Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 2** : 1–7.
ISSN-0037-8712
doi:10.5269/bspm.80464

From Theory to Implementation: Leveraging Zero-Knowledge Proofs for Secure Blockchain Transactions

M. Vijay Bhasker Reddy and Soujanya Duvvi

ABSTRACT: The blockchain technologies have the potential of being decentralized and secure, yet they suffer major privacy and scalability issues in the public networks. Zero-Knowledge Proofs (ZKPs) is an influential cryptographic scheme that allows one party to demonstrate whether a statement is valid without disclosing the information. In this paper, the authors discuss the concept of integrating ZKPs into blockchain ecosystems to further their privacy in transactions, increase scalability, and enable trustless checks. We look at the theoretical concepts, challenges of implementation, and practical applications and give a framework of the deployment of ZKPs in blockchain systems. The applications of performance evaluation to decentralized finance (DeFi) and identity management and future research directions are presented. The combination of theory and practice helps develop the potential of ZKPs to develop safe and effective blockchain infrastructures [1]-[3] in this work.

Keywords: Zero-Knowledge Proofs (ZKP), blockchain, zk-SNARKs, zk-STARKs, privatizing transactions, scalability, Decentralized Finance (DeFi), cryptographic protocols.

Contents

2020 *Mathematics Subject Classification:* 68W15, 94A60.
Submitted November 29, 2025. Published March 14, 2026

1. Introduction

The blockchain technology has revolutionized digital trust to provide decentralized and tamper-resistant registers [4]. Transparency is guaranteed by public blockchains, including Bitcoin and Ethereum, but these blockchains by definition publish all transaction-related information, posing a risk to the privacy of individuals and organizations [5]. This loss of confidentiality may result in surveillance, analysis of transaction patterns, and front-running on decentralized finance websites (DeFi) [6].

1.1. Zero-Knowledge Proofs (ZKPs) Overview

When explaining the concept of zero-knowledge Proofs introduced by Goldwasser, Micali and Rackoff [7], a party (the one making the statement) is allowed to convince the other (the one that verifies the statement) that the statement is true without providing any new information. Recent progress has seen zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) [8] and zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) [9] become computationally viable to use in blockchain applications.

1.2. Applicability of Privacy and efficiency enhancing in blockchain

The privacy saving solutions play a crucial role in the protection of identity and sensitive information of users in addition to monitoring the stipulations [10]. Meanwhile, the blockchain networks are currently encountering bottlenecks of scalability as the number of transactions increases. ZKPs address the privacy and efficiency issues by reducing the amount of data to be stored on the chain and maximizing throughput [11].

1.3. Motivation and the Research Gap

Even though ZKPs have successfully been implemented in these projects such as zkSync [13] and Zcash [12], challenges to their wider adoption are interoperability, computational complexity, and trusted setup issues. It has not done any comprehensive research on how theoretical models are connected with practical solutions in varying blockchain conditions.

1.4. Statement of Objectives and Scope of the Paper

The article studies safe blockchain transactions integration by ZKP with the design concepts, performance, and practical application. These are privacy preserving payments, DeFi, decentralised identification and enterprise blockchain systems.

1.5. Paper Organization Background

Second section is the review of related work. In section III, the theoretical background of ZKPs is provided. Section IV contains information about the implementation issues and the performance measurement. Section V discusses the applications and future of research. Key findings and outlook are mentioned in section VI.

1.6. Related Work

Zk-SNARK protocols and practical ZKPs to blockchain privacy were first published by Ben-Sasson et al. [8]. The Zcash was the first to implement shielded transactions based on zk-SNARK, demonstrating that privacy-preserving cryptocurrencies can work at scale [12]. To improve privacy and scalability, Butterin et al. [14] suggested the implementation of ZKPs in Ethereum, which resulted in zk-Rollup applications such as zkSync [13] and StarkNet [9]. Recent papers discuss the integration of ZKPs with secure multiparty computation and federated learning to expand the blockchain uses [15]. Nevertheless, such unresolved problems as trusted setup ceremonies [8], proof size optimization [9], and post-quantum security are still under active research.

1.7. Zero-knowledge proofs The basics of zero-knowledge proofs

zk-SNARKs are required to be complete, sound and have a zero-knowledge property [7]. zk-STARKs achieve post-quantum security without any trusted setups at the expense of larger proofs [9].

1.8. Privacy Blockchain Mechanisms

The traditional techniques, such as CoinJoin and ring signature, are more privacy-enhancing, yet not scalable and have no formal security applications [5], [17]. ZKPs are more guaranteed as they are able to perform transactions without giving out sensitive information.

1.9. Relevance of J. Scalability and Efficiency

The expanded use of succinct proofs of transactions (e.g., zk-Rollups) is used by ZKPs to reduce on-chain data, on-chain throughput, and on-chain fees [13], [14]. This makes them both needed to scale Layer-1 blockchains and also facilitate high-performance Layer-2 applications.

2. Methodology

Capacity: Zero-Knowledge Proofs (ZKPs) Secure Blockchain Transaction Algorithm.
Input: Tx, User identity ID, Blockchain network BC
Output: Authenticated and privacy protected deal stored in the blockchain.
Transaction Initialization: This step identifies the transaction type to be completed.
Step 1: Transaction Initialization: This step determines the kind of transaction that is to be made.

- At the end of user U, U creates a transaction Tx with:
  - Create the details of amount / Asset transfer.
  - Recipient address
  - Timestamp
- To provide authenticity, user U signs the transaction by using his or her private key.

Step 2: Generation of Zero-Knowledge Proof.

- Choose the ZKP protocol:
  - zk-SNARK of succinct, non-interactive proofs (trusted setup needed).
  - zk-STARK of transparent, post-quantum secure proofs (better sized proof)
- Cipher transaction information into a statement S such that:
  - S is valid provided that the transaction is legal.
- Produce evidence Pi = ZKPProver(S, Witness) with Witness being hidden transaction data (e.g. sender balance).

Step 3: Proof Verification

- Post Tx and Pi to blockchain validators / smart contract.
- Validators carry out ZKPVerifier(Pi, S):
  - If proof is valid: proceed
  - Else: reject transaction
- None of the information of sensitive transactions is disclosed to validators.

Step 4: Submission of a Transaction.

- Tx to a block is included in the blockchain as append Tx.
- Apply Layer-2 scaling (non-compulsory e.g. zk-Rollups) to achieve efficiency:
  - Bring together a number of transactions off-chain.

  - Network A single succinct submission of transactions.
  - Minimise data and transaction costs through the block chain.

Step 5: Consensus and Recording

- The block is verified by blockchain consensus mechanism (PoW/ PoS).
- Record of transaction is eternal.
- The data of the transactions is kept in secret and at the same time, integrity is maintained.

Step 6: Non-compulsory: Post-Quantum Security.

- For future-proofing:
  - zk-STARKs can be used to provide post-quantum security.
  - Make sure the protocol is not based on trusted setup.

Step 7: Audit and Access Control

- Validity of transactions can be checked by auditors or smart contracts without having to access sensitive data.
- Keep records of compliance to regulatory standards and also maintain privacy.

2.1. Complications of Calculations and Formation of Proofs

Zk-SNARKs are resource intensive to generate and need hardware acceleration and batching to achieve this [18]. zk-STARKs are cheaper to set up but demand more bandwidth [9].

2.2. Trusted Setup and Assumption of Security.

zk-SNARKs have their trusted setup as a single point of failure in case it is compromised [8]. This risk is addressed by multi-party computation protocol and transparent methods such as zk-STARKs [9].

2.3. Network Overhead and Scalability

ZKP integration raises both the cost of computing and communicating to the validators and full nodes [14]. zk-Rollups solve this problem by offloading computation, but retaining security guarantees [13].

2.4. Performance Evaluation

The current benchmarks indicate that zk- Rollups are capable of a throughput of up to 100x more than on-chain processing [13]. In DeFi systems, the generation of proof is hardware-accelerated, which increases the user experience by lowering the latency [18], [19].

3. Results

ZKPs have radical potential of blockchain interoperability, scalability, and privacy. Their successful implementation will be reliant on the handling of standardisation loopholes, trusted setups and computing expenses. The paradigm introduced in this paper promotes scalable blockchain ecosystems that are safe because it closes the gap between theory and practice.

Table 1: Performance Analysis

Metric	Description	Notes
Transaction Initialization Time	Time to generate and sign Tx	Normally insignificant in comparison to ZKP generation
Generation Time Proof generation Time	Time taken by ZKP prover to generate Pi	ZKP type: zk-SNARK is faster, and zk-STARK is slower yet quantum-secure
Proof Size	Proof size in bytes	zk-SNARKs:200-300 bytes; zk-STARKs:a few KBs
Verification Time	Time used to verify Pi	zk-SNARKs: milliseconds; zk-STARKs: a bit more.
Inclusion Time of blockchain	Time to add transaction to block	Depends on block size, consensus mechanism.
Throughput (TPS)	Transactions per second	zk-Rollup scales better TPS (e.g., zk-Rollup)
Gas / Transaction Fee	Storing proof and Tx on-chain	chain Costs Reduced by aggregation

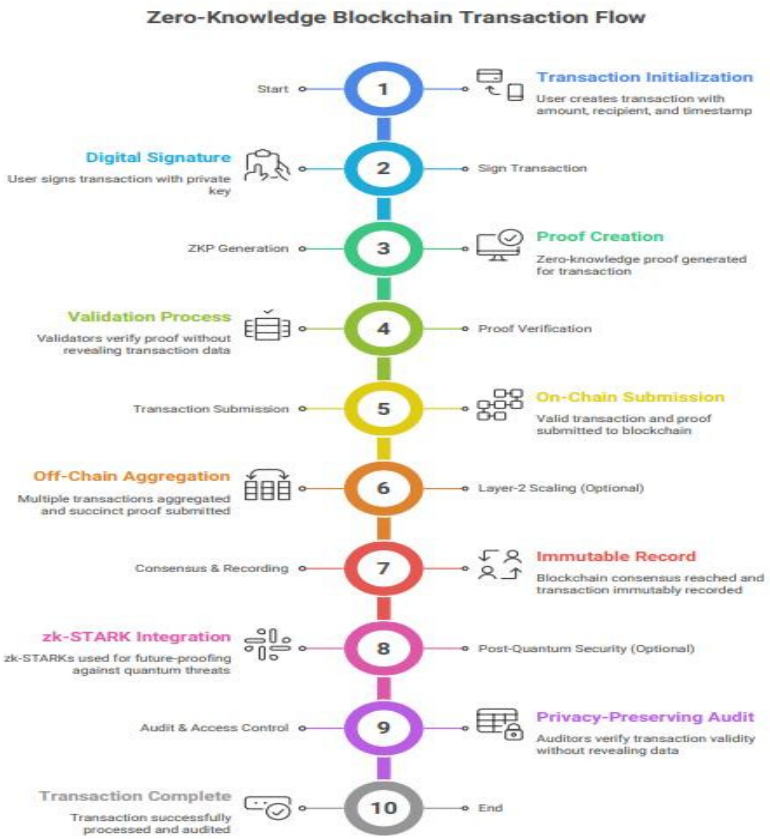

Figure 1: Zero knowledge blockchain transaction flow

4. Discussion

Uses of ZKPs in blockchain systems Secrecy of information of the transaction: Zcash protects the information concerning the transactions with the help of zk-SNARKs [12]. ZKPs are used in the anonymity transfer in Ethereum mixers, such as the Tornado Cash [20]. Decentralised Finance (DeFi): StarkNet and zkSync are more efficient and quicker in terms of transactions as zk-Rollups [13], [9]. ZKPs are used in Iden3 and Polygon ID where verifying an identity is done and it serves as access control [21]. Enterprise Blockchain and Supply Chain: Hyperledger Fabric involves the use of ZKPs in instances of privatized but audited transactions [22].

4.1. New Developments

ZKPs Post-quantum security is under investigation using zk-STARKs [9], zk-EVMs using private smart contracts [14], cross-chain interoperability [23].

4.2. Problems and limitations

The main challenges are some computational overhead [18], trusted setup problems [8], and interoperability problems [13].

4.3. Future Research prospects

The priorities should include standardisation [25], transparent, and post-quantum secure, protocols [9], integration into MPC systems and IoT systems [26], and effective generation of proofs [24].

5. Conclusion

Zero-Knowledge Proofs are also being managed in order to transform the privacy and scalability of blockchains: zk-SNARKs and zk-STARK have their own trade-offs: minimal proofs using trusted setup, or minimal trust using minimal proofs [8], [9]. Hardware acceleration and batch verification can be used to lower bottlenecks in performance [18], [24]. The increasing presence of ZKPs in DeFi, identity systems, and cross-chain protocols is significant to next-generation distributed ledgers [12], [13], [23]. Efforts should continue in future studies to seek a transparent and post-quantum system of proofs and a strong interoperability standard [9], [25]. ZKPs will be able to create privacy-preserving, scaled-up, and secure blockchain infrastructures by providing a link between theory and practical deployment strategies [7], [14].

References

1. Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system*, (2008).
2. Wood, G., *Ethereum: A secure decentralised generalised transaction ledger*, Ethereum Project Yellow Paper, (2014).
3. Zhang, F., Cecchetti, E., Croman, K., Juels, A., and Shi, E., *Town crier: An authenticated data feed for smart contracts*, Proc. ACM SIGSAC Conf. Computer and Communications Security, 270–282, (2016).
4. Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., and Capkun, S., *On the security and performance of proof of work blockchains*, Proc. 23rd ACM Conf. Computer and Communications Security (CCS), 3–16, (2016).
5. Ron, D. and Shamir, A., *Quantitative analysis of the full Bitcoin transaction graph*, Proc. Financial Cryptography and Data Security, Springer, 6–24, (2013).
6. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., and Juels, A., *Flash Boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability*, Proc. IEEE Symp. Security and Privacy (SP), 910–927, (2020).
7. Goldwasser, S., Micali, S., and Rackoff, C., *The knowledge complexity of interactive proof systems*, SIAM J. Comput. 18(1), 186–208, (1989).
8. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., and Virza, M., *SNARKs for C: Verifying program executions succinctly and in zero knowledge*, Proc. 33rd Int. Cryptology Conf. (CRYPTO), Springer, 90–108, (2013).
9. StarkWare Industries, *STARKs, scalability, and privacy*, White Paper, (2021).
10. Conti, M., Kumar, E. S., Lal, C., and Ruj, S., *A survey on security and privacy issues of Bitcoin*, IEEE Commun. Surveys Tuts. 20(4), 3416–3452, (2018).
11. Buterin, V., *On-chain scaling to 500 tx/sec through mass validation*, Ethereum Blog, (2018).
12. Zcash, *Zcash protocol specification*, Electric Coin Company, v2022.2.9, (2022).
13. zkSync, *zkSync: Scaling Ethereum with zkRollups*, Matter Labs, White Paper, (2022).
14. Buterin, V. et al., *zk-EVM: Towards privacy-preserving smart contracts*, Ethereum Foundation Blog, (2022).
15. Choudhury, A., Rahman, M. S., and Misra, S., *Combining MPC and ZKPs for secure IoT blockchain networks*, Proc. IEEE Int. Conf. Blockchain, 217–224, (2022).
16. Bernstein, D. J., Chuengsatiansup, C., Lange, T., and van Vredendaal, C., *NTRU prime: Reducing attack surface at low cost*, Proc. Int. Conf. Selected Areas in Cryptography, Springer, 235–260, (2017).
17. van Saberhagen, N., *CryptoNote v 2.0*, White Paper, (2013).
18. Bünz, B., Fisch, B., and Boneh, D., *Batching techniques for zero-knowledge proofs*, Proc. IEEE Symp. Security and Privacy (SP), 1–15, (2019).
19. Bai, X., Luo, Y., Xu, Z., and Zhang, J., *Accelerating zero-knowledge proof generation using GPUs*, IEEE Trans. Parallel Distrib. Syst. 33(12), 4567–4578, (2022).
20. Tornado Cash, *Tornado Cash: Privacy solution on Ethereum*, GitHub Repository, (2022).
21. Iden3, *Self-sovereign identity using zero-knowledge proofs*, White Paper, (2022).
22. Androulaki, E. et al., *Hyperledger Fabric: A distributed operating system for permissioned blockchains*, Proc. 13th EuroSys Conf., 1–15, (2018).

23. Zhang, L., Huang, J., and Chen, W., *Cross-chain interoperability and privacy using zero-knowledge proofs*, IEEE Access 10, 104321–104335, (2022).

24. Chiesa, A. et al., *Recursive composition of interactive proofs for succinct arguments*, Proc. 45th ACM Symp. Theory of Computing, 1–10, (2013).

25. W3C, *Decentralized identifiers (DIDs) v1.0*, W3C Recommendation, (2021).

26. Choudhury, A. et al., *Combining MPC and ZKPs for secure IoT blockchain networks*, Proc. IEEE Int. Conf. Blockchain, 217–224, (2022).

M. Vijay Bhasker Reddy,
Research Scholar, Dept. of CSE, GITAM University, Vishakhapatnam,
Sr. Assistant Professor, Dept. of CSE, Geethanjali College of Engineering and Technology, Hyderabad
India.
E-mail address: muppuvijay@gmail.com

and

Soujanya Duvvi,
Assistant Professor, Dept. of CSE, GITAM University, Vishkhapatnam
India.
E-mail address: sduvvi3@gitam.edu