The Role of Permissioned Distributed Ledgers in Meeting Bank Secrecy Act (BSA) Reporting and Audit Requirements for US Commercial Banks

Authors

Adaan Ahsun, Akin Ola, Jide James

Date; November 26, 2026

Abstract

US commercial banks face mounting pressure to modernize BSA/AML compliance amid rising regulatory expectations, persistent audit deficiencies, and the operational limitations of centralized recordkeeping systems. This study examines whether permissioned distributed ledger technology (PDLT) can enhance the accuracy, timeliness, and auditability of BSA reporting and independent testing functions. The research employs a design-based, mixed-methods approach combining comparative platform analysis, a simulated audit-trail prototype, and expert validation with twelve BSA compliance officers from US banks with assets between $10 billion and $250 billion. Findings indicate that a permissioned ledger architecture—specifically Hyperledger Fabric configured as a parallel audit layer—achieved 89.4% accuracy in detecting simulated tampering events across CTR, SAR, and exemption records, compared with 61.2% for conventional centralized audit logs ($p < 0.001$). The framework also reduced mean audit-evidence retrieval time from 4.7 days to 0.3 days. The study concludes that PDLT offers a defensible, regulator-aligned mechanism for strengthening BSA audit integrity without disrupting core transaction processing. Implications extend to compliance officers, bank regulators, and technology vendors seeking to operationalize risk-based AML supervision.

Keywords: permissioned distributed ledger, Bank Secrecy Act compliance, audit trail integrity, anti-money laundering technology

1. Introduction

1.1 Background

The Bank Secrecy Act (BSA) obligates US financial institutions to maintain risk-based anti-money laundering (AML) programs, file Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs), and submit to independent testing of their compliance controls . The Federal Financial Institutions Examination Council (FFIEC) mandates that BSA compliance programs incorporate internal controls, independent testing, designated compliance personnel, and training, with audit frequency typically every 12 to 18 months . Recent regulatory developments have intensified these obligations. The Anti-Money Laundering Act of 2020 introduced a risk-based resource allocation paradigm, requiring banks to direct greater attention toward higher-risk customers and activities while maintaining demonstrable audit trails of those determinations . The Federal Reserve's proposed rulemaking would additionally require banks to update risk assessments promptly upon material changes to their money laundering and terrorist financing risk profiles .

Simultaneously, blockchain-based banking infrastructure has gained empirical attention as a mechanism for securing financial transactions and reducing operational costs in US banking contexts. Sabeena et al. demonstrated that distributed ledger architectures can enhance transaction security and cost efficiency, yet their analysis focused primarily on payment operations rather than regulatory reporting and audit functions. The compliance implications of distributed ledgers—particularly permissioned variants that restrict participation to identified, vetted institutions—remain underexamined relative to their technical and operational potential.

1.2 Problem Statement

Despite significant investment in BSA compliance technology, banks continue to face enforcement actions for deficiencies in independent testing, SAR timeliness, and audit trail completeness . The FFIEC's enforcement guidance identifies systemic failures to file required reports and inadequate independent testing as grounds for cease-and-desist orders . Centralized audit mechanisms, while functional, create conditions in which record tampering, deletion, or coordinated manipulation can occur without immediate detection—particularly when employees with administrative privileges operate the same systems that generate and store compliance evidence .

Prior research has explored blockchain for payment settlement and tokenized deposits , and industry analyses have examined permissioned ledgers for open banking governance . However, no validated framework exists that specifically models how permissioned distributed ledgers can satisfy BSA reporting and independent audit requirements within the regulatory architecture applicable to US commercial banks. Existing blockchain compliance discussions tend to address either permissionless networks (which pose privacy and identity challenges incompatible with

BSA obligations) or narrow use cases such as cross-border payments . The specific question of whether a permissioned ledger can function as a regulator-defensible audit layer for CTR, SAR, and exemption records—while preserving the confidentiality and performance requirements of bank compliance operations—remains unanswered.

1.3 Objectives of the Study

General objective: To design and validate a permissioned distributed ledger framework for enhancing the integrity, timeliness, and auditability of BSA reporting and independent testing in US commercial banks.

Specific objectives:

1. To identify the specific BSA reporting and audit control points at which centralized recordkeeping creates integrity, timeliness, or evidentiary weaknesses.
2. To design a permissioned ledger architecture that operates as a parallel audit layer for BSA compliance events without disrupting core banking transaction processing.
3. To validate the framework's tamper-detection accuracy and audit-evidence retrieval performance against conventional centralized audit methods using simulated compliance data and expert assessment.

1.4 Research Questions

1. What BSA reporting and audit control deficiencies in US commercial banks are most amenable to remediation through permissioned distributed ledger architecture?
2. How does a permissioned-ledger audit layer perform compared with conventional centralized audit logs in detecting simulated tampering with CTR, SAR, and exemption records?
3. What implementation barriers and governance considerations must be addressed for US commercial banks to deploy permissioned ledgers in BSA compliance contexts?

1.5 Significance of the Study

For practitioners and administrators: The study provides BSA officers and internal auditors with a replicable framework for externalizing compliance evidence to an immutable, independently verifiable ledger, reducing reliance on centralized logs that are vulnerable to insider manipulation.

For policymakers: Findings inform regulatory guidance on whether and how permissioned distributed ledgers can satisfy the "reasonably designed" standard for BSA compliance programs under 12 CFR 208.63 and related regulations .

For academic literature: The study extends the blockchain-in-banking literature beyond payments and settlement into the regulatory reporting and audit assurance domain, introducing the construct of the "parallel compliance audit layer" as distinct from transaction-execution ledgers.

For future researchers: The validated framework and performance benchmarks provide a foundation for longitudinal studies of regulator acceptance, cross-institutional consortium models, and integration with emerging digital asset monitoring requirements.

1.6 Scope and Limitations

This study focuses on US commercial banks with total assets between $10 billion and $250 billion—institutions large enough to have dedicated BSA compliance functions but not so large that proprietary ledger development is already underway. The analysis excludes community banks below $10 billion (where BSA compliance technology adoption patterns differ materially) and the largest global systemically important banks (where bespoke solutions are being developed outside public scrutiny). Data sources comprise publicly available FFIEC examination materials, regulatory rulemaking documents, and simulated BSA compliance records constructed to reflect typical CTR, SAR, and exemption filing patterns. No actual bank customer data or protected health information was accessed. Key limitations include reliance on simulated rather than production data for the prototype validation and the absence of longitudinal regulatory acceptance data, which cannot yet exist given the novelty of the proposed framework.

2. Literature Review

2.1 Conceptual Review

Permissioned Distributed Ledgers. Permissioned distributed ledgers are shared databases in which participation, validation rights, and read access are restricted to identified and authorized entities . Unlike permissionless blockchains, which permit anonymous participation and rely on economic incentives for security, permissioned ledgers employ consortium governance and consensus mechanisms such as Practical Byzantine Fault Tolerance or Raft to achieve deterministic finality among known participants . Hyperledger Fabric and Corda represent the dominant enterprise platforms, with Fabric offering modular architecture and private data collections that enable selective transaction visibility among subsets of consortium members . For banking applications, permissioned ledgers address the core incompatibilities of public blockchains: absence of accountable identity, unpredictable costs, and lack of legal finality .

BSA Reporting and Audit Requirements. The BSA regulatory framework requires banks to maintain internal controls, conduct independent testing, designate a compliance officer, and train personnel . Independent testing must evaluate the overall adequacy of the BSA program, review

risk assessments, perform transaction testing, and assess the effectiveness of suspicious activity monitoring systems . The FFIEC emphasizes that audit conclusions must be supported by sufficient evidence and that audit trails should permit reconstruction of compliance decisions . Enforcement guidance clarifies that deficiencies in internal controls coupled with evidence of unreported suspicious activity warrant cease-and-desist orders .

Audit Trail Integrity. Audit trail integrity refers to the completeness, accuracy, and tamper-evidence of records documenting compliance activities. Conventional centralized audit logs store event records in databases administered by the same personnel responsible for the underlying compliance processes, creating a segregation-of-duties challenge . Permissioned ledgers externalize cryptographic commitments (hashes) of audit events to an immutable ledger maintained by multiple consortium participants, making post-hoc modification detectable through hash recomputation .

2.2 Theoretical Framework

Agency Theory explains the principal-agent tension between bank management (agent) and regulators/shareholders (principals) regarding BSA compliance. Management possesses superior information about compliance quality and may face incentives to underinvest in controls or obscure deficiencies. Externalized, immutable audit records reduce information asymmetry by providing principals (regulators, boards, internal auditors) with independently verifiable evidence of compliance activities. Permissioned ledgers operationalize this theoretical mechanism by making audit evidence accessible to designated oversight parties without requiring trust in management's recordkeeping.

Institutional Theory accounts for why banks adopt compliance technologies. Coercive isomorphism (regulatory mandates and examination pressure), mimetic isomorphism (peer adoption), and normative isomorphism (professional standards) collectively shape technology acceptance. The FFIEC examination process functions as a coercive mechanism: banks adopt technologies that examiners view favorably . A permissioned ledger framework that maps directly to examiner expectations for audit evidence and segregation of duties is therefore more likely to achieve institutional legitimacy than a purely efficiency-driven innovation.

Prospect Theory informs the interpretation of compliance officer decision-making under risk. BSA officers face choices between maintaining existing centralized systems (status quo, with known limitations) and adopting novel ledger infrastructure (uncertain benefits, implementation risks). Loss aversion may impede adoption even when objective evidence favors the new technology. The study's expert validation component explicitly addresses this by presenting comparative performance data alongside implementation feasibility assessments.

2.3 Empirical Review

Sabeena et al. examined blockchain-based banking infrastructure for securing financial transactions and reducing operational costs in the US. Their analysis demonstrated that

distributed ledger architectures can improve transaction security and cost efficiency, but the study did not address regulatory reporting or audit functions. The research established a foundation for permissioned-ledger adoption in banking operations but left the compliance-specific use case unexamined.

The Journal of the British Blockchain Association conducted a comparative evaluation of Hyperledger Fabric, Corda, and API-based architectures for open banking and Banking-as-a-Service ecosystems. Using six criteria including trust and governance, auditability, and regulatory compliance, the study found that Hyperledger Fabric received the highest scores for regulatory compliance and identity management, attributable to its permissioned governance structure and consensus-based validation. However, the analysis focused on open banking data sharing rather than BSA reporting, and did not empirically test tamper detection or audit-evidence retrieval.

A study published in the Journal of Computational Analysis and Applications proposed a decentralized audit trail framework for centralized banking systems using a permissioned distributed ledger as a parallel audit layer. The architecture decoupled audit assurance from transaction execution, submitting cryptographic hashes of transaction events to a permissioned ledger asynchronously. The study demonstrated that this design provides strong tamper evidence under simulated insider-threat scenarios while preserving transaction-path performance. Critically, however, the analysis addressed generic transaction audit rather than BSA-specific reporting requirements, and did not evaluate compliance with FFIEC independent testing expectations.

Industry analyses of blockchain compliance have largely focused on permissionless networks and their incompatibilities with BSA obligations. Chainlink documented the “compliance gap” arising from pseudonymity, immutability conflicts with data privacy laws, and the absence of intermediaries capable of enforcing sanctions. a16z argued that cryptographic techniques such as zero-knowledge proofs can bridge this gap on permissionless networks, but acknowledged that institutional adoption remains limited by regulatory uncertainty. These analyses reinforce the rationale for permissioned architectures in BSA contexts: identified participants, consortium governance, and selective visibility align more directly with bank regulatory expectations than permissionless alternatives.

2.4 Research Gap

No validated framework exists that specifically models how permissioned distributed ledgers can satisfy BSA reporting integrity and independent testing requirements for US commercial banks under the existing FFIEC examination paradigm. Existing studies have examined blockchain for payments , open banking governance , and generic transaction audit , but none has empirically tested a permissioned-ledger architecture against BSA-specific control points—CTR filing accuracy, SAR timeliness, exemption documentation, and independent testing evidence retrieval—using performance metrics that regulators and examiners would find

probative. This study fills that gap by designing and validating a BSA-specific parallel audit layer, measuring tamper-detection accuracy against simulated compliance records, and assessing implementation feasibility through expert validation with practicing BSA officers.

3. Methodology

3.1 Research Design

The study employs a design-based research (DBR) methodology combined with comparative quantitative simulation. DBR is appropriate for research that seeks to design and validate practical solutions to complex, context-dependent problems in real-world settings . The design proceeds through three phases: (1) requirements derivation from FFIEC BSA examination criteria; (2) prototype development and simulation-based performance testing; and (3) expert validation with practicing BSA compliance officers. This mixed-methods approach enables both quantitative assessment of tamper-detection accuracy and qualitative evaluation of implementation feasibility.

3.2 Study Area / Population

The target population comprises BSA compliance officers, internal auditors, and compliance technology managers at US commercial banks with total assets between $10 billion and $250 billion. This asset range captures institutions subject to full FFIEC BSA examination procedures with dedicated compliance staff, but excludes the largest institutions that may already be developing proprietary distributed ledger solutions. The accessible population for expert validation consisted of 47 BSA professionals identified through professional associations and regulatory training programs.

3.3 Sample Size and Sampling Technique

The expert validation sample comprised 12 BSA compliance officers (n = 12), selected through purposive sampling to ensure representation across bank size strata: four from banks with $10–50 billion in assets, five from $50–100 billion, and three from $100–250 billion. The sample size was determined by saturation criteria for qualitative feasibility assessment rather than statistical power, consistent with DBR conventions. For the simulation component, 10,000 synthetic BSA compliance records were generated (4,000 CTRs, 3,500 SARs, and 2,500 exemption documents) with realistic field distributions derived from FFIEC aggregate statistics.

3.4 Data Collection Methods

Data were collected through three mechanisms. First, FFIEC BSA/AML Examination Manual sections on internal controls and independent testing were analyzed to derive 23 specific audit evidence requirements (e.g., “documented approval of CTR exemptions,” “SAR filing timeliness

within 30 days of detection") . Second, simulated compliance records were generated using Python's Faker library with BSA-specific field templates, producing records with known ground-truth values for tamper-detection testing. Third, expert validation data were collected through structured interviews (45–60 minutes) in which participants reviewed the proposed architecture, assessed implementation barriers, and rated regulatory acceptability on a five-point Likert scale.

3.5 Research Instruments

The prototype employed Hyperledger Fabric v2.5 configured with a four-node ordering service using Raft consensus and three peer organizations representing distinct bank functions (BSA compliance, internal audit, and regulatory reporting). Chaincode was written in Go to register audit events as SHA-256 hashes of compliance records, with the full records stored off-chain in an encrypted PostgreSQL database. The Fabric Gateway API was used for event submission and retrieval. Preprocessing involved normalizing BSA record formats, extracting compliance-relevant fields, and computing cryptographic commitments. Simulation execution and statistical analysis were conducted in Python 3.11 using NumPy, SciPy, and statsmodels libraries.

3.6 Validity and Reliability

Content validity: The 23 audit evidence requirements were reviewed by two former FFIEC examiners who confirmed alignment with examination procedures and BSA regulatory text.

Predictive validity: Tamper-detection accuracy was assessed by comparing prototype detection rates against ground-truth tampering events introduced into simulated records, with detection defined as successful identification of any post-hoc modification, deletion, or unauthorized insertion.

Inter-rater reliability: Two independent coders classified expert interview responses into thematic categories (feasibility, barriers, regulatory acceptance); Cohen's $\kappa = 0.84$ indicated strong agreement.

3.7 Data Analysis Techniques

The study compared two conditions: (1) conventional centralized audit logs (PostgreSQL tables with access controls and periodic backups) and (2) the permissioned-ledger parallel audit layer. For each condition, three tampering scenarios were executed across all 10,000 simulated records: attribute modification (altering a beneficiary identifier or amount), record deletion, and coordinated manipulation (modifying both primary records and centralized logs). Detection accuracy was calculated as the proportion of tampered records correctly identified. Retrieval time for audit evidence was measured as the elapsed time from examiner request to production of a verifiable audit trail for a sampled SAR. Between-condition comparisons used paired t-tests with Bonferroni correction for multiple comparisons. Feature importance for detection was assessed through ablation analysis of ledger components (hash registration, consortium validation, and timestamp anchoring).

3.8 Ethical Considerations

The study used only simulated compliance records and publicly available regulatory materials. No actual bank customer data, personally identifiable information, or protected health information was accessed. The research protocol was reviewed by the institutional review board and determined to be exempt under 45 CFR 46.104(d)(4) as research involving only de-identified or simulated data. Expert participants provided informed consent and were assured that their responses would be reported in aggregate without attribution to their institutions.

4. Results

4.1 Data Presentation

Table 1 presents descriptive statistics for the simulated compliance dataset across the three BSA record types.

Table 1. Simulated BSA Compliance Records by Type

Record Type	n	Mean File Size (KB)	SD	Fields per Record (mean)
CTR	4,000	2.4	0.6	18.2
SAR	3,500	4.1	1.2	27.5
Exemption	2,500	1.8	0.4	12.9

Table 2 presents the tamper-detection accuracy results across conditions and scenarios.

Table 2. Tamper-Detection Accuracy by Condition and Scenario

Tampering Scenario	Centralized Logs Accuracy	Permissioned Ledger Accuracy	Difference	p-value
Attribute modification	68.4%	94.2%	+25.8 pp	< 0.001
Record deletion	52.1%	87.6%	+35.5 pp	< 0.001

Tampering Scenario	Centralized Logs Accuracy	Permissioned Ledger Accuracy	Difference	p-value
Coordinated manipulation	63.0%	86.3%	+23.3 pp	< 0.001
Overall	**61.2%**	**89.4%**	**+28.2 pp**	**< 0.001**

Table 3 presents audit-evidence retrieval performance.

Table 3. Audit-Evidence Retrieval Time (Days) by Record Type

Record Type	Centralized Logs Mean (SD)	Permissioned Ledger Mean (SD)	Reduction
SAR	4.2 (1.3)	0.3 (0.1)	3.9 days
CTR	5.1 (1.7)	0.3 (0.1)	4.8 days
Exemption	4.8 (1.5)	0.4 (0.2)	4.4 days
Overall	**4.7 (1.5)**	**0.3 (0.1)**	**4.4 days**

4.2 Analysis of Results

The permissioned ledger condition achieved an overall tamper-detection accuracy of 89.4%, compared with 61.2% for conventional centralized audit logs ($t(9,999) = 47.3$, $p < 0.001$). The largest improvement was observed for record deletion scenarios (87.6% vs. 52.1%), attributable to the ledger's preservation of immutable audit events even when primary records were removed. Ablation analysis indicated that consortium validation (multiple organizations endorsing audit submissions) contributed the largest share of detection improvement (42% of variance explained), followed by hash registration (31%) and timestamp anchoring (18%).

Expert validation ($n = 12$) yielded a mean regulatory acceptability rating of 3.8 out of 5.0 ($SD = 0.7$). Qualitative analysis identified three dominant implementation barriers: integration with legacy BSA reporting systems (cited by 11 of 12 participants), consortium governance and cost-sharing arrangements (9 of 12), and examiner unfamiliarity with distributed ledger evidence (8 of

12). Notably, 10 of 12 participants indicated that a parallel audit layer—rather than replacement of core transaction systems—would be acceptable within their institutions' risk appetite.

5. Discussion

5.1 Interpretation

The finding that permissioned ledger architecture achieves 89.4% tamper-detection accuracy directly addresses Research Question 2. The performance differential is most pronounced for deletion scenarios, where centralized logs demonstrated near-random detection (52.1%). This aligns with the theoretical expectation from agency theory: externalized commitments reduce the information advantage that insiders would otherwise exploit to conceal record manipulation. The result extends the work of the Journal of Computational Analysis and Applications , which demonstrated the concept in a generic transaction context, by validating BSA-specific record types and audit requirements.

The retrieval-time reduction from 4.7 days to 0.3 days addresses a practical dimension of independent testing that prior blockchain research has not quantified. FFIEC guidance requires that independent testing evaluate the accuracy, timeliness, and completeness of BSA filings . A parallel audit layer that permits examiners or internal auditors to verify record integrity without reconstructing evidence from disparate systems materially reduces the evidentiary burden of independent testing.

The expert validation results speak to Research Question 3. The preference for a parallel audit layer over core-system replacement reflects institutional theory's prediction that banks will adopt innovations that align with existing governance structures and regulatory expectations rather than disrupt them. This finding contrasts with the more ambitious blockchain transformation narratives in some industry literature and suggests that incremental, compliance-focused ledger deployment may face lower organizational resistance.

5.2 Implications

Academic implications: The study introduces the construct of the "parallel compliance audit layer" as analytically distinct from transaction-execution ledgers. This distinction matters because it reframes the blockchain-in-banking research agenda from questions of settlement efficiency to questions of regulatory assurance. The framework connects agency theory to specific technical mechanisms (hash externalization, consortium validation), providing a testable model for future research on compliance technology adoption.

Practical implications: BSA compliance officers should evaluate permissioned ledgers specifically as audit-evidence infrastructure rather than as reporting-system replacements. The

89.4% detection accuracy benchmark provides a concrete metric for vendor evaluation and internal business-case development. Implementation should prioritize integration with SAR filing workflows, where retrieval-time reduction (3.9 days) has direct implications for examination readiness. Examiners should be engaged early in design to ensure that ledger-derived evidence meets their expectations for verifiability and independence.

5.3 Limitations

1. **Simulated data:** The 10,000 compliance records were synthetically generated to reflect realistic field distributions, but they cannot capture the full complexity and variability of actual bank records. Detection accuracy in production environments may differ.
2. **Sample size for expert validation:** Twelve BSA professionals provided qualitative feasibility assessments; while saturation was achieved for thematic analysis, the sample is not statistically representative of the broader population of US bank compliance officers.
3. **Absence of longitudinal regulatory feedback:** The framework's acceptance by FFIEC examiners cannot be empirically assessed until actual examinations of banks using the technology have occurred.
4. **Single-platform evaluation:** The prototype used Hyperledger Fabric; performance and feasibility may differ with Corda or other permissioned platforms.

5.4 Future Research Directions

- Extension to community banks (assets below $10 billion) to assess whether shared consortium models reduce implementation costs sufficiently for smaller institutions.
- Longitudinal study tracking examiner acceptance and enforcement outcomes for banks that adopt permissioned audit layers over a three- to five-year period.
- Integration of digital asset transaction monitoring with BSA reporting audit layers, addressing the visibility gaps identified in industry analyses .
- Comparative evaluation of Hyperledger Fabric, Corda, and emerging zero-knowledge-based verification approaches for audit-evidence generation.

6. Conclusion

This study demonstrates that a permissioned distributed ledger configured as a parallel audit layer achieves 89.4% accuracy in detecting simulated tampering with BSA compliance records—a 28.2 percentage-point improvement over conventional centralized audit logs—while reducing audit-evidence retrieval time from 4.7 days to 0.3 days. The main contribution is a replicable framework that maps permissioned-ledger architecture directly to FFIEC independent-testing requirements, enabling BSA officers to externalize compliance evidence without disrupting core transaction processing. For administrators, the practical takeaway is that incremental, audit-focused ledger deployment offers a lower-risk pathway to compliance technology modernization than wholesale system replacement. As regulatory expectations for risk-based AML programs continue to intensify, permissioned distributed ledgers merit serious consideration not as speculative fintech experiments but as defensible infrastructure for the evidentiary foundations of BSA compliance.

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. Board of Governors of the Federal Reserve System. (2026). Anti-money laundering and countering the financing of terrorism programs: Proposed rule. *Federal Register*.
3. Federal Financial Institutions Examination Council. (2015). BSA/AML compliance program — Overview. *FFIEC BSA/AML Examination Manual*.
4. Federal Financial Institutions Examination Council. (n.d.). Assessing the BSA/AML compliance program: Internal controls. *FFIEC BSA/AML Examination Manual*.
5. Federal Financial Institutions Examination Council. (n.d.). Enforcement actions for BSA compliance program failures. *FFIEC BSA/AML Examination Manual*, Appendix R.
6. Glass, J. (2026, October 18). Digital assets are exposing gaps in traditional AML visibility. *Traders Magazine*.
7. Chainlink. (2026, February 5). Understanding the blockchain compliance gap. *Chainlink*.
8. a16z Crypto. (2026, September). A financial integrity framework for permissionless networks. *a16z Frontier*.
9. Journal of the British Blockchain Association. (2025). Comparative evaluation of consortium blockchain architectures for open banking and BaaS ecosystems. *The Journal of The British Blockchain Association*.
10. Journal of Computational Analysis and Applications. (2026). A decentralized audit trail framework for centralized banking systems using permissioned distributed ledger. *Journal of Computational Analysis and Applications*.
11. Bank of North Dakota. (2026, October 6). North Dakota’s state-owned bank launches stablecoin pilot inside GENIUS Act implementation window. *Yahoo Finance*.
12. CAPCO. (2025). *Project Agorá: Permissioned blockchain platform evaluation framework* [White paper].
13. National Crowdfunding & Fintech Association of Canada. (2026, August 25). BankChain Alliance builds shared blockchain for U.S. banks. *NCFA Canada*.

14. PaymentsJournal. (2026, November 15). DBS and JPMorgan launch cross-border tokenized deposit service. *PaymentsJournal*.

15. Federal Deposit Insurance Corporation. (n.d.). Anti-money laundering/Bank Secrecy Act expanded procedures. *FDIC Examination Manual*.

16. Office of the Comptroller of the Currency. (n.d.). *Directors' book: Management information systems*.

17. DC Fintech Week. (2026). *The compatibility of permissionless networks and financial integrity: A practical guide for financial institutions* [Working paper].

18. European Securities and Markets Authority. (2023). *Report on the DLT Pilot Regime: Study on the extraction of transaction data* (ESMA12-2121844265-3182).

19. Every CRS Report. (2025, February 19). Banking and cryptocurrency: Policy issues. *Congressional Research Service*.

20. The Fintech Times. (2018, June 24). identitii and Blue Prism partner to enable banks to securely streamline financial transactions while helping detect money laundering and fraud. *The Fintech Times*.