Privacy Preservation in Blockchain-based Applications Using Zero-knowledge Proof[*]

Wu Yuxiao

Abstract

Blockchain technology has gained significant attention due to its numerous advantages, including enhanced transparency, trustlessness, decentralization, resiliency, security, authorization, cost-effectiveness, immutability, and auditability. Despite these benefits, the openness and transparency of blockchain introduce a potential risk: malicious users gaining illegal access to private transaction data, such as transaction amounts, account addresses, and balances, thus posing a threat to various applications.

To address this concern, zero-knowledge proof, a cryptographic method enabling a prover to convince a verifier of a statement's truth without revealing additional information, emerges as a promising solution. In this thesis, I explore the application of zero-knowledge proof in two blockchain-based scenarios, demonstrating its crucial role in protecting data privacy.

On the one hand, e-voting is one of the targeted areas. As an indispensable part of establishing modern representative democratic organizations, the election is based on a voting process on-site or remotely. With the rapid development of information technology, the application of electronic voting systems in practice has significantly increased in recent years. Consequently, whether an electronic voting system is secure and reliable enough is the most critical factor. Whereas, most of the existing proposals neglect to confirm the trustworthiness of the administrator, which may impact the security and availability of the system. For this purpose, I propose an up-to-date electronic voting system based on smart contracts using

[*] Master's Dissertation, Graduate School of Science and Technology, Nara Institute of Science and Technology, December 21, 2023.

additively homomorphic encryption and non-interactive zero-knowledge proof. In our work, I utilize a concise zero-knowledge proof algorithm and an inbound oracle in combination to allow voters to verify the fidelity of the administrator. I prove our system's feasibility, efficiency, and scalability can satisfy most application scenarios, including large-scale voting. I evaluate the time performance and cost performance and demonstrate its merits including the low cost in many functions and linear performance when generating zero-knowledge proof.

On the other hand, blockchain and smart contracts are widely employed in IoT access control to establish a decentralized environment for dependable IoT access and recording. However, the application of blockchain in this domain presents a dual challenge, as account privacy is vulnerable to compromise due to the inherent transparency of blockchain and the utilization of blockchain addresses as IDs. In response to this challenge, I propose a blockchain-based IoT access control system designed to address concerns related to account anonymity and privacy preservation, particularly focusing on behavior, habit, and record privacy, through the implementation of zero-knowledge proof. By introducing an access control mechanism that combines the access control list with capability-based access control, my approach enables the verification of ownership of access rights without the need to disclose account information in the ID. To validate the system's feasibility, experiments were conducted in a smart building scenario. Quantitative analyses assess performance in time, space, and gas fees. Results highlight the system's superior cost efficiency and enhanced security features in comparison to existing works.

Keywords:

smart contract, blockchain, Internet of Things, zero-knowledge proof, access control, e-voting, homomorphic encryption, oracle