Zero-Knowledge Proofs in Blockchain Networks

Research seminar introductory presentation

Andrej Erjavec

Introduction

- Goal: review article with a proposal for implementation of ZKP

- Blockchain = public decentralized distributed ledger for storing historical data, prone to tampering.
- Transparent!
- Non-verifiable computation model: data may be manipulated
- Problem: how to **verify** the computation validity and **keep the data confidential**
- Common question: Does an entity have enough transaction amount?

Zero Knowledge Proofs

- ZKP = interactive verification protocol
- two entities: prover and verifier
- Prove the ownership of data without leaking the data and identity

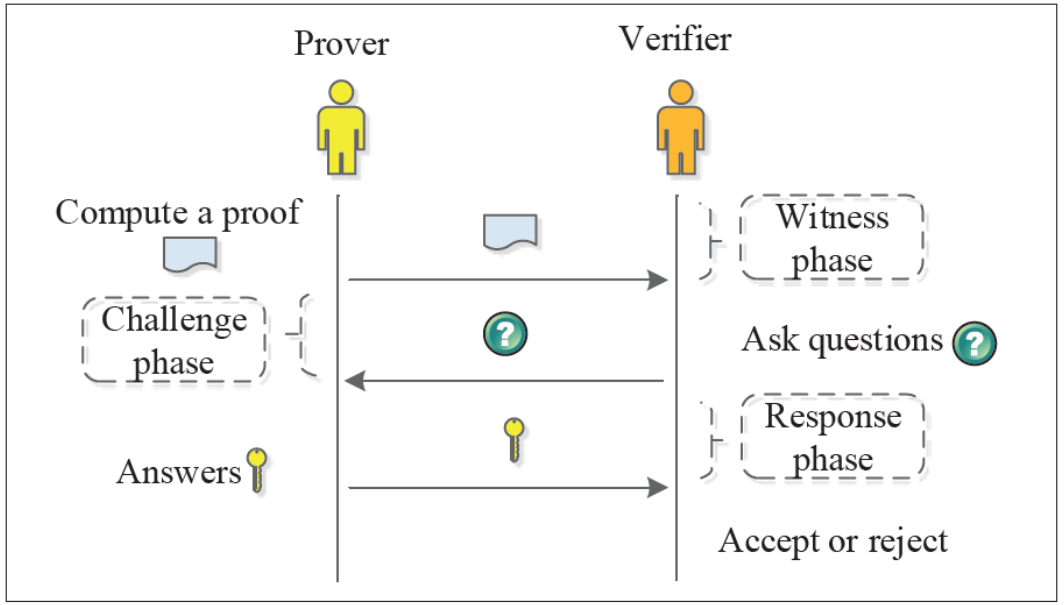


Figure 1: Framework for Zero knowledge proofs

Properties of ZKP

- **Completeness:** If the honest prover can prove to the honest verifier that his statement is true, the verifier always accepts the generated proof
- **Soundness:** If the prover's statement is false, the verifier rejects the generated proof.
- **Zero-knowledge:** If the state is true, then the verifier learns nothing more from the prover other than the statement is true.

ZKP models

zkSNARKs

- setup via trusted authority
- generate proving key and verifying key
- proof easy to verify (short running time)
- small proof size
- based on elliptic curve cryptography
- various improvements in execution time (otherwise polynomial prover complexity)
- Ben-Sasson's Model, Bulletproofs, etc.

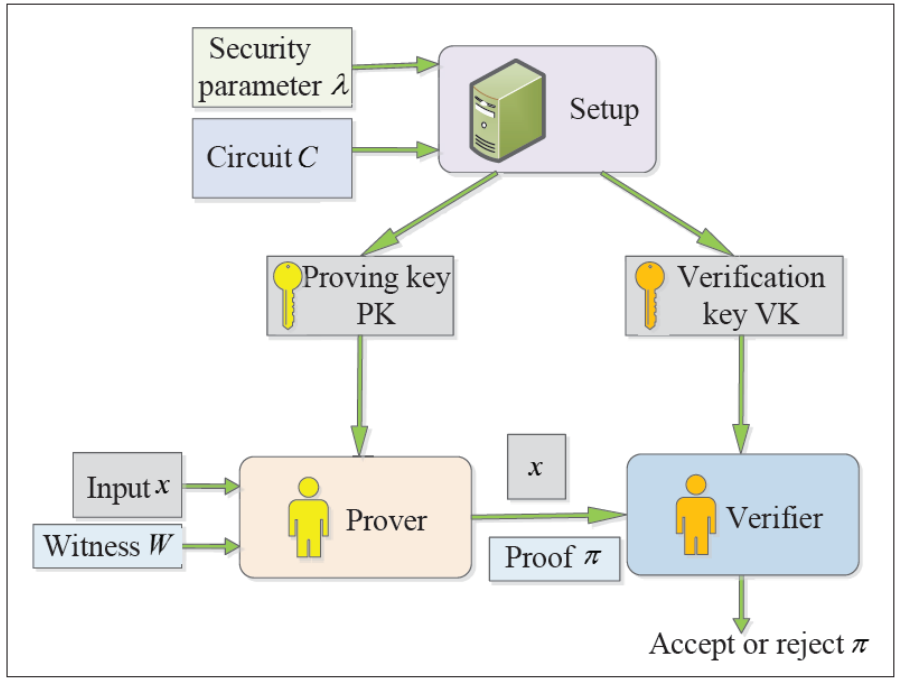


Figure 2: Framework for zkSNARKS

ZKP models (cont.)

zkSNARKs

- no trusted third party
- minimal interaction between prover and verifier
- simple cryptography (hashing, information theory)
- faster then zkSNARKS (linear prover complexity, logarithmic verifier complexity)

ZKP in blockchain

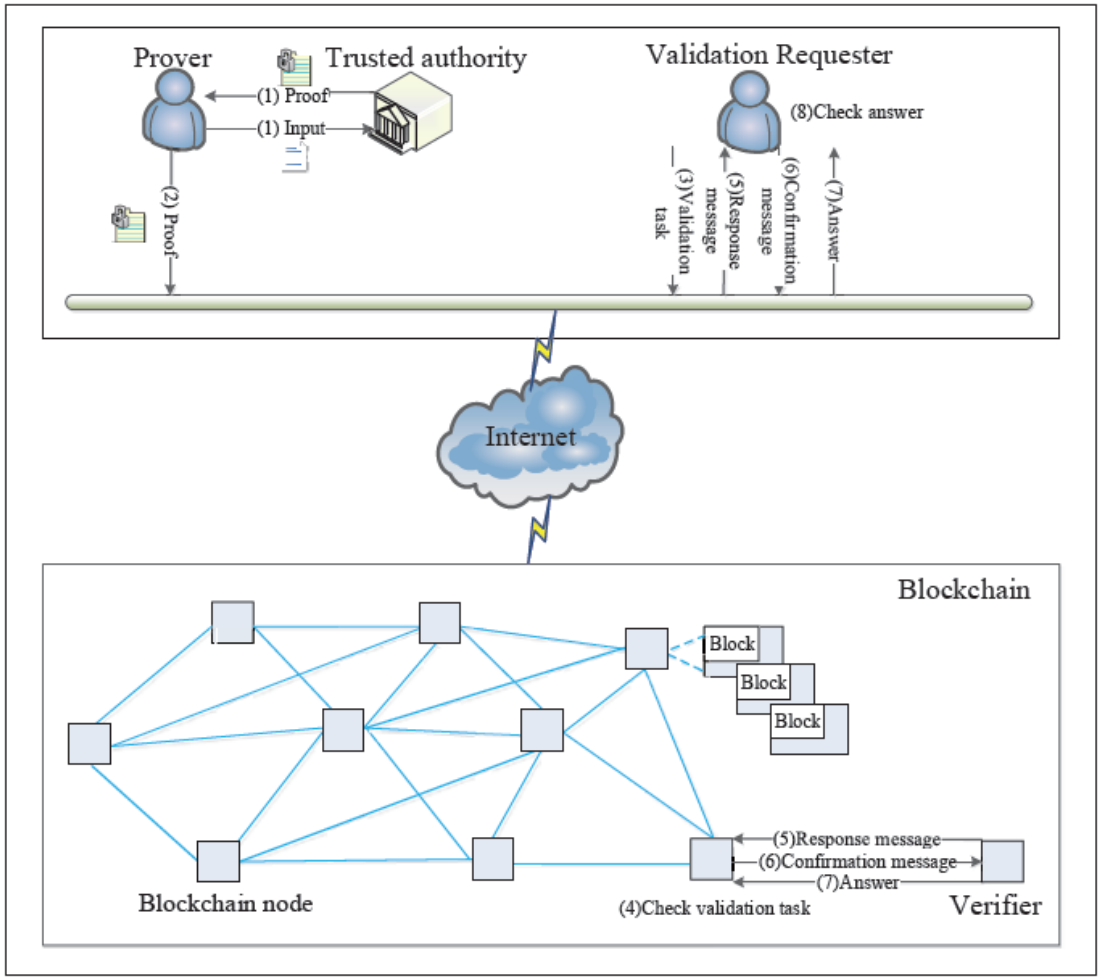
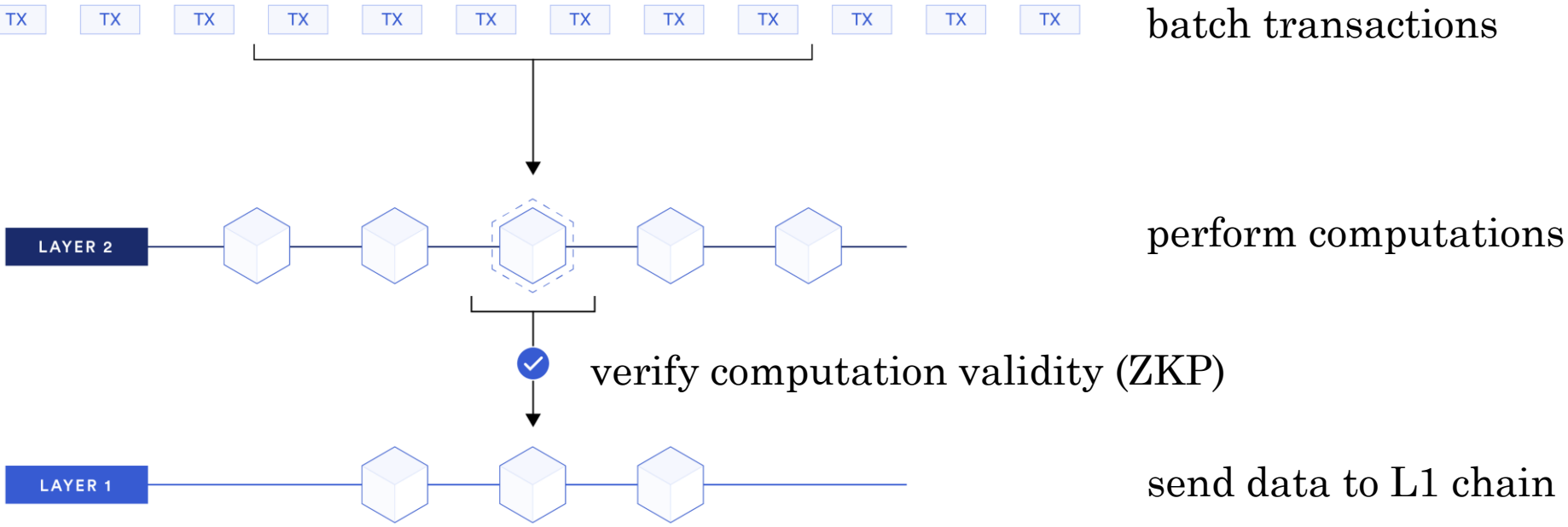


Figure 3: Framework ZKP in blockchain

ZKP on Ethereum blockchain

- Poor scalability (low transaction throughput) ➔ L2 networks (L2 scaling solutions)
- Zk-Rollups



ZKP use cases

- **Zk-Rollups on Ethereum**
- **Anonymous Verifiable Voting:** In the process of voting the voter's identity is kept private
- **Secure Exchange of Digital Assets:** The identity and transaction amount are kept private
- **Secure Remote Biometric Authentication:** fingerprints, facial images, iris or vascular patterns
- ZKP generates a proof containing a process of transaction/voting/identification...

ZKP projects

polygon zkEVM

L2 Zk-Rollup solution
zkSNARKs

Mina Protocol

L1 blockchain
Succint blockchain (constant size 22B)
Consensus state verification via ZKP

ZCASH

Extension of Bitcoin network
hides the transaction amount and destination

Further research: Nion Network

- Decentralized cloud computing network
- Transactions: migrations of Docker containers between nodes
- Problem: How to verify a node is really running the container
- Proposed solution: ZKP

References

- Čapko, Darko, Srđan Vukmirović, and Nemanja Nedić. "State of the art of zero-knowledge proofs in blockchain." _2022 30th Telecommunications Forum (TELFOR)_. IEEE, 2022.
- Sun, Xiaoqiang, et al. "A survey on zero-knowledge proof in blockchain." _IEEE network_ 35.4 (2021): 198-205.
- Zhou, Lu, et al. "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities." _Journal of Information Security and Applications_ 80 (2024): 103678.
- Chi, Po-Wen, Yun-Hsiu Lu, and Albert Guan. "A privacy-preserving zero-knowledge proof for blockchain." _IEEE Access_ (2023).
- Sasson, Eli Ben, et al. "Zerocash: Decentralized anonymous payments from bitcoin." _2014 IEEE symposium on security and privacy_. IEEE, 2014.
- zkSNARKs & zkSTARKs: A Novel Verifiable Computation Model (https://illya.sh/blog/posts/zksnark-zkstark-verifiable-computation-model-blockchain/)(Accessed: 19. 4. 2024)

Thank you for your attention!