IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
University of Kut Journal
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
js.uokut.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
Vol. 11 , Issue 1 , June 2026

Using zero-knowledge proofs to ensure private and secure blockchain transactions

Mehran Mahya Ahmed [1]

Abstract

Application of zero knowledge proofs makes blockchain technology more privacy-enhancing, without jeopardizing its transparency. Due to the privacy implications of blockchain networks — whose openness of transaction data tends to concern users — zero-knowledge proofs provide a viable alternative that allows the involved parties to verify the validity of a transaction without necessarily exposing any private data. The focus of the examination is on zk-SNARKs and zk-STARKs that are two improved forms of ZKPs that enhance scalability along with privacy. Studies of already established blockchain protocols revealed that the implementation of zk-SNARKs/STARKs and zk-Rollup was successful in enhancing the privacy, safety, and scalability of applications like Zcash and Ethereum, in spite of diverse computational and regulatory challenges.

Keywords: Zero Knowledge Proofs (ZKPs), Privacy-Preserving Blockchain, Cryptographic Proofs

استخدام براهين المعرفة الصفرية لضمان معاملات بلوكشين خاصة وآمنة

مهران محي احمد [1]

المستخلص

يؤدي تطبيق براهين المعرفة الصفرية (Zero-Knowledge Proofs) إلى جعل تقنية "البلوكشين" أكثر تعزيزاً للخصوصية، دون المساس بشفافيتها. ونظراً للتبعات المتعلقة بالخصوصية في شبكات البلوكشين —والتي تثير قلق المستخدمين بسبب الطبيعة المكشوفة لبيانات المعاملات— توفر براهين المعرفة الصفرية بديلاً فعالاً يتيح للأطراف المعنية التحقق من صحة المعاملات دون الحاجة بالضرورة للكشف عن أي بيانات خاصة .يركز هذا البحث على تقنيتي zk-SNARKs وzk-STARKs، وهما شكلان متطوران من براهين المعرفة الصفرية يعملان على تحسين قابلية التوسع جنباً إلى جنب مع تعزيز الخصوصية .وقد كشفت الدراسات التي أجريت على بروتوكولات البلوكشين القائمة بالفعل أن تطبيق تقنيات zk-SNARKs/STARKs و zk-Rollup قد نجح في تعزيز الخصوصية والأمان وقابلية التوسع في تطبيقات مثل Zcash وEthereum، وذلك على الرغم من التحديات الحسابية والقانونية المتنوعة.

الكلمات المفتاحية: براهين المعرفة الصفرية (ZKPs)، البلوكشين المحافظ على الخصوصية، البراهين التشفيرية

Affiliation of Author
[1] Mathematics and its Applications, Algebra, University of Maragheh, Iran, 34141-88186

[1] mmhy79511@gmail.com

[1] **Corresponding Author**

Paper Info.
Published: Jun. 2026

انتساب الباحث
[1] الرياضيات وتطبيقاتها، الجبر، جامعة مراغهد، إيران، -34141 88186

[1] mmhy79511@gmail.com

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر : حزيران 2026

Introduction

The technology of blockchain has gained a significant role in the past years. It is facilitating decentralisation and transparency in a variety of industries such as finance, supply chains and DeFi[1,2]. One of the greatest advantages of this technology is that an individual can trust a transaction without relying on third parties [3]. However, this inherent openness poses a massive privacy threat. In most blockchain platforms, information related to transactions, such as the identities of the senders and receivers, the transaction amount, and other confidential data, is publicly available. This visibility has the potential to enhance trust in decentralized systems [4], though at the cost of user privacy [5]. This is particularly in the rapidly developing industry of DeFi, where the user ID and transaction data are the most important security concerns. [6,7] Zero-

knowledge proofs (ZKPs) may be the solution to this privacy issue, as illustrated in Figure (1). Zero-knowledge proofs are cryptographic protocols in which one party (the prover) convinces another party (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself. In this system, validation of transactions on the blockchain is possible without the need to reveal any personal data of the parties involved, such as transaction value and the identity of senders and receivers [8].

The application of ZKPs in blockchain processes has received significant interest, and protocols such as zk-SNARKs and zk-STARKs provide effective approaches to privacy assurance of transactions in open blockchains.

Such cryptography techniques are already used in blockchain applications, such as Zcash, which allows users to keep their transactions private yet verifiable, without disclosing their personal data [9]. However, there are several problems with the adoption of these techniques in blockchain systems, including high computational resource consumption and scalability issues [10,11]. This paper has tried to examine how ZKPs will enhance privacy and security of blockchain transactions. The purposes of the study are as follows: (1) to comprehend the cryptographic background of the zk-SNARKs protocols and how they are applied to the blockchain systems; (2) to demonstrate how the zk-SNARKs protocols could be used to implement private transactions in decentralized networks; and (3) to analyze how the zk-SNARKs protocols are implemented in blockchain protocols to allow their compatibility and scaling. We also examined the contribution of zk-rollups, which use zero-knowledge proofs to enhance blockchain scalability and efficiency. As Figure (1) shows, with zero-knowledge proofs (ZKPs) blockchain technology has enhanced its privacy and scalability.

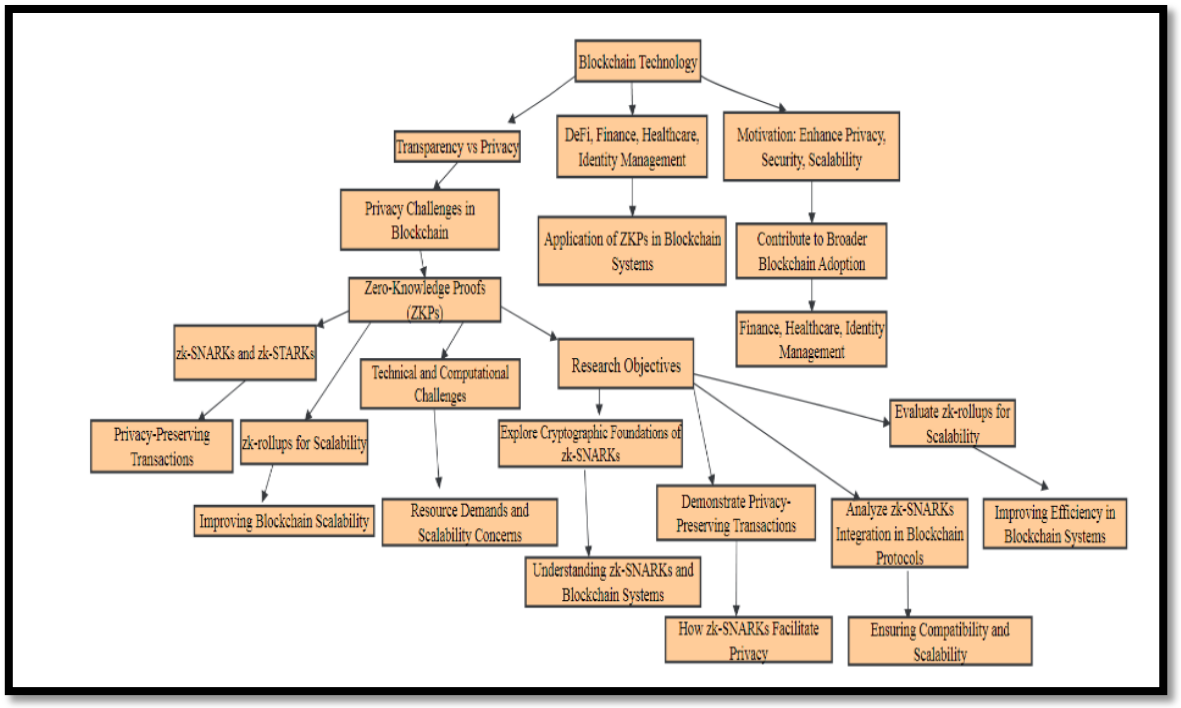

Figure (1): Enhancing privacy and scalability in blockchain technology using Zero-Knowledge Proofs (ZKPs)

Research Problem

The transparency provided by blockchain poses a problem since it reveals the identities and amounts of transactions thus threatening privacy. The privacy guarantees of blockchain systems like Ethereum and Zcash remain insufficient. Further, achieving efficient privacy and computation with Zero-Knowledge Proofs (ZKPs) such as zk-SNARKs/zk-STARKs remains very challenging.

Research Significance

The importance of this research is to provide new encryption solutions to achieve user privacy while maintaining blockchain transparency to enhance trust in networks such as Ethereum and Zcash, and facilitate decentralized finance (DeFi). It provides a unique perspective on the development of zk-SNARKs, zk-STARKs, and zk-rollups protocols that underpin transaction confidentiality, enhance scaling, and limit the intermediary requirement, while their use in supply or finance helps to conform to global privacy guidelines.

Research Objectives

The research aims to create zero-knowledge proofs (ZKPs) that can help enhance privacy and security of blockchain transactions within decentralized networks by learning the fundamentals of zk-SNARKs and their application in Zcash and Ethereum to achieve private transaction with transparency and scalability through zk-rollups. This also looks into the computational challenges and proposes applications in DeFi and supply chains.

Literature Review

Many earlier studies have already researched the topic of this study. Below are the most important of these studies:

The study by [12]: The goal of this study is to show how ZKP contributes to verifying identity in a secure way while protecting the identity of a person, identifying the most needed developments in this field as well as analyzing and critiquing the developments. The research employs a critical approach to a collection of studies and applications on the subject of the study and demonstrates that the method used on the study sample is a useful, secure, and safe the method, and that recent inventions have played an important role in enhancing its privacy and safety, but it still requires development to enhance its performance further.[12]

The study by [13]: The study sought to demonstrate the utility and role of zk-SNARKs and zk-STARKs, which are advanced forms of zero-knowledge proof. Analytic methods were used for existing blockchain protocols, Zcash and Ethereum. In conclusion, zero-knowledge proofs can enable scaling mechanisms like zk-rollups, which group multiple transactions into one proof, thus reducing blockchain congestion while also providing privacy[13]

A study by [14]: It aimed to examine crucial mechanisms applied to guarantee secure privacy in blockchain technology. It also emphasized the primary problems and complications encountered by practitioners of these methods. The research offered guidelines and solutions for achieving high privacy and security, along with a set of necessary solutions to overcome the set challenges.[14]

A study by [15]: the latest technologies under scrutiny and the difficulties and solutions of smart environments. The report also elaborated on the use of blockchain and Internet of Things (IoT)

technologies as the basics and basic block of such smart environments. An integration of different smart technologies enhances the benefits of each technology and mitigates their shortcomings. Hence, the proposed configuration achieves its goal with high efficiency .[15]

Materials and Methodology

The objective of this study is to protect blockchain platforms using the ZKP (Zero-Knowledge Proof) method.

To build the application, we will develop the Ethereum approach further using the Solidity language and deploy it inside the Truffle framework. We will combine different blockchains: Zcash and Ethereum. To enhance the study, the authors utilized zk-SNARKs, zk-Rollups, and zk-STARKs, as well as encryption techniques. The TPS technique was used for performance measurement, and the ZoKrates method was used. In addition, security and computational techniques were employed. The study tools are discussed in Table 1 along with their significance.

Table (1): Tools Used and Their Importance

Tool/Technology	Key Importance
Ethereum	**A leading smart contract platform powered by Solidity, supporting zk-Rollups to enhance scalability and privacy while reducing gas costs**
Zcash	**Focusing on privacy through zk-SNARKs, protecting transaction identities and amounts with validation.**
Solidity	**A programming language for developing smart contracts on Ethereum, the basis for integrating ZKPs into applications.**
Truffle	**A framework for deploying and testing smart contracts on Ethereum, facilitating the implementation of privacy solutions.**
zk-SNARKs	**Concise, non-interactive knowledge arguments; small, quick-verification proofs; protect transaction details (like Zcash); require a reliable setup.**
zk-STARKs	**Transparent and scalable arguments; no reliable setup required, more transparent but larger proof sizes and higher computation.**

Tool/Technology	Key Importance
zk-Rollups	Aggregating off-chain transactions with ZKPs on Ethereum improves scalability (TPS) and reduces congestion while maintaining privacy.
ZoKrates	The zk-SNARK toolkit for Ethereum generates proofs for private verification.
snark.js	A JavaScript library for efficiently creating zk-SNARK proofs.
Circom	A tool for creating zk-SNARK circuits; converting logic into special proofs.
Plonk	An encryption protocol that improves the efficiency of zk-SNARK proofs, reducing computational complexity.

Table 2 shows the process block diagram, i.e., the process inputs and outputs.

Table (2): Process Block Diagram

Outputs	Inputs
Special transaction execution: Success/Failure	Blockchain Network: Ethereum/Zcash
Impact of scalability: {Lower gas cost, improved transaction rate per second}	Transaction Details: {Sender, Receiver, Amount}
Impact of scalability: {Lower gas cost, improved transaction rate per second}	Cryptographic Proof Type: zk-SNARK / zk-STARK / zk-Rollup
Security and Compliance: {Pass/Fail, Anti-Money Laundering/Know Your Customer Status}	

The steps followed in the research are as follows:

Step 1: Library Preparation

In this step, both the blockchain libraries and the encryption were prepared first, according to Figure (2).

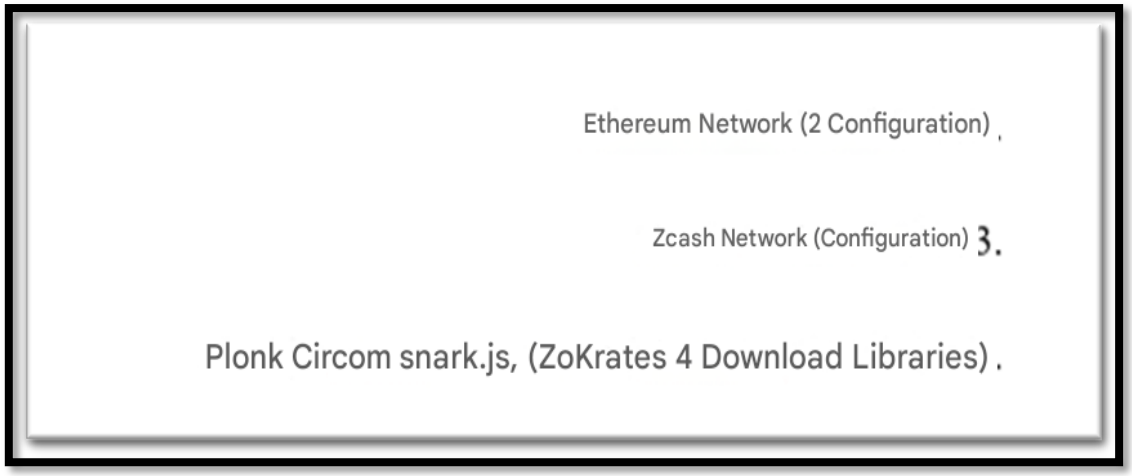

Figure (2): Library Initialization

Step 2: Designing the Function or Algorithm Used to Prove Zero Knowledge

Step 2 is implemented through Figure (3).

```
ZKP Proof (Transaction Details) (Learn more at www)

Create proof of sender, recipient, and transaction amount without disclosing details

8. proof = Generate Proof(Transaction Details)
```

Figure (3): Design of the proof function

Step 3: zk-SNARKs for special parameters

This step is illustrated in Figure (4).

```
ZK SNARKS Transaction(Sender, Receiver, Amount)

proof = ZKP Proof(Sender, Receiver, Amount)

Store Proof On Blockchain(proof)

if Verify Proof(proof) is True:
    Execute Private Transaction(Sender, Receiver, Amount)
else:
    Reject Transaction()
```

Figure (4): Step 3

Step 4: Applying zk-STARKs to special parameters

The function is illustrated in Figure (5).

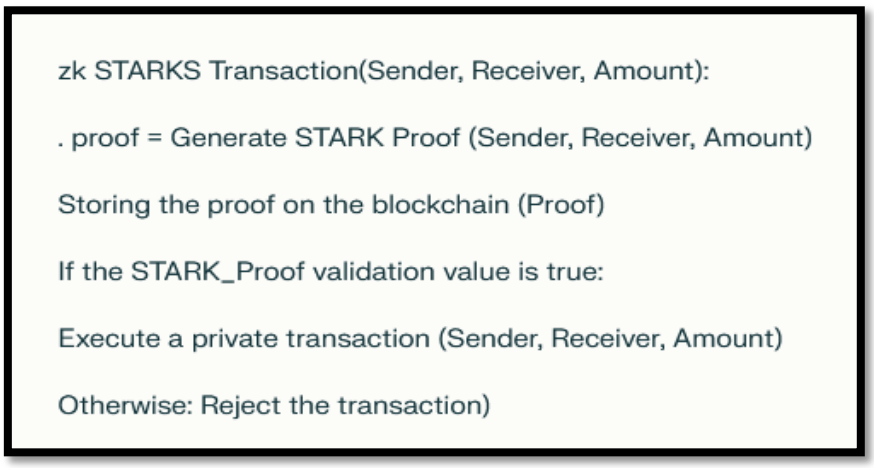

Figure (5): Step 4

Step 5: Applying zk-Rollups for scalability

This step is illustrated in Figure 6

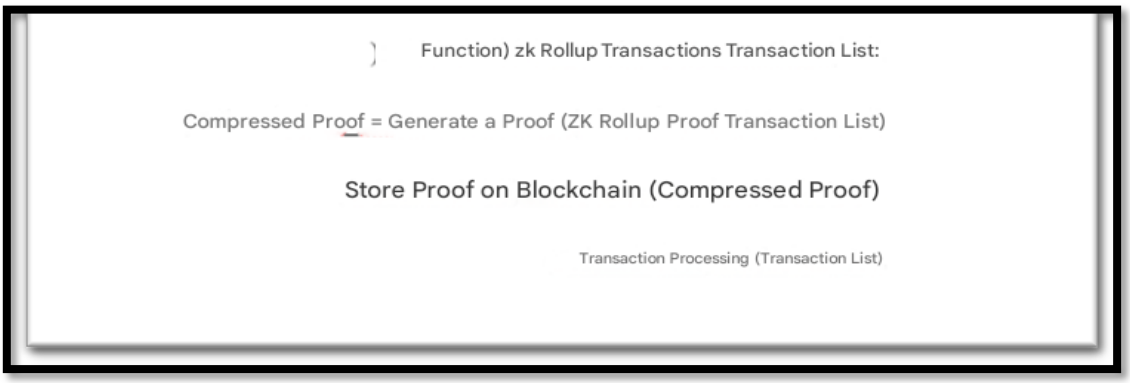

Figure (6): Step 5

Step 6: Evaluating Performance Measures

This step is illustrated in Figure (7).

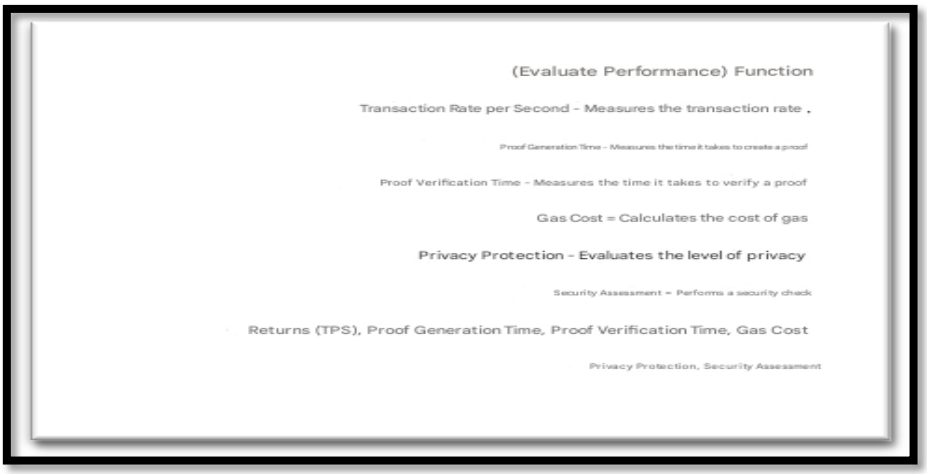

Figure (7): Step 6

Step 7: Running simulations on Ethereum and Zcash

This step is illustrated in Figure (8).

```
For each transaction in simulated transactions

42 Sender, Receiver, Amount zk SNARKS Transaction(

43 Sender, Receiver, Amount zk STARKS Transaction(

Collecting performance data
```

Figure (8): Step 7

Step 8: Conduct a security and organizational analysis

Step eight was implemented through Figure (9).

```
Security Outcomes = Security Risk Assessment

Regulatory Compliance - Verification of Regulatory Guidelines
```

Figure (9): Step 8

Step 9: Outputting the Results

Step 9 was performed using Figure (10).

```
Print "Performance Metrics:", Performance Evaluation ()

Print "Security Evaluation:", Security Results

Print "Regulatory Compliance:", Regulatory Compliance

End of pseudocode
```

Figure (10): Step 9

The system utilizes zero-knowledge proofs (ZKPs), including zk-SNARKs, zk-STARKs, and zk-Rollups, to enable private transactions on a blockchain (such as Ethereum or Zcash), with the help of libraries like ZoKrates and Circom. It automatically generates proofs to verify transactions without revealing confidential information. It processes transactions using ZKPs for privacy and optimizes scalability through zk-Rollups, aggregating several transactions into one proof. It assesses performance such as TPS, proof time, and gas costs along with security and regulatory compliance as shown in figure (11).

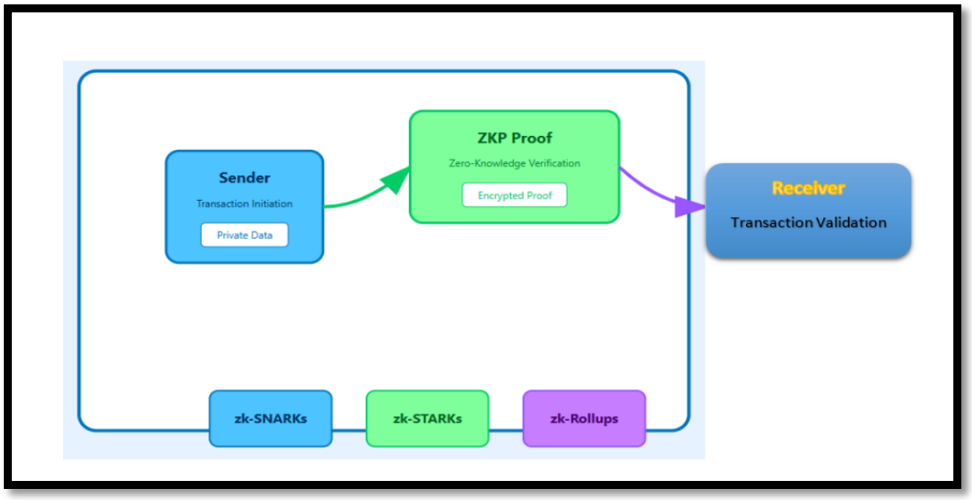

Figure (11): Blockchain Transactions Using Zero-Knowledge Proofs

This is the depiction of the ZKP implementation: the user initiates the transaction in private, forms a ZKP proof for verification while keeping the details hidden, and signs the transaction after sending it to the receiver's public key for verification. We highlight zk-SNARKs (succinct proofs, trusted setup), zk-STARKs (transparent and larger), and zk-Rollups (off-chain scaling) as shown in figure (12).

Implementation

The incorporation of zk-SNARKs/zk-STARKs and ZKPs on a blockchain ensures data privacy, as summarized in Table (3).

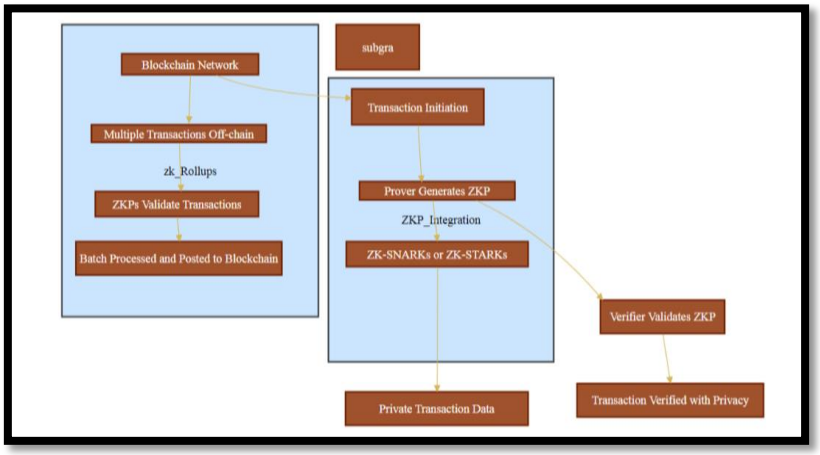

Figure (12): Privacy and scalability workflow in blockchain technology using Zero Knowledge Proofs (ZKPs)

Table (3): ZKP techniques and their importance in blockchain privacy

Technology	Main Description
ZKPs	Transactions are conducted without disclosing identities/amounts.
zk-SNARKs	Small, quick proofs (like Zcash) require a reliable setup.
zk-STARKs	Transparent, computationally larger, for dApps.
zk-Rollups	Aggregating off-chain transactions to expand Ethereum.
Hybrid encryption	With MPC/symmetric encryption for added security.
Organization	Privacy balance with AML/KYC.

6 .Results and Discussion

Results of zk-SNARKs show a promising future for securing and protecting the privacy of blockchain transactions, but also present challenges related to computational efficiency, regulatory compliance (AML/KYC), and environmental impact. zk-SNARKs/STARKs shield info (sender/recipient/amount) as seen in Zcash and Ethereum, while zk-Rollups enhance TPS and lower gas via off-chain processing as shown in figure (13).

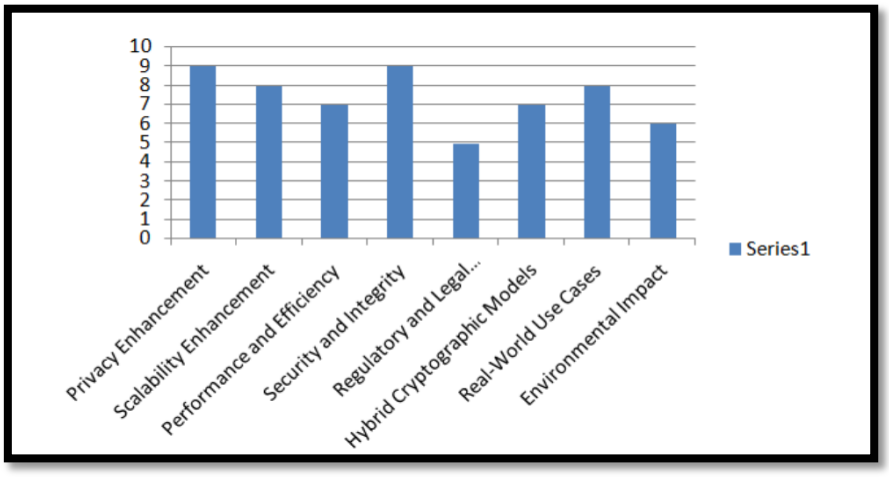

Figure 13: Distribution of Key Results in Leveraging Zero-Knowledge Proofs to Preserve Privacy in Blockchain Transactions

Figure (13) outlines the improvements in privacy (greater than conventional approaches), security, and scalability (despite computational challenges).

Key improvements are illustrated in Table 4 and figure 14.

Table (4): Key Improvements

It protects sensitive data for financial/health applications.	privacy zk-SNARKs/STARKs
Ethereum's capacity increases without loss of privacy.	expansion: zk-Rollups/STARKs
Concise but highly computational; STARKs are more transparent.	performance: zk-SNARKs
Prevents double spending/fraud with record integrity.	Security
With MPC/symmetric encryption for added security, despite the complexity	Hybrid
(Private transactions), Ethereum (dApps)	Zcash cases

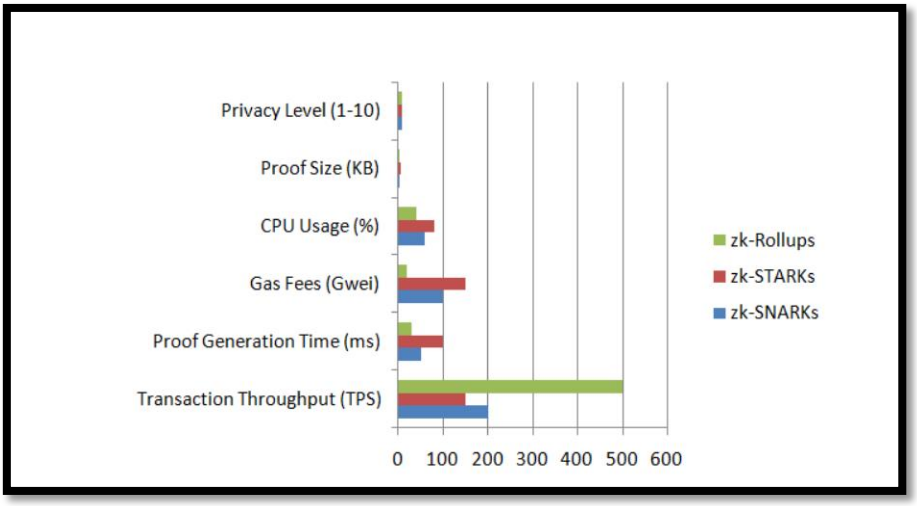

Figure (14): Performance and Privacy Evaluation of Zero-Knowledge Proofs

Environmental Impact: zk-SNARKs are energy-intensive; STARKs are better but require significant resources.

Conclusion and Future Prospects

Zero-knowledge proofs (ZKPs) have been successfully used to increase privacy, security, and scaling for blockchain transactions. ZKPs are already used in blockchain networks, such as Zcash and Ethereum. Their wider adoption is limited by several obstacles, including computational complexity, anti-money laundering

and know-your-customer (AML/KYC) regulation and environmental sustainability issues. Future work focuses on reducing the resource consumption of zk-SNARK/STARK algorithms, integrating ZKPs with MPC/hybrid cryptography, enhancing cross-chain compatibility (Ethereum/Zcash), DeFi, regulatory solutions, eco-centric systems, as well as integrating with AI/IoT for advanced data privacy.

Reference

[1] Buterin, V. (2017). *A Next-Generation Smart Contract and Decentralized Application* Platform. Ethereum White Paper.

[2] Zcash Team (2016). Zcash: The Knowledge Proof Protocol. Electronic copy available at: https://ssrn.com/abstract=5239705

[3] Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. ACM Conference on Computer and Communications Security (CCS), 459-474.

[4] Buterin, V. (2018). Ethereum's zk-Rollups: Scaling the Ethereum Network with Zero-Knowledge Proofs.

[5] Bünz, B., Kosta, E., & Ben-Sasson, E. (2021). zk-SNARKs for Blockchain Privacy and Security: Current Research and Open Problems. Journal of Cryptographic Engineering, 33(4), 123-145.

[6] Zohar, Y., & Golan, O. (2019). The Scalability and Security Trade-Offs in Blockchain Privacy Solutions. In IEEE Access, 7, 131114–131125.

[7] Arapinis, M., Ben-Sasson, E., & Lio, T. (2022). A Comprehensive Study on zk-STARKs and zk-SNARKs for Privacy-Preserving Blockchain Transactions. Cryptology and Information Security, 31(2), 99-115.

[8] Albrecht, P., et al. (2020). zk-Rollups: Scaling Ethereum with Zero-Knowledge Proofs. In Proceedings of the 2020 International Conference on Blockchain and Cryptocurrency (ICBC '20).

[9] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Symposium on Security and Privacy, 1-15.

[10] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Shacham, H. (2016). Bitcoin and Cryptocurrency Technologies.

[11] Buchmann, J., & Mühleisen, H. (2018). Blockchain and Privacy: A Study of the Transparency and Confidentiality Dilemma. [12] Krombholz, K., et al. (2016). Privacy-Preserving Payment Systems in Bitcoin: A Comprehensive Survey.

[13] Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, *80*, 103678. https://doi.org/10.1016/j.jisa.2023.103678

[14] Fatima, B., & Senthilkumar, P. (2025). *Leveraging zero-knowledge proofs for privacy-preserving blockchain transactions*. Proceedings of the International Conference on Innovative Computing & Communication (ICICC 2024). https://ssrn.com/abstract=5239705

[15] Bernal Bernabe, J., Canovas Sanchez, J. L., Hernández-Ramos, J. L., Torres Moreno, R., & others. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access, 7*, 161384–161413. https://doi.org/10.1109/ACCESS.2019.2950872

[16] Ebrahim, M., Hafid, A., & Elie, E. (2022). Blockchain as privacy and security solution for smart environments: A survey. *arXiv preprint arXiv:2203.08901*. https://doi.org/10.48550/arXiv.2203.08901