Zk-Synergy: Interoperable Blockchain Privacy

Md Omer Danish and Xiaoxue Zhang
University of Nevada, Reno

Abstract

Multi-organization applications, such as supply chain management, urgently require coordination and secure data sharing between distinct private enterprises. While blockchain technology has emerged as a promising foundation for secure, decentralized data storage, ensuring robust data privacy during cross-organization transactions remains a major, unresolved challenge. This challenge is compounded by issues in cross-chain interoperability, consensus mechanisms, and synchronization between existing private networks. In this work, we propose Zk-Synergy, a novel framework enabling secure, efficient, and privacy-preserving cross-organization transactions. To uphold privacy, our system integrates Zero-Knowledge Proofs(ZKP), performing computationally intensive proof generation off-chain using the Gnark framework and Groth16 (utilizing the compact BN254 curve). We model organizational departments as shards and implement transaction batching to optimize inter-org performance and reduce latency. Experiment results, including testing under invalid transactions, demonstrate that our framework achieves high scalability and robust, efficient performance for real-world multi-enterprise applications.

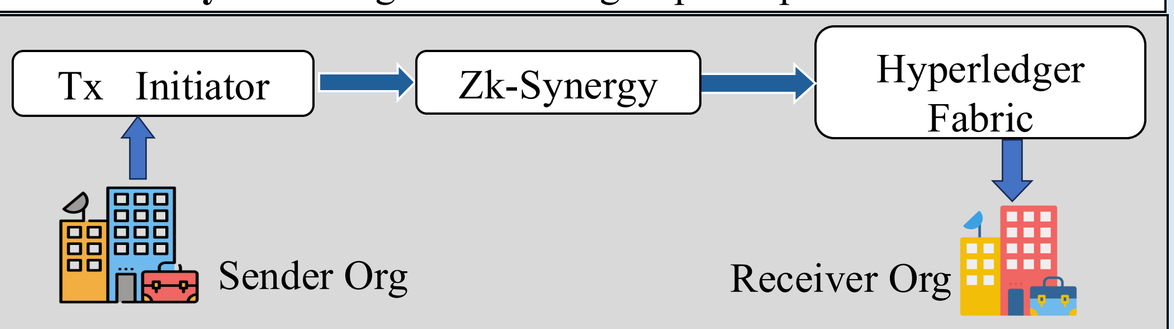
Introduction

Blockchain enables secure, decentralized, and immutable data storage, yet cross-organization transactions face challenges in interoperability, consensus, synchronization, and privacy. For example, in a supply chain involving manufacturers, logistics providers, and retailers on different blockchains, coordination becomes complex due to varying consensus mechanisms and privacy requirements. To address these limitations, we propose Zk-Synergy, a zero-knowledge framework ensuring secure, privacy-preserving, and scalable cross-organization transactions with low latency for multi-enterprise blockchains.

- **Motivation:**

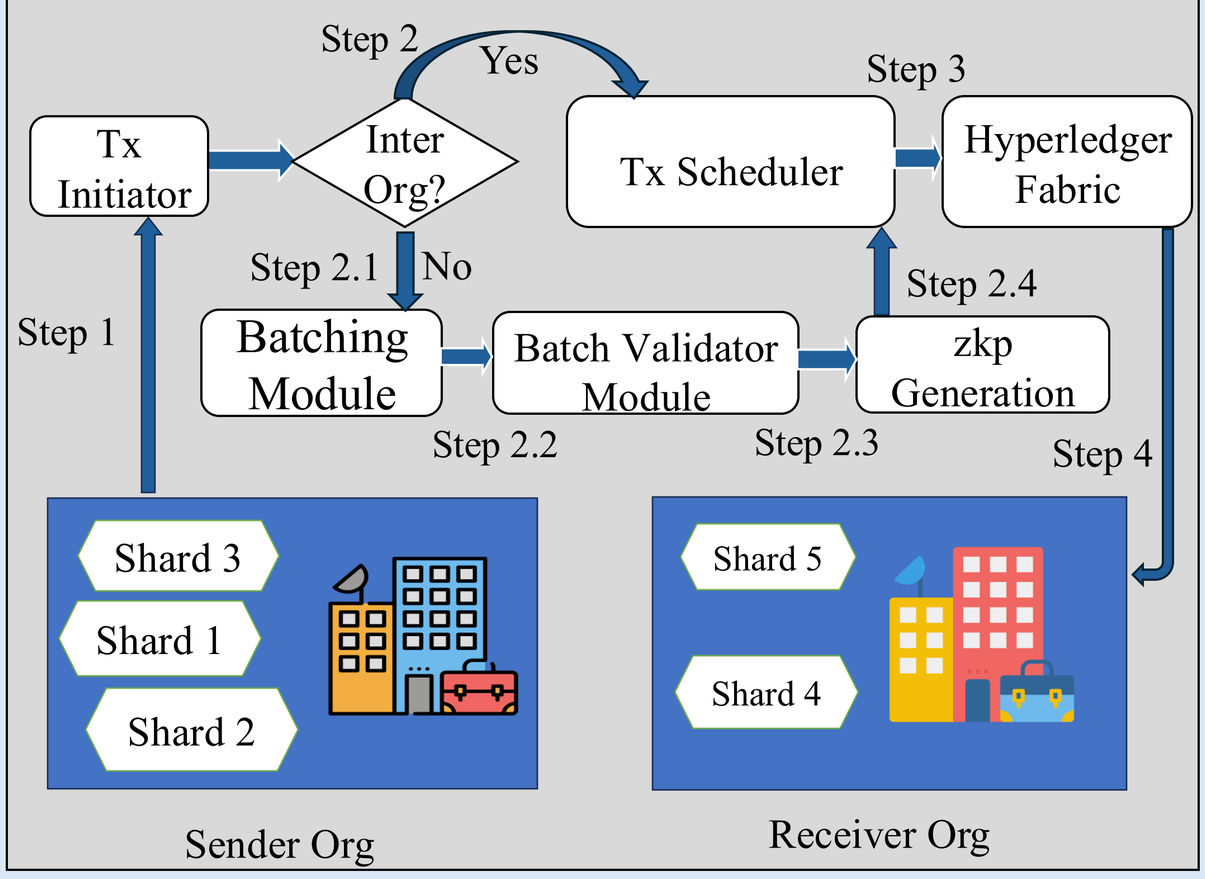
To design a privacy-preserving blockchain framework for secure, efficient cross-enterprise collaboration.

- **Interoperability**: Seamless cross blockchain data exchange.
- **Privacy**: Protect sensitive information using ZKP.
- **Efficiency:** Off-chain proof generation and on-chain verification.
- **Scalability**: Sharding and batching improve performance.



System Design

- **Challenges:**
  - **I. Privacy:** Ensuring privacy for cross-organization transactions.
  - **II. Synchronization:** Ensuring simultaneous transactions.
  - **III.Security:** Preventing data tampering by untrusted participants.
  - **IV.Efficiency:** Efficient ZKP proof processing in Hyper LedgerFabric.



Zk-Synergy:

- Sender initiate Tx with Tx Initiator module.
- Batching module combine multiple Tx request.
- Batch validator module filter valid Tx and forward to ZKP Gen module.
- ZKP module creates proof and key, sends to scheduler, Fabric verifies, then updates sender and receiver balances.

Preliminary Results

We implement the prototype on top of the Hyperledger Fabric blockchain framework, integrating zk-SNARKs through the Gnark library.The framework employs Groth16 ZKP over elliptic curve BN254. Experiments are conducted on a system with an Intel Core i7- 11700 CPU,32 GB RAM, and NVIDIA T1000 8 GB GPU.

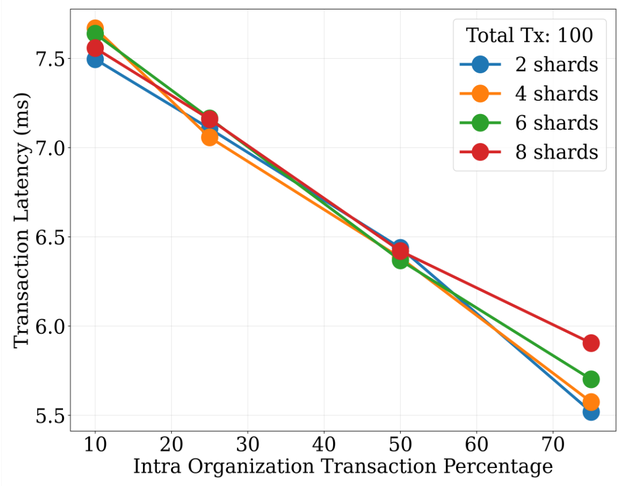


Fig1: Tx Ratio and Shard Count Impact on Tx Latency

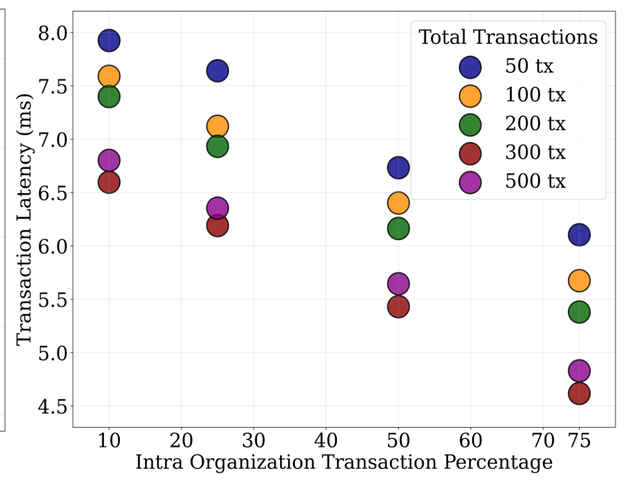


Fig2: Tx Ratio and Tx Count Impact on Tx Latency

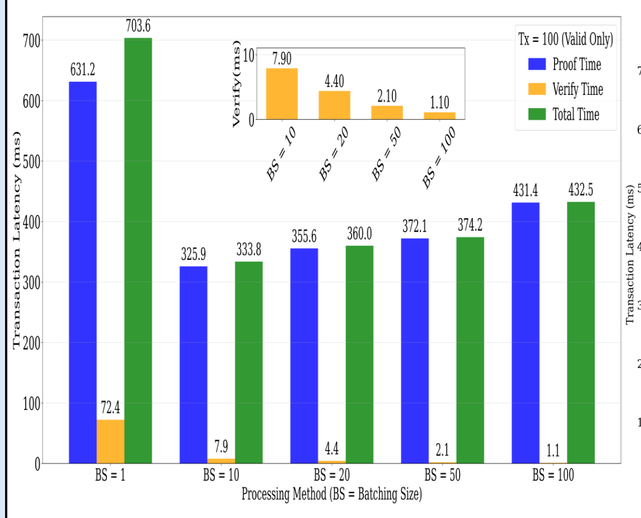


Fig3: Tx Latency for Different Batching Settings

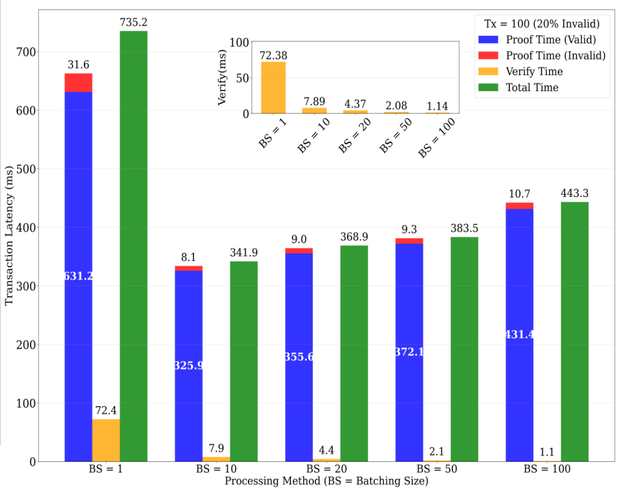


Fig4: Invalid Tx Impact on Latency for Different Batching Settings

Conclusion

- Zk-Synergy enables seamless, synchronized, and private data exchange across enterprises.
- The framework uses ZKP with off-chain proving and on-chain verification for compact, secure transactions.
- Transaction batching and sharding reduce latency, ensuring scalable and robust real-world performance.

References:

[1] ConsenSys, “gnark: A fast zk-snark library,” https://github.com/ConsenSys/gnark, 2023, accessed: 2025-05-14.
[2] M. J. Amiri, D. Agrawal, and A. E. Abbadi, “SharPer: Sharding permissioned blockchains over network clusters,” SIGMOD, 2019.
[3] P. -W. Chi, Y. -H. Lu and A. Guan, "A Privacy-Preserving Zero-Knowledge Proof for Blockchain," in IEEE Access, vol. 11, pp. 85108-85117, 2023.
[4] T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh, and D. Song, “zkBridge: Trustless cross-chain bridges made practical,” *Proc. ACM CCS*, 2022.
[5] J. Groth, “On the size of pairing-based non-interactive arguments,” *EUROCRYPT*, 2016.
[6] M. J. Amiri, B. T. Loo, D. Agrawal, and A. E. Abbadi, “Qanaat: A scalable multi-enterprise permissioned blockchain system with confidentiality guarantees,”VLDB, 2022.