Advanced Industrial SCIence
Vol. 3, No. 3, pp. 8-13, 2024
ISSN 2951-2476
https://doi.org/10.23153/AI-Science.2024.3.3.008

Research on A Comprehensive Study on Building a Zero Knowledge Proof System Model

Sunghyuck Hong
Professor, Division of Advanced IT, IoT major, Baekseok University

영지식 증명 시스템 구축 연구

홍성혁
백석대학교 첨단IT학부, IoT 전공 교수

Abstract Zero Knowledge Proof (ZKP) is an innovative decentralized technology designed to enhance the privacy and security of virtual currency transactions. By ensuring that only the necessary information is disclosed by the transaction provider, ZKP protects the confidentiality of all parties involved. This ensures that both the identity of the transacting parties and the transaction value remain confidential.ZKP not only provides a robust privacy function by concealing the identities and values involved in blockchain transactions but also facilitates the exchange of money between parties without the need to verify each other's identity. This anonymity feature is crucial in promoting trust and security in financial transactions, making ZKP a pivotal technology in the realm of virtual currencies. In the context of the Fourth Industrial Revolution, the application of ZKP contributes significantly to the comprehensive and stable development of financial services. It fosters a trustworthy user environment by ensuring that transaction privacy is maintained, thereby encouraging broader adoption of virtual currencies. By integrating ZKP, financial services can achieve a higher level of security and trust, essential for the continued growth and innovation within the sector.

Key Words : Zero Knowledge Proof, Virtual Currency, Privacy Protection, Financial Services Development, 4th Industrial Revolution

요 약 제로 지식 증명(ZKP)은 가상 화폐 거래의 프라이버시와 보안을 향상시키기 위해 설계된 혁신적인 분산 기술이다. ZKP는 거래 제공자가 필요한 정보만을 공개함으로써 모든 관련 당사자의 기밀성을 보호한다. ZKP는 블록체인 거래에서 신원과 가치를 숨기는 강력한 프라이버시 기능을 제공할 뿐만 아니라, 당사자들이 서로의 신원을 확인할 필요 없이 돈을 교환할 수 있게 합니다. 이러한 익명성 기능은 금융 거래에서 신뢰와 보안을 촉진하는 데 매우 중요하며, 가상 화폐 영역에서 ZKP를 핵심 기술로 만든다. 4차 산업혁명 시대의 맥락에서 ZKP의 응용은 금융 서비스의 포괄적이고 안정적인 발전에 크게 기여합니다. 거래 프라이버시를 보장하여 신뢰할 수 있는 사용자 환경을 조성함으로써 가상 화폐의 광범위한 채택을 장려합니다. ZKP를 통합함으로써 금융 서비스는 보안과 신뢰의 높은 수준을 달성할 수 있으며, 이는 부문 내 지속적인 성장과 혁신을 위해 필수적이다.

주제어 : 영지식 증명, 가상 화폐, 프라이버시 보호, 금융 서비스 발전, 4차 산업혁명

*This research was supported by 2024 Baekseok University research fund.

*Corresponding Author : Sunghyuck Hong(shong@bu.ac.kr)

Received July 8, 2024
Revised August 7, 2024
Accepted September 20, 2024
Published September 30, 2024

1. Introduction

Zero Knowledge Proof (ZKP) represents a significant advancement in cryptographic techniques, enabling one party (the prover) to convince another party (the verifier) of the truth of a statement without revealing any additional information. The concept, introduced by Goldwasser, Micali, and Rackoff in the 1980s, has since evolved, finding applications in areas requiring privacy and security, such as blockchain technology, secure communications, and privacy-preserving protocols.

Table 1. Description of Network Configuration Terminologies

Items	Description
Node	It is divided into transaction nodes (hereinafter referred to as 'transaction nodes') that exchange transactions and service nodes that provide permission services, network map services, notary services, etc. (*In theory, transaction nodes can also provide services), and each node operates independently. Identified through a unique ID you specify
Permitted Service	This is a service that issues and manages TLS certificates, and all nodes communicate directly using an encrypted communication channel based on the issued certificate.
Certification Service	It is a service that verifies and confirms transactions (hereinafter referred to as 'agreement'). There is one or more notary services in each network, and each notary service is provided by a single node or a cluster of multiple nodes (hereinafter referred to as 'notary').
Network Map Service	It provides node information necessary for transactions and communication between nodes, and nodes newly participating in the network must first register their information in this service.

The primary objective of this thesis is to develop a comprehensive model for Zero Knowledge Proof systems, focusing on both theoretical foundations and practical implementations. The study aims to:

- Analyze the fundamental properties and types of ZKP.
- Design and implement interactive and non-interactive ZKP protocols.
- Evaluate the security and efficiency of these protocols.
- Explore real-world applications and future potential of ZKP [1,2].

This thesis is structured into eight chapters. Chapter 2 provides the theoretical foundations of ZKP. Chapter 3 discusses the building blocks and design of ZKP systems. Chapter 4 focuses on security and efficiency analysis. Chapter 5 explores various applications of ZKP and concludes the study.

2. Related Work

The development and application of Zero Knowledge Proof (ZKP) systems have been extensively studied across various domains, including cryptography, blockchain technology, privacy-preserving protocols, and secure communication systems. Here is an overview of some significant related work in these areas:

2.1. Foundational Work in Zero Knowledge Proofs

- Goldwasser, Micali, and Rackoff (1985): The seminal paper "The Knowledge Complexity of Interactive Proof Systems" introduced the concept of Zero Knowledge Proofs. This work laid the theoretical foundation for ZKPs by defining the key properties of completeness, soundness, and zero-knowledgeness.
- Interactive Proof Systems: Early work focused on interactive proof systems where the prover and verifier engage in multiple rounds of communication. This

includes protocols for specific problems such as Graph Isomorphism and the Hamiltonian Cycle problem.

2.2. Non-Interactive Zero Knowledge Proofs

- Fiat and Shamir (1986): Proposed a method to transform interactive ZKPs into non-interactive ones using cryptographic hash functions, known as the Fiat-Shamir heuristic. This transformation is crucial for practical applications where interaction is not feasible.
- zk-SNARKs and zk-STARKs: Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) and Zero-Knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs) represent significant advancements. zk-SNARKs are efficient and require a trusted setup, while zk-STARKs offer scalability and transparency without the need for a trusted setup. These technologies have been extensively explored in academic research and practical implementations.

2.3. ZKP in Blockchain and Cryptocurrencies

- Zcash: One of the most well-known applications of zk-SNARKs in the blockchain space is Zcash, a privacy-focused cryptocurrency. Zcash uses zk-SNARKs to enable shielded transactions, ensuring transaction privacy and confidentiality on a public blockchain.
- Ethereum: The Ethereum blockchain has integrated zk-SNARKs into its protocol to enhance privacy and scalability. Research and development efforts continue to explore the use of ZKPs for improving Ethereum's efficiency and security.

2.4. Privacy-Preserving Protocols

- Secure Multi-Party Computation (MPC): ZKPs have been used in conjunction with MPC to enable parties to jointly compute a function over their inputs while keeping those inputs private. This work includes applications in privacy-preserving data analysis and secure voting systems.
- Anonymous Credentials: Systems like Microsoft's U-Prove and IBM's Idemix leverage ZKPs to create anonymous credential systems, allowing users to prove their attributes without revealing their identities.

2.5. Formal Methods and Verification

- Formal Verification: Research has also focused on formally verifying the correctness and security of ZKP protocols. This includes using formal methods to ensure that the protocols adhere to their intended security properties and do not contain vulnerabilities.
- Cryptographic Libraries: Libraries such as libsnark, Bulletproofs, and Halo have been developed to provide tools for implementing and experimenting with ZKP protocols. These libraries facilitate the development and deployment of ZKP-based applications.

2.6. Challenges and Future Directions

- Scalability and Efficiency: Ongoing research aims to improve the scalability and efficiency of ZKPs. This includes optimizing proof generation and verification times and reducing the computational overhead associated with ZKP systems.
- Post-Quantum Security: With the advent of quantum computing, researchers are

investigating ZKP protocols that are secure against quantum attacks. Post-quantum ZKPs are essential for ensuring long-term security.

- Standardization: Efforts are being made to standardize ZKP protocols and frameworks to ensure interoperability and widespread adoption. Organizations such as the IETF and W3C are involved in these standardization efforts.

The field of Zero Knowledge Proofs has seen substantial progress since its inception, with foundational theoretical work leading to practical applications in blockchain, privacy-preserving protocols, and secure communication systems. Key advancements such as zk-SNARKs and zk-STARKs have enabled the deployment of ZKPs in real-world systems, while ongoing research continues to address challenges related to scalability, efficiency, and post-quantum security. The integration of ZKPs into various domains highlights their potential to enhance privacy and security in the digital age [3-5].

3. Proposed Zero Knowledge Proof (ZKP) System Model

The configuration of Proposed ZKP System is based on Table 1.

Components:

- Transaction Nodes: Nodes that handle the exchange of transactions. These can also theoretically provide services.
- Service Nodes: Nodes that provide various services such as permission services, network map services, and notary services. These include:
  - Permissioned Service Nodes: Manage and verify permissions.
  - Network Map Service Nodes: Provide necessary node information for transactions and communication.
  - Notary Service Nodes: Verify and confirm transactions.

Services:

TLS Certificate Management:

- Description: Issues and manages TLS certificates.
- Function: Ensures all nodes communicate using an encrypted communication channel based on the issued certificate.

Transaction Agreement Service:

- Description: Verifies and confirms transactions.
- Function: Ensures the integrity and agreement of transactions within the network. Each network has one or more notary services, which can be provided by a single node or a cluster of multiple nodes.

Node Information Service:

- Description: Provides necessary node information for transactions and communication between nodes.
- Function: Ensures that newly participating nodes register their information before joining the network.

Processes:

- Transaction Message Provision:
  - Transaction nodes provide transaction messages.
- Transaction Request Information Secure Encryption:
  - Encrypt transaction request information to ensure security.

Network Participation:

- New nodes require approval and signature from the Root Certification Authority to join the network.

TLS Certificate Granting:

- Issue TLS certificates to nodes for encrypted communication.

Node Information Acquisition:

- Nodes verify information with transaction nodes and service nodes.

Visual Model:

- Root Certification Authority: Central authority that issues and manages certificates.
- Network Map Service Node: Provides the map of the network, including node information.
- Permissioned Service Node: Manages permissions for nodes and transactions.
- Transaction Node: Handles transaction requests and processes them.
- Representative Node: Acts on behalf of a group of nodes in certain transactions or verifications.
- Notary Service Node Cluster: Group of nodes that provide transaction verification and agreement services [6-8].

Fig. 1 is based on procedures above.

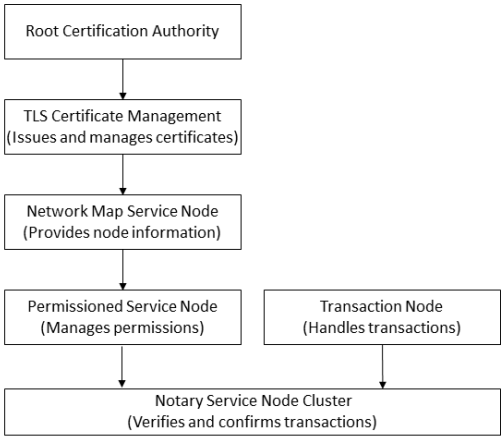

Fig. 1. The Flowchart of ZKP system Model process

The detail explanation of the model for Fig. 1 is follows.

Explanation of the Model:

1. Root Certification Authority: The root of trust, issuing certificates for secure communication.
2. Network Map Service Node: Keeps an updated map of nodes in the network, providing essential information for communication and transactions.
3. Permissioned Service Node: Ensures that only authorized nodes can participate in transactions.
4. Transaction Node: Initiates and processes transactions.
5. Notary Service Node Cluster: A cluster of nodes that ensures transaction integrity and agreement through verification.

This model highlights how Zero Knowledge Proof systems maintain security, privacy, and trust in a decentralized network, particularly for virtual currency transactions. Each component and service works together to ensure that transactions are processed securely and efficiently without compromising the privacy of the involved parties[9-13].

4. Conclusion

In conclusion, Zero Knowledge Proof systems hold immense promise for the future of secure digital transactions. By safeguarding privacy and ensuring trust in decentralized environments, ZKP technology aligns with the goals of the 4th Industrial Revolution, promoting the comprehensive and stable development of financial services. As research and development in this field continue to advance, ZKP systems are poised to become a cornerstone of modern cryptographic practices, driving innovation and enhancing the security of digital ecosystems.

This thesis has provided a thorough examination of ZKP systems, offering valuable

insights and paving the way for further exploration and implementation of this transformative technology.

REFERENCES

[1] Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing, 14(4),* 397-429.
DOI : 10.1137/0218012

[2] Peeters, R. (2020). *Zero-knowledge proofs: A primer.* arXiv preprint arXiv:2004.07523. https://arxiv.org/abs/2301.02161

[3] Brassard, G., & Auclair, M. (1993). *A simple and secure way to do computations on integers in the presence of an adversary.* In Advances in Cryptology?CRYPTO'93 (pp. 201-212). Springer, Berlin, Heidelberg.
https://arxiv.org/pdf/2401.09277

[4] Blum, M., & Feldman, L. (1984). *The canonical form for zero-knowledge proofs.* In Advances in Cryptology?CRYPTO'84 (pp. 41-56). Springer, Berlin, Heidelberg.
https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.pdf

[5] Fiat, U., & Shamir, A. (1986). *How to prove yourself a liar without revealing any other secret.* In Advances in Cryptology?EUROCRYPT'86 (pp. 206-221). Springer, Berlin, Heidelberg.
https://www.sciencedirect.com/science/article/pii/S0306457322003296

[6] Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography.* Cambridge University Press .
http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf

[7] Ben-Sasson, E., Chiesa, M., Genkin, D., Kristjansen, E., & Roos, A. (2013). Scalable transparent proof of knowledge systems. In Cryptology (CRYPTO 2013) (pp. 487-508). Springer, Berlin, Heidelberg.
https://eprint.iacr.org/2018/046.pdf

[8] Bunz, B., Bootle, J., Lindqvist, A., & Groth, D. (2018). *Transparent proofs of partial knowledge. In Theory of Cryptography* (TCC 2018) (Part I) (pp. 313-344). Springer, Cham.
https://link.springer.com/chapter/10.1007/3-540-48658-5_19

[9] Kiayias, A., & Apostolakos, I. (2014). Zero-knowledge proofs of knowledge for bitcoin transactions. In Financial Cryptography and Data Security (pp. 283-300). Springer, Berlin, Heidelberg.
https://link.springer.com/chapter/10.1007/978-3-031-33386-6_6

[10] Gentry, C., Gentry, R., & Halevi, S. (2015). *Secure multi-party computation for every user.* In Proceedings of the forty-sixth annual ACM symposium on theory of computing (pp. 109-118).
https://dl.acm.org/doi/10.1145/3387108

[11] Chase, M., & Lysyanskaya, A. (2004). Efficient constructions for anonymous credentials. In Theory of Cryptography (TCC 2004) (pp. 195-211). Springer, Berlin, Heidelberg.
https://eprint.iacr.org/2021/1680.pdf

홍 성 혁 (Sunghyuck Hong) [종신회원]

· 2007년 8월 : Texas Tech University, Computer Science (공학박사)
· 2012년 3월 ~ 현재 : 백석대학교 첨단IT학부, IoT 전공 주임 교수

· 관심분야 : 핀테크, 딥러닝, 블록체인, 사물인터넷 보안
· E-Mail : shong@bu.ac.kr