|| Volume 9 || Issue 9 || September 2025 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

Privacy-Preserving KYC Verification System Using Blockchain and Zero-Knowledge Proofs (Zident)

Mr. Aditya S. G[1], Mr. Ram Anil Ainkar[2], Prof. Ms. Pranalini Joshi[3]

ZCOER, Pune, MH, India[1,2,3]

Abstract: The current Know Your Customer (KYC) ecosystem is largely built on centralized systems, which are vulnerable to data breaches, incur high operational costs, and often require customers to repeat verification steps unnecessarily [1], [2]. Such centralized designs concentrate sensitive data in single repositories, creating “honeypots” that conflict with modern data privacy standards like the General Data Protection Regulation (GDPR) [3], [4]. At the same time, the transparent nature of public Distributed Ledger Technology (DLT) presents challenges for maintaining privacy in financial transactions, giving rise to what is often called the “Blockchain-Privacy Paradox” [5]. This survey explores cutting-edge DLT-based solutions that integrate Self-Sovereign Identity (SSI) and Zero-Knowledge Proof (ZKP) techniques. Key challenges in current approaches include scalability limitations in certain permissioned blockchains [6], inadequate mechanisms to fully support GDPR’s Right to Erasure [3], [4], [7], and the absence of reliable protocols to ensure legal access for Anti-Money Laundering (AML) compliance when users are uncooperative [8], [9].

Keywords:*Index Terms Blockchain, Zero-Knowledge Proofs, KYC, Privacy Preservation, Decentralized Identity, IPFS.*

I.INTRODUCTION:

A. Challenges of Traditional KYC and the Rise of SSI

The traditional KYC process is a regulatory necessity for financial institutions (FIs) to prevent money laundering and terrorist financing, yet it remains cumbersome and costly. Institutions worldwide spend substantial amounts—sometimes millions of USD annually—on compliance and managing regulatory workloads [2], [5]. Customers are often required to repeatedly submit and re-verify identity documents across multiple FIs, leading to frustration and redundant administrative effort [2], [10].

Centralized databases storing Personally Identifiable Information (PII) become prime targets for cyberattacks [1], creating significant privacy and security risks [1], [10]. These risks are further compounded by the fragmentation of identity data across siloed systems.

To address these shortcomings, the industry is moving toward Decentralized Identity (DI) frameworks and Self-Sovereign Identity (SSI) models. SSI empowers individuals to fully control their digital identities, leveraging Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to securely present identity claims [11], [12]. Distributed Ledger Technology (DLT) underpins this approach, providing an immutable and auditable foundation to ensure data integrity [1], [12].

B. The Role of Blockchain and Zero-Knowledge Proofs

Blockchain introduces decentralization and tamper-resistance, yet the transparency of public ledgers can inadvertently reveal user activity when pseudonymous addresses are linked to real identities [5]. This "Blockchain-Privacy Paradox" highlights the need for advanced cryptographic solutions.

Zero-Knowledge Proofs (ZKPs) are a key technology addressing this challenge [1], [10]. ZKPs enable individuals to prove statements—such as satisfying regulatory requirements—without revealing underlying sensitive data [1], [12]. This allows for selective disclosure, satisfying compliance checks while preserving privacy [3], [12]. In financial applications, ZKPs reconcile stringent regulatory demands with fundamental privacy rights, making them indispensable for modern KYC systems.

II. LITERATURE SURVEY:

Approaches in Decentralized KYC

Decentralized KYC solutions are built upon three fundamental technological pillars: Distributed Ledger Technology (DLT), decentralized storage solutions like IPFS, and privacy-preserving cryptographic techniques such as Zero-Knowledge Proofs (ZKP) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

A. Decentralized Identity and ZKP Integration

SSI-based systems leverage tailored distributed ledgers specifically designed to manage digital identities. For example, the Casper platform implements a Decentralized Identifier (DID) architecture on its proprietary Rahasak blockchain [1]. In Casper, personally identifiable information (PII) remains off-chain in the user’s mobile wallet, while only cryptographic proofs are recorded on the ledger, incorporating ZKP mechanisms to enhance privacy and traceability [1].

Similarly, frameworks built on Hyperledger Indy, such as the KYC2 platform, adopt SSI principles to allow privacy-preserving selective disclosure of identity attributes [11], [10]. Using Verifiable Credentials (VCs) combined with AnonCreds, a ZKP-based protocol, these systems minimize the risks associated with centralized identity storage, eliminating potential data “honeypots” [11], [10].

B. Permissioned Ledger and Off-Chain Storage Approaches

Public blockchains, such as Ethereum Layer 1, face inherent limitations in scalability and privacy, handling only limited transaction throughput [5]. To overcome these constraints, many enterprise KYC solutions employ permissioned DLTs. Hyperledger Fabric, for instance, establishes a permissioned network to secure sensitive information and ensure accountability [8], [6]. In this model, non-sensitive data can reside on shared ledgers, while confidential information is maintained in private channels, streamlining KYC processes across multiple financial institutions [8], [6].

Off-chain storage is another widely adopted strategy to handle large KYC documents and satisfy data retention requirements. Solutions leveraging IPFS encrypt user documents and store only hash references on-chain for verification and access control [11]. For instance, Optimised KYC Blockchain Systems utilize AES encryption along with LZ compression to reduce storage costs while securing off-chain data [11].

C. Advanced Cryptographic Mechanisms

Beyond basic hashing and encryption, advanced cryptographic methods enhance access control and auditability. The e-KYC TrustBlock framework applies Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to encrypt sensitive transaction data directly on the blockchain, enabling fine-grained access based on financial institution attributes [3]. Additionally, this framework mandates digital signatures on electronic consents to ensure non-repudiation and comply with GDPR regulations [3].

D. Interoperability and Regulatory-Centric Models

Some studies focus on addressing structural and regulatory challenges in digital identity systems. The Cross-Chain Identity framework emphasizes interoperability by integrating Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) across multiple heterogeneous blockchains, enabling seamless identity verification and asset transfers across distinct networks [12].

On the regulatory front, models tested on Ethereum-based KYC frameworks propose that central banks, such as the Reserve Bank of India (RBI), maintain a comprehensive registry of financial institutions. This approach allows continuous monitoring of compliance with KYC and Anti-Money Laundering (AML) regulations [10].

Additionally, the Experimentation Framework offers a structured environment to deploy and test blockchain Proof-of-Concepts (PoCs) for KYC, helping identify performance bottlenecks and operational constraints under real-world conditions [6].

III. PROBLEM STATEMENT:

Gaps in Existing Systems

Despite the cryptographic sophistication of current decentralized KYC implementations, several critical challenges hinder their practical adoption and compliance with legal frameworks.

1. Centralized Storage Vulnerability and Redundancy

Traditional KYC systems rely on centralized databases, which act as single points of failure—making them attractive targets for cyberattacks [1], [10]. These systems also force customers to repeatedly submit identity documents across multiple financial institutions [2], [9], creating redundancy, increasing operational costs (potentially millions of USD per bank annually [2]), and exposing personal data unnecessarily [10].

2. Scalability and Performance Bottlenecks

Enterprise-grade KYC solutions require high throughput, yet many platforms face inherent limitations. Permissioned ledgers like Hyperledger Indy [11] restrict write operations, slowing critical functions such as credential updates [6], [8]. Similarly, Ethereum Layer 1 solutions often struggle with low transaction throughput, rendering them inadequate for high-volume financial services [10], [12].

3. Lack of Granular Privacy (Absence of ZKP)

Several existing systems, including off-chain storage solutions and symmetric key-based approaches [11], [10], [2], require users to share decryption keys, resulting in "all-or-nothing" access to sensitive documents. This approach fails to achieve selective disclosure and data minimization, core benefits provided by Zero-Knowledge Proofs (ZKP) [1], [11], [12].

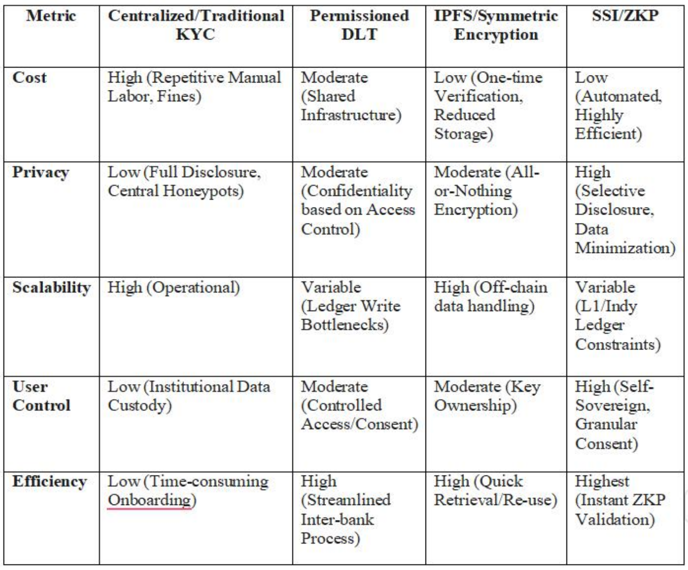
4. GDPR Right to Erasure Conflict

Blockchain immutability conflicts with GDPR Article 17, the "Right to be Forgotten," which mandates deletion of personal data upon request [3]. Even storing encrypted PII on an immutable ledger prevents literal compliance [4], [10]. These limitations underscore the need for verifiable mechanisms that support GDPR-compliant data erasure.

5. Unresolved Lawful Access Dilemma (AML/CFT)

Total anonymity can conflict with regulatory requirements for Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) [8], [5]. Privacy-preserving applications must enable accountable selective de-anonymization (SeDe) when illicit activity is detected [9], [8]. Current systems relying on voluntary disclosure assume cooperation from malicious actors, a flaw that leaves regulatory enforcement ineffective [6].

Table1: Comparative Analysis of Decentralized KYC Approaches by Metric



Metric	Centralized/Traditional KYC	Permissioned DLT	IPFS/Symmetric Encryption	SSI/ZKP
Cost	High (Repetitive Manual Labor, Fines)	Moderate (Shared Infrastructure)	Low (One-time Verification, Reduced Storage)	Low (Automated, Highly Efficient)
Privacy	Low (Full Disclosure, Central Honeypots)	Moderate (Confidentiality based on Access Control)	Moderate (All-or-Nothing Encryption)	High (Selective Disclosure, Data Minimization)
Scalability	High (Operational)	Variable (Ledger Write Bottlenecks)	High (Off-chain data handling)	Variable (L1/Indy Ledger Constraints)
User Control	Low (Institutional Data Custody)	Moderate (Controlled Access/Consent)	Moderate (Key Ownership)	High (Self-Sovereign, Granular Consent)
Efficiency	Low (Time-consuming Onboarding)	High (Streamlined Inter-bank Process)	High (Quick Retrieval/Re-use)	Highest (Instant ZKP Validation)

IV.PROPOSED DIRECTION:

The Zident Architectural Framework

The Zident framework is designed to bridge the gaps in privacy, scalability, and regulatory compliance identified in Section IV. It employs a hybrid on-chain/off-chain architecture, emphasizing cryptographic data minimization, auditable consent, and secure identity management.

A. Core Architectural Components

1. ZKP for Selective Disclosure

Zident leverages Zero-Knowledge Proofs (ZKP) to enable selective, attribute-based verification [11], [10]. This allows a user (Prover) to satisfy a financial institution (Verifier) that they meet a certain criterion—such as being over a specific age—without revealing the underlying personally identifiable information (e.g., Date of Birth) [1], [10]. This approach ensures compliance with GDPR principles of data minimization while offering privacy guarantees unattainable with traditional symmetric encryption [14], [10].

2. Blockchain and IPFS Integration

The framework anchors Decentralized Identifiers (DIDs), ZKP validation tokens, and cryptographic commitments on a blockchain ledger. All sensitive personal data remains strictly off-chain in a decentralized storage system such as IPFS [11], [12]. The blockchain itself functions as an immutable ledger for proofs and verification tokens, ensuring transparency and auditability without exposing raw personal data [12].

3. User-Controlled Consent and Revocation

Following Self-Sovereign Identity (SSI) principles [11], Zident gives users full control over their data-sharing decisions. Every proof request must be explicitly approved through the user's secure digital wallet. GDPR's Right to Erasure is addressed via crypto-shredding, whereby off-chain personal data is encrypted with unique keys that can be verifiably deleted or overwritten. This renders the data mathematically unrecoverable while preserving the integrity of the blockchain ledger [3], [11].

B. Novel Feature: Time-Limited Watermarked Document Viewing

Zident incorporates a distinctive security and auditability feature not available in conventional non-disclosure systems like KYC2 [11], [12]:

Feature: For situations where standard ZKP verification may be insufficient—such as enhanced due diligence or regulatory review—the verifier can request time-limited access to the document [12].

Mechanism: With the user's explicit consent, the requested document is displayed for a strictly enforced one-minute window [12]. During this brief access period, the document is dynamically watermarked with the verifier's unique identifiers, including organization name, Organization ID, or device-specific identifiers such as a MAC address [12].

Purpose: This feature provides a controlled and traceable channel for regulatory inspection, enhancing auditability. The dynamic watermark acts as a deterrent against unauthorized copying or misuse, ensuring accountability while maintaining strict privacy standards [12].

C. Zident System Diagrams

To illustrate the integration of these features, the Zident architecture and data flow models from the Project SRS are referenced here:

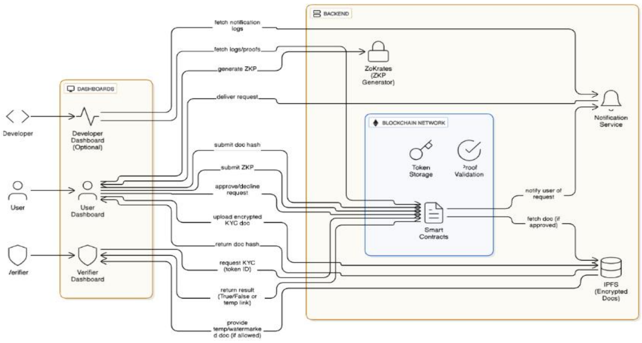


Figure 1 System Architecture

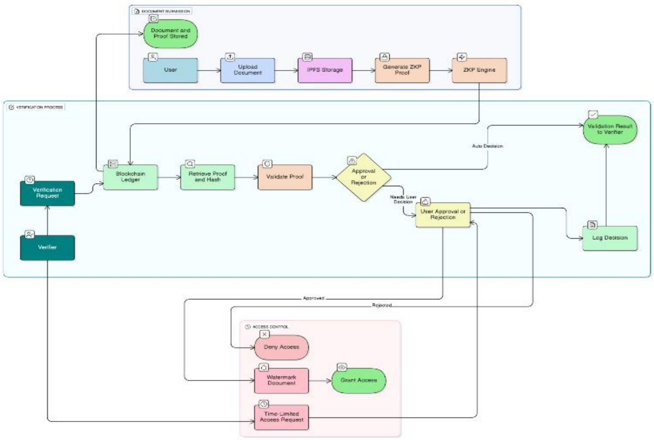


Figure 2 Data Flow Diagram

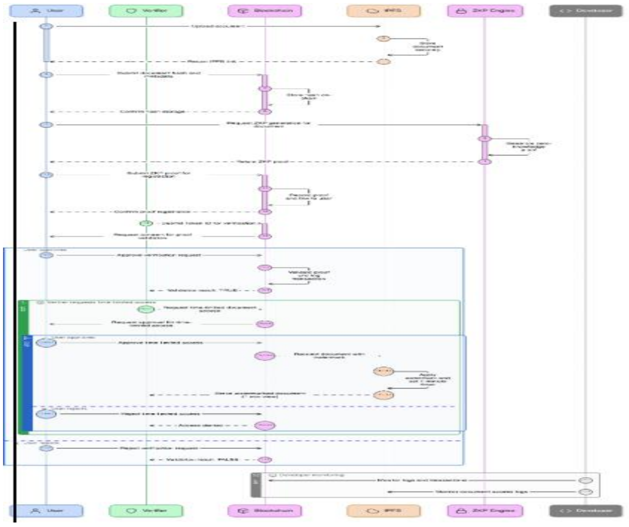


Figure 3 UML Diagram

V.DISCUSSION:

How Zident Overcomes Existing Limitations

The Zident framework is intentionally designed to address the core shortcomings observed in existing decentralized KYC solutions:

1. Scalability and Performance

Zident tackles performance bottlenecks seen in platforms like Hyperledger Indy [11] and Ethereum Layer 1 [10] by strictly minimizing on-chain writes [6], [8]. Computationally intensive tasks, such as ZKP generation, are performed on the user's local device or secure wallet [12], leveraging verifiable off-chain computation to maintain system efficiency.

2. Granular Privacy vs. All-or-Nothing Disclosure

Unlike conventional symmetric encryption approaches [14], [10], Zident uses ZKP to allow selective, attribute-based verification [1], [11]. Users can prove compliance or eligibility without exposing entire documents, preserving privacy while meeting regulatory verification needs [10], [12].

3. Regulatory Compliance (GDPR Right to Erasure)

By storing sensitive PII off-chain and tying it to unique encryption keys, Zident enables crypto-shredding. Destroying the relevant key renders the data unrecoverable, achieving verifiable erasure and satisfying GDPR requirements without compromising the immutability of the blockchain [3], [11].

4. Lawful Access (AML/CFT)

Zident supports regulatory oversight while maintaining privacy. It implements Involuntary Selective De-Anonymization (SeDe) using a threshold encryption scheme, ensuring that only a consensus of authorized regulatory entities can access minimal PII during suspicious activity detection [8], [9]. This design aligns with FATF Risk-Based Approach (RBA) recommendations.

5. Auditability and Deterrence

The Time-Limited Watermarked Document Viewing feature provides controlled, traceable document inspection [12]. This mechanism overcomes the auditability limitations of pure ZKP systems [11], allowing regulators to temporarily view documents while uniquely watermarking them to prevent unauthorized sharing or copying.

VI. FUTURE RESEARCH DIRECTION

The Zident architecture opens several avenues for future exploration to enhance its global applicability:

1. Cross-Chain and Global Interoperability

Research should focus on robust cross-chain communication protocols to ensure credentials are universally recognized [12]. Alignment with W3C standards for DIDs and VCs [1], [16] is crucial for global adoption across government, banking, and international trade networks.

2. AI/ML Integration for Enhanced Fraud Detection

Integrating AI-driven analytics could strengthen regulatory compliance. Future studies may explore trust scoring and identity reputation systems that leverage Zero-Knowledge Machine Learning (zkML) [1] to maintain privacy while detecting fraudulent activity [12].

3. Post-Quantum Security

As digital identities are long-term assets, quantum computing poses a potential threat. Research should target quantum-resistant ZKP methods like zk-STARKs [1], [12], ensuring Zident remains secure against future cryptographic advances.

VII.CONCLUSION

The demand for high-assurance digital identity systems that comply with global regulations (AML/CFT) while safeguarding user privacy (GDPR) defines the next generation of financial technology. Existing decentralized KYC solutions exhibit critical gaps, including limited transaction scalability [11], conflicts with the Right to Erasure [3], and insufficient mechanisms for lawful access [8], [9].

The Zident framework addresses these challenges through:

- ZKP-based selective verification [1] for privacy-preserving compliance
- Crypto-shredding and off-chain storage [11] for GDPR adherence
- Time-Limited Watermarked Document Viewing [12] for auditable regulatory oversight

By minimizing on-chain operations and employing scalable off-chain computation, Zident achieves a balance of performance, privacy, and accountability suitable for enterprise deployment. This framework establishes a robust, user-centric foundation for the future of digital identity verification.

VIII.REFERENCES

[1] C. V. Kumar, P. Selvaprabhu, N. Baska, U. V. Menon, V. B. Kumaravelup, S. Chinnadurai, and F. Ali, "Ethereum Blockchain Framework Enabling Banks to Know Their Customers," IEEE Access, vol. 12, 2024.

[2] S. Fugkeaw, "Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain," IEEE Access, vol. 10, 2022.

[3] E. Bandara, X. Liang, P. Foytik, S. Shetty, and K. De Zoysa, "A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform," in 2021 International Conference on Computer Communications and Networks (ICCCN), 2021.

[4] T. G. Allam, A. B. M. M. Hasan, A. Maag, and P. W. C. Prasad, "Ledger Technology of Blockchain and its Impact on Operational Performance of Banks: A Review," in 2021 6th International Conference on Innovative Technology in Intelligent System and Industrial Applications (CITISIA), 2021.

[5] R. R. Biradar and M. Dakshayini, "Blockchain Enabled KYC Solutions using Hyperledge Fabric," in Proceedings of the

International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020.

[6] A. A. Mamun, S. R. Hasan, M. S. Bhuiyan, M. S. Kaiser, and M. A. Yousuf, "Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology," in 2020 IEEE Region 10 Symposium (TENSYMP), 2020.

[7] P. Yadav and R. Chandak, "Transforming the Know Your Customer (KYC) Process using Blockchain," in 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), 2020.

[8] N. Sundareswaran, S. Sasirekha, I. J. L. Paul, S. Balakrishnan, and G. Swaminathan, "Optimised KYC Blockchain System," in 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), 2020.

[9] H. Yu, X. Wang, and T. Huang, "Unified Cross-Chain Digital Identity System," in 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2020.

[10] N. Lalitha and D. Soujanya, "Financial sector Innovations: Empowering Microfinance through the application of KYC Blockchain technology," in 2019 International Conference on Innovative Trends in Information Technology (ICITIIT), 2019.

[11] W. M. Shbair, M. Steichen, J. François, and R. State, "Blockchain Orchestration and Experimentation Framework: A Case Study of KYC," in 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS), 2018.

[12] U. T. Nguyen and A. An, "Client Onboarding Framework based on Hyperledger Indy and SSI Principles," in 2018 IEEE International Conference on Cybernetics and Computational Intelligence (Cybernetics), 2018.

Works cited

1. A systematic literature review of blockchain-based e-KYC systems - PMC - PubMed Central, accessed on October 3, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10100622/
2. SeDe: Balancing Blockchain Privacy and Regulatory Compliance by Selective De-Anonymization - Labyrinth, accessed on October 3, 2025, https://labyrinth.ac/sede.pdf
3. SeDe: Balancing Blockchain Privacy and Regulatory Compliance By Selective De-Anonymization - arXiv, accessed on October 3, 2025, https://arxiv.org/html/2311.08167v4
4. What is Zero-Knowledge Proof - a hot technology bringing trustworthiness to Web3 privacy?, accessed on October 3, 2025, https://www.nttdata.com/global/en/insights/focus/2024/what-is-zero-knowledge-proof
5. From Ledger Technology to Global Interoperability | U.S. Customs and Border Protection, accessed on October 3, 2025, https://www.cbp.gov/trade/ace/Innovation/ledger-technology-global-interoperability
6. Being “Real” about Hyperledger Indy & Aries / Anoncreds - Identity Woman, accessed on October 3, 2025, https://identitywoman.net/being-real-about-hyperledger-indy-aries-anoncreds/
7. Comparing ZK-SNARKs & ZK-STARKs: Key Distinctions In Blockchain Privacy Protocols, accessed on October 3, 2025, https://hacken.io/discover/zk-snark-vs-zk-stark/
8. Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity - arXiv, accessed on October 3, 2025, https://arxiv.org/pdf/2112.01237
9. FATF GUIDANCE Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures, accessed on October 3, 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf
10. A Survey on Zero-Knowledge Proof in Blockchain | Request PDF - ResearchGate, accessed on October 3, 2025, https://www.researchgate.net/publication/354051666_A_Survey_on_Zero-Knowledge_Proof_in_Blockchain
11. A guide to Zero Knowledge Proofs - Medium, accessed on October 3, 2025, https://medium.com/@Luca_Franceschini/a-guide-to-zero-knowledge-proofs-f2ff9e5959a8
12. The Zero-Knowledge Proof Technique: Limitations and Challenges - ResearchGate, accessed on October 3, 2025, https://www.researchgate.net/publication/376563994_The_Zero-Knowledge_Proof_Technique_Limitations_and_Challenges
13. All you need to know about uPort Identity management | by moslah hamza - Medium, accessed on October 3, 2025, https://medium.com/@hamzamaslah/all-you-need-to-know-about-uport-identity-management-3fc49db25332
14. Zero Knowledge Proof: Complete Guide and Applications - Infisign, accessed on October 3, 2025, https://www.infisign.ai/blog/what-is-zero-knowledge-proof-zkp
15. Decentralized Identity: The Ultimate Guide 2025 - Dock Labs, accessed on October 3, 2025, https://www.dock.io/post/decentralized-identity
16. Zero Knowledge Proof Solutions to Linkability Problems in Blockchain-Based Collaboration Systems - MDPI, accessed on October 3, 2025, https://www.mdpi.com/2227-7390/13/15/2387
17. AI-Driven Blockchain for Decentralized Identity and Secure Authentication in Cloud-Based Enterprises - ResearchGate, accessed on October 3, 2025, https://www.researchgate.net/publication/390271243_AI-Driven_Blockchain_for_Decentralized_Identity_and_Secure_Authentication_in_Cloud-Based_Enterprises
18. Zero-Knowledge Proof: The Future of Secure KYC - Zyphe,

accessed on October 3, 2025, https://www.zyphe.com/resources/blog/what-is-zero-knowledge-proof-in-kyc-verification

19. A Self-Sovereign Identity Blockchain Framework for Access Control and Transparency in Financial Institutions - MDPI, accessed on October 3, 2025, https://www.mdpi.com/2410-387X/9/1/9
20. arXiv:2209.09584v1 [cs.CR] 20 Sep 2022, accessed on October 3, 2025, https://arxiv.org/pdf/2209.09584
21. Blockchain, Personal Data and the GDPR Right to be Forgotten - Insights - Proskauer, accessed on October 3, 2025, https://www.proskauer.com/blog/blockchain-personal-data-and-the-gdpr-right-to-be-forgotten
22. A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility - MDPI, accessed on October 3, 2025, https://www.mdpi.com/1999-5903/17/1/1
23. Transaction Proximity: A Graph-Based Approach to Blockchain Fraud Prevention - arXiv, accessed on October 3, 2025, https://arxiv.org/pdf/2505.24284
24. Enabling secure and self determined health data sharing and consent management - PMC, accessed on October 3, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12398500/
25. Enhancing Blockchain Cross-Chain Interoperability: A Comprehensive Survey - arXiv, accessed on October 3, 2025, https://arxiv.org/html/2505.04934v1
26. Decentralized Identity: User Consent Guide 2024, accessed on-October3,2025, https://www.krayondigital.com/blog/decentralized-identity-user-consent-guide-2024
27. Zero-Knowledge Proofs: A Beginner's Guide - Dock Labs, accessed on October3, 2025, https://www.dock.io/post/zero-knowledge-proofs
28. FATF publishes new Guidance on Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures, accessed on October 3, 2025, https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/guidance-financial-inclusion-aml-tf-measures.html
29. Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs - a16z crypto, accessed on October 3, 2025, https://api.a16zcrypto.com/wp-content/uploads/2022/11/ZKPs-and-Regulatory-Compliant-Privacy.pdf
30. Hyperledger Indy in Blockchain Technology - Rain Infotech, accessed on October 3, 2025, https://www.raininfotech.com/hyperledger-indy-development/
31. Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, accessed on October 3, 2025, https://sovrin.org/library/sovrin-protocol-and-token-white-paper/
32. Decentralized Identity and KYC: Strengthening Trust in Global Trade Finance Networks, accessed on October 3, 2025, https://www.researchgate.net/publication/395920917_Decentralized_Identity_and_KYC_Strengthening_Trust_in_Global_Trade_Finance_Networks
33. uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain - SciSpace, accessed on October 3, 2025, https://scispace.com/pdf/uport-open-source-identity-management-system-an-assessment-xdhgws7hym.pdf
34. Blockchain for Quality: Advancing Security, Efficiency, and Transparency in Financial Systems | MDPI, accessed on October 3, 2025, https://www.mdpi.com/2674-1032/4/1/7
35. Zero Knowledge Proofs: Challenges, Applications, and Real-world Deployment, accessed on October 3, 2025, https://csrc.nist.gov/csrc/media/presentations/2024/wpec2024-3b1/images-media/wpec2024-3b1-slides-akira-tjerand--ZKP-Overview.pdf
36. Blockchain Technology: Core Mechanisms, Evolution, and Future Implementation Challenges - arXiv, accessed on October 3, 2025, https://arxiv.org/html/2505.08772v1
37. International Journal of Intelligent Systems and Applications in Engineering Vol. 12 No. 19s (2024) - Research Article
38. Novel Perceptive Approach for Automation on Ideal Self-Regulating Video Surveillance Model
39. International Journal of Applied Mathematics, Vol. 38 No. 1s (2025) ,Jubber Nadaf, Amol K. Kadam, A Mathematical Modeling Perspective For Automation On Ideal Self-Regulating Video Surveillance Systems, DOI: https://doi.org/10.12732/ijam.v38i1s.35