A Zero-Trust Architecture Framework Integrating Permissioned Blockchains for Enhanced Data Protection in US Federal Reserve and Commercial Interfacing

Authors

Sunday Oladele, Jimy Tide, Ahmed Khan

Date; November 25, 2026

Abstract

The interface between the Federal Reserve System and commercial banking organizations represents one of the most consequential data-exchange surfaces in the U.S. financial system, yet it remains governed by perimeter-based security assumptions inherited from an earlier era of closed network topologies. This study addresses the absence of a validated architectural framework that fuses zero-trust principles with permissioned blockchain infrastructure specifically for this inter-organizational context. A design-based research methodology was employed, combining systematic synthesis of Federal Reserve operational requirements, simulation of a proof-of-concept permissioned ledger environment, and structured expert validation with fifteen domain practitioners. The proposed Zero-Trust Permissioned Interfacing Framework (ZTPIF) demonstrated a 89.4% reduction in simulated unauthorized data-access events relative to baseline perimeter models, while preserving transaction settlement latency within Federal Reserve Operating Circular No. 5 tolerances. Identity verification accuracy reached 94.2% under adversarial test conditions. The findings indicate that permissioned blockchain ledgers can operationalize zero-trust continuous verification at institutional

boundaries without sacrificing the auditability and performance required for Fedwire and FedNow integration. The framework offers a replicable reference architecture for supervisory agencies and commercial banks seeking to move beyond trust-but-verify postures toward cryptographically enforced, least-privilege data exchange.

Keywords: Zero-trust architecture, permissioned blockchain, Federal Reserve interfacing, financial data protection

1. Introduction

1.1 Background

The architectural relationship between the Federal Reserve Banks and the commercial banking institutions they serve has historically rested on a trust model that presumes authenticated institutional identity implies authorized subsequent access. Under Operating Circular No. 5, institutions accessing Reserve Bank services such as Fedwire, FedACH, and FedNow are required to implement security controls and report cyber incidents, but the underlying access paradigm remains boundary-oriented: once an institution establishes an electronic connection, its subsequent data requests are evaluated against static authorization profiles rather than continuous behavioral and contextual verification . This model has proven increasingly inadequate as cyber threats against financial infrastructure grow in sophistication and frequency .

Zero-trust architecture (ZTA) has emerged as the dominant paradigm for addressing the limitations of perimeter security, premised on the principle of "never trust, always verify" . The Federal Reserve Board itself has begun adopting zero-trust principles internally, requiring continuous credential verification for access to internal resources . However, the extension of zero-trust principles to the *inter-organizational* boundary between the Federal Reserve and commercial banks presents distinct challenges: verification must occur without a central authority controlling both endpoints, data exchanges involve highly sensitive settlement and supervisory information, and the performance requirements of real-time payment rails leave little tolerance for latency introduced by security controls.

Permissioned blockchain architectures offer a complementary technological substrate. Unlike public blockchains, permissioned ledgers restrict participation to identified, vetted institutions, making them suitable for regulated financial contexts . Recent scholarship has demonstrated the viability of consortium-based permissioned ledgers for interbank settlement, with simulations indicating throughput improvements of up to 85% and latency reductions of 60% relative to traditional systems . The integration of zero-trust principles with permissioned ledgers for Federal Reserve–commercial interfacing, however, remains unexplored in the peer-reviewed literature.

1.2 Problem Statement

Existing approaches to securing Federal Reserve–commercial bank data exchanges exhibit three interrelated limitations. First, they are predominantly perimeter-based: security controls authenticate institutional connections but do not continuously evaluate the legitimacy of each data transaction against behavioral baselines and contextual risk signals . Second, they lack cryptographic auditability across organizational boundaries: while individual institutions maintain internal logs, no shared, tamper-evident record exists that both the Federal Reserve and the commercial bank can independently verify without relying on a trusted intermediary . Third, they impose a false dichotomy between security and performance: stronger verification controls are assumed to degrade settlement latency, discouraging their adoption in time-sensitive payment rails .

Attempts to address these limitations have been partial. Risk-adaptive zero-trust models have been proposed for secure transaction networks, demonstrating improved attack detection rates and reduced false positives, but these models assume a single administrative domain and do not address inter-organizational trust negotiation . Permissioned blockchain designs for interbank settlement have demonstrated technical feasibility, but they treat identity verification as a static admission-control function rather than a continuous, risk-adaptive process . No validated framework exists that integrates continuous zero-trust verification with permissioned ledger auditability specifically for the Federal Reserve–commercial interfacing context.

1.3 Objectives of the Study

General objective: To design and validate a zero-trust architecture framework integrating permissioned blockchain infrastructure for enhanced data protection at the Federal Reserve–commercial banking interface.

Specific objectives:

1. To identify the critical data-exchange points and security requirements governing Federal Reserve–commercial bank interfacing under current operational circulars and supervisory guidance.
2. To design a hybrid framework that operationalizes continuous zero-trust verification through permissioned blockchain smart contracts and distributed identity attestation.
3. To validate the framework through simulation against baseline perimeter models, measuring unauthorized access reduction, verification accuracy, and settlement latency impact.
4. To assess implementation barriers and formulate practitioner-oriented deployment guidance.

1.4 Research Questions

1. What are the principal data-exchange surfaces and associated security vulnerabilities at the Federal Reserve–commercial banking interface under existing regulatory frameworks?
2. How can permissioned blockchain infrastructure operationalize zero-trust continuous verification across organizational boundaries without introducing a central trusted intermediary?
3. To what extent does the proposed framework reduce unauthorized data-access events while maintaining performance within Federal Reserve operational tolerances?
4. What organizational and regulatory barriers must be addressed for practical deployment?

1.5 Significance of the Study

For practitioners and administrators: The framework provides a concrete reference architecture for commercial banks and Federal Reserve service providers seeking to strengthen inter-organizational data protection without abandoning existing payment rails. The simulation results offer quantified expectations for security improvement and performance impact.

For policymakers: The study informs supervisory guidance by demonstrating that zero-trust principles can be extended to inter-organizational contexts through permissioned ledger mechanisms, potentially updating the assumptions underlying Operating Circular No. 5 and related guidance.

For academic literature: This research extends zero-trust theory beyond single-domain enterprise security into federated financial infrastructure, introducing the construct of *cryptographically attested continuous verification* as a bridge between ZTA and permissioned blockchain scholarship.

For future researchers: The validated framework and simulation methodology provide a foundation for empirical deployment studies and for extension to other regulated inter-organizational data-exchange contexts.

1.6 Scope and Limitations

This study focuses on the data-exchange interface between Federal Reserve Banks and federally insured depository institutions accessing Reserve Bank payment services (Fedwire, FedACH, FedNow). The temporal scope addresses the regulatory and technological landscape as of 2025–2026. Geographically, it is limited to the U.S. federal financial regulatory context.

The study excludes: (a) internal Federal Reserve Board systems not directly interfacing with commercial institutions; (b) non-bank payment service providers accessing Reserve Bank accounts under emerging “skinny account” proposals ; (c) non-U.S. central bank interfaces. Key limitations include reliance on simulated rather than production deployment data for performance metrics, and the assumption that institutional participants possess the technical

capacity to operate blockchain nodes—an assumption that may not hold for smaller community banks.

2. Literature Review

2.1 Conceptual Review

Zero-Trust Architecture (ZTA). ZTA is a cybersecurity paradigm that eliminates implicit trust based on network location or prior authentication, requiring continuous verification of every access request against identity, device posture, behavioral context, and policy . In financial services, ZTA implementation has focused on internal identity and access management, with privileged access governance and just-in-time elevation emerging as critical controls . The Federal Reserve Board has adopted zero-trust principles internally, and the Office of Management and Budget's M-22-09 mandates federal agencies to move toward ZTA .

Permissioned Blockchain. A permissioned blockchain is a distributed ledger restricted to identified, authorized participants, typically governed by a consortium agreement . Unlike public blockchains, permissioned ledgers can achieve Byzantine Fault Tolerance with lower computational overhead and can enforce privacy through channels and private data collections. In banking, permissioned ledgers have been proposed for interbank settlement, with Hyperledger Fabric identified as a suitable framework for consortium-based financial applications .

Federal Reserve–Commercial Interfacing. This construct encompasses the technical, procedural, and legal mechanisms through which commercial banks access Reserve Bank services. Operating Circular No. 5 governs electronic access, requiring institutions to implement security controls, report cyber incidents within specified timeframes, and obtain prior approval for certain connection configurations . The Federal Reserve's supervisory posture emphasizes operational resilience and third-party risk management, with IT/operational risk findings among the most frequently cited issues at community and regional banks .

2.2 Theoretical Framework

This study is guided by two complementary theoretical perspectives.

Zero-Trust Security Theory. The foundational premise of zero-trust is that trust should never be granted implicitly based on network location or prior authentication, but must be continuously earned through verification of identity, device integrity, and behavioral context . Applied to inter-organizational financial data exchange, this theory implies that the Federal Reserve should not trust a commercial bank's data requests merely because the bank has an established connection; each request must be evaluated against cryptographic attestation of the requesting system's state and the transaction's conformity to established patterns.

Institutional Economics of Trust. Permissioned blockchain infrastructure addresses a fundamental problem in inter-organizational exchange: the absence of a mutually trusted record-keeping authority . By distributing the ledger across consortium members and requiring cryptographic consensus for state transitions, permissioned blockchains create *algorithmic trust* that substitutes for institutional trust. This theoretical lens explains why permissioned ledgers are particularly suited to the Federal Reserve–commercial interface: both parties can independently verify the integrity of shared records without ceding control to the other.

2.3 Empirical Review

Zero-Trust in Financial Services. A 2026 IEEE study proposed a multi-layered ZTA for FinTech platforms incorporating micro-segmentation, identity and access management, AI-driven behavioral analytics, and continuous monitoring . While comprehensive within a single platform, the model does not address federated trust negotiation between institutions. A separate risk-adaptive ZTA for financial transaction networks demonstrated improved attack detection and reduced false positives through closed-loop feedback that adjusts trust thresholds based on observed outcomes . This study, however, assumed a centralized administrative domain and did not incorporate distributed ledger auditability.

Permissioned Blockchain for Banking. The Integrated Blockchain Layer for Hybrid Banking (IBL-HB) framework proposed a consortium-based permissioned ledger for interbank fiat settlement, reporting 85% higher throughput and 60% reduced latency compared to traditional banking systems in simulation . A U.S. patent granted in 2026 describes a blockchain-based interbank clearing and settlement network with permissioned shared distributed ledger and encrypted direct communication channels between bank nodes . These studies establish technical feasibility but treat identity and access management as static admission-control functions rather than continuous verification processes.

Federal Reserve Cybersecurity Posture. The Federal Reserve Board's 2024 cybersecurity report documents the Board's internal adoption of zero-trust principles and its supervisory focus on institutions' cyber-risk management . The 2025 Supervision and Regulation Report identifies IT/operational risk as the most frequently cited category of outstanding supervisory findings at community banking organizations, underscoring persistent vulnerabilities at the interface . However, neither document specifies architectural mechanisms for extending zero-trust to inter-organizational data flows.

2.4 Research Gap

No validated architectural framework exists that integrates continuous zero-trust verification with permissioned blockchain auditability specifically for the Federal Reserve–commercial banking interface. Existing zero-trust models address internal enterprise security or single-domain transaction networks; existing permissioned blockchain designs for banking treat identity verification as a binary admission decision. The intersection of these two literatures—

continuous, risk-adaptive verification operationalized through distributed ledger smart contracts at a regulated inter-organizational boundary—remains unexplored. This study fills that gap by designing, simulating, and validating the Zero-Trust Permissioned Interfacing Framework (ZTPIF).

3. Methodology

3.1 Research Design

A design-based research (DBR) methodology was employed, appropriate for studies that seek to design and validate practical solutions to complex, real-world problems through iterative analysis, design, and evaluation . The design proceeded in three phases: (1) requirements analysis through systematic review of Federal Reserve operational circulars and supervisory guidance; (2) framework design and proof-of-concept simulation; (3) expert validation through structured interviews with domain practitioners.

3.2 Study Area / Population

The target population comprised professionals with direct experience in Federal Reserve interfacing, financial institution cybersecurity, or permissioned blockchain implementation in banking. The accessible population for expert validation consisted of fifteen practitioners: five from Federal Reserve Bank technology or supervision functions, six from commercial bank treasury or technology divisions with direct Fed interface responsibilities, and four from blockchain infrastructure firms serving financial clients.

3.3 Sample Size and Sampling Technique

A purposive sampling approach was used, selecting participants based on documented professional experience (minimum five years) in at least one of the three domains. The sample size of fifteen was determined by the principle of saturation for structured expert validation in design research, where the objective is architectural assessment rather than statistical generalization . Stratification ensured representation across the three stakeholder groups.

3.4 Data Collection Methods

Phase 1: Requirements Analysis. Federal Reserve Operating Circular No. 5, Board cybersecurity reports, and supervisory guidance documents were systematically analyzed to extract interface requirements, security mandates, and performance constraints .

Phase 2: Simulation Data. A synthetic dataset representing 500,000 inter-organizational data-exchange transactions was generated, with parameters calibrated to published Federal Reserve payment volume statistics and security incident rates. Simulated transactions included legitimate

settlement instructions, status queries, and supervisory data requests, along with injected adversarial events representing unauthorized access attempts, credential compromise, and data exfiltration scenarios. All simulation data were clearly designated as synthetic; no production Federal Reserve or commercial bank data were accessed.

Phase 3: Expert Validation. Semi-structured interviews (45–60 minutes) were conducted remotely, focusing on framework feasibility, implementation barriers, and alignment with operational realities. Interviews were transcribed and thematically analyzed.

3.5 Research Instruments

The proof-of-concept simulation was implemented using Hyperledger Fabric v2.5 as the permissioned ledger platform, selected for its support of private data collections and pluggable consensus . Smart contracts (chaincode) were written in Go to enforce verification policies. Behavioral analytics for continuous trust scoring were implemented in Python 3.11 using scikit-learn for anomaly detection. Network simulation was conducted using Mininet for topology emulation. All code and simulation configurations are available for replication upon request.

3.6 Validity and Reliability

Content validity: The framework's components were mapped against the seven pillars of zero-trust architecture specified in NIST SP 800-207 and against Federal Reserve Operating Circular No. 5 security requirements, with an external reviewer confirming alignment.

Predictive validity: Simulation outcomes were compared against baseline metrics derived from published industry incident rates and payment latency benchmarks.

Inter-rater reliability: Two independent coders analyzed expert interview transcripts; Cohen's $\kappa = 0.81$ indicated substantial agreement on thematic categories.

3.7 Data Analysis Techniques

The following models were compared:

1. **Baseline Perimeter Model:** Static authentication with role-based access control, representing current practice.
2. **ZTPIF (Proposed):** Zero-trust continuous verification with permissioned blockchain attestation.
3. **ZTA-Only:** Zero-trust verification without blockchain auditability (single-domain implementation).

Performance metrics included: unauthorized access event rate (events per 10,000 transactions), verification accuracy (true positive rate for legitimate transactions + true negative rate for adversarial transactions), settlement latency (mean milliseconds per transaction), and false positive rate. Comparisons used paired t-tests with Bonferroni correction for multiple

comparisons ($\alpha = 0.05/3 = 0.017$). Ten-fold cross-validation was applied to the anomaly detection component.

3.8 Ethical Considerations

This study used no human subjects data and accessed no protected health information (PHI) or non-public Federal Reserve data. All simulation data were synthetically generated. Expert validation participants provided informed consent and are identified only by role category. The study protocol was reviewed and determined to be exempt under 45 CFR 46.104(d)(2) (research involving only educational tests, survey procedures, interview procedures, or observation of public behavior).

4. Results

4.1 Data Presentation

Table 1. Simulation Transaction Composition by Category

Transaction Category	Count	Percentage
Legitimate settlement instructions	312,450	62.5%
Status and inquiry queries	124,800	25.0%
Supervisory data requests	37,500	7.5%
Injected adversarial events	25,250	5.0%
Total	**500,000**	**100%**

Table 2. Performance Comparison Across Security Models

Metric	Baseline Perimeter	ZTA-Only	ZTPIF (Proposed)
Unauthorized access events (per 10k tx)	47.3	12.6	5.0
Verification accuracy	82.1%	91.3%	94.2%
Mean settlement latency (ms)	142	168	159
False positive rate	3.8%	2.1%	1.4%

Note: Latency measurements represent simulated smart contract execution plus consensus overhead for the permissioned ledger configuration.

4.2 Analysis of Results

The ZTPIF model achieved an 89.4% reduction in unauthorized access events relative to the baseline perimeter model (47.3 to 5.0 per 10,000 transactions, $p < 0.001$, Cohen's $d = 2.31$). The ZTA-only model achieved a 73.4% reduction (47.3 to 12.6), indicating that the blockchain attestation layer contributed an additional 16.0 percentage points of reduction beyond continuous verification alone.

Verification accuracy for ZTPIF reached 94.2%, compared to 82.1% for baseline and 91.3% for ZTA-only. The false positive rate declined from 3.8% (baseline) to 1.4% (ZTPIF), a 63.2% improvement that reduces the operational burden of investigating legitimate transactions incorrectly flagged as anomalous.

Settlement latency under ZTPIF averaged 159 ms, representing a 12.0% increase over the baseline (142 ms) but remaining within the sub-200 ms threshold generally considered acceptable for real-time payment processing. The ZTA-only model exhibited higher latency (168 ms) because it lacked the distributed consensus optimization that the permissioned ledger provides through parallel endorsement.

Feature importance analysis for the continuous verification component identified three dominant predictors of adversarial events: (1) transaction request timing relative to established institutional patterns (weight = 0.34), (2) deviation from historical data-request payload characteristics (weight = 0.28), and (3) mismatches between cryptographic attestation state and declared device posture (weight = 0.22).

Expert validation (n=15) identified implementation barriers including: lack of internal blockchain expertise at community banks (cited by 11 of 15 participants), uncertainty regarding supervisory acceptance of permissioned ledger records as authoritative audit trails (9 of 15), and the absence of standardized inter-organizational identity federation (8 of 15).

5. Discussion

5.1 Interpretation

Research Question 1: Data-exchange surfaces and vulnerabilities. The requirements analysis confirmed that Federal Reserve Operating Circular No. 5 establishes incident reporting and security control obligations but does not prescribe continuous verification mechanisms for ongoing data exchanges . The supervisory finding that IT/operational risk constitutes the leading category of outstanding issues at community banks aligns with the simulation finding that perimeter-based authentication is particularly vulnerable to credential compromise and session hijacking scenarios.

Research Question 2: Permissioned blockchain operationalization of zero-trust. The ZTPIF design demonstrates that permissioned ledgers can operationalize zero-trust continuous verification through two mechanisms: (a) smart contracts that enforce verification policy consistently across all participants without a central enforcement point, and (b) distributed identity attestation that allows each participant to independently verify the other's state without relying on self-reported claims. This extends the zero-trust literature beyond single-domain implementations and provides a concrete architecture for the "algorithmic trust" that permissioned blockchain scholarship has theorized .

Research Question 3: Security-performance tradeoff. The finding that ZTPIF achieved superior security outcomes with *lower* latency than ZTA-only (159 ms vs. 168 ms) contradicts the common assumption that stronger security necessarily degrades performance. The explanation lies in the permissioned ledger's parallel endorsement architecture, which distributes verification workload across consortium nodes rather than concentrating it at a central policy engine. This finding aligns with IBL-HB results showing that consortium-based permissioned ledgers can improve both security and throughput relative to centralized alternatives .

Research Question 4: Implementation barriers. The expert-identified barriers point to a critical distinction between technical feasibility and organizational readiness. While the framework's technical performance is promising, the human capital gap at community banks and the regulatory uncertainty regarding blockchain records as audit evidence represent substantial deployment obstacles. These barriers are consistent with broader findings on the chasm between zero-trust ambition and legacy infrastructure reality in banking .

5.2 Implications

Academic implications: This study introduces the construct of *cryptographically attested continuous verification* as a theoretical bridge between zero-trust architecture and permissioned blockchain scholarship. It extends zero-trust theory from the single-enterprise domain to federated, regulated inter-organizational contexts, demonstrating that the absence of a central trust authority—previously a barrier to zero-trust implementation—can be addressed through distributed ledger mechanisms.

Practical implications: For Federal Reserve service providers and commercial bank administrators, the framework suggests a phased adoption pathway: (1) implement internal zero-trust identity and access management for Fed interface personnel (baseline ZTA); (2) establish a consortium permissioned ledger for audit trail sharing among a limited pilot group; (3) extend the ledger to enforce verification policies for high-risk data exchanges (e.g., supervisory data requests, large-value settlement instructions). Expected metrics to monitor include unauthorized access event rate (target: <10 per 10,000 transactions), verification false positive rate (target: <2%), and settlement latency (target: <200 ms). Lead time for a pilot consortium is estimated at 9–12 months based on expert input.

5.3 Limitations

1. **Simulated performance data:** Settlement latency and throughput results derive from simulation calibrated to published benchmarks, not production deployment. Actual performance in Federal Reserve operational environments may differ.
2. **Sample size for expert validation:** Fifteen participants provided sufficient saturation for architectural assessment but cannot support statistical generalization to the broader population of financial institutions.
3. **Assumption of institutional technical capacity:** The framework assumes consortium participants can operate blockchain nodes and maintain cryptographic key management infrastructure—an assumption that may not hold for smaller community banks without third-party service providers.
4. **Regulatory uncertainty:** The study does not resolve whether permissioned ledger records would be accepted by Federal Reserve supervisors as authoritative for examination or dispute-resolution purposes.

5.4 Future Research Directions

1. **Pilot deployment study:** Implement ZTPIF in a limited production pilot involving one Federal Reserve Bank and three to five commercial banks to generate empirical performance and adoption data.

2. **Community bank accommodation models:** Investigate shared-node or service-bureau architectures that would allow smaller institutions to participate in the consortium without requiring in-house blockchain expertise.
3. **Supervisory acceptance study:** Engage Federal Reserve supervision and regulation staff to assess whether permissioned ledger records can satisfy examination documentation requirements and what modifications to guidance would be necessary.
4. **Longitudinal security effectiveness:** Conduct a multi-year study tracking adversarial event rates under ZTPIF as threat actors adapt, assessing whether the closed-loop trust threshold adjustment mechanism maintains effectiveness over time.

6. Conclusion

This study designed and validated the Zero-Trust Permissioned Interfacing Framework (ZTPIF), demonstrating an 89.4% reduction in simulated unauthorized data-access events at the Federal Reserve–commercial banking interface while maintaining settlement latency within operational tolerances. The framework's principal contribution is a replicable reference architecture that operationalizes continuous zero-trust verification through permissioned blockchain smart contracts and distributed identity attestation, overcoming the single-domain limitation of prior zero-trust models and the static admission-control limitation of prior banking blockchain designs. For administrators, the practical takeaway is that security and performance need not be traded off: the permissioned ledger's parallel endorsement architecture actually reduced latency relative to zero-trust implementation without distributed consensus. As the Federal Reserve continues its internal zero-trust journey and commercial banks confront increasingly sophisticated adversaries, the ZTPIF framework offers a technically grounded and regulatorily informed pathway toward cryptographically enforced, least-privilege data exchange across the most consequential boundary in American finance.

References

1. Sabeena, A. A., Ahmed, A., Sharmin, S., Hassan, A., Kamal, F. A. M. B., Islam, A., & Bhuiyan, M. F. H. (2025). Blockchain-based banking infrastructure for securing financial transactions and reducing operational costs in the US. *Journal of Financial Technology and Innovation*.
2. Zero-trust architectures for next-generation in FinTech platforms: A multi-layer security model. (2026). In *2026 IEEE International Conference on Computing and Informatics* (pp. 1–8). IEEE. https://doi.org/10.1109/xxxxx
3. Integrated blockchain layer for hybrid banking (IBL-HB): A decentralized infrastructure for seamless coexistence of digital currencies and traditional banking. (2026). In *2026 IEEE International Conference on Blockchain and Cryptocurrency* (pp. 1–10). IEEE.
4. Federal Reserve Banks. (2024). *Operating Circular No. 5: Electronic access*. Federal Reserve Bank Services. https://frbservices.org
5. Provenir. (2026, February 9). Zero trust in digital banking: Why risk leaders need a bridge between legacy and next-gen systems.
6. Design and implementation of a risk-adaptive zero-trust architecture for secure financial transaction networks. (2026). In *2026 International Conference on Computational Modelling, Simulation and Optimization* (pp. 243–250). IEEE Computer Society.
7. System and method for implementing an interbank information network. (2026). U.S. Patent No. 12,664,528 B2. U.S. Patent and Trademark Office.
8. Board of Governors of the Federal Reserve System. (2025). *Supervision and regulation report*. Federal Reserve Board.
9. Board of Governors of the Federal Reserve System. (2024). *Cybersecurity report*. Federal Reserve Board.
10. Mane, I. M. (2026). Secure decentralized interbank transfer system using Hyperledger Fabric and AI. IEEE Xplore Author Profile.
11. Identity and access management in banking: Governance automation, privileged access, and zero trust enablement. (2026). *Journal of Information Systems Engineering and Management*, *11*(2s).
12. Bank Policy Institute. (2025). *Federal Reserve payment accounts: A primer*.

13. ABA Banking Journal. (2026, July 15). Banking agencies promise new approach for handling sensitive information.

14. Board of Governors of the Federal Reserve System. (2025). *Testimony of Governor Bowman before the Senate Committee on Banking, Housing, and Urban Affairs*.

15. Federal Reserve Board. (2019). *FedNow commentary*.