Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 5
AIDML 2024

Research and Application Analysis of Key Technologies of Zero-Knowledge Proof under the Background of Blockchain

Keyi Guo[1,*], Haoyu Ren[2] and Peiyu Wang[3]

[1]School of computing, Henan University of Economics and Law, Zhengzhou, China

[2]School of computing, Hebei Normal University, Shijiazhuang, China

[3]School of computing, Tianjin University of Science and Technology, Tianjin, China

* Corresponding Author Email: 202134070803@stu.huel.edu.cn

Abstract. In recent years, blockchain technology has evolved significantly, enabling a decentralized network application model that offers both user anonymity and transparency. This unique characteristic of blockchain has led to its adoption in various sectors, including healthcare, finance, and transportation. The advancement of modern zero-knowledge proof technology has further enhanced blockchain's applications across these fields, bolstering privacy protection. Zero-knowledge proofs have become a key mechanism in blockchain smart contracts, offering a balance between transparency and privacy. Moreover, the integration of zero-knowledge proof technology with blockchain is facilitating technical advancements in areas facing challenges, such as autonomous driving technology. It is also addressing security concerns in more established technologies like the Internet of Things. This synergy between zero-knowledge proof and blockchain technologies is paving the way for innovative solutions across a wide range of applications.

Keywords: Blockchain; Zero-Knowledge Proof; Smart Contract.

1. Introduction

In recent years, blockchain technology has undergone significant evolution, transitioning from the inception of Bitcoin to the advanced integration of Ethereum with smart contracts. This evolution has expanded the application of blockchain from mere virtual currency transactions to a myriad of fields, thereby ushering in a shift from traditional centralized network systems to distributed, decentralized ones. This paradigm shift has opened up avenues for the implementation of numerous technologies in previously inconceivable ways.

One of the most notable advancements within the blockchain domain is the rise in prominence of concepts such as smart contracts and zero-knowledge proofs. Initially, the technological landscape was not equipped to actualize smart contract technology; however, blockchain development has since paved the way for its realization and application. In conjunction, the modern iteration of zero-knowledge proof technology has seen significant growth and development. Notably, in current smart contract technologies, zero-knowledge proofs play a crucial role, offering robust information protection within the transparent nature of blockchain. The synergistic combination of zero-knowledge proof technology with blockchain has found applications in numerous fields. For instance, it's being leveraged in autonomous driving, the Internet of Things (IoT), and various smart contract solutions. Recently, scholars have been employing this combination to address practical challenges and introduce novel technical solutions.

This paper meticulously reviews and summarizes these technological solutions proposed by scholars, while also highlighting potential future directions and conclusions in this rapidly evolving field. The analysis underscores the transformative impact of blockchain and zero-knowledge proofs in shaping the technological landscape.

2. Related Theories

2.1. Blockchain

Blockchain technology is characterized by its decentralization, trustless nature, collaborative maintenance, and immutability. It addresses trust issues in data interactions and usage between conventional institutions and centralized systems, as noted in [1]. In a blockchain network, there are no permanent central nodes. Instead, each node can participate in updating and processing data. The data is stored and processed across a distributed network of nodes. When data is updated, certain specialized nodes in the network update and package the data into blocks, which are then broadcast throughout the network. This process allows all nodes to synchronize data updates. Each user's identity information is represented on the blockchain by a public key. Data processing is publicly packaged into blocks, and these blocks are interconnected through a hash function. For example, in Bitcoin, each user acts as a node, and each transaction forms a block. The inherent nature of blockchain provides a degree of anonymity for users while also ensuring transparency.

2.2. Zero-Knowledge Proof

Zero-knowledge proofs serve to ensure the secure transmission of information between two parties, with the sender substantiating the veracity of a claim based on specific knowledge. These proofs are characterized by several key properties:

Completeness: If the prover presents a valid proof, the verifier can confirm its accuracy.

Soundness: If a claim is false, the prover cannot convince the verifier of its truthfulness. Moreover, the prover can reveal no information beyond what is necessary for the zero-knowledge proof to authenticate the statement's correctness.

Witness Indistinguishability: It's impossible for the verifier to differentiate between genuine and simulated data.

Simulation: If P has enough computing power to make $x \in L$ true, then P can prove the judgment of $x \in L$, and then P has information interaction with V, which has verification ability. To determine whether P has completed the proof.

3. Zero-Knowledge Proof and Application Research of Blockchain

3.1. Use of Smart Contracts in Combination

In the realm of computing, the concept of smart contracts, though existent, remained underutilized due to constraints in computational scenarios of the time. This changed dramatically in 2008 with Satoshi Nakamoto's introduction of Bitcoin. The blockchain technology underpinning Bitcoin revealed how smart contracts could benefit from a decentralized, immutable, and transparent architecture. This environment fosters trustless execution, setting the stage for technical realization of smart contracts. A pivotal advancement in this field is the integration of zero-knowledge proof technology, especially in ensuring user privacy while preserving the blockchain's openness and transparency. This combination enhances both the security and credibility of contracts. In the context of smart contracts, zero-knowledge proof technology, notably the zk-SNARK variant, emerges as a crucial tool for privacy preservation.

The application of zk-SNARK in smart contracts allows for the verification of data exchanges between data owners and cloud service providers while safeguarding privacy [2]. In this model, the cloud provider generates a zero-knowledge proof via zk-SNARKs that encompasses certain attribute requirements. This process involves computing a result, generating a corresponding hash, recording this hash in the smart contract, and releasing select keywords. For verification purposes, the data owner submits a zero-knowledge proof to the smart contract. The smart contract is then tasked with verifying this proof using the zk-SNARK verification key [3]. It conducts a comparative analysis of

the zero-knowledge proofs, computational results, and hash values from both the data owner and the cloud server, employing the zero-knowledge proof method for validation. Further literature indicates the effective application of zero-knowledge proof technology in protecting prosumer privacy within Energy Transactions. This approach employs zero-knowledge proofs to secure consumers' energy data and utilizes smart contracts for verifying consumer activities on the blockchain. Such synergy between zero-knowledge proof technology and smart contracts demonstrates a promising pathway for enhancing privacy and security in blockchain applications [4].

3.2. Applications in Smart Devices

The integration of blockchain technology with the Internet of Things (IoT) is highlighted in various studies. For instance, a ledger-based architecture for IoT access control is explored in [5], emphasizing blockchain's role in managing access permissions efficiently. Further, in [6], the feasibility of implementing blockchain within resource-constrained IoT devices is investigated. This approach notably employs smart contract technology for policy management and leverages crown-jewel assets in IoT systems to represent devices. This method effectively addresses significant IoT security challenges, such as the high computational demands and the limited processing capabilities of individual devices. Additionally, the literature [7] delineates a framework where blockchain ensures that only authenticated devices interact with official mobile applications, enhancing security in IoT ecosystems. Another notable application is presented in [8], where blockchain is utilized in military IoT environments. This approach involves verifying the location information of combat units, even under unreliable communication channels, by tracking specific continuous path coordinates. This capability is particularly crucial for operational integrity and security in military scenarios.

3.3. Applications in the Field of Transportation

In recent literature, a novel distributed firmware update mechanism employing Blockchain and smart contract technologies has been proposed [9]. This mechanism is particularly applicable to subsystems used in self-driving cars. It incorporates autonomous vehicles as distributors in the update process, leveraging their mobility to ensure timely and accessible delivery of firmware updates. A significant feature of this mechanism is its distribution proof system, designed to address trust issues among autonomous vehicles. Another study presents a centralized, location-aware architecture that effectively addresses privacy and data integrity concerns in blockchain-based traffic management systems [10]. This architecture integrates modular deep-peering networks with non-interactive zero-knowledge range proof (ZKRP) protocols. A key innovation is the concept of a gateway linking adjacent blockchain-based traffic management systems. This gateway employs a non-interactive ZKRP scheme, facilitating the transition of vehicles from one blockchain system to another. Here, the vehicle serves as the prover, and its ZKRP-encrypted data is transmitted to the gateway for verification. This process ensures that vehicle information is authenticated without exposing sensitive data. Additionally, the study introduces a blockchain-based vehicle network developed on a hyperledger platform. This network maintains regionally distributed ledgers within different blockchain networks, recording and sharing vehicle data to support traffic management systems. Furthermore, a concept known as zero-knowledge proof of Traffic (zk-PoT) has been introduced [11]. Zk-PoT can either extend existing co-awareness standards or serve as a robust trust provider for integration with numerous existing trust models. It is particularly well-suited for processes that require the establishment of initial trust.

4. Challenges

The blockchain technology, having been proposed just over a decade ago, continues to hold immense potential for innovative applications, especially when combined with zero-knowledge proof technology. As noted in the referenced paper [12], the adoption of blockchain in the Internet of Things is still in its nascent stages. Thus, there's a significant opportunity to leverage the latest technological advancements from established sectors to address practical challenges in emerging fields. For

instance, the IoT and autonomous driving share certain technological parallels. Techniques successfully implemented in one domain could be adapted to solve analogous issues in the other.

5. Conclusions

The integration of zero-knowledge proof with blockchain technology not only ensures transparency and immutability, essential for the fairness of information, but also establishes sufficient informational gaps to safeguard privacy. This synergy is poised to address technical challenges across various domains. This paper reviews recent advancements in combining blockchain and zero-knowledge proof. Key areas of exploration include facilitating network access for functionally diverse devices within the resource-constrained Internet of Things (IoT) landscape, and enhancing privacy in autonomous driving by enabling vehicles to comprehend road conditions without compromising privacy. These cutting-edge studies demonstrate that with advancements in the application of zero-knowledge proof within blockchain, coupled with enhanced engineering and adaptability, blockchain, as an emergent internet technology, is increasingly vital in a broader spectrum of scenarios and fields.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review.

[2] Nazir, S., Ali, Y., Ullah, N., & García-Magariño, I. (2019). Internet of things for healthcare using effects of mobile computing: a systematic literature review. Wireless Communications and Mobile Computing, 2019, 1-20.

[3] Feng, T., Yang, P., Liu, C., Fang, J., & Ma, R. (2022). Blockchain data privacy protection and sharing scheme based on zero-knowledge proof. Wireless Communications and Mobile Computing, 2022, 1-11.

[4] Pop, C. D., Antal, M., Cioara, T., Anghel, I., & Salomie, I. (2020). Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. Sensors, 20(19), 5678.

[5] Alfandi, O., Otoum, S., & Jararweh, Y. (2020, April). Blockchain solution for iot-based critical infrastructures: Byzantine fault tolerance. In NOMS 2020-2020 IEEE/IFIP network operations and management symposium (pp. 1-4). IEEE.

[6] Song, L., Ju, X., Zhu, Z., & Li, M. (2021). An access control model for the Internet of Things based on zero-knowledge token and blockchain. EURASIP Journal on Wireless Communications and Networking, 2021(1), 1-20.

[7] Tomaz, A. E. B., Do Nascimento, J. C., Hafid, A. S., & De Souza, J. N. (2020). Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE access, 8, 204441-204458.

[8] Shi, M., C., & Zhang, C. (2023). Design and Simulation of a Location Privacy Protection Scheme Based on Zero-knowledge Proof for Military IoT. Journal of System Simulation, 35(10), 2237-2248.

[9] Basar, E. (2019, June). Transmission through large intelligent surfaces: A new frontier in wireless communications. In 2019 European Conference on Networks and Communications (EuCNC) (pp. 112-117). IEEE.

[10] Li, W., Guo, H., Nejad, M., & Shen, C. C. (2020). Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. IEEE access, 8, 181733-181743.

[11] Kolberg, M., Merabti, M., & Moyer, S. (2008). Consumer communications and networking [guest editorial]. IEEE Communications Magazine, 46(12), 30-31.

[12] Lunardi, R. C., Michelin, R. A., Neu, C. V., & Zorzo, A. F. (2018, April). Distributed access control on IoT ledger-based architecture. In NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium (pp. 1-7). IEEE.