# IMPLEMENTING PRIVACY-PRESERVING IDENTITY VERIFICATION WITH ZK-SNARKS: A TECHNICAL EXAMINATION OF ZERO-KNOWLEDGE PROOFS AND THE LEO PROGRAMMING LANGUAGE

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Youssef Cherrat

Spring, 2025.

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date 5-6-25
Youssef Cherrat

Signature _____ Date 5-6-25
Technical Advisor: Aaron Bloomfield, Department of Computer Science

# Utilizing zK Snarks for Data Transfer

CS 4991 Capstone Report, 2024

Youssef Cherrat
Computer Science
University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia US
jja3em@virginia.edu

**ABSTRACT**
Securing data transmission in decentralized networks presents a significant challenge, especially within blockchain environments where transparency often conflicts with privacy needs. This proposal explores zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) as a cryptographic solution that allows for verifiable data transactions without revealing the actual data. Embedding zk-SNARKs into blockchain protocols enables trustless verification, enhancing both scalability and data confidentiality. Preliminary findings indicate zk-SNARKs hold promise for secure, private communication channels in decentralized systems, with potential applications in privacy-focused financial and healthcare blockchains. Future work will focus on optimizing zk-SNARK integration for enhanced processing speed and reduced computational costs.

## 1. INTRODUCTION

In recent years, blockchain technology has become integral to decentralized digital transactions, offering transparent and immutable data records across diverse applications. However, this transparency often conflicts with users' needs for data privacy, especially when sensitive information is involved. For example, financial and medical data, while benefiting from blockchain's security features, require high standards of confidentiality. Traditional cryptographic methods can safeguard data, but they often hinder the scalability and efficiency necessary for widespread blockchain adoption.

To address these challenges, zk-SNARKs emerge as a promising cryptographic technique. They enable a party to prove knowledge of specific information, such as a secret key or computation result, without disclosing the actual data. By integrating zk-SNARKs into blockchain systems, we can achieve both trustless verification and robust privacy, allowing data to be transmitted securely without compromising transparency.

This proposal investigates zk-SNARKs' potential to enhance data security in blockchain networks. We will explore the technical foundation of zk-SNARKs, outline the primary implementation hurdles, and analyze their anticipated impact on scalability and privacy. Ultimately, this study aims to illustrate how zk-SNARKs can transform data handling practices within decentralized systems, promoting safer, more efficient data exchanges.

## 2. RELATED WORKS

The use of zero-knowledge proofs, particularly zk-SNARKs, in blockchain technology has been explored to address issues of privacy and efficiency. Ben-Sasson

et al. (2014) introduced zk-SNARKs as a succinct and non-interactive form of zero-knowledge proof, allowing users to verify information without revealing the underlying data. This development laid the groundwork for integrating zk-SNARKs into blockchain protocols, where trustless verification is essential. Their research demonstrated the feasibility of zk-SNARKs in reducing the computational costs associated with zero-knowledge proofs, thereby making them more practical for real-world applications.

In subsequent work, Buterin (2018) highlighted the potential of zk-SNARKs in enhancing blockchain scalability and privacy. Buterin explored zk-SNARKs' application within the Ethereum network, showcasing how they could allow users to verify transactions without revealing transaction details. His research emphasized zk-SNARKs' role in enabling private smart contracts and reducing data redundancy across the network. Buterin's insights inspired many blockchain developers to consider zk-SNARKs as a foundational element in privacy-focused blockchain projects, illustrating how these proofs can support both privacy and efficiency.

Another significant contribution to zk-SNARKs in blockchain is the practical work done by Parno et al. (2013), who focused on the challenges of efficiently implementing zk-SNARKs in various cryptographic protocols. Their study provided a technical breakdown of zk-SNARKs' components and discussed how these components could be optimized to fit within the resource constraints typical of decentralized systems. Parno et al. also addressed potential vulnerabilities in zk-SNARK protocols, proposing several mitigations to enhance security. This work informed the security considerations necessary for zk-SNARK implementation in blockchain, ensuring both privacy and resilience against attacks.

## 3. PROPOSAL DESIGN

The design of this proposal aims to integrate zk-SNARKs into blockchain protocols to enhance data privacy and scalability in decentralized systems. This section outlines the core components of the proposed design, addressing key implementation challenges and their potential solutions.

### 3.1 Cryptographic Foundation of zk-SNARKs

The integration of zk-SNARKs into blockchain relies on establishing a cryptographic foundation that supports zero-knowledge proofs. zk-SNARKs enable one party to verify data possession without revealing the data itself, achieved through cryptographic hash functions and polynomial commitments (Ben-Sasson et al., 2014). This approach minimizes the data transmitted over the blockchain, helping to maintain privacy while ensuring verifiable interactions.

### 3.2 Implementation Challenges and Solutions

Implementing zk-SNARKs in a blockchain network introduces several challenges, primarily related to computational efficiency and scalability. Zero-knowledge proofs are resource-intensive, and zk-SNARKs are no exception. Buterin (2018) noted the high computational demands of zk-SNARKs, which could potentially limit their feasibility in high-throughput environments like blockchain. To mitigate this, we propose utilizing recursive zk-SNARKs, which aggregate proofs to minimize redundancy and optimize processing time.

Another critical issue is the "trusted setup" required for zk-SNARKs, where a set of

cryptographic parameters must be pre-generated securely. Parno et al. (2013) identified the vulnerability in this setup, as any compromise during this phase could impact the entire protocol's security. To address this, our design includes a multi-party computation (MPC) approach for the trusted setup, ensuring a decentralized and tamper-resistant parameter generation process.

### 3.3 Proposed Integration with Blockchain Protocol

The final component of the proposal involves embedding zk-SNARKs into the blockchain protocol itself. This can be achieved through smart contracts designed to handle zk-SNARK verifications directly on the blockchain. Our design incorporates a modular framework, allowing zk-SNARKs to be used in various blockchain environments without extensive modifications to the underlying protocol. By adopting an adaptable architecture, we aim to streamline zk-SNARK deployment across different blockchain networks, thus making private transactions more accessible.

## 4. ANTICIPATED RESULTS

The proposed integration of zk-SNARKs into blockchain protocols is expected to enhance data privacy and scalability in decentralized networks. By enabling trustless verification without disclosing data, zk-SNARKs allow users to confirm transaction validity without compromising sensitive information. This approach addresses one of the primary limitations in traditional blockchain systems, where data transparency can conflict with privacy requirements. We anticipate that this implementation will be especially beneficial in applications where confidentiality is crucial, such as financial transactions, healthcare data management, and identity verification.

In addition to privacy benefits, zk-SNARKs are expected to improve blockchain scalability by reducing data storage and transmission requirements. Recursive zk-SNARKs, which allow for the aggregation of multiple proofs into a single, compact proof, are likely to reduce the computational burden on network nodes. This reduction will make it feasible to handle a higher volume of transactions without significantly increasing resource consumption. The multi-party computation (MPC) approach for the trusted setup phase is also anticipated to bolster the security of zk-SNARK-based systems, minimizing the risk of compromise and ensuring a tamper-resistant cryptographic foundation.

Overall, the anticipated outcomes suggest that zk-SNARKs will contribute to more secure and efficient data transfer within blockchain networks, creating new opportunities for privacy-preserving applications in decentralized systems. If successful, this proposal could lay the groundwork for future blockchain protocols that prioritize both privacy and performance, setting a new standard for data protection in distributed environments.

## 5. CONCLUSION

The integration of zk-SNARKs into blockchain protocols represents a significant advancement in balancing data privacy with transparency within decentralized networks. This project addresses the growing demand for secure data transmission methods that protect user confidentiality without compromising the verifiability essential to blockchain's trustless nature. By enabling trustless verification, zk-SNARKs allow transactions and data exchanges to occur without exposing sensitive information, making them particularly suited for applications in finance, healthcare, and

identity verification where privacy is critical.

This approach also enhances scalability, as zk-SNARKs reduce the storage and computational load on network nodes, paving the way for more efficient data transfer in high-transaction environments. The study underscores zk-SNARKs' potential to shape the future of privacy-preserving applications within blockchain, offering a solution that aligns with both performance demands and user privacy expectations. Through this work, we contribute to establishing a new standard for secure, privacy-conscious data handling practices in decentralized systems, promising lasting impact on data protection in blockchain.

## 6. FUTURE WORK

Future efforts will focus on optimizing zk-SNARK integration to reduce computational costs further and enhance processing speed, thereby improving the feasibility of zk-SNARKs in large-scale, high-throughput environments. Specifically, implementing recursive zk-SNARKs will be explored to reduce redundancy and optimize proof aggregation, which could enable blockchain networks to handle higher transaction volumes with minimal increases in resource consumption.

Additionally, research into alternative methods for the trusted setup phase, such as transparent zk-SNARKs, could offer solutions that remove the reliance on multi-party computation (MPC), further securing the cryptographic foundation. Expanding this project to test zk-SNARKs across various blockchain networks will provide insights into adaptability and scalability, identifying application-specific optimizations to maximize their effectiveness in fields such as finance, healthcare, and secure identity verification.

## 7. ACKNOWLEDGMENTS

I would like to thank Professor Bloomfield for his guidance throughout this project, particularly through his CS 4501 Cryptocurrency course, which provided foundational knowledge and inspiration for exploring zk-SNARKs in the context of blockchain. His expertise and insights have been invaluable to this work, as have the contributions of the wider academic community in advancing zero-knowledge proof research.

## REFERENCES

Aleo. (n.d.). An introduction to zero-knowledge proofs. Aleo. https://www.aleo.org/technology

Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., & Virza, M. (2014). Succinct non-interactive zero-knowledge for a von Neumann architecture. In 23rd USENIX Security Symposium (USENIX Security 14) (pp. 781-796).

Bloomfield, P. (n.d.). CS 4501 Cryptocurrency. University of Virginia.

Buterin, V. (2018). Zk-SNARKs: Privacy, scalability, and Ethereum 2.0. Retrieved from [Ethereum Foundation Blog].

Parno, B., Howell, J., Gentry, C., & Raykova, M. (2013). Pinocchio: Nearly practical verifiable computation. In 2013 IEEE Symposium on Security and Privacy (pp. 238-252).

Stanford University. (n.d.). Blockchain and cryptography: Ensuring privacy with zero-knowledge proofs. Stanford. https://cs.stanford.edu/research/blockchain

ZK Proof. (n.d.). What is zero-knowledge proof? ZK Proof Community. https://zkproof.org/overview