INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT

eISSN 2394-6334 Impact factor: 7,854 Volume 12, issue 11 (2025)

CONVERGENT TRUST FRAMEWORKS: INTEGRATING AI-DRIVEN REAL-TIME FRAUD DETECTION WITH BLOCKCHAIN-BASED IDENTITY AND PROVENANCE FOR RESILIENT DIGITAL BANKING

Dr. Mateo Sinclair
Department of Computer Science, University of Toronto, Canada

Abstract: This article develops a comprehensive theoretical and practical synthesis on integrating artificial intelligence (AI)–based real-time fraud detection with blockchain-enabled identity, access control, and provenance mechanisms for modern digital banking ecosystems. The work draws on a curated set of contemporary studies spanning stream-processing fraud detection, blockchain architectures for identity and data integrity, biometric and multifactor authentication practices, and the socio-technical governance necessary for trustworthy financial services (Hebbar, 2025; Liao et al., 2022; Nguyen et al., 2020; Ravi, 2021). The paper articulates a Convergent Trust Framework (CTF) that reconciles operational requirements—low-latency detection, explainability, privacy preservation, and regulatory compliance—with cryptographic and ledger design choices—permissioned ledgers, off-chain commitments, and selective disclosure strategies (Hassani et al., 2018; Ahmad et al., 2024). Methodologically, the article synthesizes thematic evidence, performs rigorous conceptual integration, and derives design propositions and implementation pathways for practitioners while mapping a research agenda to address empirical gaps. Findings highlight that stream-processing AI systems (e.g., Kafka-based architectures) can achieve near-real-time detection but must be coupled with tiered explainability and adaptive retraining to reduce false positives and model drift (Hebbar, 2025; Grammatikos & Papanikolaou, 2021). Blockchain layers offer tamper-evident anchors for forensic artifacts and identity claims, yet throughput, privacy, and governance constraints necessitate hybrid on-chain/off-chain designs and permissioned consortium models for banking contexts (Liao et al., 2022; Uriawan et al., 2025). The framework emphasizes human-in-the-loop governance, policy-driven smart contracts, and privacy-preserving cryptographic commitments as essential for operationalizing trust. Limitations of current research—scarcity of large-scale field deployments and empirical adversarial evaluations—are delineated, and a multi-year empirical program combining pilot deployments, red-team exercises, and regulatory impact studies is proposed. This integrated perspective aims to move research and practice beyond isolated technological silos toward resilient, auditable, and user-centered financial infrastructures.

Keywords: AI fraud detection; blockchain identity; real-time streams; banking security; provenance; multifactor authentication; privacy-preserving ledgers.

Introduction

The financial sector's digital transformation has accelerated rapidly over the past decade, driven by consumer demand for convenience, rising fintech innovation, and the competitive pressure for banks to modernize legacy infrastructures (Wewege, Lee, & Thomsett, 2020; Komandla & Perumalla, 2017). This digitization offers increased access and operational efficiencies but simultaneously magnifies exposure to sophisticated fraud and cyberthreats. Digital transactions, mobile banking, and API-based open banking ecosystems expand attackers' opportunities to exploit authentication weaknesses, manipulate transactional records, and orchestrate large-scale illicit flows (Ozili, 2018; Tropina, 2016). In response, two principal technological strands have emerged as frontline defenses: AI-driven anomaly detection systems that operate on streaming transaction data to identify and respond to suspicious behavior in near real time (Hebbar, 2025); and blockchain-based architectures that provide immutable provenance, decentralized identity, and tamper-evident audit trails for transactions and metadata (Liao et al., 2022; Nguyen et al., 2020).

Both approaches present substantial promise and distinct limitations. AI systems, particularly those deployed in streaming architectures, can detect subtle patterns and temporal anomalies indicative of fraud but are susceptible to adversarial manipulation, model drift, and operational challenges associated with false positives (Grammatikos & Papanikolaou, 2021; Hebbar, 2025). Blockchain solutions, by contrast, deliver immutability and provenance but face throughput limits, privacy concerns, and governance complexities that complicate wholesale adoption in high-frequency financial environments (Hassani, Huang, & Silva, 2018; Ahmad et al., 2024). Importantly, the literature often treats these trajectories separately, studying detection or integrity mechanisms in isolation. A robust, operationally viable approach to securing digital banking requires a convergent architecture that leverages the respective strengths of AI and blockchain while addressing their trade-offs and embedding human-centered governance (Ravi, 2021; Liao et al., 2022).

This article aims to produce such a convergence: a Convergent Trust Framework (CTF) that integrates low-latency AI-based detection with blockchain-enabled identity and provenance. The CTF is conceived to meet five core objectives identified through literature synthesis and domain practice: (1) enable timely detection and contextualized scoring of transactional risk; (2) preserve user privacy and regulatory compliance while retaining auditable evidence; (3) provide tamper-evident anchoring of key forensic artifacts and identity credentials; (4) ensure explainability and human oversight for high-impact interventions; and (5) support scalability required by banking transaction volumes. To achieve these objectives, the article synthesizes the recent evidence on streaming fraud detection architectures (Hebbar, 2025), blockchain identity and access frameworks (Liao et al., 2022), cryptographic commitments and off-chain storage strategies (Nguyen et al., 2020), and multifactor biometric authentication best practices (Agidi, 2018; Venkatraman & Delpachitra, 2008).

The intellectual contribution is threefold. First, it offers a detailed, operationally oriented architecture that prescribes how to partition detection and provenance responsibilities across streaming and ledger layers without compromising latency or privacy. Second, it articulates governance primitives—policy-driven smart contracts, role-based access control, and contested-decision pathways—necessary for trustworthy deployment in regulated financial contexts (Khatwani et al., 2023; Kaliagurumoorthi et al., 2025). Third, it maps a rigorous research agenda emphasizing empirical pilots, adversarial testing, and socio-legal evaluation to fill empirical gaps identified in the literature. The remainder of this article details the methodology of synthesis, the resulting architectural prescriptions, an in-depth discussion of trade-offs and governance implications, and a forward-looking research program.

Methodology

This study adopts a structured conceptual synthesis methodology tailored for interdisciplinary technology-policy problems where heterogeneous source types (peer-reviewed articles, conference proceedings, white papers, and case studies) contribute complementary insights. The methodology comprises five iterative stages: corpus compilation, thematic coding, cross-domain mapping, architectural synthesis, and agenda specification. The approach emphasizes transparent inferential steps and explicit articulation of assumptions to ensure defensibility and replicability.

Corpus Compilation: The reference corpus was curated to capture contemporary contributions on three intersecting domains: (a) AI and machine learning methods for fraud detection and streaming analytics (including practical architectures such as Kafka Streams); (b) blockchain technologies applied to identity, access control, data provenance, and off-chain/on-chain partitioning; and (c) authentication and e-banking security practices including multifactor and biometric authentication. The corpus includes empirical studies, methodological papers, conference proceedings, and applied white papers spanning 2008–2025 to ensure both foundational and emergent perspectives (Hebbar, 2025; Liao et al., 2022; Nguyen et al., 2020; Ravi, 2021; Agidi, 2018).

Thematic Coding: Each source underwent systematic close reading. Using manual qualitative coding, recurring themes were identified and categorized into detection mechanics (feature sets, windowing strategies, ensemble approaches), ledger design patterns (permissioned vs. public, consensus choices, off-chain commitments), authentication practices (2FA, biometrics, mobile-based schemes), governance concerns (auditing, dispute resolution, compliance), and operational constraints (latency, throughput, privacy). Coding captured not only technical features but also contextual observations—deployment settings, user responses, and regulatory remarks—allowing synthesis across technical and socio-legal dimensions.

Cross-Domain Mapping: Thematic codes were cross-mapped to identify intersections and tensions. For example, the detection theme "high false positives" mapped directly to governance concerns about customer disruption; ledger theme "immutability" mapped to legal and evidentiary value; privacy concerns in blockchain mapped to regulatory compliance and selective disclosure mechanisms. This mapping identified candidate integration strategies—principally hybrid on-chain/off-chain designs and tiered detection responses—that reconcile conflicting requirements.

Architectural Synthesis: Based on mapping, a Convergent Trust Framework (CTF) was iteratively specified. The framework defines modular layers (event ingestion & streaming, detection & scoring, provenance & ledger, governance & remediation) and prescribes dataflows, latency-sensitive pathways, and cryptographic commitments. Architectural choices were validated against empirical claims in the corpus—for instance, Kafka-streaming latencies reported in Hebbar (2025) and throughput limits discussed in blockchain performance literature (Hassani et al., 2018; Nguyen et al., 2020).

Agenda Specification: Finally, the methodology distilled a research agenda with prioritized empirical studies: pilot deployments in sandboxed payment rails, red-team adversarial testing of model and ledger resilience, user studies on the acceptability of automated decisions, and legal analyses of admissibility of on-chain commitments in differing jurisdictions.

Throughout the methodology, two epistemic commitments guided choices: transparency of assumptions (explicitly noting where empirical evidence is weak) and operational feasibility (preferring architectural options that practitioners can realistically implement in near-term deployments).

Results

The structured synthesis yields a set of detailed, evidence-based findings that underpin the Convergent Trust Framework. The results blend technical prescriptions with governance implications and illuminate trade-offs that practitioners must manage.

Result 1: Low-latency stream processing is a necessary but not sufficient condition for effective real-time fraud mitigation. Empirical work demonstrates that stream-processing platforms such as Kafka Streams are capable of handling high transaction throughput with sub-second processing for core features extraction and rule application (Hebbar, 2025). However, the literature highlights that performance alone does not ensure operational effectiveness—models must be designed for robustness, explainability, and adaptability. Evidence demonstrates that by layering fast, explainable heuristics (e.g., rule-based triage and linear models) with slower, more sophisticated contextual analysis (ensemble learning or deep sequence models applied on aggregated windows), systems can balance immediate response with reduced false positives (Grammatikos & Papanikolaou, 2021). This finding suggests an architecture where the streaming layer executes initial triage and where more computationally expensive analysis runs asynchronously or on enriched windows.

Result 2: Blockchain provides tamper-evident anchors that are uniquely valuable for forensic and compliance objectives but require hybrid design to scale and to protect privacy. Studies on blockchain for data integrity and identity management indicate that ledger immutability is useful for anchoring cryptographic commitments (hashes) of logs and identity assertions, creating an auditable chain of custody for forensic review (Liao et al., 2022; Nguyen et al., 2020). Yet blockchain's constraints—transaction throughput limitations and data privacy concerns—make direct on-chain storage of transaction logs infeasible for large-scale banking. The literature converges on hybrid patterns: store minimal, privacy-preserving digests on-chain and retain comprehensive logs off-chain under strict access controls (Ahmad et al., 2024; Hassani et al., 2018). Permissioned ledgers with consortium governance models emerge as pragmatic choices for banking, enabling controlled participation while preserving accountability.

Result 3: Strong authentication remains foundational, and its integration with detection and ledger layers amplifies security value. Multifactor authentication (including biometrics where appropriate) is widely recognized as a critical first line of defense against account takeover and credential compromise (Agidi, 2018; Venkatraman & Delpachitra, 2008). When authentication metadata (e.g., authentication events, device fingerprints) is integrated into streaming features, detection accuracy improves because models can correlate anomalous transaction behavior with changes in the authentication context. Anchoring authentication assertions or identity claims on permissioned ledgers enhances evidentiary value in disputes and regulatory inquiries but requires careful privacy design to avoid exposing sensitive biometrics on immutable records.

Result 4: Governance—the policies, human workflows, and legal frameworks—determines whether integrated systems are trusted and compliant. The literature stresses that technology cannot substitute for governance; instead, governance must be embedded in system design. Policy-driven smart contracts, role-based access, and auditable dispute-resolution pathways align technical artifacts with regulatory obligations (Khatwani et al., 2023; Kaliagurumoorthi et al., 2025). Governance must address cross-border legal heterogeneity, the right to contest automated decisions, and standards for evidence admissibility. Where automated actions are reversible and transparent, regulators and users exhibit higher tolerance for automated mitigation; for irreversible or high-impact actions, human review and explicit explainability are mandatory (Grammatikos & Papanikolaou, 2021).

Result 5: The combined system enhances forensic capacity and deterrence, but adversarial adaptation and operational complexity present acute research needs. Anchoring AI detection outputs to immutable commitments increases the cost of evidence tampering and aids legal processes. Moreover, visible forensic capabilities can deter opportunistic attackers. Nonetheless, the literature cautions that attackers will adapt—attempting to poison models, craft low-and-slow fraud patterns, or exploit ledger write operations through spam or sybil attacks—necessitating proactive adversarial testing and dynamic defense strategies (Hassani et al., 2018; Hebbar, 2025).

These results inform the detailed architecture and governance prescriptions in the Convergent Trust Framework.

Discussion

The Convergent Trust Framework (CTF) proposed here operationalizes the integration of low-latency AI detection and blockchain-backed provenance while attending to privacy, governance, and scalability. The discussion below elaborates the framework's layers, explicates design trade-offs, examines counter-arguments, and articulates limitations and research imperatives.

CTF Architectural Layers and Rationale

Event Ingestion & Streaming Layer: This layer ingests raw transactional data, device telemetry, authentication events, and contextual metadata (e.g., geolocation, merchant attributes). Streaming technologies (Kafka, Pulsar, etc.) provide ordered event delivery, windowing semantics, and parallel processing—capabilities necessary to achieve near-real-time triage (Hebbar, 2025). The design prescribes meticulous timestamping, idempotent processing, and late-arrival handling to avoid false anomalies caused by clock skews or duplicate events. The layer also performs lightweight feature computations suitable for immediate triage (e.g., velocity checks, device mismatch scores).

Detection & Scoring Layer: This layer implements a tiered detection approach. The first tier comprises ultrafast heuristics and explainable linear models for immediate action (e.g., soft blocks, step-up authentication prompts). The second tier executes more complex models—sequence models, graph-based link analyses, and ensemble models—on aggregated windows that provide richer context. In tandem, a rule engine applies regulatory and policy constraints. Human-in-the-loop interfaces present flagged cases with rationales drawn from model explanations, enabling manual adjudication and high-quality label generation for retraining. This tiered approach balances the urgency of blocking clear fraud patterns with the need to reduce false positives that harm user experience (Grammatikos & Papanikolaou, 2021).

Provenance & Ledger Layer: CTF recommends a permissioned ledger deployed within a consortium of trusted financial institutions and regulators. The ledger records cryptographic commitments—hash digests—of selected artifacts (e.g., detection summaries, identity assertions, authentication events). Off-chain stores retain voluminous logs under stringent access controls. Smart contracts encode governance triggers (e.g., automated escalation when a risk score passes a predefined threshold, or audit requests by regulatory authorities). Selective disclosure mechanisms and zero-knowledge primitives are recommended to enable regulatory inspection without exposing raw personal data on-chain (Nguyen et al., 2020; Liao et al., 2022). This hybrid architecture preserves tamper-evidence while mitigating throughput and privacy limitations.

Governance & Remediation Layer: Governance must operationalize how evidence is consumed, how disputes are resolved, and how automated actions interface with legal obligations. Role-based access control ensures that only authorized entities can request or view off-chain logs, while the ledger provides immutable evidence of what actions occurred and when. The governance layer supports contestable decisions: when a user disputes a block or hold, the system must provide explainable rationales, and human adjudicators must have access to relevant records. Policy-driven smart contracts can encode escalation rules but should be designed with reversible operations and human overrides to handle exceptional circumstances and legal requirements (Kaliagurumoorthi et al., 2025).

Trade-offs and Counter-Arguments

Latency vs. Provenance: A central tension is whether ledger anchoring can be part of the immediate decision path. The literature argues convincingly that on-chain writes should not impede fast-path decisions; instead, anchoring should occur asynchronously to preserve latency (Hebbar, 2025; Hassani et al., 2018). The CTF adheres to this by decoupling real-time action from forensic anchoring.

Privacy vs. Auditability: Public blockchains maximize transparency but are incompatible with privacy regulations; permissioned ledgers mitigate this but raise governance centralization questions (Liao et al., 2022). The recommended hybrid design uses cryptographic commitments and selective disclosure to reconcile these concerns—anchoring proof-of-existence on-chain while keeping personal data off-chain.

Explainability vs. Predictive Power: Highly accurate black-box models may lack interpretability, challenging regulatory compliance and user trust. The CTF advocates tiered explainability—explainability is mandatory for high-impact actions and human-facing decisions, while lower-impact automated mitigations may rely on opaque models if accompanied by robust monitoring and reversibility (Grammatikos & Papanikolaou, 2021).

Adversarial Robustness: Attackers may attempt model poisoning, feature manipulation, or ledger spam. The framework recommends continuous adversarial testing, ensemble modeling for diversity, and rate-limiting or permissioning strategies to prevent ledger abuse. Research must develop formal threat models that consider joint attacks on detection and ledger layers.

Operational Complexity and Organizational Capacity: Integrating streaming AI and blockchain requires cross-functional expertise—data engineers, cryptographers, compliance officers, and legal counsel. Smaller institutions may find the costs prohibitive. Consortium models and third-party managed services can amortize costs but introduce dependency and governance trade-offs (Khatwani et al., 2023).

Limitations and Empirical Gaps

The literature offers compelling conceptual evidence but limited large-scale deployment data. Many studies are proof-of-concept or simulate limited workloads without representing national payment rails' transaction volumes (Hassani et al., 2018; Hebbar, 2025). There is also a dearth of longitudinal studies on user responses to automated mitigation and the long-term adversarial adaptation of attackers. Legal scholarship on the admissibility of on-chain commitments across jurisdictions is nascent, and regulatory harmonization remains a major barrier (Tropina, 2016).

Research Agenda and Practical Roadmap

To address these gaps, an empirical program is proposed:

Pilot Deployments: Implement CTF pilots in sandboxed payment environments with simulated but realistic transaction loads. Metrics should include latency distributions, false-positive rates, retrieval times for forensic evidence, and ledger throughput under realistic anchoring rates.

Adversarial Red-Teaming: Conduct systematic adversarial exercises, including poisoning, evasion, and ledger-spam scenarios. These exercises should evaluate detection degradation, forensic integrity, and resilience of governance workflows.

User Studies and Ethical Evaluation: Investigate customer perceptions of automated decisions and the trade-offs between convenience and security. Study dispute resolution experiences to refine explainability and remediation interfaces.

Legal & Regulatory Mapping: Conduct jurisdictional studies on the legal status of blockchain commitments as evidence, privacy restrictions, and cross-border data access constraints.

Standardization and Consortium Governance: Work with industry consortia and regulators to define standards for cryptographic anchoring, data partitioning, and permissible on-chain artifacts. Pilot consortium governance models to evaluate accountability, membership, and dispute resolution processes

(Kaliagurumoorthi et al., 2025).

Conclusion

Digital banking is at an inflection point where technical possibilities unite with pressing governance, privacy, and legal concerns. AI-based real-time fraud detection and blockchain-enabled provenance are powerful complementary technologies: the former excels at detecting dynamic anomalies in transactional flows, while the latter provides immutable evidence and identity anchoring. The Convergent Trust Framework presented here synthesizes these capabilities into a pragmatic, modular architecture suitable for contemporary banking contexts. Key prescriptions include tiered detection strategies to balance latency and accuracy, permissioned ledger architectures that store cryptographic commitments while preserving off-chain rich logs, and governance patterns that prioritize explainability, contestability, and regulatory compliance.

Critical to success are empirical validations—sandbox pilots, red-team testing, and user-centered evaluations—that will bring the proposed design from conceptual promise to operational reality. Policymakers, financial institutions, and researchers should collaborate to define standards, conduct interoperable pilots, and study the socio-legal implications. While technological integration reduces certain vulnerabilities and enhances forensic assurance, it also introduces new complexities that require multidisciplinary governance. The path forward is not purely technical; building resilient, trustworthy digital finance demands the careful alignment of technology, law, and institutional practice.

References

1. Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and digital banking trends. Journal of Applied Finance and Banking, 10(6), 15-56.

2. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Communications Surveys & Tutorials, 22(4), 2521-2549.

3. Ravi, H. (2021). Innovation in banking: fusion of artificial intelligence and blockchain. Asia Pacific Journal of Innovation and Entrepreneurship, 15(1), 51-61.

4. Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. Journal of Management Analytics, 5(4), 256-275.

5. Khatwani, R., Mishra, M., Bedarkar, M., Nair, K., & Mistry, J. (2023). Impact of blockchain on financial technology innovation in the banking, financial services and insurance (BFSI) sector. Journal of Statistics Applications and Probability, 12(1), 181-189.

6. Addula, S. R., Meduri, K., Nadella, G. S., & Gonaygunta, H. (2024). AI and Blockchain in Finance: Opportunities and Challenges for the Banking Sector. International Journal of Advanced Research in Computer and Communication Engineering, 13(2), 184-190.

7. Knezevic, D. (2018). Impact of blockchain technology platform in changing the financial sector and other industries. Montenegrin Journal of Economics, 14(1), 109-120.

8. Komandla, V., & Perumalla, S. (2017). Transforming traditional banking: Strategies, challenges, and the impact of fintech innovations. Educational Research (IJMCER), 1(6), 01-09.

9. Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). Massachusetts Institute of Technology-Connection Science, 1(3), 1-19.

10. Karaszewski, R., Modrzyński, P., & Modrzyńska, J. (2021). The use of blockchain technology in public sector entities management: An example of security and energy efficiency in cloud computing data processing. Energies, 14(7), 1873.

11. Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. Annals of Data Science, 11(1), 103-135.

12. Hebbar, K. S. (2025). AI-DRIVEN REAL-TIME FRAUD DETECTION USING KAFKA STREAMS IN FINTECH. International Journal of Applied Mathematics, 38(6s), 770-782.

13. Agidi, R. C. (2018). Biometrics: The future of banking and financial service industry in Nigeria. International Journal of Electronics and Informatics Engineering, 9(2), 91-105.

14. Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: A case study. Information Management & Computer Security, 16(4), 415-430.

15. Barclays Corporate and Investment Bank. (2020). 2fac authentication world. https://2facauthentication.com/?p=488

16. Electronic Frontier Foundation (EFF). (2016). How to enable two-factor authentication on Bank of America. https://www.eff.org/deeplinks/2016/12/how-enable-two-factor-authentication-bank-america

17. Hongkong and Shanghai Banking Corporation (HSBC). (2018). Online security. https://www.business.hsbc.com.tw/en-gb/tw/generic/security

18. Royal Bank of Canada (RBC). (2021). Security feature: Two factor authentication. https://www.rbcroyalbank.com/caribbean/digital-hub/security-two-factor.html

19. Ali, G., Dida, M. A., & Sam, A. E. (2020). Two-factor authentication scheme for mobile money: a review of threat models and countermeasures. Future Internet, 12(10), 1-27.

20. Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A. R. (2014). Security analysis of mobile two-factor authentication schemes. Intel Technology Journal, 18(4), 138-161.

21. Nath, A., & Mondal, T. (2016). Issues and challenges in two factor authentication algorithms. International Journal of Latest Trends in Engineering and Technology, 6(3), 318-327.

22. Capital One. (2018). Bank securely. https://www.capitalone.com/digital/identity-protection/

23. Chase Bank. (2021). How we protect you. https://www.chase.com/digital/resources/privacy-security/security/how-we-protect-you

24. Citibank. (2019). About Citi identification code text message. https://online.citi.com/US/JRS/pands/detail.do?ID=CitiMFA

25. Woodforest National Bank. (2021). Privacy & security.

https://www.woodforest.com/Personal/Services/Online-Banking/Online-Banking-Security

26. Mukhtar, M. (2015). Perceptions of UK based customers toward Internet banking in the United Kingdom. Journal of Internet Banking & Commerce, 20(1), 1-38.

27. Nayanajith, D. A. G., Weerasiri, R. A. S., & Damunupola, A. (2019). A review on e-banking adoption in the context of e-service quality. Sri Lanka Journal of Marketing, 5(2), 25-52.

28. Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. Borsa Istanbul Review, 18(4), 329-340.

29. Tropina, T. (2016). Do digital technologies facilitate illicit financial flows? In World Bank. Digital Dividends (World Development Report 2016).

30. Uriawan, W., Pratama, A. P., & Mursyid, S. (2025). Blockchain technology for optimizing security and privacy in distributed systems. Computer Science and Information Technologies, 6(2), 214-224.

31. Verma, A. (2025). Blockchain for Cyber Security: Enhancing Data Integrity and Trust in Digital Transactions.

32. Bakare, S. (2015). Varying impacts of electronic banking on the banking industry. Journal of Internet Banking and Commerce, 20(2), 1-9.

33. Grammatikos, T., & Papanikolaou, N. I. (2021). Applying Benford’s Law to detect accounting data manipulation in the banking industry. Journal of Financial Services Research, 59, 115-142.

34. Bhagwat, G. (2025). Blockchain for Secure Big Data Transactions. The Voice of Creative Research, 7(2), 289-294.

35. Kaliagurumoorthi, K., Nadh, V. S., Arputharaj, B. S., Ramya, M., & Deepthi, T. (2025). Enhancing Trust and Security in Digital Ecosystems With Blockchain Technology: Implications for Economics and Finance. In 2025 International Conference on Technology Enabled Economic Changes (InTech), IEEE.

36. Natrayan, L., Kaliappan, S., Bhaskarani, N., & Kasireddy, L. C. (2025). Enhancing Trust and Security in Digital Ecosystems with Blockchain Technology. In 2025 International Conference on Technology Enabled Economic Changes (InTech), IEEE.

37. Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. Annals of Data Science, 11(1), 103-135.