Service and Technology Transaction Framework and Confidentially Mechanism Based on Blockchain

Junxue Zhou[1,a], Donglin Chen[1,b], Min Fu[1,c,*]

[1]*Institute of Economics, Wuhan University of Technology, Hongshan Street, Wuhan, China*
a. 79501909@qq.com, b. chendl@whut.edu.cn, c. 728609236@qq.com
**corresponding author*

Abstract: The science and technology service industry is an indispensable part of the innovation system. Since the science and technology service transaction is platform dependent, they have the drawbacks of centralized transactions. As these services involve intellectual property, it is critical to preserve the confidentiality of transaction information. To address this issue, this study builds a science and technology service framework, which includes a provider and a demander, data temporary storage, timestamp and confidentiality verification, followed by the construction of a confidentiality mechanism for science and technology service transactions based on zero-knowledge proof technology. This mechanism can decentralize science and technology service transactions and keep the information of both parties confidential, which can promote the effective circulation of science and technology information. Finally, from the perspectives of economic value, industrial value, and commercial value, this study analyzes the value of combining blockchain with technology service transactions, considering the practical significance in promoting the development of scientific and technological services.

Keywords: Privacy Mechanism, Science and Technology Service Platform, Confidentially Mechanism, Zero Knowledge Proof, Blockchain

1. Introduction

With the deep integration of science and technology, the science and technology service industry has emerged as a new force, gradually realizing the professional development while achieving consistent growth. The science and technology service is a source of innovation activities, and increasingly being hailed as the “second knowledge infrastructure” [1]. The industry is a source of knowledge for innovative enterprises and has significantly contributed to regional innovation [2]. Thus, the science and technology service industry is an indispensable part of the innovation system [3]. It has become an important parameter for measuring the innovation ability of a region or country in the era of the knowledge economy.

The science and technology services industry is formed by the deep integration of science and technology with the service industry, and it’s a supporting industry and an important symbol of modern science and technology development [4]. With science and technology at their core, they provide efficient and convenient integrated services for social and economic activities [5]. Let us consider the example of ZBJ.com, a large science and technology service website based in China that offers “centralized” science and technology service resources and information. The demander searches for the relevant service they need on the platform or posts the problem to be solved on the platform, after which the platform receives the search application, allowing the demander to connect with the provider [6]. After the service transaction is completed, the demander evaluates and submits it, directly affecting the provider's historical evaluation. In this traditional centralized transaction mode, the transaction core relies on the platform [7], and the information data are relatively centralized [8], but affects the fairness of the transaction to a certain extent. Currently, blockchain has helped make breakthroughs in research in the fields of energy, banking, supply chain finance, and smart cities [9], with research directions including, but not limited to reputation management, digital economy, traceability, and privacy protection [10-11]. Integrating blockchain and science and technology services is expected to reduce the drawbacks of traditional centralized platforms and facilitate reliable data management. The characteristics of blockchain are highly consistent with those of the science and technology service platform, which can effectively guarantee point-to-point transactions between subjects and avoid potential leaks in information interaction [12].

2. Technology Service Transaction Framework based on Blockchain Technology

This study defines the science and technology service industry as an emerging industry that fully uses modern science and technology knowledge, analysis and research methods, modern technology, experience, information, and other elements to provide intellectual services to the public, and illustrate the technology service transaction framework based on blockchain technology in Figure 1.

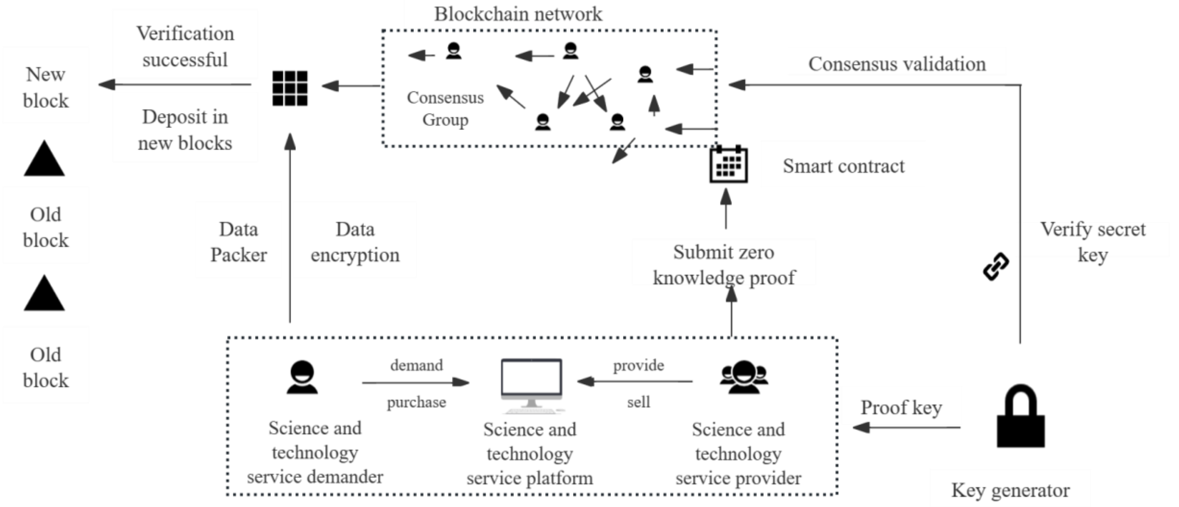

Figure 1: Service and technology transaction framework based on blockchain technology.

An science and technology service transaction includes a provider and a demander. The technology service provider uploads the available technology services to the blockchain network center and attaches relevant keywords. The system matches keywords to the demander. The technology demander can make a service query using keywords describing the required technology service, select the appropriate service provider, and then send the transaction demand to them, or send their own scientific and technological service demand to the blockchain network, where each node of the scientific and technological service provider responds to the demand and makes a quotation. As the quotation is transparent in the blockchain network, other nodes will also provide more standard pre-solutions and lower prices based on this standard. Finally, the price converges, and the demander can access the pre-solutions and make comprehensive choices based on the quality of the pre-solutions.

Data temporary storage: After the technology service transaction, both parties must package the transaction data, encrypt it with their own private key, temporarily store it in the blockchain network, and wait for other nodes to verify the transaction.

Timestamp: It is evidence that proves the existence of certain information at a given point in time. This study proposes a concept of trusted timestamp based on the decentralized transaction of science and technology services, which allows both parties of an science and technology service transaction to take a timestamp when they temporarily store the science and technology service transaction. The authenticating user can then retrieve and verify the timestamp submitted to the blockchain temporary transaction and verify the time of the transaction. This also provides a basis for transaction traceability and information tampering prevention.

Confidentiality verification: Due to the high intellectual property characteristics of science and technology services, when the consensus group verifies the transaction, it can construct a simple and non-interactive knowledge proof (commitment) based on zero knowledge of the blockchain, which can be combined with the smart contract to form a transaction mode with no one controlling the cost of trust. Thus, both parties can prove the completion of the transaction without disclosing any transaction details. Once the verification is completed, the transaction is verified throughout the network and stored in a new block.

3. Confidentially Mechanism Based on Zero-knowledge Proof Technology

3.1. Application Scenario

This study applies zero knowledge-proof technology to verify the decentralized transactions of science and technology services. Firstly, both parties involved in technology service transactions conduct end-to-end technology service transactions in the blockchain network. After the transaction is completed, in order to prevent the leakage of transaction data, both parties package and encrypt the transaction data; Then, the key generator generates new proof and verification keys for this transaction. The proof party (both parties in the technology service transaction) generates a zero knowledge proof (commitment) through the proof key and sends it to the blockchain network and smart contract. The smart contract and other nodes verify the authenticity of the proof (commitment) through the verification key; Finally, if the verification is successful, the transaction will be deposited into a new block; otherwise, it will be rejected. The above scenario emphasizes that the verification party completes the verification of the technology service transaction without contact with the transaction information, achieving data protection for both parties involved in the technology service transaction.

3.2. Provisioning Process of Zero Knowledge Proof

When the technology service trading parties conduct a transaction, the transaction amount is transferred from the demander’s account to the service provider’s account. The process of providing knowledge proof has two components (see Figure 2). The first proves that the demander’s balance before the transaction is no less than the transaction amount; the demander provides evidence. The other component involves proving that both parties’ input and output are equal and provides proof.

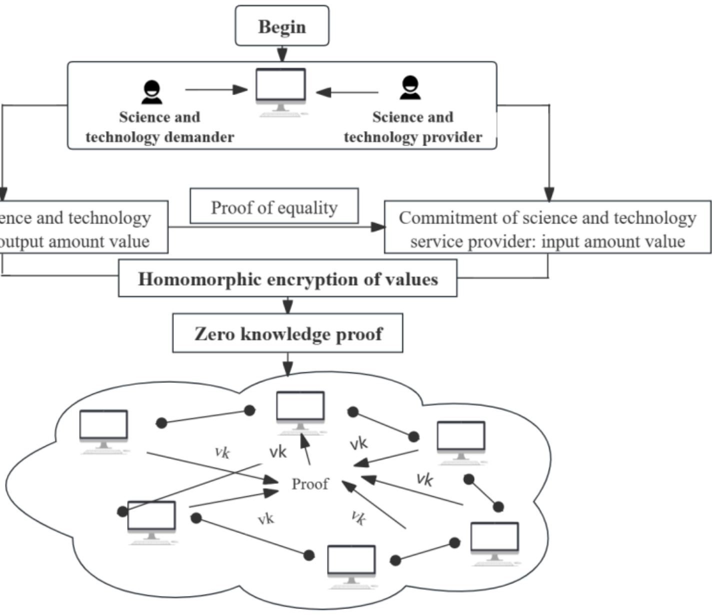
Begin
Science and technology demander
Science and technology provider
Proof of scope
Proof of equality
Commitment of science and technology service demander: output amount value
Commitment of science and technology service provider: input amount value
Homomorphic encryption of values
Zero knowledge proof
vk
Proof

Figure 2: Zero-knowledge proof process of science and technology service transaction.

3.3. Verification Process of Zero Knowledge Proof

The next process is verifying the zero-knowledge proof (see Figure 3). First, both parties of the technology service transaction (the certifier) create a smart contract. The certifier sends the smart contract and evidence to the blockchain network, with a digital signature attached, to apply for zero-knowledge verification of the technology service transaction. Other nodes also perform non-interactive zero-knowledge verification through smart contracts. After the above process, only those who pass both equality and range verifications can be saved in a new block. Otherwise, the request for data storage for science and technology service transactions is rejected.

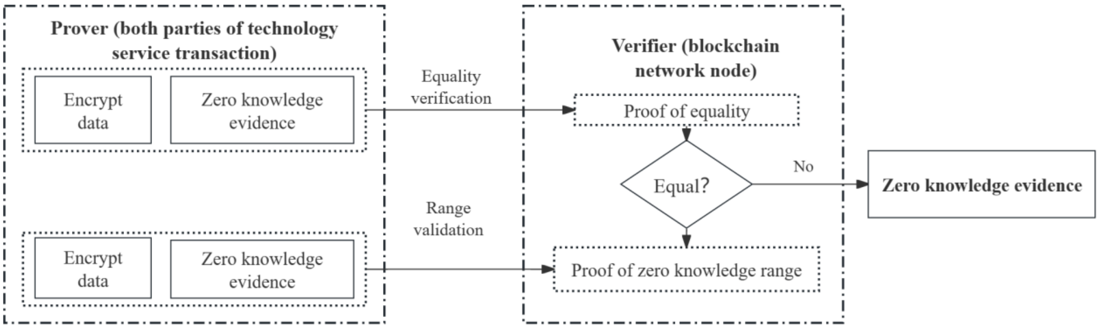

Figure 3: Zero-knowledge proof verification process.

4. Conclusion

This study constructs a confidentiality mechanism for science and technology service transactions based on zero-knowledge proof technology. This mechanism can maintain the confidentiality of science and technology service transaction information, promote the effective circulation of science and technology information, and have obvious practical significance in promoting the development of science and technology services. The combination of science and technology service transactions and blockchain technology has economic and industrial value (see Figure 4), which can be further transformed into commercial value to fuel the advancement of science and technology service transactions.

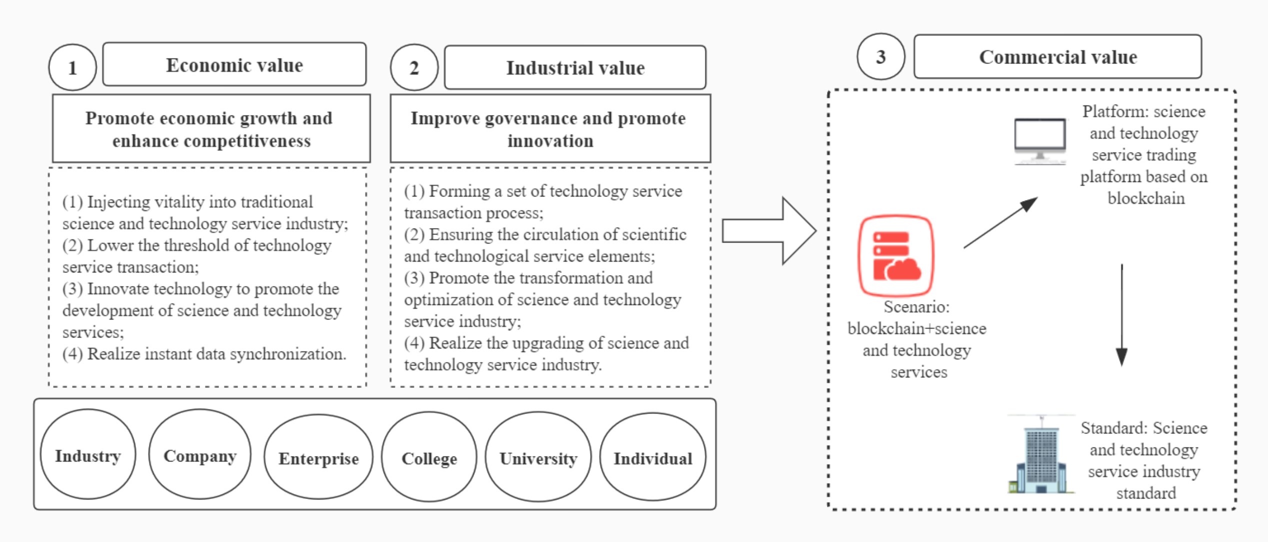
1
Economic value
Promote economic growth and enhance competitiveness
(1) Injecting vitality into traditional science and technology service industry;
(2) Lower the threshold of technology service transaction;
(3) Innovate technology to promote the development of science and technology services;
(4) Realize instant data synchronization.
2
Industrial value
Improve governance and promote innovation
(1) Forming a set of technology service transaction process;
(2) Ensuring the circulation of scientific and technological service elements;
(3) Promote the transformation and optimization of science and technology service industry;
(4) Realize the upgrading of science and technology service industry.
Industry
Company
Enterprise
College
University
Individual
3
Commercial value
Platform: science and technology service trading platform based on blockchain
Scenario: blockchain+science and technology services
Standard: Science and technology service industry standard

Figure 4: Business value of combination of technology service transaction and blockchain technology.

(1) Economic value. A combination of technology service transactions and blockchain technology can strengthen the competitiveness of technology service enterprises. Combining science and technology service transactions with blockchain technology can help achieve decentralization and information security in science and technology service transaction platforms. In this new mechanism, science and technology service transaction data are stored in the chain to achieve real-time data synchronization and in which open data can be queried, thus promoting the sharing of the data. Distributed data storage can make information transparent, verifiable, and traceable. Smart contract technology is a code set in advance that can be executed when trigger conditions are met. This can ensure the transparency of all decisions made during the transaction process and solve problems caused by differences in human operations.

(2) Industrial value. The combination of technology service transactions and blockchain technology is conducive to promoting the transformation and upgrading of the technology service industry. Blockchain technology can create a credible P2P platform for science and technology service transactions, connect the entire science and technology service industry chain and the data flow and information flow on the chain, and form a set of innovative science and technology service transaction processes. On the one hand, by connecting the upstream and downstream of the industry chain, timestamp technology enables the traceability of transactions to be traceable to prevent information tampering. On the other hand, blockchain can optimize the technology service industry.

(3) Commercial value. The combination of technology service trading and blockchain technology. That is, the combination of key fields and new technologies is conducive to the establishment of an innovative technology service industry trading platform, which would enable the formation of a technology service trading ecology and promote the integration and development of various fields of technology service.

Acknowledgements

The authors gratefully acknowledge the financial supports by the National Key R&D Program Industrial Software Key Special Project “Research and Application of Multi chain Collaborative Platform for Supply Chain of Parts in Large scale Manufacturing Industry”(No. 2022YFB3305600).

References

[1] Akbari, M.. (2021) Technological innovation research in the last six decades: A bibliometric analysis. European Journal of Innovation Management, 24(5): 1806-1831.

[2] Li, W. J.. (2021) Strategies for the high-quality development of China's mega-regions during the 14th five-year plan. Academic Research, 1: 90-96.

[3] Naveed, N.H., Yuen, C., Niyato, D.. (2019) Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions. IEEE Industrial Electronics Magazine, 14(4): 106-118.

[4] Laspia, A., Sansone, G., Landoni, P., Racanelli, D., Bartezzaglhi, E.. The organization of innovation services in Science and technology parks: Evidence from a multi-case study analysis in Europe. Technological Forecasting and Social Change, 173: 121095.

[5] Zhou, D., Kautonen, M., Wang, H.. (2016) How to interact with knowledge-intensive business services: A multiple case study of small and medium manufacturing enterprises in China. Journal of Management Organization, 23(2):297-318.

[6] Awasthy, P., Hazra, J.. (2020) Collaboration under outcome-based contracts for information technology services. European Journal of Operational Research, 286(1):350-359.

[7] Diniz, E.H., Siqueira, E.S., Heck, E.. (2019) Taxonomy of digital community currency platforms. Information Technology for Development, 25(1):69-91.

[8] Yang, L.. (2019) The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15: 80-90.

[9] Li, X., Russell, P., Mladin, C., Wang, C.G.. (2021) Blockchain-enabled applications in next-generation wireless systems: Challenges and opportunities. IEEE Wireless Communications, 28(2): 86-95.

[10] Cheng, J.R., Zhang, Y., Yuan, Y.M., Li, H., Tang, X.Y., Sheng, V.S., Hu, G.J.. (2022) PoEC: A cross-blockchain consensus mechanism for governing blockchain by blockchain. CMC-Computers Materials & Continua, 73(1): 1385-1402.

[11] Fan, X., Niu, B.N., Liu, Z.L.. (2022) Scalable blockchain storage systems: research progress and models. Computing, 104(6): 1497-1524.

[12] Wang, T.T., Zhao, C.H., Yang, Q.. (2021) Ethna: Analyzing the underlying peer-to-peer network of Ethereum blockchain. IEEE Transactions on Network Science and Engineering, 8(3):2131-2146.