Mitigating Smart Contract Risk in Clearing and Settlement

Laura Kouadio - January 31st, 2026

Tokenization is at the forefront of project development pipelines for the largest banks, evidenced by J.P. Morgan's JPM Coin launch and Citi's partnership with SDX. As the financial industry moves toward "atomic settlement," the reliance on smart contracts to enable tokenization introduces a new layer of operational and model risk. this article explores how institutional-grade governance can safeguard the next generation of DLT-based market infrastructure.

Smart contracts: The risks of a shift to using code as policy

A smart contract is a self-executing computer program or transaction protocol hosted on a blockchain. It automatically performs, controls, or documents relevant events and actions according to the terms of an agreement. They allow the issuance, transfer, and redemption of tokenized assets, ensuring the digital "token" accurately reflects the underlying value and legal rights of the physical or financial asset. Smart contracts are increasingly viewed as "digital plumbing", the foundational infrastructure for automated financial services but their usage comes with critical risks:

The Logic Flaw (Model Risk / Deterministic Risk): The smart contract code can be written with a logic flaw and generate unintended bugs. If the code has a flaw, the failure is automatic, instantaneous, and potentially systemic. (e.g., calculating interest incorrectly). In the current state of art, majority of smart contracts aren't audited. This generates an important model risk for frozen logic.

The Blockchain Reversibility issue (Operational Risk and Technology Risk): By design, blockchain technology is immutable. Any mistake in the sender or receiver address, or a vulnerability in the contract code, can result in permanent loss. (e.g., "If issuer send $10M to the wrong address or get hacked").

Oracle Reliance (Data Risk): Smart contract require access to real-time external data to fulfil code obligations (e.g., "If the S&P 500 hits 4,000, pay the dividend"). If the data feed (Oracle) is hacked or glitched, the contract executes incorrectly putting the institutions at risk.

Legal Enforceability Gap (Compliance Risk): Smart contract can generate a **conflict of authority if the execution of the contract results in the** violation of the law or of a superior paper contract. (e.g., A bankruptcy court freezes assets, but the smart contract automatically liquidates them anyway).

The Protocol Bridge (The interoperability Risk): institutions bridge assets because no single blockchain offers everything, they need to move value to access different benefit as Blockchains cannot speak to each other. The intent of bridging is to acknowledging data from a blockchain to another one. As of 2026, this processus is the one that caused the highest loss in decentralized finance. An example of bridging would be JPMorgan issuing a "Tokenized Bond" on its own private, secure blockchain (Onyx) to comply with regulations. However, the buyers (hedge funds) are holding their stablecoins on a public blockchain (Ethereum). To sell the bond, JPMorgan will bridge the asset (or the ownership rights) from their private fortress to the public market where the liquidity is.

Bridging the Gap: Designing Decentralized ledger Technology (DLT) Specific Controls and Applying Traditional SDLC to DLT

To mitigates the risks enounced, the DTCC, backbone of United States financial market, enacted specific solutions based on their Digital Asset Securities Control Principles (DASCP) and Security of DLT Networks whitepapers.

Firstly, the DTCC is planning to enforce standards where smart contracts must have "administrative backdoors" (controlled by governance) to pause, upgrade, or terminate a contract if a bug is found. For instance, if a "Tokenized Bond" smart contract has a coding error that prevents it from paying a coupon, the DTCC would use its governance key to pause trading and deploy a patched contract, ensuring the market doesn't freeze.

To manage irreversibility risk, the DTCC is building the Compliance Aware Token Framework. This embeds logic inside the token that checks "Is this receiver allowed to hold this asset?" before moving. More importantly, they manage the "Clawback" function: The DTCC will retain the right to "burn" stolen tokens and "mint" replacements for the rightful owner, effectively reversing the transaction on the ledger.

Moreover, The DTCC plans to be the **ultimate vetted Oracle**. Instead of relying on a third-party crypto oracle (like a random node), the smart contract will be hardcoded to only accept pricing/corporate action data signed by the DTCC’s private key.

The institution is also creating a framework where every smart contract is legally mapped to a traditional paper contract. The code is merely the *execution arm* of a legal agreement, not the agreement itself.

Finally, in order to properly monitor interoperability risk, the DTCC is actively testing **Chainlink's CCIP (Cross-Chain Interoperability Protocol)** to create a standard "messaging layer" that connects private bank chains securely. They manage the risk by validating the *message* between chains rather than just moving the token blindly.

These DLT focused risks would need to be covered by controls.

In my experience, leading the migration of over 200 high-risk models and tools to SDLC platforms at Morgan Stanley, the primary lesson was that technical security is inseparable from governance. For smart contracts to be "clearinghouse-ready," they must undergo a rigorous lifecycle:

Pre-Deployment Validation: Much like the 235 models I governed, smart contracts require independent data validation and control testing to ensure the logic aligns with internal risk policies.

Immutable Audits: Every update to a settlement contract must be treated as a "major version" change, requiring full audit traceability—a standard I enforced to ensure data security and technology control standards.

Level 1 Control Automation: By building automated risk reporting dashboards (using tools like Python and Power BI), firms can monitor contract execution in real-time, detecting anomalies before they impact the broader ledger.

The successful integration of tokenized assets depends on our ability to wrap innovative technology in the "safety and soundness" frameworks that have protected capital markets for decades. By leveraging existing expertise in **model risk and tool governance**, we can ensure that the move to blockchain is a move toward a more resilient, rather than more volatile, financial future.

Laura Kouadio