Connecting Banking Systems with Blockchain: Comprehensive Challenges and Solutions

Report Preparation and Publication Details

Authors

This report was prepared by Muhammad Yusri Adib Samsudin, who serves as the Founder and Lead Researcher at ADCX Lab. His work centers on integrating financial systems, developing blockchain validation frameworks, and ensuring compliance with ISO 20022 standards across digital asset ecosystems.

Reviewers

Muhammad Mustafa, CPA, CFE, CMA, CIA, Co-Founder and Finance & Compliance Lead at ADCX Lab, reviewed this report. He leveraged his expertise in audit governance, regulatory alignment, and financial compliance to confirm the technical accuracy and reliability of the report's conclusions.

Publisher Information

The report is published by the ADCX Lab Research Division, which is committed to advancing compliant blockchain infrastructure and promoting research on ISO 20022 interoperability. For further details or to discuss potential collaborations, please visit: https://autodigitalcoin.com.

Publication Date and Copyright

Date of Publication: October 2025

Referencing Guidelines

This report may be cited or referenced in academic or industry research, provided that proper attribution is given to ADCX Lab as the original publisher.

ADCX Lab — Bridging banks and blockchains through compliance, auditability, and trust.

Introduction

The integration between traditional banking systems (“TradFi”) and blockchain technology has become a strategic necessity for driving innovation within the financial sector. However, significant technical and legal gaps make collaboration between these two systems highly challenging. Traditional banking systems operate according to industry-standard frameworks, such as SWIFT/ISO 20022 for payment messaging, and adhere to strict compliance requirements including KYC/AML protocols and GAAP/IFRS audit standards. In contrast, blockchain ecosystems offer openness and automation without intermediaries, but still lack comparable compliance infrastructure. An OECD (2022) report highlights that a large portion of DeFi participants operate outside existing regulatory frameworks—including AML/CFT, tax, and sanctions—which poses risks to market integrity. For blockchain technology to achieve its full potential, systematic integration with financial institutions, regulators, and enterprises is essential.

This in-depth, PhD-level report identifies the primary weaknesses in integrating banking systems with blockchain technology across major networks such as Ethereum, Solana, Avalanche, Kadena, XRP Ledger, Hedera, Polkadot, Cardano, Tron, and Arbitrum. The report is structured into the following key sections:

- Technical and Legal Challenges of Bank–Blockchain Integration: Analyzes messaging standards (such as ISO 20022), audit standards (GAAP/IFRS), differences in data structures, privacy and transparency issues, and regulatory compliance requirements.
- Current Infrastructure Shortcomings (RWA, DeFi, Validators, Risk Scores): Assesses ongoing limitations related to real-world asset tokenization (RWA), decentralized finance (DeFi), blockchain validator architectures, and risk scoring mechanisms to meet financial institution needs.
- Proposed Technical Solutions and Strategies: Provides concrete recommendations on architecture, industry standardization, and digital infrastructure development to address integration gaps. This includes concepts such as stateless validators, the use of AI in risk scoring, and data export in ISO XML format.
- Evaluation of ADCX Lab's Role: Assesses whether ADCX Lab’s approach, with components like GuardianX and its innovative technologies, offers a strategic advantage as a potential leading solution for future bank–blockchain integration.

Each section includes the latest statistical highlights (2023–2025) and citations from reputable sources, including financial institutions (IMF, Bank Negara Malaysia), blockchain analytics firms (Chainalysis), market research firms (PitchBook, Gartner), and leading universities (MIT, Oxford).

Technical and Legal Challenges in Bank–Blockchain Integration

The integration between banking infrastructure and blockchain technology faces significant issues of technical incompatibility and regulatory barriers. The following are the main aspects contributing to these integration difficulties:

1. Message and Data Standards (ISO 20022 vs Blockchain Data)

International payment systems are transitioning to ISO 20022, a global financial messaging standard rich in data. By April 2025, nearly 38.5% of SWIFT cross-border transactions will use this standard, with full implementation mandated by SWIFT in 2026. ISO 20022 enables more comprehensive transaction information, such as sender/receiver details and payment purpose, facilitating processing and enhancing fraud detection.

In contrast, blockchain transaction data typically includes only wallet addresses, transaction amounts, and smart contract information, lacking compliance metadata such as customer names or transaction purpose. As ADCX Lab notes, "raw blockchain data is not equivalent to an audit-ready report." Without adaptation processes, banking institutions cannot directly use hashes or addresses for compliance purposes. Major networks like Ethereum, Solana, or Tron are not specifically designed to generate reports in banking formats. Even networks like RippleNet/XRP, which claim ISO 20022 compatibility, require additional processing layers to produce truly compliant messages. This results in a data language gap: banks use "XML ISO 20022," while blockchains use "ledger blocks."

Integration, therefore, requires complex data translation processes. On-chain transactions must be converted into messages such as pacs.008 (credit transfer) or camt.052/053 (account statements). The absence of unified standards forces banks to rely on ad-hoc middleware solutions, which can introduce errors and increase operating costs.

Impact: Without uniform messaging standards, direct integration of blockchains with banking systems is difficult. Collaborative efforts are needed to ensure blockchain transactions can be presented in a format understood by financial institutions. Innovations like ISO 20022 validators are critical: "For successful integration, blockchains must be able to communicate in the ISO 20022 language."

2. Data Structure & Financial Records (Audit, GAAP & IFRS)

The comparison between blockchain ledgers and traditional accounting ledgers presents various challenges. Blockchain operates as a distributed ledger, recording transactions permanently and transparently, while banking institutions use tightly controlled internal ledgers that allow for corrections or adjustments. Accounting standards further complicate this integration: IFRS and US GAAP have yet to provide a specific framework for crypto assets. Currently, companies typically record crypto assets at cost or market value, with any increase in value booked under Other Comprehensive Income (OCI), not profit or loss. The US FASB introduced ASU 2023-08 in December 2023, requiring certain crypto assets to be measured at fair value, with changes reported in net income (P&L), and mandates detailed disclosures in the balance sheet.

The divergence between IFRS and GAAP highlights confusion in the accounting industry regarding blockchain. A firm may report different financial positions depending on the framework used, and the absence of guidance for new transactions like DeFi complicates interpretation. Banks face difficulties auditing and recognizing on-chain transactions consistently—especially when holding stablecoins as reserves, whose status as cash, cash equivalents, or intangible assets remains unclear. These ambiguities heighten audit and compliance risks.

Additionally, the pseudonymous nature of blockchain audit trails complicates traditional auditing processes. Auditors need proof of asset existence and ownership, but on-chain identities are unavailable by default, complicating due diligence and forensic accounting.

3. Privacy, Confidentiality, and Immutability vs Banking Requirements

The traditional banking sector operates within strong client confidentiality frameworks enforced by privacy laws such as BAFIA or GDPR. In contrast, public blockchains are open, allowing all transactions to be publicly observed. This presents a dilemma: how can financial institutions use public networks without exposing sensitive data?

In some jurisdictions, storing personal data on a public ledger is prohibited, and the EU's "right to be forgotten" principle under GDPR is difficult to uphold on blockchain. Although blockchain addresses are pseudonymous, sophisticated de-anonymization and KYC data leaks can tie addresses to real identities, increasing data protection risks.

Traditional banking relies on transaction reversibility, such as chargebacks or error corrections, but blockchain transactions are final once confirmed. This finality, while providing certainty, is less suitable for institutions needing correction mechanisms. Alternatives like escrow smart contracts or transaction insurance are not yet industry norms.

Privacy is also critical for cross-border transactions. For example, Project Guardian in Singapore used Chainlink CCIP with private transactions, encrypting key details to comply with regulations. This demonstrates the need for additional encryption technologies to ensure compliance.

Public blockchains currently lack sufficient privacy features for banking applications. Solutions may involve permissioned chains or advanced cryptographic techniques like zero-knowledge proofs, but large-scale integration will require industry privacy standards, an area still under development.

4. KYC/AML Compliance and Sanctions: The Gap

Financial institutions must comply with KYC, AML, and international sanctions. Bank transactions include sender/receiver identity data, but blockchain transactions typically only involve wallet addresses. This makes it hard for banks to ensure compliance with requirements like the FATF Travel Rule. Without rigorous controls, using blockchain can expose banks to legal violations. Real-time address filtering is needed, but public blockchain infrastructure does not fully support this yet. Analytics firms can assist, but integration with banking systems is still emerging. Most DeFi protocols lack user identity consideration, so institutions prefer licensed platforms that require KYC.

Compliance issues are a key barrier but also create innovation opportunities for developing compliance bridges between banks and blockchain systems.

5. Cross-Blockchain Fragmentation & Interoperability

Many different blockchains, each with their own protocols and formats, complicate banks’ efforts to accept digital assets from multiple networks. Every network requires its own integration, and while cross-chain efforts exist, solutions to connect blockchains to banking systems are still lacking. Banks prefer licensed blockchains for easier control and compliance.

Effective integration requires a system that can connect multiple blockchains to banks uniformly and in compliance with legal requirements.

Current Infrastructure Weaknesses (RWA, DeFi, Validator, Risk Score)

Analysis of RWA, DeFi, validators, and risk scores is key to understanding current integration gaps.

Tokenization of Real-World Assets (RWA)

Tokenizing real-world assets on blockchains is gaining traction due to the potential for 24/7 liquidity and easier institutional access. However, challenges remain:

- Lack of uniform laws and standards; unclear token ownership status.
- Small secondary markets and low liquidity.
- Reliance on third-party oracles introduces manipulation risk.
- No unified reporting standard for RWA tokens, complicating background checks.

The industry believes RWA will grow rapidly once legal, technical, and compliance issues are resolved. Banks require strong assurances before becoming more actively involved.

In summary, integrating blockchain with institutional banking demands innovation in compliance, interoperability, and support, so risks are minimized and benefits maximized.

Weaknesses of DeFi and Permissionless Protocols

DeFi protocols operate without intermediaries, using smart contracts on public blockchains for lending, trading, and more. From the perspective of banks and regulators, DeFi presents several key issues:

- Absence of KYC/AML: DeFi users are typically anonymous, contrary to banking regulations. This increases risks of mingling with unlicensed or sanctioned parties, limiting institutional participation in public pools.
- Smart Contract Risks: DeFi code can contain bugs or vulnerabilities leading to major losses. Regulated institutions cannot assume the risk of coding errors. Third-party audits are helpful but not foolproof, and DeFi insurance remains limited.
- Market Volatility & Uncertainty: DeFi tokens are volatile, and interest rates fluctuate, making it less suitable for institutions unless returns justify increased risk.
- Scalability & Fees: Transaction fees can be unpredictable, and processing can be delayed during peak periods, making DeFi less ideal for large-volume transactions.
- Lack of Clear Governance: DeFi is governed by token holders, not a single entity, complicating support, error correction, and accountability.

In response, institutional-grade DeFi platforms like Aave Arc, Compound Treasury, and JPMorgan Onyx have emerged, offering DeFi features with access restrictions and regulatory compliance. The trend for 2025 points to increased modular DeFi integration by institutions through controlled approaches. While this creates ‘walled gardens’ for institutions, the challenge remains to connect open and institutional DeFi without compromising their respective benefits.

Current Infrastructure for Blockchain Validators

All public blockchain networks rely on validators or nodes for consensus and security. However, from an institutional integration perspective, current validator designs have several shortcomings:

- Storage & Maintenance Requirements: Running a full node requires significant resources. Stateless validation concepts, like ADCX Lab’s storage-less validators, offer lighter compliance nodes that generate compliance reports without full ledger synchronization.
- Lack of Built-in Compliance Functions: Validators typically only check technical validity, not legal compliance. Initiatives like Project Mandala propose embedding compliance into protocol design.
- Decentralization vs. Compliance Risks: Decentralized validators pose trust issues for banks. Closed networks or “sovereign validators” are alternatives but may reduce decentralization. A neutral validator layer acting as a compliance checkpoint is a proposed solution, as pioneered by ADCX Lab.

Weaknesses of Risk Score & Analytics Mechanisms

Banking relies on risk evaluations for customers and transactions, but blockchain risk assessment mechanisms are still maturing. Major challenges include:

- Limited Use of AI/Machine Learning: Most risk analyses rely on static rules, while AI and machine learning could improve anomaly detection. However, applying AI requires extensive, high-quality data and entity tagging.
- No Standard “Compliance Health” Score: There is no industry standard for wallet or DApp compliance scoring, though such initiatives are emerging.
- Siloed and Proprietary Approaches: Risk assessment methodologies are often proprietary, leading to vendor lock-in and transparency issues.
- Data Limitations: Current risk assessments focus on on-chain data, neglecting off-chain context. Integrating digital identity infrastructure is still a challenge.

Without robust risk scoring, banks hesitate to interact with unverified on-chain addresses. ADCX Lab is addressing these gaps by developing AI-based risk scores and stateless validators for privacy protection. However, bridging the gap between financial institution needs and crypto infrastructure requires cross-sector collaboration and industry standard development.

Technical Solution Recommendations and Strategies to Bridge the Gap

Based on identified weaknesses, the following solutions are proposed from system architecture, industry standardization, and digital infrastructure perspectives. The recommended approach is holistic, combining technological advancements with standards and regulatory support.

3.1 Layered Compliance-Oriented Architecture

A key strategy involves constructing a compliance middleware layer between public blockchains and banking systems. This middleware acts as an intelligent firewall, intercepting transaction data for validation and format conversion before forwarding it to bank core systems. Main features include:

- Stateless Validator Layer: Operated by stakeholders (banks, regulators, compliance providers), these open-source, auditable validators evaluate criteria such as address approval, risk score thresholds, and transaction value limits. ADCX Lab has prototypes for networks like XRPL, Hedera, and Kadena, with validators exporting on-chain transactions into banking-compliant formats.
- Data Mapping Engine & Standard Export: Middleware should translate blockchain data into industry standards, such as converting Ethereum transactions into ISO 20022 messages (e.g., pacs.008, camt.052/053, pain.001). This enables banks to import data directly into compliance systems, overcoming interoperability challenges.
- Compliance Smart Contract Implementation: Compliance logic can be embedded directly into smart contracts, such as programming RWA tokens to only transfer between KYC-verified wallets. A hybrid approach, combining smart contracts and external validators, is also possible.
- Permissioned Subnet Framework: Some blockchains enable subnets or sidechains tailored for compliance, allowing institutions to control nodes and legal aspects at the protocol level. The optimal strategy likely integrates both private and public models, maintaining compliance through validator layers.

This layered, compliance-focused design aligns with BIS recommendations on "compliance-by-design architecture," ensuring policy requirements are built into foundational protocols. Successful implementation requires collaboration among blockchain developers, banks, and regulators on automated rule sets and data standards, potentially forming the basis for a future "Internet of Finance."

3.2 Integration of Industry Standards: ISO 20022, IVMS101, and Others

Technical solutions should be grounded in industry standards for interoperability. Key actions include:

- Broad ISO 20022 Implementation: Promote ISO 20022 support within blockchain applications. Standard tools should allow generation of ISO outputs as needed, enabling banks to record crypto transactions using familiar formats. Collaboration with ISO bodies is encouraged.
- Identity Standard & Travel Rule (IVMS101): IVMS101 enables sharing of sender/receiver information per FATF Travel Rule. In bank–blockchain integration, it can be used by validators to request KYC data for certain transactions, harmonizing identity data exchange.
- Digital Accounting Standards for Crypto Assets: The accounting sector must establish clear guidance for digital assets, possibly adopting fair value treatment and triple-entry accounting frameworks. Collaboration between IASB and FASB is crucial, along with proposals for crypto-accounting frameworks combining blockchain and AI.
- Taxonomy and Risk Data Labeling: On-chain entities should be labeled using standards like LEI, enabling automated whitelisting and risk assessment. Integration of decentralized identity standards is also beneficial.
- Interoperability Standards for Permissioned/Public Networks: Secure bridging protocols are required for banks using both permissioned and public networks. Industry standards should address data governance, encryption, and transaction integrity.
- Automated Compliance & Joint RegTech: Regulators should establish standards for digital asset reporting, encouraging industry development of compliant tools and frameworks such as the OECD’s Crypto Asset Reporting Framework (CARF).

In summary, harmonizing standards is essential for scalable solutions. The financial industry’s willingness to adopt ISO 20022 demonstrates the importance of standardized frameworks, and collaboration between TradFi standards organizations and blockchain consortia must be institutionalized.

3.3 Digital Infrastructure: Identity, AI, and Advanced Cryptography

Strengthening digital infrastructure is critical to successful integration:

- Integration of Digital Identity: Linking real-world identity with on-chain identity in a privacy-preserving way is optimal for KYC/AML. Verifiable Credentials (VCs) or Soulbound tokens can serve as digital “passports” for wallet addresses, with mechanisms like Zero-Knowledge Proofs (ZKP) protecting privacy.
- Artificial Intelligence for Surveillance & Risk Assessment: AI and machine learning can enhance fraud detection and risk assessment, both off-chain (analyzing historical data) and in real time. ADCX Lab plans AI-assisted risk scoring, with transparency and explainability prioritized for compliance officers.
- Privacy-Preserving Cryptography: Technologies like zk-SNARKs and secure multi-party computation (MPC) allow compliance proofs without revealing sensitive data, enabling secure transaction monitoring and regulatory compliance.
- Collaborative Neural Networks: Banks can use federated learning to jointly train AI models without sharing raw data, managed by trusted parties for privacy and security.
- Cloud Infrastructure and Open APIs: Open APIs and cloud-ready compliance validators enable easy integration and scalability. ADCX Lab plans to offer public API endpoints and SDKs, supporting concepts like Banking-as-a-Service and Compliance-as-a-Service.

These solutions must align with institutional strategy at the industry, national, and institutional levels, encouraging collaborative pilot projects, regulatory sandboxes, and readiness plans for digital asset integration.

Strategic Assessment of ADCX Lab as a Bridge Solution

Following the discussion of general issues and solutions, the report assesses ADCX Lab—a Web3 security and compliance innovation lab—as a strategic bridge for bank–blockchain integration. ADCX Lab's development of the Stateless ISO 20022 Validator and cross-chain compliance framework, including GuardianX, HGuard, ProetorX, and CryptoGuard, positions it as a potential leader in this space.

4.1 Advantages of the ADCX Lab Approach

- Compliance Validator Focus: ADCX Lab does not compete as a payment network, but rather acts as a compliance layer, validating blockchain data and exporting it into existing formats. This collaborative stance facilitates institutional acceptance.
- Multi-Chain Interoperability: ADCX Lab prototypes support a range of ecosystems—XRPL, Hedera, Kadena, Ethereum, and more—demonstrating horizontal viability. Its open-source model encourages community auditing and integration.
- End-to-End Functionality: ADCX Lab offers wallet validation, AI-based risk scoring, and ISO XML export, delivering audit-ready reports and streamlining institutional integration.
- Stateless & Non-Custodial Design: Validators do not store user assets or data, reducing risk and liability. The stateless design allows for easy scalability and regulatory alignment.
- AI Integration and Strategic Planning: Plans for AI risk scoring and developer SDKs highlight ADCX's commitment to innovation and automation, enhancing operational efficiency.
- Early Ecosystem Recognition: Grants from Hedera, Kadena, and RippleX, as well as active industry engagement, demonstrate broad acknowledgment of ADCX Lab's compliance layer vision.
- Timely Market Alignment: ADCX Lab's roadmap aligns with industry trends—such as the mainstreaming of crypto assets, RWA tokenization, and the SWIFT ISO 20022 mandate—giving it a first-mover advantage.

4.2 Challenges and Recommendations to Strengthen ADCX Lab

- Banking System Integration: ADCX Lab should partner with core banking system providers to streamline integration and reduce barriers for banks.
- Regulatory Recognition: Pilot projects and certifications from regulators can boost confidence and position ADCX as the preferred solution.
- Scalability and Availability: Enterprise-level service standards and partnerships with cloud providers are recommended for reliability and performance.
- Competitive Landscape: Building a broad user network and developer community will help ADCX Lab maintain its competitive edge.
- Business Model: A robust model could include tiered services, premium SaaS offerings, and monetized AI modules.
- Security and Trust: Emphasizing cybersecurity, regular audits, and transparent reporting will enhance user trust and distinguish ADCX Lab from competitors.

In summary, ADCX Lab demonstrates a clear vision and advanced technology for bridging banking systems and blockchain. With first-mover advantages and a compliance-focused approach, ADCX Lab is well positioned to become a critical infrastructure component in the digital financial sector—provided it addresses challenges related to technical development, stakeholder engagement, and enterprise-level operations.

Conclusion and Recommendations

Integrating traditional banking systems and blockchain is increasingly essential for financial institutions to remain competitive. Key barriers include data standard incompatibility, accounting ambiguities, privacy and finality issues, and the lack of on-chain compliance infrastructure. The current limitations of RWA and DeFi systems further underscore the need for trust bridges to integrate real-world assets and bank capital into the blockchain ecosystem.

Current trends indicate that the TradFi–blockchain gap must be addressed promptly, with asset tokenization emerging as a primary focus. The value of on-chain real-world assets is expected to rise to trillions of USD in the coming decade, and major institutions are already exploring tokenization and regulated DeFi. Regulatory bodies like IMF-FSB and BIS are introducing new crypto policies and demonstrating the feasibility of cross-border compliance automation.

Strategic and technical recommendations include:

- Building a compliance validator layer to filter blockchain transactions before entering banking systems.
- Expanding the use of ISO 20022 and cross-platform KYC standards (IVMS101).
- Integrating cryptography-based digital identity for harmonized privacy and compliance.
- Leveraging AI and smart analytics for proactive risk detection.
- Encouraging close collaboration among banks, crypto firms, standards bodies, technology companies, and regulators.
- Shifting institutional attitudes to view blockchain as a legitimate, regulated element of the modern financial ecosystem.

Based on detailed analysis, ADCX Lab stands out as a uniquely positioned connector between TradFi and DeFi, offering dedicated compliance and data solutions. Through innovative approaches aligned with industry transitions for 2024–2026, ADCX Lab has the potential to become a leading compliance Web3 infrastructure provider, much as SWIFT unified global financial communications in the 20th century. ADCX or similar solutions could become the “SWIFT of the blockchain era,” complementing existing frameworks by linking digital assets to traditional financial systems.

Concrete Recommendations

- For the Financial Industry & Regulators: Explore compliance-layer technologies like ADCX Lab. Launch joint pilot projects (e.g., CBDC collaborating with ADCX Lab on ISO 20022 automated reporting) and support open standards development.
- For ADCX Lab & Similar Innovators: Refine technologies for reliability and integration. Obtain relevant certifications and conduct independent security audits. Communicate benefits through case studies demonstrating real-world impact.
- For Educational Institutions & Research Community: Undertake research on AI-based on-chain risk estimation, compliance automation, and cost-benefit analysis of blockchain integration. Collaborate with industry to assess economic impacts and strengthen the business case for solutions like ADCX.

In conclusion, efforts to connect banking systems and blockchain are progressing. The current weaknesses and gaps should be seen as temporary challenges, not permanent obstacles. By combining the strengths of both ecosystems and managing risks prudently, the financial landscape can evolve to be more inclusive, efficient, and transparent, while maintaining stability and trust. The timely emergence of ADCX Lab and similar initiatives will accelerate the integration of TradFi and DeFi—a shared objective for the future.

References

- Adib, Yusri (2025). Blockchain Is Broken Without Compliance: Why ADCX Lab Is Building the Stateless ISO 20022 Validator. Medium.
- ADCX Lab (2025). Stateless ISO 20022 Validator Layer – Bridging Blockchain Transactions into Bank Compliance Systems. Gitcoin Forum.
- Howell, James (2025). What ISO 20022 Means for Blockchain and Payments? 101 Blockchains.
- Reuters (2024). Illicit crypto addresses received at least $24.2 billion in 2023 – report.
- OECD (2022). Institutionalisation of Crypto-assets and DeFi–TradFi Interconnectedness.
- Cointelegraph (2025). DeFi lending rises 72% on institutional interest, RWA collateral adoption.
- AInvest (2025). The Institutional RWA Revolution: Unlocking Trillions in DeFi.
- Ledger Insights (2024). Project Guardian: ADDX, ANZ, Chainlink test cross border commercial paper tokenization.
- BIS (2024). Project Mandala: shaping the future of cross-border payments compliance.
- HLB Global (2025). Accounting for crypto assets under IFRS vs FASB.
- PitchBook via Coinspeaker (2024). Web3 VC Funding Totaled $1.9B in Q4 2023.