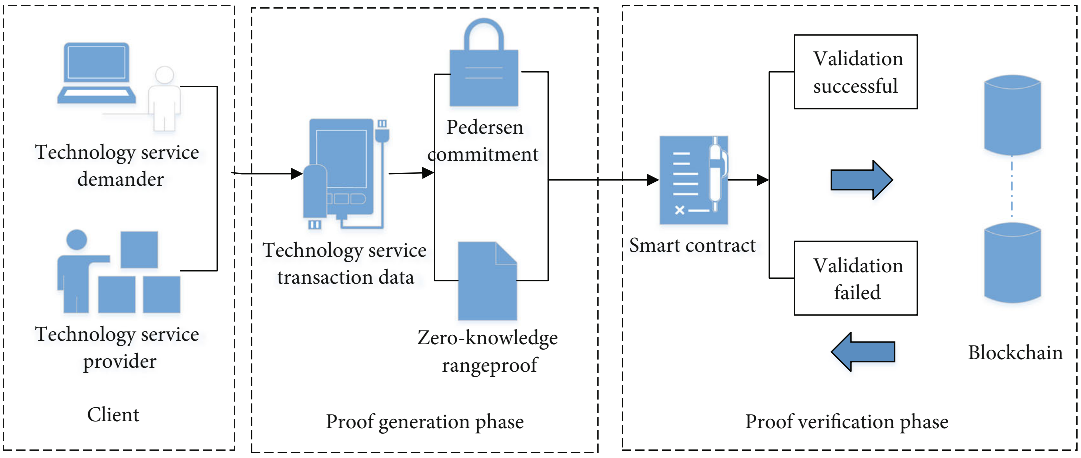

Figure 4: Zero-knowledge proof implementation mechanism.

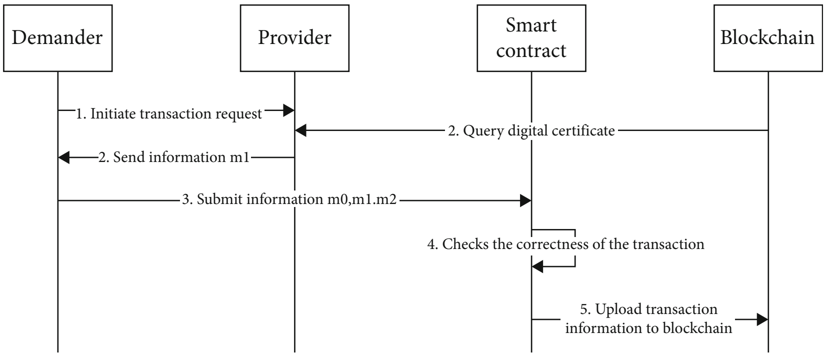
Demander
Provider
Smart contract
Blockchain
1. Initiate transaction request
2. Query digital certificate
2. Send information m1
3. Submit information m0,m1.m2
4. Checks the correctness of the transaction
5. Upload transaction information to blockchain

Figure 5: Technology service transaction process.

Table 2: Comparison of time complexity in different schemes.

Schemes	Privacy	Scalability	On-chain computability	Storage overhead
[16]	Poor	Strong	Strong	High
[17]	Neutral	Strong	Poor	Low
[18]	Poor	Neutral	Neutral	Low
[20]	Strong	Neutral	Strong	Low
[21]	Strong	Neutral	Strong	Low
[22]	Poor	Neutral	Neutral	Low
This paper	Strong	Strong	Neutral	Low

mainly compares privacy, scalability, on-chain computability, and storage overhead. It can be seen that the scheme proposed in this paper does not sacrifice its scalability while improving privacy. Moreover, it can reduce the storage cost.

5. Conclusions

This paper is based on the issue of blockchain privacy security. The zero-knowledge proof technology in various blockchains and its corresponding scheme applications are described. To solve the problem of transaction privacy in technology services, this paper proposes a privacy protection scheme for technology service transaction based on blockchain and bulletproof. The blockchain stores digital certificates to ensure the identity privacy of technology service users. At the same time, bulletproof is introduced into blockchain technology service transactions to hide the specific information of transaction data. Finally, the comparative analysis shows that the proposed scheme has the advantages of strong privacy, scalability, and low storage cost.

In the future work, it is necessary to fully apply zero-knowledge proof to the blockchain platform to improve the privacy and security of the blockchain. Although the performance of the bulletproof used in this paper is optimized relative to other zero-knowledge proof methods, the verification operation of its smart contract is relatively complicated, and there is still a problem of high computational cost in application. Therefore, future work will focus on improving the algorithm of bulletproof to meet the needs of efficient verification of blockchain smart contracts.

Data Availability

The data used to support the finding of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Project under grant 2018YFB1404400. This work was supported by the Major Science and Technology Project of Haikou under grant 2020-009. This work was supported by the Key R&D Project of Hainan Province under grant ZDYF2021SHFZ243.

References

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Bitcoin White Paper*, 2008.

[2] R. Chen, F. Shu, S. Huang et al., "BIdM: A Blockchain-Enabled Cross-Domain Identity Management System," *Journal of Communications and Information Networks*, vol. 6, no. 1, pp. 44–57, 2021.

[3] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, and R. Sharma, "Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G," *Journal of Information Security and Applications*, vol. 67, p. 103179, 2022.

[4] D. Ravi, S. Ramachandran, R. Vignesh, V. R. Falmari, and M. Brindha, "Privacy preserving transparent supply chain management through Hyperledger Fabric," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100072, 2022.

[5] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.

[6] Q. L. Liu and C. C. Chen, "Blockchain-based V2G anonymous authentication scheme," *Computer Engineering*, vol. 47, no. 11, p. 7, 2021.

[7] B. Gong, C. Cui, M. Hu, C. Guo, X. Li, and Y. Ren, "Anonymous traceability protocol based on group signature for blockchain," *Future Generation Computer Systems*, vol. 127, pp. 160–167, 2022.

[8] M. Qingtao and L. Qian, "Research hotspots of science and technology service industry and its development trend based on CiteSpace," *Science and Management*, vol. 40, no. 4, p. 7, 2020.

[9] L. Zhang, X. Hao, Y. Zhang, and Y. Wang, "Research on the industrial economic development driving by scientific and technological service system innovation," *E3S Web of Conferences*, vol. 235, p. 02008, 2021.

[10] X. Chen, G. Huang, Y. Zhang, and J. Li, "Research on service value chain model based on technology service platform," *Journal of Physics: Conference Series*, vol. 2078, no. 1, p. 012043, 2021.

[11] D. Wang, J. Zhao, and Y. Wang, "A survey on privacy protection of blockchain: the technology and application," *IEEE Access*, vol. 8, pp. 108766–108781, 2020.

[12] X. Li, C. Xu, and Q. Zhao, "Shellproof: more efficient zero-knowledge proofs for confidential transactions in blockchain," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Toronto, ON, Canada, May 2020.

[13] S. Ma, Y. Deng, D. He, J. Zhang, and X. Xie, "An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 641–651, 2021.

[14] L. Lourinho, S. Kendzierskyj, and H. Jahankhani, "Securing the digital witness identity using blockchain and zero-knowledge proofs," in *Strategy, Leadership, and AI in the Cyber Ecosystem*, pp. 159–194, Strategy, Leadership, and AI in the Cyber Ecosystem, 2021.

[15] J. Zhang, G. Zhou, J. Wang, and L. Huang, "Anonymous hidden transaction model for blockchain systems," in *2021 IEEE Region 10 Symposium (TENSYMP)*, Jeju, Republic of Korea, August 2021.

[16] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Computers & Security*, vol. 99, p. 102050, 2020.

[17] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020.

[18] Z. Wan, Z. Guan, Y. Zhou, and K. Ren, "zk-AuthFeed: how to feed authenticated data into smart contract with zero knowledge," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, July 2019.

[19] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: short proofs for confidential transactions and more," in *2018 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 2018.

[20] M. Maller, S. Bowe, M. Kohlweiss, and S. Meiklejohn, "Sonic: zero-knowledge SNARKs from linear-size universal and updatable structured reference strings," in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, UK, November 2019.

[21] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, May 2016.

[22] C. Donglin, T. Yixian, N. Planning, and W. Qian, "Data confidentiality mechanism of science and technology service transactions based on zero-knowledge proof," *Science and Technology Management Research*, vol. 41, no. 20, pp. 80–86, 2021.

[23] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, N. A. A. Bakar, and N. Maarop, "Performance evaluation of DLT systems based on Hyperledger Fabric," in *2022 4th International Conference on Smart Sensors and Application (ICSSA)*, pp. 70–75, Kuala Lumpur, Malaysia, July 2022.