Enhancing IoT Sidechain Security and Efficiency: A Restaking and Contract Approach

Zitao Zhou, Hang Su, Yibing Li, Fang Ye

College of Information and Communication Engineering,

Harbin Engineering University, Harbin, China.

Abstract

Sidechain technology aids in building lightweight and rapid-response blockchain services in resource limited Internet of Things (IoT) environments, yet the low trust model of sidechains is a concern. The restaking mechanism offers a way to aggregate mainchain trust on sidechains. Inspired by this, our paper introduces a security reuse solution suitable for IoT sidechains. Addressing the principal-agent problems aggravated by information asymmetry and restaking mechanism in IoT sidechain networks, we propose a solution strategy based on contract theory and exemption limits. The feasibility and effectiveness of this approach are confirmed through simulation analysis. Our work contribute to advancing a more secure, efficient, and decentralized approach to integrating IoT and blockchain.

Background

Sidechains' security and trustworthiness lag behind mainchains, primarily due to their smaller number of nodes, making them more vulnerable to attacks. The restaking mechanism allows validators to restake their assets from the mainchain onto sidechains, thereby enabling sidechains to share the security resources of the mainchain. However, the process presents challenges:

- **Security reuse**: Restaking ties mainchain security to sidechains, potentially creating cascading risks.
- **Information asymmetry**: Validators may not fully disclose their risk preferences or capabilities, complicating trust and resource allocation.
- **Incentive balance**: Incentives must carefully balance the benefits and risks across the network.

Methods

This paper introduces a security reuse strategy for IoT sidechains through a restaking and incentive mechanism. The approach addresses the principal-agent problems caused by information asymmetry between validators and blockchain service providers by using contract theory.

The method involves:

- **Discriminatory Contracts:** Validators with different risk preferences are offered customized contracts, known as discriminatory contracts, to optimize task allocation and ensure fair incentives. These contracts are designed based on validators' risk tolerance and expected returns.
- **Exemption Limits**: To mitigate potential security risks, the mainchain imposes exemption limits on validators' restaked tokens. These limits help prevent costless attacks and ensure that validators lock sufficient assets to cover potential losses.
- **Optimization Model**: The paper formulates an optimization problem to maximize the utility of sidechain service providers while satisfying incentive compatibility and individual rationality constraints. This model is solved using contract theory techniques to determine optimal rewards and security deposits for validators.

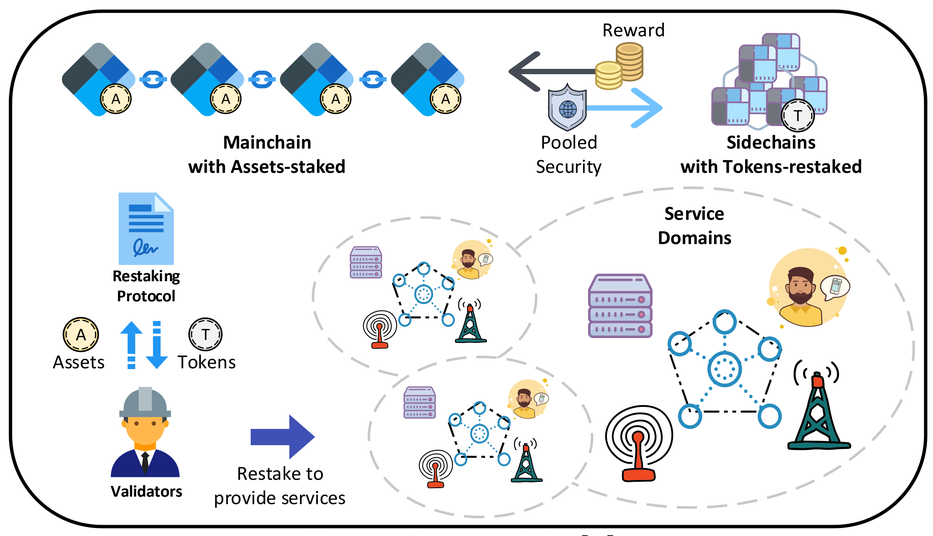

Fig. 1: System Model.

Main Contributions:

- A security-reuse method for IoT sidechains.
- A contract-based solution to tackle information asymmetry.
- Optimization models for validator incentives and security.

Simulation Results

This outcome indicates that the algorithm effectively encourages validators to act in accordance with their actual risk preferences, leading to an optimal alignment of contracts with validator types.

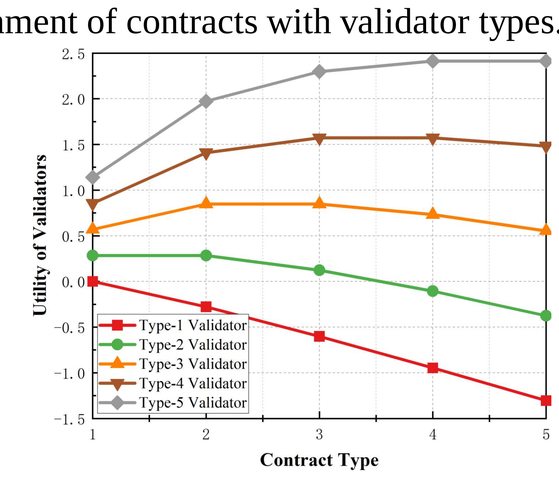

Fig. 2: Validators' utility across different contract types.

Higher-type validators lock more assets, restake more tokens, and receive higher rewards, reflecting their greater risk tolerance and tendency to pursue higher returns through restaking.

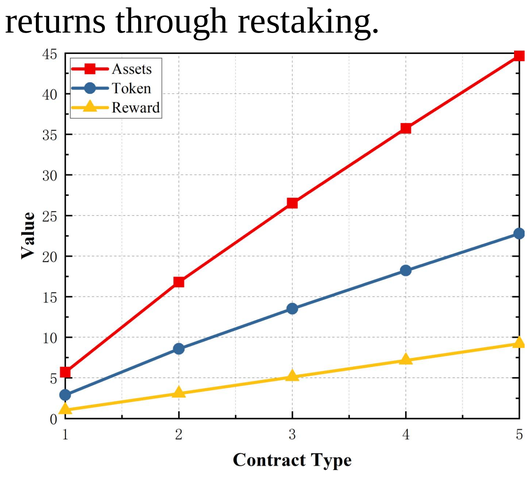

Fig. 3: Analysis of assets staked, token restaked, and reward returns in different contract types.

The method enhances security and incentives in IoT sidechains, but as the permissible scope of restaking expands, stricter mainchain limits reduce security risks while lowering sidechains aggregable trust.

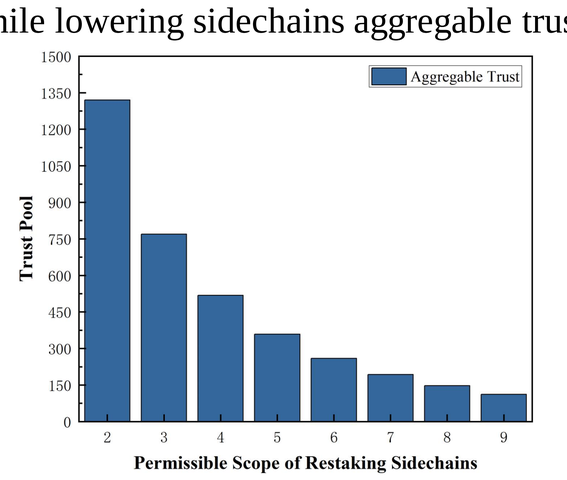

Fig. 4: Trust aggregation in sidechain under different permissible scope of restaking.

Conclusion

Acknowledgement:

This paper is funded by Heilongjiang Touyan Innovation Team Program.

This paper discusses a trust aggregation method for IoT sidechains based on the restaking mechanism. Addressing the inherent restaking risks and information asymmetry, we propose a contract and exemption based approach totackle these issues. The simulation results validate the effectiveness and feasibility of our method in optimizing validator incentives. Nevertheless, due to the constraints of conference paper length, our discussion is limited. Future work will focus on further refining our approach and delving deeper into the complex principal-agent problems present in the system.