Engineering and Technology Journal e-ISSN: 2456-3358

Volume 10 Issue 07 July-2025, Page No.- 5755-5761

DOI: 10.47191/etj/v10i07.23, I.F. – 8.482

Zero-Knowledge Proofs For Privacy-Preserving Systems: A Survey Across Blockchain, Identity, And Beyond

Sandeep Gupta
SATI, Vidisha

ABSTRACT: The cryptographic protocol developments are transforming digital trust is the capacity to verify without revealing any underlying information. Traditional authentication and authorization systems are usually prone to leakage of sensitive data, resulting in compromise of privacy and low scalability in distributed systems. The root of these problems is eliminated through the so-called zero-knowledge techniques that allow demonstrating to one party ownership of some information without exposing it. This paper explores the origin and development of zero-knowledge protocols in light of its efficiency, trustless design, and privacy focus to illustrate why the application is worth the hype. Particular attention is paid to such structures as zk-SNARKs, zk-STARKs, and bulletproofs, as well as their application to constructing transparent, scalable systems. Blockchain aptitudes used anywhere in confidentiality of transactions, decentralized identity systems allow a self-sovereign identity without exaggerating personal information, and the healthcare and finance industries enjoy the ability to share information securely without any effect on compliance aspects. The next discussion points are implementations, the scalability issue, cryptographic assumptions, and integration issues. This survey outlines evaluations of deployments from 2021 to 2025 to determine the following top benefits, barriers, and trends in building systems that safeguard privacy without compromising their performance or trust to the client. Future requirement conclusions provide some insights about future requirements in terms of efficient construction of proofs, standardizations, and ease of usability to expand the adoption of infrastructures built on zero-knowledge into a constantly more integrated digital world.

KEYWORDS: Trustless Systems, Blockchain Security, Cryptographic Protocols, Decentralized Identity, Zero-Knowledge Proofs, Privacy-Preserving, and ZK-SNARKs.

I. INTRODUCTION

At the time when digital interactions are gaining ground in their social, economic, and governmental systems, mechanisms of privacy preserving in the exchange of data are becoming a crucial necessity [1]. With the increasing focus on decentralized and trust less platforms, especially in the case of blockchain, systems based on digital identity and financial technologies, verifying the data in such systems with a reasonable level of certainty but without any breach of sensitive data is an essential issue [2][3]. Even though normal cryptographic techniques ensure confidentiality of information being transmitted and stored, the techniques tend to leak some portions of the privacy details when authenticating or validating, thereby endangering the privacy of their users.

To overcome these limitations, ZKPs have emerged as a revolutionary cryptographic primitive. ZKPs enable a user to prove to another that a statement holds without revealing anything other than the fact that this particular statement holds [4]. The theoretical underpinnings of this paradigm were established by Goldwasser, Micali and Rackoff, who proposed the idea of knowledge complexity as a gauge of the volume of information disclosed in interactive proofs. Later work by Gold Reich and others demonstrated the flexibility of ZKPs in computational aspects, with the extension of the use of ZKPs to a far wider set of NP-complete problems.

Building on these theoretical developments, contemporary cryptographic research has produced useful and effective ZKP protocols, including Bulletproof, Sigma, zk-SNARKs, and zk-STARKs. These constructions have enabled ZKPs to move from theoretical tools into scalable, real-world applications. Their features, non-interactivity, succinctness, transparency, and low verification overhead have made them especially suitable for deployment in blockchain-based systems, where performance and trustworthiness are essential [5][6]. These innovations bridge the gap between privacy and auditability, making it feasible to design systems that preserve confidentiality without undermining integrity or transparency [7].

Privacy-preserving blockchain systems are one of the most well-known application spheres. Although the public blockchain networks are designed to be transparent, they present serious privacy problems since transaction history as well as metadata of the user are was told The privacy issues of user transactions and the associated metadata are of great concern Public blockchain networks are inherently transparent, and they reveal user transaction history and the associated metadata to potential privacy risks [8][9]. ZKPs have been integrated into such platforms to allow private transactions, identity protection, and

regulatory compliance. For instance, cryptocurrencies like Zcash use zk-SNARKs to ensure transaction privacy, while identity frameworks such as Sovrin leverage ZKPs and decentralized identifiers (DIDs) to facilitate anonymous, verifiable credentials. These implementations highlight the critical role of ZKPs in building decentralized trust without data exposure.

Besides, ZKPs applicability is not limited to blockchain and identity systems. They are finding escalating use in areas where information security is essential, e.g., in safe electronic voting, privacy-sensitive machine learning, cloud computation with confidence and healthcare data sharing [10]. The various use cases indicate the increasing interest in ZKPs as the core technology of new secure systems, which are expected to enable privacy guarantees in permissioned as well as open ecosystems.

Considering such an evolution, this piece of work addresses the development and influence of ZKP technologies through the addressment of pertinent advancements, implementation techniques, and application patterns. By analyzing literature across blockchain, digital identity, and other privacy-sensitive domains, it highlights existing capabilities, unresolved technical challenges, and emerging research directions. This integrated perspective enhances understanding of ZKPs as foundational tools for secure, transparent, and privacy-preserving digital systems.

A. Structure of the Paper

The article is organized as follows: The basics of Zero-Knowledge Proof are covered in Section II, followed by Types such as zk-SNARKs, zk-STARKs, and Bulletproof in Section III, Blockchain applications in Section IV, while Section VI presents conclusions and recommendations for more study, Section V summarizes current studies.

II. UNDAMENTALS AND TYPES OF ZERO-KNOWLEDGE PROOFS

ZKPs are powerful cryptographic algorithms that enable information verification without revealing the underlying facts.This feature is crucial for enhancing privacy in fields like blockchain, encrypted communication, and digital identity. Simpler ZKP varieties, such as Bullet proofs, ZK-STARKs, and ZK-SNARKs, provide scalable, useful, and trust less privacy-protective authentication methods. Their usefulness to a decentralized system is expanded by this differentiation between interactive and non-interactive proofs. This review traces the maturation and application of the ZKPs between 2021 and 2025 and their revolutionary nature in privacy-conscious systems and leading to the determination of the trends, obstacles, and emerging trends in zero-knowledge innovation.

A. Principles of Zero-Knowledge Protocols

ZKPs are a collection of cryptographic techniques that let one party persuade another that a claim is true without revealing any of the underlying details. The frameworks documented by ZKPs can offer innovative solutions to digital systems whose security and privacy are prioritized [11]. Compared to the previously available privacy-sensitive computational protocols in distributed systems, including such methods as safe multiparty computing and homomorphic encryption, it introduced an innovative perspective to the topic of cryptography. Privacy-preserving authentication has become a popular interest in the use of ZKPs.ZKPs reduce the dangers of identity theft and data leakage by enabling users to authenticate themselves without worrying about their data being compromised. It is shown that authentication systems are feasible and beneficial, and have been explored in numerous frameworks and implementations in this field.

B. Interactive vs. Non-Interactive Proofs

ZKPs reduce this danger by providing evidence to support a claim without revealing further information. ZKPs may be divided into two groups:

- **Zero-knowledge interactive proofs (IZKPs):** A turn-around sequence occurs when the prover answers the verifier's questions in a way that suggests they are aware of a secret without really disclosing it.
- **Non-interactive zero-knowledge proofs (NIZKPs):** The prover and the verifier do not need to communicate with one another.Rather, the prover only produces a single, independent piece of evidence that the verifier can independently confirm without additional assistance. More efficient (and possible) than interactive proofs since there is no need to have the prover and the verifier online simultaneously and to send many messages to each other.

The degree to which the prover and verifier must have mutual trust is a key distinction between interactive and non-interactive zero-knowledge proofs.. In an interactive proof, the verifier has to have faith that the prover will be honest in their inquiries and adhere to the rules.However, with a non-interactive proof, the verifier may independently check the proof without depending on any information the prover has given him, thus he has absolutely no reason to believe the prover.

C. Commonly Used ZKP Constructions (ZK-SNARKs, ZK-STARKs, Bulletproofs)

ZKPs also offer a new way of authentication that is privacy-preserving. ZKP Three protocols that are significant are Bulletproof, ZK-STARKs, and ZK-SNARK. Some noteworthy uses of these protocols in fields like blockchain technology, privacy-preserving computations, and other secure communications protocols are discussed in the following section:

- **ZK-SNARKs:** By using ZK-SNARKs, a prover can persuade a verifier that a certain assertion is true without disclosing any further information and maintaining the confidentiality of the data in question.
- **ZK-STARK:** ZK-STARKs provide such a breakthrough by eliminating the need to trust a setup, as well as providing an efficient method of proving about large volumes of data. ZK-STARKs have practical applications in the real world because they are practical in developing evidence and verifying them. To validate

in real-time, the fast verification and tiny proofs are needed.

- **Bulletproof:** Bulletproof, a cryptographic protocol, simplify a technique called range proofs, in which the correctness of a hidden numerical value being in a given interval is checked without revealing its value. The introduction of bulletproof that enhance security and privacy proves to be particularly important in safe authentication of credit checks and economic systems.

III. REAL-WORLD IMPLEMENTATIONS AND USE CASES OF ZKPS

ZKPs are increasingly operated in real-world systems to secure sensitive data across data integrity and compliance. Blockchain and cryptocurrency transactions are made possible via ZK-SNARKs and ZK-STARKs, protocols that conceal the sender, receiver, and amount of a transaction. ZKPs guarantee safe data sharing in industries like healthcare and finance, enabling the verification of critical properties without exposing them. Furthermore, confidential smart contracts and privacy-aware supply chain systems harness ZKPs to enforce trust, automation, and compliance.

A. Privacy in Blockchain and Cryptocurrencies (e.g., ZK-SNARKs, ZK-STARKs)

In the beginning, people discovered that it wasn't truly anonymous, as all the addresses and wallet balances were visible on the public ledger. Without sacrificing the blockchain's integrity, ZKPs now assist in protecting people's financial information. In Figure 1, it is explained.

1) ZK-SNARKs: Compact Privacy with a Caveat

It allows someone to demonstrate that they are aware of a secret without ever disclosing it. [12]. Each proof takes only a little space (just a few hundred bytes) and can be checked quickly by the network.

- Zcash was released in 2016 and turned out to be the first major triumph. It is able to give users privacy for their transactions by making the sender, recipient, and amount completely secret.
- Creating a quadratic arithmetic program (QAP) and setting it up with trust are the secrets behind it. The way it is set up makes things difficult: holders of the toxic waste have the potential to make new fake coins.

2) ZK-STARKs: Transparency and Quantum Resistance

Focusing on things such as the lack of anonymity and taking care of ZK-SNARKs' main problems.

- Being inherently quantum-resistant, as they rely on hash functions rather than number-theoretic assumptions.
- Enabling scalability with high transaction and batch proof volumes, which is perfect for Layer-2 systems like Stark Ex and Stark Net and mainly used in private DeFi, NFTs, and trading platforms (e.g., dYdX, Immutable X).

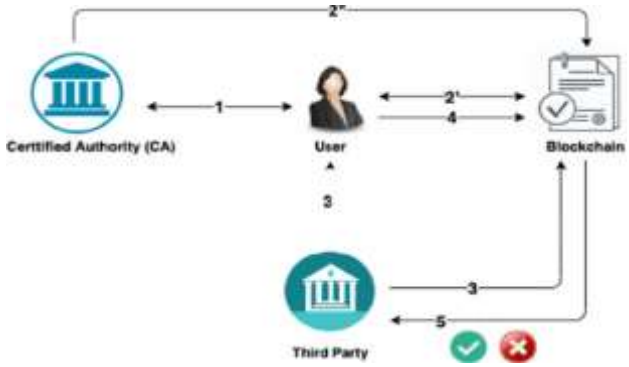

Fig. 1.ZK-SNARKs and ZK-STARKs in Blockchain-based Identity Management

B. Secure Data Sharing in Healthcare and Finance

Particularly in the current day, where big data, cloud computing, and the Internet of Things are all embracing one another, data is a precious asset. Nowadays, several breaches of healthcare data occur every day. To enhance medical data governance, HIPAA and other privacy protection legislation must to be reinforced. [13]. While zero-knowledge proofs are essential to blockchains, they are having a big impact on healthcare and finance privacy [14][15]. If a person or company wants something verified but wishes to hide private information, ZKPs are the right choice.

- **Healthcare:** Sharing Without Oversharing: Patient privacy is critical in the healthcare industry. Imagine a situation in which a hospital needs to demonstrate a patient's insurance eligibility or specific test results, without disclosing the patient's whole medical history.
- **Finance:** Confidentiality Meets Compliance: In the financial sector, maintaining customer privacy is as essential as ensuring institutional trust. ZKPs enable users to prove financial attributes, such as having a sufficient bank balance for a transaction or meeting a credit score threshold without revealing exact values. The commitment–challenge–verification protocol is the foundation of a flexible ZKP system: the prover commits to a secret, creates a proof, answers a challenge from a verifier, and the verifier verifies the proof's accuracy. This ensures that only the proof is disclosed, not the underlying sensitive data, thereby supporting compliance and confidentiality simultaneously.

C. Confidential Smart Contracts and Supply Chain Systems

SCs are blockchain programs that can be executed automatically based on contract conditions. The technological center of the second-generation blockchain is what it is called. Terms of confidentiality are often used to outline the responsibilities of pertinent parties for maintaining the privacy of information. SLC is the bridge between them. Different from a smart contract, SLC belongs to a legally binding agreement described in natural language, in which some terms could be expressed and implemented by computer-readable code.

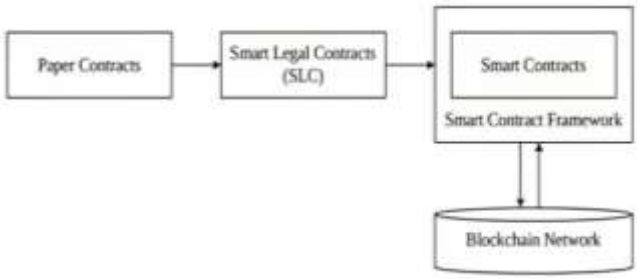

Fig. 2.The procedure of contract conversion

The general contract conversion process is shown in Figure 2. First, a contract written in natural language may be changed into smart legal contract programs in SLC language, which can then be further transformed into smart contracts in smart contract language (such as Solidity or Serpent). At last, the smart contract is added to blockchain networks as a transaction [16]. Before the bid opens, the auctioneer should ensure that the reserve price is kept secret. They should also assume the associated legal responsibility for any repercussions that may arise from the price reveal.

IV. CHALLENGES AND FUTURE DIRECTIONS

ZKPs hold great promise for privacy-sensitive domains like blockchain, identity, healthcare, and finance, but face significant deployment challenges [17]. Scalability issues, computational inefficiencies, and latency in complex proof generation hinder performance. Usability is further limited by the lack of intuitive development tools and seamless UI integration. Fragmented standards among ZKP types ZK-SNARKs, ZK-STARKs, and Bulletproofs create interoperability issues. Current efforts focus on standardization, modular design, and developer education to address these limitations. Overcoming these barriers is essential to enable broader adoption of ZKPs and support the creation of secure, privacy-preserving systems across diverse digital infrastructures.

A. Scalability and Efficiency Concerns

The efficiency and scalability of ZKPs, which still serve as the foundation for privacy-preserving systems, remain significant challenges, especially in high-demand sectors like banking, blockchain, identification, and healthcare Non-interactive proofs, like zk-SNARKs, are used in many implementations to reduce the proof's size and verification time [18]. However, producing these proofs is still computationally and resource-intensive, especially for complicated claims, which frequently results in latency problems in real-world deployments.

Moreover, frequent, concurrent proof generation is required for large-scale ZKP applications in IoT or healthcare, such as verifying test results or insurance eligibility. According to a recent MDPI assessment on intelligent energy and transportation systems, real-time responsiveness is still hampered by the combinatorial proliferation of ZKP computations, even though hierarchical blockchains lessen on-chain load pdfs.semanticscholar.org. Similarly, as the number of identities increases, throughput loss is observed in credential verification systems that use zk-SNARKs on identity platforms.

B. Usability and Integration in Real-World Systems

Zero Knowledge Proofs (ZKPs) useful in real-life cases often depends on how simply developers can use them and keep user experience smooth that working with ZKPs can turn into a challenge due to the complexity of setting up the environment. The technical difficulties of setting up ZKP-based solutions often lead smaller organizations and identity providers to choose other options, even if these address compliance and privacy at the same time. Both healthcare and smart credential systems are delayed because there are still no simple and unified SDKs or integration tools.

The actions of encryption and decryption must be well hidden from end users, yet this idea is not commonly found in UIs. Using web dashboards and QR codes, MDPI's Sensors explains how a ZKP-based university credentialing system managed to hide all generation activities, making the interactions straightforward and recognizable to all involved [19]. Still, introducing these systems into existing systems or workflows is usually resisted since traditional setup and strict regulations mean there are not enough people fully experienced with them. Thus, making cryptography easier to use for everyone is still crucial. Having best practices and simple abstraction layers, coupled with training developers, helps increase use of blockchain, identity, healthcare, and financial products.

C. Standardization and Interoperability Frameworks

The lack of robust standards and interoperability frameworks is a significant barrier as (ZKPs) go from lab prototypes to real-world systems in blockchain, identity, healthcare, and finance. Currently, many proof formats, APIs, and parameter configurations are implemented by schemes like as zk-SNARKs, zk-STARKs, Bulletproofs, and PLONK. For developers and organizations looking to create multi-domain systems, this fragmentation creates a challenging integration curve [20]. A ResearchGate survey on cross-platform ZKP tooling highlights this barrier, noting that "inconsistent serialization, varied cryptographic assumptions, and divergent proof interfaces make end-to-end integration difficult and error-prone.

There are currently Initiatives like the ZK Proof Community Group under Linux Foundation's Open SSF are standardizing circuit representation, proof serialization, and verification APIs across ZKP schemes. Academic efforts support modular design through reusable components and benchmark comparisons. Such standardization is vital for enabling interoperability, accelerating adoption, streamlining deployment, and improving security audits across applications in blockchain, identity, and healthcare.

V. LITERATURE OF REVIEW

This section reviews recent advancements in zero-knowledge proofs for privacy-preserving systems, focusing on applications in blockchain, identity, federated learning, and IoT.

It explores techniques like zk-SNARKs and smart contracts used to enhance security and data confidentiality.

Kumar and Devi. (2025) an integrated ZKP-based Route Verification Framework which uses blockchain technology to establish tamper-resistant privacy-preserving route validation. The framework includes five fundamental elements that provide ZKP proof generation for route credentials and blockchain-based proof storage and automated proof verification with BGP extension and off-chain IPFS-based proof management systems. The system architecture uses zk-SNARKs for cryptographic verifications while it relies on Hyperledger Fabric for decentralized proof validation. The proposed solution achieved superior routing security because it maintains both efficient storage scalability and minimal computational overhead, according to performance testing results [21].

Zhou et al. (2024) This study proposes a coordinated heat-electricity-gas dispatch mechanism that addresses privacy, incentive, and anti-forgery issues. Two challenges may be distinguished in the Nash bargaining-based coordination model: a dispatch problem that maximizes the total profit and a profit reallocation problem that provides incentives. The exponential The profit reallocation issue is resolved using ElGamal encryption, which also stops the profit variation of each system before and after coordination from being disclosed Additionally, provide a knowledge-proof anti-forgery method that protects privacy and prevents any system from deceitfully obtaining more redistributed profit [22].

Mackic and Antic. (2024) research focuses on implementing the ZKP protocol as part of IoT systems, specifically within smart home environments. The system relies on the WISE protocol for communication between physical devices and the central controller. As the system evolved, the optimization concept led to migrating the central controller's logic to the cloud. In the latest development phase, the cloud-based central controller is utilized for data processing and analysis, leveraging the WISE protocol's features for efficient data collection from both applications and devices. As an example of a physical device, set-top boxes are utilized for real-time transmission of critical logs for diagnostic purposes[23]

Ahmadi and Nourmohammadi (2024) propose a ZKP-based aggregator (zkDFL) that allows users to share their large-scale model parameters with a trusted, centralized server without sharing personal data with other users. Utilize blockchain technology and smart contracts to manage the aggregation algorithm. The server executes a ZKP algorithm to show the clients that the aggregate is done according to the accepted way. Using a publicly accessible wearable IoT dataset, the server may also show that each client input was utilized to evaluate their measure. According to numerical evaluations, zkDFL significantly reduces the cost of gas while simultaneously enhancing the scalability and privacy security of DFL systems. Additionally, it increases the aggregation process's verifiability and accuracy [24].

Naidu et al. (2023) This article suggests a safe way to use the ZKP algorithm in Blockchain for authentication. With ZKP, users may show that they hold certain knowledge or information without telling the verifier. Because of this, ZKP is perfect for privacy-preserving authentication, which is necessary to safeguard private user information. This enables storing the record of all the payment history, keeping transaction tracking, and making the record storage immutable and tamper-proof. With added features of better payment authentication and payment tracking, the system mitigates any chances of corruption, unauthorized transactions, and payment discrepancies [25].

Hou et al. (2022) created a privacy-preserving, zero-knowledge proof energy trading system based on blockchain technology. A peer-to-peer energy trading system is implemented using blockchain technology. Although public blockchains are often visible, sensitive data related to energy trade necessitates a privacy-preserving technique. A user uploads a commitment rather than the original bid amount, and the blockchain gets the zero-knowledge evidence of commitment [26].

Table I summarizes core studies, highlighting their approaches, key outcomes, limitations, and future research directions in decentralized privacy-preserving frameworks.

TABLE I. COMPARATIVE ANALYSIS OF RECENT RESEARCH ON PRIVACY-PRESERVING TECHNIQUES USING ZERO-KNOWLEDGE PROOFS IN DECENTRALIZED SYSTEMS

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Kumar and Devi (2025)	Route verification in ISPs using ZKP	Integrated zk-SNARK-based framework with blockchain (Hyperledger Fabric), BGP extension, and IPFS	Identified constructs, models, methods, and instantiations across cloud layers	Integration complexity in decentralized routing and real-time validation	Expand to support inter-domain routing, improve real-time performance
Zhou et al. (2024)	Privacy-preserving coordination in energy systems	Nash bargaining with ElGamal encryption and ZKP for anti-forgery	Proved secure profit coordination with nonlinear KKT constraints,	Complexity of nonlinear constraint verification and encryption cost	Broaden ZKP usage in real-time energy dispatch and decentralized market scenarios

			preserving privacy and fairness		
Mackic and Antic (2024)	Smart home IoT privacy	Cloud-based WISE protocol with ZKP-enhanced data sharing for set-top boxes	Enabled real-time monitoring and privacy-preserving log transmission in IoT	Dependency on cloud processing and central controller	Extend WISE protocol with decentralized verification and edge-based ZKP deployment
Ahmadi and Nourmohammadi (2024)	Federated learning with privacy	zkDFL: ZKP-verified aggregation over blockchain smart contracts	Ensured correctness and privacy in federated learning with reduced gas costs	Smart contract complexity and system scalability	Generalize zkDFL to cross-platform FL settings and real-time AI systems
Naidu et al. (2023)	Payment authentication via blockchain	ZKP-based mechanism for secure, tamper-proof transactions	Improved transaction transparency and privacy in payment systems	Scalability and latency in blockchain-based authentication	Apply ZKP to broader identity management and compliance tracking
Hou et al. (2022)	P2P energy trading with privacy	Blockchain with ZKP for bid commitment and auction verification	Maintained trade privacy while ensuring verifiable correctness	High gas cost on Ethereum and limited throughput	Optimize ZKP efficiency and explore Layer-2 integration for energy markets

VI. CONCLUSION AND FUTURE WORK

Innovations in cryptography are reshaping the future of secure and private digital interactions. As digital ecosystems grow more interconnected, the need for trust less verification becomes increasingly essential. Techniques like Zero-Knowledge Proofs (ZKPs) are emerging as foundational elements in privacy-preserving systems. ZKPs offer a powerful method for verifying information without revealing underlying data, enabling secure operations in areas like blockchain transactions, identity verification, and healthcare data sharing. Protocols such as ZK-SNARKs, ZK-STARKs, and Bulletproof provide diverse approaches tailored to different scalability and trust requirements. Although there are still limitations presented in today (i.e., computational costs, trusted setup, and interoperability), ZKPs are actively developing in terms of research and practical use. Some of their examples include projects such as Zcash, Stark Net and digital ID framework. In the future, it will be promising to implant ZKPs into decentralized platforms and regulatory systems and cross-domain architectures. The contribution to creating secure user-centric systems is already a turning point that takes us to becoming more private, transparent, and trustful.

In the future, more emphasis should be made to make ZKP systems, user-friendly, efficient, and scalable to be embedded in the real world. Creating cross-industry compatible standards such as standardized frameworks, modular toolkits will also drive adoption sooner. Also, conducting research on the quantum-resistant cryptography application on ZKP protocols and introducing much-needed user-friendly interfaces can enable the approach of advanced cryptography to practice in the context of blockchain, identity, healthcare, and finance.

REFERENCES

1. N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.
2. A. Goyal, "Optimizing Project Timelines with Strategic Vendor Management and Blockchain-Enabled LEAP Collaboration," *Int. J. Res. Anal. Rev.*, vol. 10, no. 3, pp. 94–100, 2023.
3. W. Shalannanda, "Using Zero-Knowledge Proof in Privacy-Preserving Networks," 2023, pp. 1–6. doi: 10.1109/TSSA59948.2023.10367041.
4. A. Satybaldy and M. Nowostawski, "Review of techniques for privacy-preserving blockchain systems," *BSCI 2020 - Proc. 2nd ACM Int. Symp. Blockchain Secur. Crit. Infrastructure, Co-located with AsiaCCS 2020*, pp. 1–9, 2020, doi: 10.1145/3384943.3409416.
5. S. Pandya, "Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 865–876, Aug. 2022, doi: 10.48175/IJARSCT-12467H.
6. R. Lavin, X. Liu, H. Mohanty, L. Norman, G. Zaarour, and B. Krishnamachari, "A Survey on the Applications

of Zero-Knowledge Proofs," pp. 1–81, 2024.
7. V. Prajapati, "Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, pp. 1011–1020, Mar. 2025, doi: 10.38124/ijisrt/25mar1062.
8. A. Goyal, "Integrating Blockchain for Vendor Coordination and Agile Scrum in Efficient Project Execution," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 12, 2024.
9. B. O. Roelink, M. El-Hajj, and D. Sarmah, "Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication," *Secur. Priv.*, vol. 7, no. 5, pp. 1–59, Sep. 2024, doi: 10.1002/spy2.401.
10. L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *J. Inf. Secur. Appl.*, vol. 80, pp. 1–20, Feb. 2024, doi: 10.1016/j.jisa.2023.103678.
11. S. M. R. Motlagh, C. Pahl, H. R. Barzegar, and N. El Ioini, "A Comparative Evaluation of Zero Knowledge Proof Techniques," in *Proceedings of the 10th International Conference on Internet of Things, Big Data and Security*, SCITEPRESS - Science and Technology Publications, 2025, pp. 237–244. doi: 10.5220/0013269100003944.
12. L. Herskind, P. Katsikouli, and N. Dragoni, "Privacy and Cryptocurrencies - A Systematic Literature Review," *IEEE Access*, vol. 8, pp. 54044–54059, 2020, doi: 10.1109/ACCESS.2020.2980950.
13. S. Pandya, "A Systematic Review of Blockchain Technology Use in Protecting and Maintaining Electronic Health Records," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, 2021.
14. G. Modalavalasa, "Advanced Blockchain Mechanisms for Strengthening Data Security and Ensuring Privacy in Decentralized Systems," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, 2023.
15. H. Jin, Y. Luo, P. Li, and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019, doi: 10.1109/ACCESS.2019.2916503.
16. H. Yin, Y. Zhu, G. Guo, and W. C.-C. Chu, "Privacy-Preserving Smart Contracts for Confidential Transactions Using Dual-Mode Broadcast Encryption," *IEEE Trans. Reliab.*, vol. 73, no. 2, pp. 1090–1103, 2024, doi: 10.1109/TR.2023.3328146.
17. P. Chatterjee, "Blockchain Technology as the Backbone of Fintech Innovation : Opportunities and Challenges," vol. 10, no. 12, pp. 798–810, 2023.
18. B. Zhang *et al.*, "A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing," *Electronics*, vol. 13, no. 21, 2024, doi: 10.3390/electronics13214260.
19. J. Watkins, "Zero-Knowledge Proof Techniques for Enhanced Privacy and Scalability in Blockchain Systems," in *IEEE International Symposium on High-Performance Computer Architecture*, 2025, pp. 1–10.
20. T. Burns, J. C. Dr, and F. Doyle, "A Review of Interoperability Standards for Industry 4.0.," *Procedia Manuf.*, vol. 38, pp. 646–653, 2019, doi: 10.1016/j.promfg.2020.01.083.
21. S. M. M, N. S. Kumar, and R. K. Devi, "A Privacy-Preserving Route Verification Framework Using Zero-Knowledge Proofs and Blockchain in Inter-Domain Routing," in *2025 8th International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, Apr. 2025, pp. 660–667. doi: 10.1109/ICOEI65986.2025.11013246.
22. X. Zhou, B. Wang, H. Zhao, H. Sun, Q. Guo, and B. Chen, "Incentivized Coordinated Heat-Electricity-Gas Dispatch: A Zero Knowledge Proof-Based Solution Considering Privacy and Anti-Forgery," *IEEE Trans. Sustain. Energy*, vol. 15, no. 2, pp. 713–725, 2024, doi: 10.1109/TSTE.2023.3295086.
23. D. Mackic and M. Antic, "Managing IoT Data Transmission in Smart Home Environments with Zero-Knowledge Proof Protocol," in *2024 Zooming Innovation in Consumer Technologies Conference (ZINC)*, 2024, pp. 134–137. doi: 10.1109/ZINC61849.2024.10579339.
24. M. Ahmadi and R. Nourmohammadi, "zkFDL: An efficient and privacy-preserving decentralized federated learning with zero knowledge proof," in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, 2024, pp. 1–10. doi: 10.1109/ICAIC60265.2024.10433831.
25. D. Naidu, B. Wanjari, R. Bhojwani, S. Suchak, R. Baser, and N. K. Ray, "Efficient Smart contract for Privacy Preserving Authentication in Blockchain using Zero Knowledge Proof," in *2023 OITS International Conference on Information Technology (OCIT)*, 2023, pp. 969–974. doi: 10.1109/OCIT59427.2023.10430710.
26. D. Hou, J. Zhang, S. Huang, Z. Peng, J. Ma, and X. Zhu, "Privacy-Preserving Energy Trading Using Blockchain and Zero Knowledge Proof," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 412–418. doi: 10.1109/Blockchain55522.2022.00064.