iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** X **Month of publication:** October 2025

DOI: https://doi.org/10.22214/ijraset.2025.74471

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

A Survey on Blockchain Based Secured Banking Using Self Sovereign Identity (SSI) and Verifiable Credentials (VC)

Anuradha Badage[1], Aman[2], Harshit Mohanty[3], Kumar Ayush[4], Md Jaki Imam[5]
[1]*Assistant Professor, Dept. Of CSE Sapthagiri College of Engineering*
[2, 3, 4, 5]*Dept. of CSE, Sapthagiri College of Engineering*

Abstract: ***Traditional digital banking is hampered by inefficient, repetitive and costly identity verification processes like Know Your Customer (KYC), which create significant friction for customers and operational burdens for financial institutions. This paper introduces a novel framework that integrates Self-Sovereign Identity (SSI) and Verifiable Credentials (VCs) with a permissioned blockchain ecosystem to address these challenges. The proposed user-centric model enhances security, streamlines regulatory compliance, reduces fraud, and empowers users with direct control over their digital identities. By leveraging the immutability of blockchain for trust and the portability of VCs for data exchange, this framework fundamentally re-architects the trust relationship between customers and banks, paving the way for a more efficient, secure, and inclusive financial future.***

I. INTRODUCTION

The digital transformation of the financial sector has accelerated, yet the foundational processes for establishing and managing customer identity remain a significant bottleneck. Banks and financial institutions face a "complex challenge" in fulfilling their Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations, which involve extensive data and document verification, navigation of siloed legacy systems, and adaptation to constantly changing regulations.1 This friction translates into a poor customer experience, with studies indicating that a significant percentage of customers abandon digital onboarding processes due to their complexity.3 For institutions, these manual, repetitive procedures are not only costly, consuming a substantial portion of operational resources but also create centralized data repositories that are prime targets for large-scale.

On The advent of decentralized technologies, particularly blockchain, offers a path to fundamentally change this dynamic by reducing reliance on trusted intermediaries for transaction validation. Central banks and consortiums adopt certain permissioned blockchains to maintain regulatory oversight over digital currencies (CBDCs) and other tokenized assets.

Moreover, a hybrid framework for blockchain-based banking that integrates the security of permissioned ledgers with the user-centric control of SSI and Verifiable Credentials (VCs). The structure of this paper, adapted from a survey-based methodology, will first outline the foundational technologies, review the current literature to identify the research gap, detail the proposed framework and its key processes, discuss its broad implications, and offer a conclusion on its transformative potential. To systematically evaluate the proposed evolution, it is useful to compare the features of traditional banking, its modern digital counterpart, and the emerging CBDC models. Furthermore, the combination of CBDC with SSI and VC can reshape financial inclusion by empowering individuals with secure, portable, and universally recognized digital identities. This integration supports cross-border interoperability, reduces fraud, and promotes transparency without compromising data sovereignty. Consequently, exploring a CBDC framework built on SSI and VC represents a significant step toward creating a resilient, user-centric, and future-ready digital financial ecosystem.

II. BACKGROUND AND MOTIVATION

A. Need for Trustworthy Digital Currency Systems:

1) Traditional financial systems depend heavily on intermediaries, which create inefficiencies, higher transaction costs, and delays.
2) Existing CBDC pilot models face challenges in balancing privacy with regulatory compliance, often leaving gaps in identity management.
3) Without strong identity verification, digital currencies are vulnerable to fraud, money laundering, and unauthorized access, reducing overall trust.

B. Technological Advancements Role of Self Sovereign Identity and Verifiable Credentials

1) SSI provides users with decentralized control over their digital identity, reducing reliance on centralized databases that are prone to breaches.

2) Verifiable Credentials enable secure, tamper-proof identity proofs, ensuring compliance with KYC/AML regulations without exposing unnecessary personal information.

C. Advancements in Digital Infrastructure

1) This Technology ensures transparency, immutability, and security for CBDC transactions.

2) Cryptographic protocols like zero-knowledge proofs enhance confidentiality while maintaining regulatory oversight.

III. LITERATURE SURVEY

A. Self-Sovereign Identity: The Future of Identity Management C. Allen (2016) [1]

METHODOLOGY: This work defines the principles of Self-Sovereign Identity, emphasizing decentralized identifiers (DIDs) and verifiable credentials. It highlights how blockchain ensures immutability and transparency for identity records. SSI shifts the identity ownership from institutions to individuals, creating user-centric control. Cryptographic proofs enable secure verification without revealing excess information. LIMITATIONS: The framework is conceptual, lacking large-scale implementations. Scalability and interoperability challenges remain unresolved. Widespread adoption requires standardized governance and regulatory clarity. [1]

B. Efficient Verifiable Credentials Data Model M. Sporny, D. Longley, and C. Allen (2019, W3C Recommendation) [2]

METHODOLOGY: This specification defines verifiable credentials for trusted, tamper-evident data exchange. JSON-LD and Linked Data Proofs enable interoperability and machine-readable trust frameworks. Issuers sign credentials using public-private key pairs, and verifiers validate proofs cryptographically. Holders present selective disclosure, maintaining privacy while ensuring authenticity. LIMITATIONS: The model assumes strong cryptographic infrastructure. Deployment is complex for low-resource environments. Governance models for cross-jurisdiction adoption are not fully established. [2]

C. Central Bank Digital Currencies: Foundational Principles and Core Features) Bank for International Settlements (BIS), Bank of Canada, ECB, Federal Reserve et al. (2020) [3]

METHODOLOGY: The report outlines key design considerations for CBDCs, focusing on resilience, security, and accessibility. It examines wholesale and retail CBDC use cases, ensuring financial stability and efficiency. The framework stresses privacy, AML/CFT compliance, and technological neutrality. Principles of monetary sovereignty and legal clarity underpin CBDC issuance. LIMITATIONS: The paper avoids specific technical designs. Real-world pilot projects are limited in scope. Interoperability with legacy banking systems is insufficiently addressed. [3]

D. The Decentralized Identity in Financial Services S. Preukschat and A. Reed (2021) [4]

METHODOLOGY: This book examines practical applications of decentralized identity within financial ecosystems. SSI is positioned as a tool for KYC simplification and fraud reduction. Verifiable credentials integrate smoothly with CBDC frameworks for regulatory compliance. It highlights trust frameworks, governance models, and interoperability standards for digital finance. LIMITATIONS: Case studies are limited to early-stage pilots. Regulatory uncertainties persist across jurisdictions. Deployment at scale requires collaboration between governments, banks, and identity providers. Practical integration with central banking systems also remains underexplored. [4]

E. Privacy-Preserving Digital Currency Transactions Using Zero-Knowledge Proofs F.R. Chaudhuri, A. Kate, and T. Rabin (2019) [5]

METHODOLOGY: This study explores how zero-knowledge proofs ensure transaction privacy in digital currencies. Users can validate transactions without revealing sensitive details. The scheme balances regulatory oversight with anonymity. Cryptographic efficiency is achieved using zk-SNARKs, enabling lightweight verification. It further explores integration of privacy-preserving protocols into central bank infrastructures. Advanced cryptographic primitives are tested for compliance with AML standards. LIMITATIONS: High computational overhead hinders real-time scalability. Implementation requires advanced cryptographic expertise. Widespread adoption depends on hardware acceleration and protocol standardization. Energy consumption in large-scale deployments raises sustainability concerns. Lack of interoperability with existing CBDC pilots limits real-world validation. [5]

F. Messenger End-to-End Encryption Overview Meta Security Team (2023) [6]
METHODOLOGY: Messenger adopts a modified version of the Signal protocol to ensure E2EE across chat and voice communication. Secure Real-time Transport Protocol (SRTP) handles media encryption. Devices sync using locally stored private keys and Meta servers validate integrity via public certificates. Encryption keys are rotated frequently to support forward secrecy and reduce compromise risk. The system models shared liquidity pools for faster settlement of multiple currencies. Collaborative testing among central banks validates the feasibility of unified infrastructures. LIMITATIONS: The solution is platform-bound and lacks interoperability with other messaging platforms. Legacy systems and older Messenger versions do not fully support E2EE. Potential security risks exist if users do not update regularly or revoke compromised sessions. User adoption challenges persist due to limited awareness of multi-CBDC platforms. Technical complexity increases operational costs for participating financial institutions. [6]

G. Design Choices for Central Bank Digital Currencies R. Auer and R. Böhme (2021, BIS Quarterly Review) [7]
METHODOLOGY: This study categorizes CBDC designs into retail and wholesale models, highlighting their impact on financial ecosystems. It analyzes account-based and token-based approaches, comparing accessibility, scalability, and anonymity. The research employs case studies of pilot projects to assess resilience and usability. LIMITATIONS: The framework is high-level, lacking deep technical validation. Risks in large-scale deployment are not tested. Trade-offs between privacy and compliance remain unresolved. Operational guidelines for interoperability are limited. [7]

G. Retail CBDC: The Next Generation of Money International Monetary Fund Staff Discussion Note (2020) [8]
METHODOLOGY: The paper explores retail CBDC as a tool for enhancing financial inclusion and payment efficiency. It evaluates direct, hybrid, and intermediated distribution models using simulation-based analysis. Emphasis is placed on improving access for unbanked populations and reducing transaction costs. The framework considers economic, legal, and technological implications for CBDC adoption. LIMITATIONS: Real-world consumer behavior data is missing. Legal frameworks for digital issuance vary widely. The model lacks detailed cybersecurity evaluation. Transition risks from physical to digital currency are not addressed fully. [8]

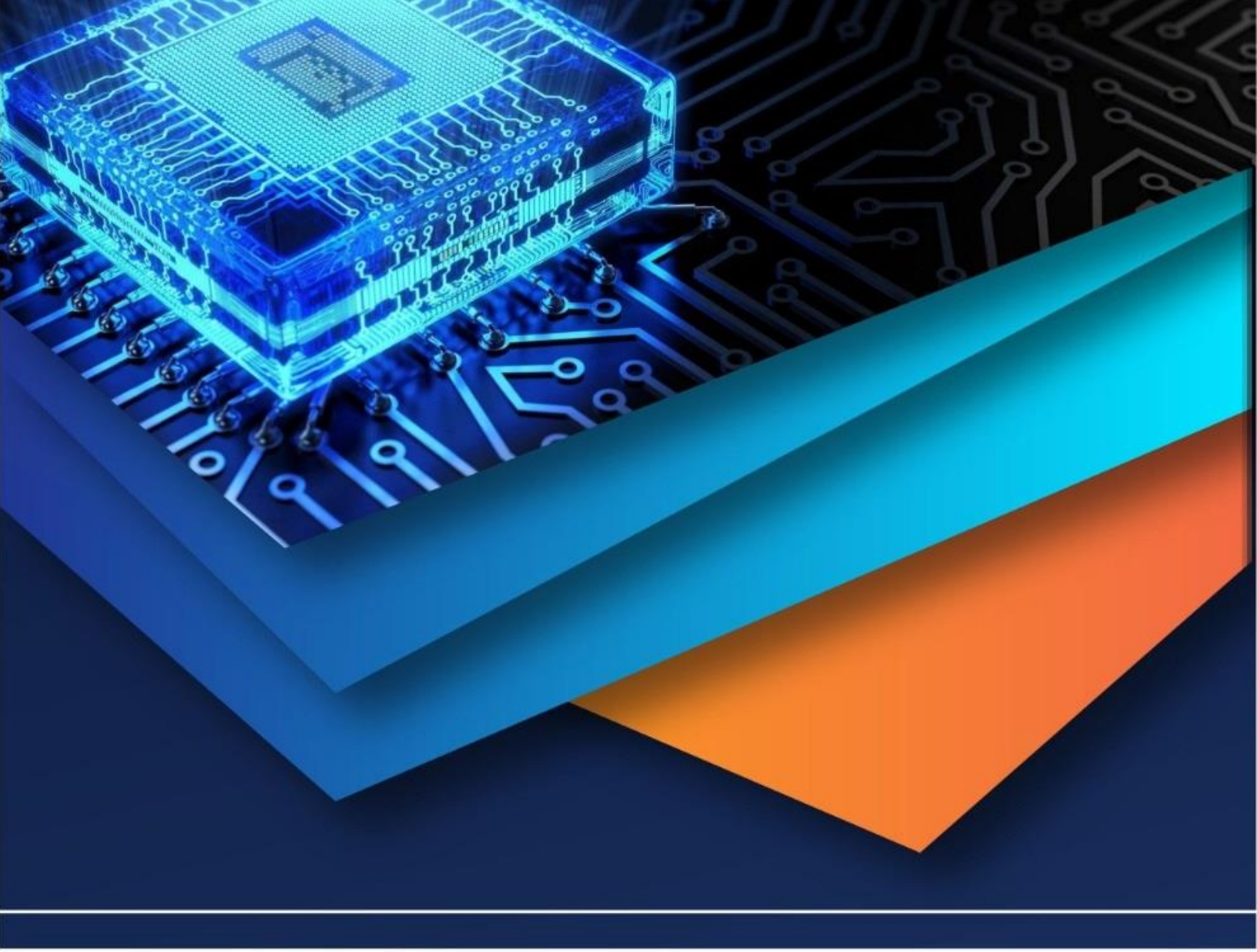
H. Digital Euro: Design and Distribution Options European Central Bank Report (2022) [9]
METHODOLOGY: The report investigates different distribution mechanisms for a digital euro, including direct issuance and intermediated models. It proposes safeguards for privacy while ensuring AML/CFT compliance. The study employs stress-testing for scalability, security, and resilience under peak loads. Design choices emphasize cross-border interoperability and user accessibility. LIMITATIONS: Pilot trials remain limited to regional experiments. Cross-border settlements are not fully validated. Implementation challenges in offline transactions persist. Integration with private payment providers remains uncertain. [9]

I. The Technology of Retail Central Bank Digital Currency Bank of England Staff Working Paper (2020) [10]
METHODOLOGY: This paper explores technical architectures for retail CBDCs, focusing on distributed ledger technologies and cryptographic safeguards. It compares centralized versus decentralized infrastructure trade-offs in terms of efficiency and scalability. The research considers smart contracts for programmable money use cases. Security measures are evaluated against cyberattacks and systemic risks. LIMITATIONS: The analysis is largely conceptual, lacking large-scale empirical testing. Energy efficiency concerns are not fully addressed. Operational costs for central banks remain uncertain. Compatibility with legacy systems is underexplored. The Collaboration with the early technologies become difficult as the old technologies do not comprehend well with the new Technologies in this domain. [10]

REFERENCES

[1] R. Chaudhuri, A. Kate, and T. Rabin, “Privacy-preserving digital currency transactions using zero-knowledge proofs,” in International Conference on Financial Cryptography and Data Security (FC’19), Springer, pp. 65–84, 2019.
[2] Bank for International Settlements Innovation Hub, “Project Dunbar: Multi-CBDC platforms for cross-border payments,” BIS Report, pp. 1–47, 2022. BIS
[3] M. Bordo and A. Levin, “Central bank digital currency and the future of monetary policy,” National Bureau of Economic Research (NBER) Working Paper, no. 23711, pp. 1–32, 2017. NBE
[4] K. Rogoff, “Costs and benefits to phasing out paper currency,” NBER Macroeconomics Annual, vol. 29, no. 1, pp. 445–456, 2014. NBER
[5] A. Berentsen and F. Schär, “The case for central bank electronic money and the non-case for central bank cryptocurrencies,” Federal Reserve Bank of St. Louis Review, vol. 100, no. 2, pp. 97–106, 2018.

[6] European Central Bank, "Exploring anonymity in central bank digital currencies," ECB In Focus Report, pp. 1–19, Dec. 2019. ECB
[7] C. Boar, H. Holden, and A. Wadsworth, "Impending arrival: A sequel to the survey on central bank digital currency," Bank for International Settlements Quarterly Review, pp. 1–12, March 2020. BIS
[8] Y. Auer and R. Böhme, "The technology of retail central bank digital currency," Bank for International Settlements (BIS) Quarterly Review, pp. 85–100, March 2020. BIS
[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008. Bitcoin.org
[10] C. Catalini and J. Gans, "Some simple economics of the blockchain," National Bureau of Economic Research (NBER) Working Paper, no. 22952, pp. 1–37, 2016. NBER
[11] H. Qian, C. Li, and Y. Zhang, "Cross-border payments with blockchain-based central bank digital currency," Journal of Banking and Finance, vol. 145, pp. 106–118, 2023. Elsevier
[12] M. Khan and S. Rashid, "Blockchain-based CBDC models for efficient and transparent digital payments," International Journal of Financial Innovation in Banking (IJFIB), vol. 6, no. 2, pp. 112–127, 2022.
[13] S. Ali, S. Narula, R. Iyer, and D. Nelson, "Central bank digital currencies: A comparative review," International Monetary Fund (IMF) FinTech Note, pp. 1–40, 2020. IMF
[14] D. Kiff, J. Alwazir, S. Davidovic, A. Farias, P. Khan, T. Khiaonarong, C. Malaika, H. Monroe, and N. Sugimoto, "A survey of research on retail central bank digital currency," International Monetary Fund (IMF) Working Paper, WP/20/104, 2020. IMF
[15] J. Bindseil, "Tiered CBDC and the financial system," European Central Bank (ECB) Working Paper Series, no. 2351, pp. 1–25, 2020. ECB.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY