

## ABSTRACT

Self-Sovereign Identity (SSI) has emerged as a promising approach to digital identity management by enabling individuals to control their identity information without relying on centralized authorities. While SSI enhances privacy, security, and user autonomy, establishing trust among decentralized entities remains a significant challenge. Existing trust management approaches often require the disclosure of endorsement relationships, reputation information, or trust scores during verification, creating privacy risks. Recent studies have explored the use of Zero-Knowledge Proofs (ZKPs) to enable privacy-preserving verification; however, conventional ZKP-based solutions do not inherently bind proofs to the identity of the prover, making them vulnerable to replay and impersonation attacks. This research proposes a privacy-preserving, identity-bound trust evaluation framework for SSI systems that combines endorsement-driven trust aggregation, zero-knowledge proof-based verification, and cryptographic identity binding within a unified decentralized architecture. A multi-dimensional trust model is developed using direct trust, reputation-weighted endorsements, and temporal validity factors to compute trust scores within a decentralized identity graph. To preserve privacy, trust evaluation is performed off-chain and encoded within zk-SNARK circuits, allowing users to prove compliance with trust-based access policies without revealing endorsement relationships, trust scores, or identity attributes. To mitigate replay and impersonation attacks, each proof is cryptographically bound to a prover-specific secret and a verifier-issued nonce through a commitment mechanism, ensuring proof non-transferability. The framework is implemented using the ZoKrates toolkit integrated within the Ethereum Remix IDE and deployed using Solidity-based smart contracts for on-chain proof verification. Experimental evaluation is conducted using simulated trust datasets consisting of twenty-five decentralized identities and multiple endorsement configurations. Performance is assessed in terms of proof generation time, circuit complexity, verification cost, scalability, and authentication accuracy. Results demonstrate that proof generation time increases from 1.19 seconds to 3.38 seconds as verification workload grows from one to twenty-five trust checks, while on-chain verification cost remains nearly constant at approximately 1.6 million gas. Comparative analysis against the zkSSI framework shows significantly lower proof generation times and improved scalability. Security evaluation further demonstrates resistance to replay attacks and achieves perfect classification performance with a False Acceptance Rate (FAR) of 0% and a False Rejection Rate (FRR) of 0% under the experimental conditions. The proposed framework contributes to the advancement of decentralized trust management by providing a secure, scalable, and privacy-preserving mechanism for trust-based access control in SSI ecosystems. By integrating identity-bound zero-knowledge verification with endorsement-driven trust evaluation, the framework addresses critical limitations of existing SSI trust solutions and provides a practical foundation for secure trust enforcement in decentralized digital identity environments.

**Keywords**—self-sovereign identity, decentralized identity management, endorsement-based trust, identity binding, zero-trust principles.