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

(Technical Paper)

PRIVACY AND TRUST IN THE AGE OF DEEP FAKES: A SOCIOTECHNICAL EXPLORATION OF ZERO-KNOWLEDGE PROOFS ON THE ALEO BLOCKCHAIN

(STS Paper)

A **Thesis Prospectus** submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia | Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Youssef Cherrat
STS 4500, Fall 2024

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 Youssef Cherrat **Date** 5-6-25
Youssef Cherrat

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

A. Introduction

In today's digital landscape, verifying identity has become increasingly complex, especially with the advent of deepfake technology, which enables the creation of highly realistic, artificial representations of individuals. Deepfakes can impersonate voices, faces, and behaviors, undermining trust and posing substantial security threats in contexts where identity verification is critical. According to the US Department of Homeland Security, deep fakes are another version of synthetic media in which simple digital techniques are applied to content to alter the observer's perception of an event. Current identity verification systems, such as those that rely on biometric data or personal identification information (PII), introduce their own risks. They often expose sensitive data, which can be stolen, misused, or manipulated. In this environment, there is an urgent need for a robust, privacy-preserving solution that can authenticate identities without compromising personal information.

Blockchain technology, specifically through the Aleo framework, offers a promising path forward. Blockchain's decentralized, secure structure is inherently resistant to tampering, which makes it an attractive platform for identity verification. The Aleo framework enhances this potential by incorporating zero-knowledge proofs, a cryptographic method that allows one party to prove knowledge of specific information without revealing the actual information itself. For identity verification, this means that an individual can prove their authenticity without disclosing personal data, effectively eliminating the privacy risks inherent in traditional methods. By storing only validation proofs on the ledger rather than personal details, Aleo's blockchain system provides an advanced level of security that is difficult to breach or forge.

This approach holds particular value for organizations that require the highest level of security, such as large corporations, financial institutions, and government agencies. In these

settings, the combination of blockchain with zero-knowledge proofs can protect against digital impersonation tactics like deepfakes while ensuring compliance with stringent data privacy standards. My thesis will investigate the application of Aleo's blockchain framework in these high-security contexts, aiming to establish it as a viable solution for identity verification in a world where digital trust is increasingly challenged.

B. Technical Discussion

As digital systems grow increasingly complex, the demand for secure, privacy-preserving identity verification has intensified, particularly in light of the rapid rise of deepfake technology. Deepfakes can convincingly mimic individuals, undermining trust and posing significant risks in digital environments where authentic identity is crucial. Existing identity verification methods, like biometric scans or the use of personal identification information (PII), often compromise user privacy, exposing sensitive data to exploitation. This project proposes integrating the Aleo blockchain framework into a Decentralized Autonomous Organization (DAO), leveraging zero-knowledge proofs (ZKPs) to establish a secure, privacy-focused identity verification system. This setup enables participants to join and engage in the DAO without disclosing underlying identity data, ensuring both security against deepfake threats and privacy protection.

A DAO is a decentralized organization managed by code, where participants can join, vote, and make decisions collectively without a central authority. The proposed DAO will use the Aleo blockchain to verify each member's identity through zero-knowledge proofs, allowing users to prove their authenticity without revealing personal data on the public ledger. This approach addresses a key challenge: ensuring each participant is genuine while preserving privacy. When new members apply to join the DAO, they generate cryptographic proof based on verification

criteria (e.g., using a government-issued ID or a trusted third party), without exposing these details. The Aleo blockchain then verifies this proof, allowing members to see that the applicant's identity has been validated without accessing their personal information.

Zero-knowledge proofs are essential to Aleo's privacy-preserving approach. A ZKP allows one party (the prover) to demonstrate to another party (the verifier) that they possess specific information—such as valid identity credentials—without actually revealing it. In the context of the DAO, each new member generates a ZKP that confirms their eligibility for membership. This ZKP acts as a cryptographic handshake, allowing only verified individuals into the DAO without exposing sensitive data. For instance, a user who has completed third-party identity verification submits only a ZKP to the Aleo blockchain, proving that they meet the membership criteria. Aleo's blockchain can validate this proof without ever accessing the actual identity data, preventing data breaches, and protecting privacy.

This system also protects against deepfake impersonation by validating members' interactions within the DAO through cryptographic proofs. Deepfakes pose a risk in many digital environments by mimicking voices or appearances to gain unauthorized access. However, within a DAO on the Aleo blockchain, members' interactions are authenticated through cryptographic proofs, making it extremely difficult for a deepfake to impersonate someone without access to the original ZKP. For example, if a member participates in a DAO meeting, a voice-based ZKP can verify their voice against their original identity proof, ensuring only authorized voices are recognized.

To further prevent unauthorized participation, the DAO can issue time-sensitive ZKPs for specific actions, like voting or proposing initiatives. This cryptographic validation ensures that

all interactions come from verified members, as any deepfake attempt would lack the unique ZKP tied to each member. This structure offers a reliable defense against impersonation, fostering a trustworthy DAO where identity remains secure and private.

The project will develop a technical framework integrating Aleo's ZKP protocols for identity verification and build the necessary architecture to support real-time cryptographic checks within the DAO. The system will include an encrypted identity verification gateway and a cryptographic validation layer that continuously authenticates member interactions. The technical report for this capstone will detail each stage of development, from designing the ZKP-based verification gateway to implementing measures against deepfake impersonation. Additionally, the report will evaluate the trade-offs between privacy, security, and performance, highlighting Aleo's potential to meet these demands in real-world settings. The ultimate goal, under the guidance of Professor Bloomfield, is to present a prototype DAO that displays how ZKPs can facilitate a secure, decentralized identity verification system resistant to deepfake threats.

Through this project, I aim to contribute to the application of blockchain technology in identity verification, demonstrating how DAOs can leverage zero-knowledge proofs to protect members against deepfake manipulation. This work could lay the groundwork for future DAOs, corporations, or governments seeking to incorporate privacy-preserving verification in their systems, ensuring both security and trust in our increasingly digital world.

C. STS Discussion

The integration of blockchain technology into identity verification systems raises important questions about privacy, trust, and the future of secure digital interactions in a world

increasingly affected by cyber threats, including deepfakes. This research addresses these questions, particularly in light of the complex social, ethical, and regulatory dimensions involved. My central research question explores whether zero-knowledge proof systems, such as those utilized by the Aleo framework, can offer a privacy-preserving solution for verifying identity in digital environments. Examining this question requires an analysis of not only technology's capabilities but also its broader societal implications, including its influence on public trust, privacy norms, and the ethical responsibilities of organizations adopting such solutions.

Blockchain technology, especially frameworks like Aleo's, represents a significant shift in how data can be managed and protected. Traditional identity verification methods, which often rely on sharing PII or biometric data, expose sensitive information to potential misuse. Such methods place individuals in a vulnerable position where their data can be exploited, stolen, or exposed through data breaches. By contrast, blockchain-based zero-knowledge proofs allow individuals to validate their identity without revealing personal details, thereby respecting privacy and enhancing user trust in digital systems. The significance of this shift extends beyond technical efficiency; it reflects a deeper societal commitment to protecting individual privacy in the digital sphere. As blockchain technology gains traction, understanding the social implications of this privacy-preserving model becomes essential for responsible adoption.

One primary area of focus is the role of blockchain-based verification systems in addressing the growing issue of deep fakes. Deep Fakes represent a societal threat by enabling malicious actors to impersonate individuals, thereby eroding public trust in digital interactions. By employing zero-knowledge proofs within a blockchain, organizations can offer a level of

security that is resilient to deep fake manipulation. For example, in a decentralized autonomous organization (DAO) that uses Aleo's framework, members could engage in secure interactions where each participant's identity is cryptographically authenticated. This system minimizes the risk of unauthorized access by malicious deep fake actors, as any attempt to impersonate a user would require access to their unique cryptographic proofs, which are not accessible on the public ledger.

The implications of such systems are particularly relevant to high-security environments, including finance, healthcare, and government sectors, where trust and privacy are paramount. Large corporations and government agencies managing sensitive personal and organizational data stand to benefit significantly from Aleo's zero-knowledge proof system. These organizations often operate in regulatory environments that demand the highest standards of privacy and data protection. By adopting a blockchain-based approach, such entities could not only bolster their security protocols but also improve their compliance with privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union. Blockchain's immutable nature could ensure compliance with record-keeping standards, while zero-knowledge proofs prevent exposure of unnecessary data, meeting regulatory requirements for minimal data disclosure.

However, while zero-knowledge proof systems promise enhanced privacy, there are also risks and challenges associated with their use in identity verification. For one, the reliance on cryptographic proofs to secure identity raises questions about the transparency of the verification process and the accessibility of the technology to users unfamiliar with blockchain. As privacy becomes a central concern, public trust in blockchain verification systems may depend on users'

understanding of the technology's implications. Individuals may be hesitant to adopt systems they perceive as opaque or overly complex. Therefore, one aspect of my STS research will involve examining how trust can be cultivated among users and stakeholders, especially in contexts where blockchain technology remains unfamiliar.

Another significant consideration is the ethical responsibility of organizations using such verification methods. While zero-knowledge proofs minimize data exposure, they also introduce potential ethical dilemmas around data control and surveillance. For instance, while zero-knowledge proofs provide a privacy shield, the system's design might still enable organizations to track user interactions and behaviors on the blockchain, raising concerns about potential surveillance. Thus, the ethical use of blockchain technology in identity verification requires a balance between data security and respecting users' autonomy and privacy rights. In examining these issues, my research will draw on existing studies and frameworks on data ethics and privacy, analyzing how zero-knowledge systems can be structured to prioritize user agency.

In addition to privacy and ethical considerations, regulatory compliance and adoption barriers present challenges for organizations interested in implementing blockchain-based identity verification. Governments and regulatory bodies may view blockchain with caution, due to its association with cryptocurrency and other decentralized finance applications. Introducing zero-knowledge proof-based verification within regulated sectors will require collaboration with policymakers to clarify the technology's benefits and limitations. My research will explore existing regulatory frameworks and identify pathways for integrating privacy-focused blockchain technologies within these frameworks. This investigation will examine the role of policy in

fostering blockchain adoption in secure identity verification and consider how organizations might navigate regulatory challenges to leverage zero-knowledge proofs responsibly.

The central questions this research seeks to answer—whether zero-knowledge proof systems like Aleo's can provide a privacy-preserving solution for digital identity verification and how such systems affect broader societal structures—are crucial as digital identities become increasingly central to our interactions. The outcome of this project will aim to inform stakeholders about the potential and limitations of privacy-preserving verification models, especially in highly secure environments. By examining the Aleo framework as a case study, I will identify how zero-knowledge proofs can contribute to trustworthy digital ecosystems and what ethical, regulatory, and technical safeguards might be necessary for their adoption in sensitive fields.

This project aspires to influence the future of secure communication in digital spaces, contributing to policy discussions and technical frameworks that prioritize both security and user privacy. As blockchain technologies evolve, this research could offer insights that encourage responsible, privacy-conscious approaches to identity verification, helping establish trust in digital systems for years to come. The findings may serve as a foundation for future studies on blockchain's role in digital identity and its integration into corporate and governmental frameworks, contributing to an interconnected world that values privacy and security in equal measures.

D. Research Question and Methods

The central research question guiding this study is: Can zero-knowledge proof systems, specifically those implemented via Aleo's blockchain framework, offer a privacy-preserving

solution for secure identity verification in digital environments vulnerable to deepfake manipulation? To explore this question, I am conducting an independent study under the supervision of Professor Bloomfield, focusing on the technical implementation of the Leo programming language on the Aleo blockchain. By using Leo, a language designed for zero-knowledge applications, I aim to enhance Aleo's identity verification processes, particularly for contexts requiring robust privacy and security standards. This project will involve developing and testing identity verification protocols within a decentralized autonomous organization (DAO) framework, examining both technical efficacy and broader social implications.

E. Conclusion

This project has the potential to contribute significantly to the field of privacy-preserving identity verification, especially in sectors requiring elevated levels of security, such as finance and government. By implementing zero-knowledge proofs on the Aleo blockchain, I hope to develop a model that balances privacy, security, and user trust. The findings could inform future blockchain applications in identity verification, offering insights into ethical and regulatory considerations for protecting digital identities in an increasingly interconnected world.

F. References

Aleo. (n.d.). *An introduction to zero-knowledge proofs*. Aleo. Retrieved from 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).

Blockchain Identity Verification. (n.d.). *Identity verification in a blockchain world.* Blockchain Identity Verification. Retrieved from https://www.blockchainidentityverification.com/research

IBM Blockchain. (n.d.). *Blockchain and privacy: Zero-knowledge proofs.* IBM. Retrieved from https://www.ibm.com/blockchain/privacy

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. Retrieved from https://cs.stanford.edu/research/blockchain

Tech News. (n.d.). *Deepfakes and digital trust: A growing concern.* Tech News. Retrieved from https://www.technews.com/deepfakes-and-security

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