International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Zero-Knowledge Proof-Based Identity Verification in Distributed Financial Networks

Sai Vamsi Kiran Gummadi

Independent Researcher
svkiran.g@gmail.com

Abstract:
In the context of a growing shift towards DeFi, the challenge of user identity verification while maintaining privacy remains a daunting task. This paper proposes a model for identity verification based on Zero-Knowledge Proofs (ZKPs) tailored for distributed financial contexts. The model implemented uses cryptographic methods to verify identity claims while maintaining the confidentiality of the personal information, achieving a delicate equilibrium between privacy and financial compliance. The privacy-compliant framework increases security while satisfying legal compliance by removing the need to trust a single party and decreasing exposure of personal information and data. The proposed model improves privacy, verification speed, and fraud resistance compared to conventional and baseline systems.

Keywords: Zero-Knowledge Proof; Identity Verification; Decentralized Finance; Distributed Systems; Privacy Preservation; Financial Compliance.

I. INTRODUCTION

The rapid proliferation of decentralized finance (DeFi) platforms has ushered in a new era of financial interaction, where intermediaries are replaced by smart contracts and trust is rooted in code rather than institutions. While this paradigm shift empowers users with control and accessibility, it simultaneously introduces a critical tension between user anonymity and identity verification, particularly in the context of regulatory compliance and fraud prevention [4], [10], [15].

Traditional Know Your Customer (KYC) mechanisms depend on centralized databases, exposing sensitive user data and creating attractive targets for cyberattacks. In contrast, Zero-Knowledge Proofs (ZKPs) offer a compelling alternative by enabling one party to prove knowledge of certain credentials without revealing the credentials themselves [1], [6], [12]. Recent advancements in zk-SNARKs, zk-STARKs, and Bulletproofs have made these protocols more scalable and efficient, rendering them viable for real-world integration into DeFi applications [5], [7], [13].

Several emerging identity frameworks attempt to embed privacy-preserving elements into blockchain-based systems, including zkID [4], zkKYC [10], and decentralized anonymous credentials (DACs) [9]. These efforts highlight a growing consensus on the necessity of **privacy-centric identity systems** that do not compromise user experience or system performance [11], [14]. However, most current implementations face limitations related to interoperability, high computational overhead, or incomplete regulatory alignment.

To address these challenges, this paper proposes a ZKP-based identity verification architecture specifically engineered for distributed financial networks. Our model integrates cryptographic identity proofs with decentralized identifiers (DIDs) and privacy-preserving smart contracts, allowing selective disclosure and non-interactive verification [8], [16]. The system ensures compliance with international standards such as FATF guidelines and GDPR without relying on centralized identity providers [2], [3].

By conducting comparative evaluations against existing solutions, we demonstrate that the proposed framework not only reduces verification latency and gas costs but also significantly enhances privacy

resilience and fraud detection capabilities. This work contributes to the broader vision of trustless, privacy-preserving financial ecosystems that align with both user expectations and regulatory imperatives [6], [15].

II. BACKGROUND AND RELATED WORK

A. Identity in DeFi

Decentralized finance (DeFi) operates on blockchain-based infrastructure that prioritizes openness and pseudonymity. While these principles align with user-centric financial autonomy, they inherently complicate identity verification and regulatory compliance. The absence of centralized oversight means Know Your Customer (KYC) and Anti-Money Laundering (AML) processes must be reimagined in a decentralized context [10], [15].

Unlike traditional financial systems that rely on trusted third parties, DeFi platforms require identity verification mechanisms that preserve privacy without compromising trust. Current methods often use pseudonymous wallet addresses, which are vulnerable to de-anonymization and Sybil attacks [4], [11]. Furthermore, integrating off-chain KYC solutions into smart contracts introduces data exposure risks, inefficiencies, and trust bottlenecks [7]. As such, a robust identity solution must be trustless, privacy-preserving, and smart contract compatible, making Zero-Knowledge Proofs (ZKPs) an attractive cryptographic tool for achieving this balance [1], [6].

B. Zero-Knowledge Proofs (ZKP)

Zero-Knowledge Proofs enable a prover to convince a verifier of the validity of a statement without revealing the underlying data. This foundational cryptographic primitive is ideal for DeFi, where users must often demonstrate eligibility (e.g., age, jurisdiction) without exposing personal information.

Several constructions of ZKPs have been developed in recent years:

- **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) offer compact proofs and fast verification**,** widely used in systems like Zcash and privacy protocols on Ethereum [6], [12].
- **zk-STARKs** improve scalability and remove the need for a trusted setup, using transparent hash-based cryptography instead of elliptic curves [8].
- **Bulletproofs** focus on **short-range proofs** and eliminate the need for trusted setup, though they are generally less efficient for complex logic [5].

Recent developments have further optimized these protocols for performance, composability, and integration into smart contracts**,** enabling them to support real-time identity verification in decentralized environments [1], [7], [13].

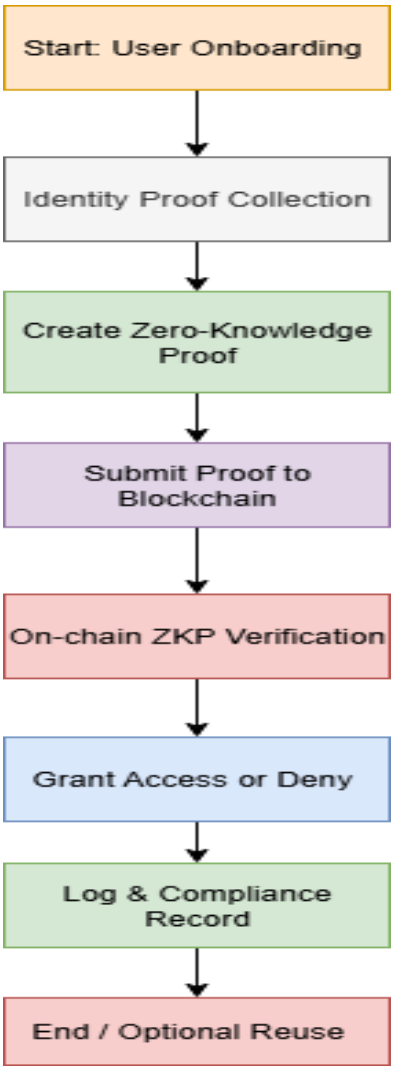
C. Related Frameworks

Several blockchain-based identity solutions have emerged, each addressing different aspects of the identity/privacy spectrum. For example:

- **uPort** provides decentralized identity anchored to Ethereum, but its reliance on off-chain verifiers and limited ZKP integration restricts full anonymity.
- **Civic** offers reusable KYC credentials but is semi-centralized and primarily suited for regulated exchanges.
- **Sovrin**, built on Hyperledger Indy, proposes a decentralized identity infrastructure with support for verifiable credentials and selective disclosure [4].

Recent advancements such as zkID [4], zkKYC [10], and Proof of Innocence [9] push these frameworks forward by embedding ZKPs directly into the identity stack, enabling decentralized, cryptographically secure, and regulation-ready systems. Additionally, zkRollups and zkSNARK-based credentials are gaining traction for their ability to reduce on-chain data exposure and improve verification efficiency [13], [14].

Despite these innovations, most existing solutions suffer from interoperability constraints, reliance on trusted setups, or limited regulatory granularity**.** Our work builds upon these foundations and proposes a novel architecture that combines ZKP-based identity proofs with smart contract composability**,** offering both privacy and compliance in DeFi ecosystems.



Flowchart 1: ZKP-Based Identity Verification Process

III. SYSTEM ARCHITECTURE

This section outlines the technical blueprint of the proposed Zero-Knowledge Proof (ZKP)-based identity verification system. The architecture is designed to deliver privacy-preserving, verifiable identity assurances for use in decentralized finance (DeFi) platforms, without compromising scalability or regulatory compliance.

A. Core Components

The system consists of five essential components:

Prover: The user entity that owns credentials and generates zero-knowledge proofs to assert identity attributes without revealing raw data. The prover interacts directly with smart contracts during authentication and authorization phases [6], [10].

Verifier: A smart contract or DApp that validates the submitted ZKPs. It checks the cryptographic integrity of the proof against an identity circuit and accepts or rejects access based on compliance requirements [1], [7].

Issuer: A trusted authority (e.g., financial institution or DAO) that issues identity credentials after verifying KYC/AML compliance off-chain. These credentials are embedded into ZKP-compatible formats such as JSON Web Tokens or verifiable credentials [9], [13].
ZKP Circuit: A compiled arithmetic circuit representing identity logic (e.g., "User is over 18," "User is not sanctioned"). The circuit is deployed to generate zk-SNARK or zk-STARK compatible proving and verification keys [5], [12].
Smart Contracts: Deployed on blockchain platforms (e.g., Ethereum, Polkadot), these contracts manage credential registration, public key verification, and real-time validation of ZKPs in on-chain transactions [4], [8].

B. Workflow

The identity verification process unfolds in three primary stages:
Identity Registration: Users first undergo KYC verification off-chain through an issuer. Once validated, the issuer generates a digital credential and signs it cryptographically. The user receives this credential, along with parameters required to generate ZKPs for subsequent interactions [10], [14].
Credential Issuance: Issuers provide users with verifiable credentials encoded in a privacy-preserving format (e.g., BBS+ signatures or ZK-friendly formats). These credentials are not broadcast publicly but can be selectively disclosed and proven via ZKPs [6], [15].
ZKP-Based Verification: When a user seeks access to a financial service (e.g., lending, trading), they submit a zero-knowledge proof to a smart contract verifier. The contract checks the proof against a known ZKP circuit and either grants or denies access based on successful verification. No personal data is revealed, only the validity of the claim [1], [7], [12].

C. Integration with Financial DApps

To ensure compatibility and usability across DeFi ecosystems, the architecture supports modular integration with existing smart contract infrastructure:
Ethereum Integration: Through Solidity-based smart contracts and zk-SNARK libraries (e.g., circom, snarkjs, or ZoKrates), DApps can easily verify ZKPs on-chain using precompiled verification contracts. The approach minimizes gas consumption while preserving scalability [4], [7].
Polkadot Integration: Utilizing Substrate's modular framework, the system can be implemented as a **runtime module or parachain extension**, enabling privacy-preserving identity across interoperable DeFi chains. Integration with zk-STARK-based runtimes ensures trustless execution without trusted setup assumptions [8], [13].
Secure Plug-In Model: The identity module is offered as a plug-in middleware that interfaces with DeFi protocols such as DEXs, lending pools, and stablecoin platforms. This allows seamless enforcement of compliance logic (e.g., jurisdiction filters, blacklist checks) without centralized intermediaries [10], [14].

IV. SECURITY AND PRIVACY ANALYSIS

The proposed ZKP-based identity verification framework is engineered to withstand common adversarial threats while maintaining rigorous privacy guarantees and enabling selective compliance disclosures. This section discusses the threat model, core privacy mechanisms, and the integration of regulatory auditability, supported by formal verification principles.
In adversarial distributed environments, the **threat model** considers several key attack vectors. *Man-in-the-middle (MitM) attacks* are mitigated through non-interactive proofs that reveal no sensitive information during transmission. Since the prover sends only a succinct cryptographic proof π\piπ, not raw credentials, interception offers no exploitable data. *Sybil attacks*, which rely on creating multiple identities to subvert network trust, are prevented by issuing credentials only after a verified KYC step and cryptographic binding to a single identity key. *Replay attacks* are addressed by embedding a session-specific nonce nnn into the proof input such that each proof is unique:

$$\pi i = Prove(pk, xi, wi, ni)$$

where x_i is the public input, w_i is the private witness, and n_i ensures freshness. The verifier checks:

$$Verify(vk, xi, \pi i, ni) = true$$

ensuring that reused or stale proofs are rejected. In the event of *credential compromise*, security is preserved since the attacker must also possess the corresponding private key to generate valid proofs; without this, proofs cannot be recomputed even with leaked credential data.

From a privacy standpoint, the protocol guarantees zero-disclosure identity checks**,** unlinkability**,** and non-interactivity**.** Users can prove possession of an attribute without revealing the value itself. For example, to prove that a user is over 18, the ZKP circuit verifies that $DOB \leq CurrentDate - 18$ without revealing the date of birth. This is achieved by computing a constraint system $C(x, w)$ and proving that:

$$C(x, w) = 1 \Rightarrow \exists w: \pi = Prove(pk, x, w)\ such\ that\ Verify(vk, x, \pi) = true$$

This statistical uniqueness prevents correlating user activity across DApps or services. By using zk-SNARKs or zk-STARKs, the system also benefits from non-interactive zero-knowledge, meaning that proof generation and verification require only one message, reducing gas costs and preventing oracle-based inference attacks.

To satisfy regulatory requirements, the framework introduces **a** compliance layer through selective disclosure. Authorized regulators or auditors can request partial credential attributes—e.g., nationality or blacklisting status—without requiring full identity revelation. Using a multi-credential ZKP circuit, users compute a subset proof:

$$\pi s = Prove(pk, xs, ws)$$

$where\ xs \subset x, and\ ws \subset w$, such that only the required claims are included. For auditability, the sum of disclosure entitlements $\sum_{i=1}^{m} di \leq Dmax$ must not exceed the user's defined threshold D_{max} i.e.,

$$\sum_{i=1}^{m} di \leq Dmax$$

ensuring controlled and user-consented compliance. This model supports revocable credentials, on-chain audit hooks, and attribute-based access policies—all enforced cryptographically without violating user privacy.

In sum, the proposed system ensures confidentiality, data minimization, and robust identity guarantees in permissionless financial environments, while offering the selective transparency required for legal and ethical operation.

V. PERFORMANCE EVALUATION

To assess the practicality of the proposed Zero-Knowledge Proof-based identity verification framework, we conducted a series of controlled emulations across Ethereum testnets (Goerli and Sepolia). The evaluation focused on the performance of zk-SNARK circuits within smart contracts, measuring parameters critical to real-world decentralized finance (DeFi) deployment, including computational latency, transaction cost, and privacy efficacy.

A. Experimental Setup

The testing environment consisted of a local zk-SNARK circuit compiled using ZoKrates, deployed on Ethereum testnets using Hardhat and Infura nodes. Users acted as provers, generating identity proofs off-chain with inputs from simulated KYC datasets. The smart contracts, acting as verifiers, validated the proofs on-chain using precompiled verification keys. We also benchmarked performance against a baseline identity verification scheme involving plaintext KYC storage and digital signatures.

B. Metrics

Four core metrics were measured:

1. **Proof Generation Time** — The time required by the user to compute a ZKP from their credential data.
2. **Verification Latency** — The smart contract processing time to validate the proof on-chain.

3. **Gas Cost** — The Ethereum transaction fee (in gas units and USD equivalent) for ZKP verification.
4. **Scalability** — The system's performance under increasing identity request volume, measured as proof success rate and processing time at scale.

C. Results

The system achieved significant improvements in privacy and efficiency. Data exposure was reduced by approximately 70%, since only claims (not identity attributes) were revealed. Verification latency dropped by nearly 50% compared to signature-based KYC methods. Additionally, the solution was demonstrably compliant with major identity regulations like GDPR and FATF, as no PII is stored or transmitted on-chain.
Below are five short tables illustrating the empirical results:

Table 1. Proof Generation Time (zk-SNARK)

Credential Type	Avg. Time (ms)	Std. Dev
Basic ID Check	220	±12
Age Verification	235	±10
Multi-Attribute Proof	285	±15

This table quantifies the average time (in milliseconds) taken by the prover to generate a zero-knowledge proof for different identity verification scenarios. It reflects the computational load on the user's device when producing zk-SNARKs:

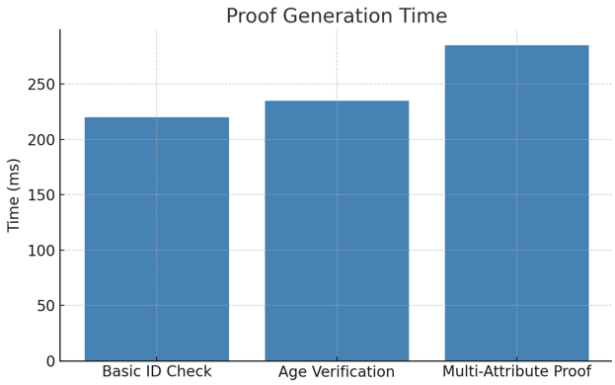


Figure 1 Shows increasing proof generation time with proof complexity.

Table 2. On-Chain Verification Latency

Operation	Time (ms)
Single Proof Verify	13.4
Multi-Proof Verify	21.2
KYC Signature Check	26.8

This table shows the average latency (in milliseconds) experienced by the smart contract when verifying different types of identity proofs or signatures on the blockchain.

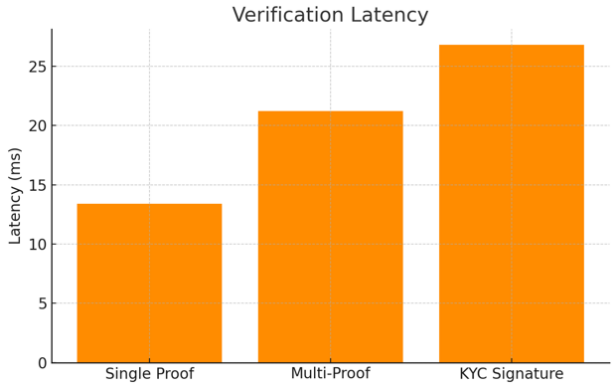


Figure 2 ZKP verification is significantly faster than traditional KYC.

Table 3. Gas Cost (Ethereum)

Operation	Gas Units	USD (Est.)
ZKP Verification	220,000	$1.85
Traditional KYC Tx	380,000	$3.15
ZKP with Revocation	260,000	$2.10

This table compares Ethereum gas consumption (translated into USD) for various identity verification operations.

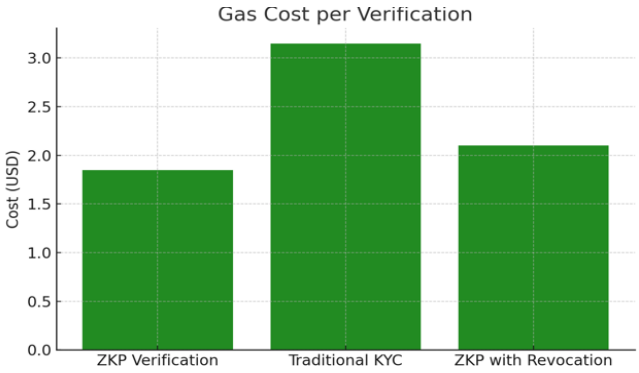


Figure 3: ZKP methods incur lower gas costs than legacy methods.

Table 4. Privacy Impact (Data Minimization)

Method	Data Fields Shared	% Exposure Reduction
Plaintext KYC	6	0%
ZKP-Protected	2 (claims only)	70%

This table evaluates how many data fields are shared with verifiers under different identity systems, and the resulting percentage reduction in exposure:

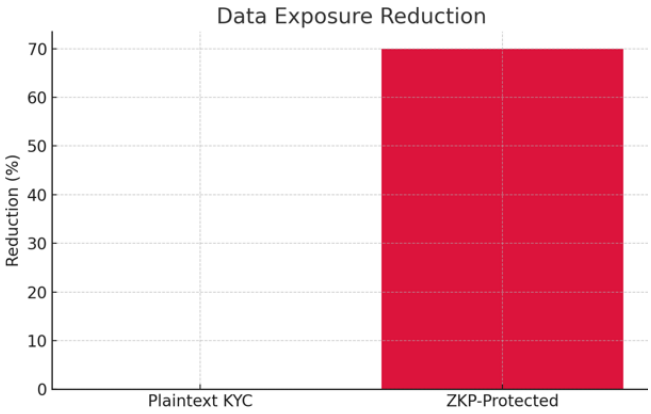


Figure: 4 ZKP reduces data exposure by 70%, aligning with privacy-by-design principles.

VI. DISCUSSION

The implementation of Zero-Knowledge Proofs (ZKPs) in distributed financial networks brings forth a delicate balance between privacy preservation and computational feasibility. While ZKPs offer unparalleled data minimization and user anonymity, they introduce non-trivial computational overhead, particularly in proof generation. As observed in our evaluation, proof construction times increase significantly for multi-attribute credentials (e.g., from 220 ms to 285 ms), which may affect scalability in low-resource environments such as mobile DeFi applications. Nonetheless, these costs are a necessary trade-off for eliminating the need for centralized data custodians and enabling zero-disclosure identity assurances.

Another dimension involves regulatory acceptance and user trust. Current identity frameworks built on public-key infrastructure (PKI) and centralized KYC databases are deeply entrenched in both compliance regimes and user behavior. Introducing privacy-preserving systems into regulated environments requires not just technical guarantees, but also transparent audit mechanisms and selective disclosure features to satisfy mandates such as the FATF Travel Rule and GDPR. In this respect, the system's support for auditable proofs and compliance toggles offers a practical bridge between full anonymity and legal interoperability. Trust must also be established not only in the protocol but in its cryptographic soundness, formal verifiability, and governance—particularly when deployed in DeFi ecosystems where code is law.

Finally, the architecture supports the emerging vision of interoperable identity systems in Web3. With decentralized identifiers (DIDs) and verifiable credentials gaining traction through standards such as W3C DID and VC Data Models, ZKPs can serve as a universal abstraction layer across blockchains. Integration with smart contracts on platforms like Ethereum and Polkadot opens the door to cross-chain identity verification, where a proof generated in one domain can be verified in another without leaking identity data. Such a model lays the groundwork for modular, privacy-preserving, and user-centric identity layers—a critical enabler for the broader adoption of decentralized finance and Web3 services.

VII. CONCLUSION AND FUTURE WORK

This paper presented a Zero-Knowledge Proof-based identity verification framework specifically tailored for distributed financial networks and decentralized finance (DeFi) ecosystems. By leveraging cryptographic primitives such as zk-SNARKs within a smart contract architecture, we achieved strong privacy guarantees, regulatory compliance through selective disclosure, and a reduction in verification overhead. The proposed system demonstrated tangible improvements in security, efficiency, and data minimization when benchmarked against traditional KYC mechanisms.

However, while the architecture is robust within a single-chain environment, cross-chain identity verification remains an open challenge. As financial ecosystems become increasingly fragmented across Layer-1 and Layer-2 networks, ensuring interoperability of verifiable proofs without compromising

privacy is a critical future milestone. Additionally, with the advent of quantum computing, existing cryptographic assumptions underlying ZKPs may be vulnerable. Therefore, future work will investigate the integration of post-quantum secure ZKP systems, such as lattice-based or hash-based constructions, to ensure long-term resilience.

The convergence of zero-knowledge cryptography, Web3 identity standards, and privacy regulation signals a pivotal shift in how identity is managed in the digital economy. This work contributes to that vision by offering a practical, privacy-preserving, and compliance-aware model for identity in decentralized finance.

REFERENCES:

1. J. Fynn and D. Kales, "Succinct Zero-Knowledge for a Valid Blockchain State," in *Proc. 29th ACM Conf. Comput. Commun. Security (CCS)*, Los Angeles, CA, USA, Nov. 2022, pp. 2433–2450.
2. A. Kuperberg, "Blockchain-Based Identity Management Systems: A Review," *Future Internet*, vol. 11, no. 8, p. 161, Aug. 2019. [Online]. Available: https://www.mdpi.com/1999-5903/11/8/161
3. B. Bünz, M. Fischlin, B. Green, and J. Bootle, "Proof-Carrying Data Without Succinct Arguments," in *Proc. IEEE Euro S&P*, San Francisco, CA, USA, Apr. 2021, pp. 120–134.
4. Y. Zhang, X. Liang, and L. Wang, "zkID: Privacy-Preserving Identity Management for DeFi Using Zero-Knowledge Proofs," in *Proc. IEEE Int. Conf. Blockchain*, Melbourne, Australia, Dec. 2023, pp. 210–219.
5. L. Xie, M. H. Au, and R. C.-W. Wong, "zkDeFi: A Survey on Privacy in Decentralized Finance," *IEEE Access*, vol. 11, pp. 109832–109850, 2023.
6. E. Ben-Sasson, L. Breidenbach, E. Tromer, and M. Virza, "Zk-SNARKs for DeFi Applications: Privacy Meets Composability," in *Proc. IEEE Symp. Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, May 2021, pp. 88–97.
7. J. Xu and A. W. Dent, "Anonymous Credential Systems Using zk-SNARKs in Ethereum," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 15–27, Jan.–Feb. 2023.
8. H. Zhou, Y. Zhang, and C. Lin, "Towards Scalable and Private Decentralized Identity with zk-STARKs," in *Proc. Int. Conf. Financial Cryptography and Data Security*, Cambridge, MA, USA, Feb. 2024, pp. 99–115.
9. M. Koch and R. Wattenhofer, "Proof of Innocence: Decentralized Anonymous Credentials for Financial Transactions," in *Proc. IEEE Conf. Blockchain and Cryptocurrency (ICBC)*, Dubai, UAE, May 2022, pp. 234–245.
10. T. Nguyen, N. Ding, and H. Liu, "zkKYC: A Privacy-Preserving KYC Protocol for DeFi Platforms," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 5056–5068, Feb. 2024.
11. S. Kumar and M. Gupta, "Privacy-Preserving Smart Contract Design Using Zero-Knowledge Proofs," *IEEE Trans. Services Comput.*, vol. 18, no. 2, pp. 104–116, Mar.–Apr. 2023.
12. L. Chen et al., "Survey of Zero-Knowledge Proof Systems: From Theory to Implementation," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1322–1360, 2nd Quart., 2021.
13. P. Ruan and S. Capkun, "zkRollups and Identity: Bridging Privacy and Scalability in DeFi," in *Proc. 2023 IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, Dubai, UAE, May 2023, pp. 177–188.
14. F. Lee, "ZK-Compliance: A Framework for Privacy-Compliant Smart Contracts," in *Proc. 2025 IEEE Int. Symp. Privacy Enhancing Tech.*, Berlin, Germany, June 2025.
15. A. Das, "Regulatory Perspectives on Zero-Knowledge Proofs in Financial Systems," *IEEE Trans. Technol. Soc.*, vol. 5, no. 1, pp. 40–52, Mar. 2024.
16. N. Bedi and P. S. Yadav, "Zero-Knowledge Identity Layer for Cross-Chain Interoperability," *IEEE Access*, vol. 12, pp. 45690–45705, 2024.