When Banks Deploy Smart Contracts, Who Governs the Code?

Code-Level Governance for Institutional Programmable Finance: A Policy and Infrastructure Analysis

Olivier Laurette

Senior Executive, Dedge Security

First published in MAC's Payments and Cash Management Directory (macsdirectory.com)

March 2026

Executive Summary

Programmable finance is restructuring the operational foundations of institutional banking. As banks, central securities depositories, and financial market infrastructure operators deploy smart contracts for tokenized deposits, stablecoin settlement, and programmable payment flows, they are embedding executable logic into systems that have historically been governed through committees, manual checkpoints, and periodic audits.

This transition introduces a structural governance gap. The smart contract that governs the issuance, transfer, and redemption of a tokenized deposit is, in operational terms, the policy of that financial product expressed as code. Yet the governance frameworks applied to these contracts remain largely static: a point-in-time security audit before deployment, followed by limited structured oversight during operation.

The pattern is not new. When enterprises migrated from on-premises infrastructure to cloud computing, a comparable governance gap emerged and was closed through the discipline of Security Posture Management. Cloud Security Posture Management (CSPM) and Application Security Posture Management (ASPM) became standard enterprise infrastructure. The same structural logic now applies to programmable finance, where Web3 Security Posture Management (W3SPM) addresses the continuous governance requirements of smart contract lifecycles.

Regulatory frameworks across the European Union, Switzerland, and the United States are converging on the expectation that institutions deploying blockchain-based financial products must demonstrate continuous operational governance over the code that powers them. MiCA, DORA, FINMA's evolving DLT supervisory regime, the GENIUS Act, and the European Central Bank's acceptance of DLT-issued collateral all reinforce this direction.

This report examines the governance gap in institutional programmable finance, analyses where controls must move, draws on the cloud governance parallel, surveys the regulatory convergence, and outlines what institutional control must become as financial logic shifts from process to code.

Key Findings

The deployment of smart contracts within institutional financial infrastructure introduces a governance surface that existing frameworks do not adequately address. Where operational policies have historically been expressed through human-interpretable procedures subject to periodic review, programmable finance embeds equivalent logic in code that executes autonomously once deployed.

Current institutional governance remains predominantly process-oriented, structured around committees, manual checkpoints, and point-in-time assurance. These controls do not provide continuous oversight of executable financial logic, its dependencies, or the evolving risk environment in which deployed contracts operate.

Institutions deploying blockchain-based financial products will require a continuous governance capability across the full smart contract lifecycle, from development through deployment through operation, comparable to the posture management disciplines that emerged when enterprise computing infrastructure became programmable.

Analytical Context

The adoption of smart contracts by banks, central securities depositories, and payment infrastructure operators reflects a broader transition in which financial systems are incorporating programmable components into their operational architecture. This transition parallels earlier shifts in enterprise computing, where the move from static to programmable infrastructure required corresponding changes in governance, risk management, and supervisory oversight.

In programmable finance, operational logic that was previously expressed through institutional procedures, committee decisions, and manual controls is increasingly encoded in software that executes autonomously on distributed ledger networks. Once deployed, this code determines the behavior of financial products and processes without further human intervention at the point of execution.

This creates a governance surface that sits below traditional process controls and above the infrastructure layer: executable financial logic that must be subject to continuous institutional oversight across its full lifecycle. The analytical question for institutions and regulators is how existing governance architectures should extend to accommodate this new layer.

1. The Structural Shift: From Process Governance to Code Governance and Continuous Monitoring

For most of the history of institutional banking, governance has been built around processes. Approvals flow through committees. Controls are applied at operational checkpoints. Risk is assessed through frameworks designed for human decision-making, paper trails, and periodic audits. This architecture has served institutions well, and for good reason: the processes being governed were themselves manual, sequential, and interpretable.

Programmable finance changes the underlying assumption.

When a bank issues a tokenized deposit, deploys a stablecoin, or integrates a smart contract into its settlement infrastructure, it is not simply adopting a new technology. It is embedding executable logic into the operational layer of its business. The contract does not wait for an approval committee. It executes. Automatically, immutably, and on the terms encoded at the time of deployment.

This shift introduces a governance question that existing frameworks were not designed to answer: if financial logic is now expressed as code, who governs the code itself?

2. The Governance Gap in Programmable Finance

The institutional conversation around blockchain has matured considerably. Treasury and payments professionals no longer debate whether distributed ledger technology has a role in banking.

Regulatory frameworks are now operational on both sides of the Atlantic: MiCA in Europe, the GENIUS Act in the United States, FINMA's evolving DLT regime in Switzerland, and DORA's operational resilience requirements across the EU financial sector. Select institutions have moved into live products and market-infrastructure integrations, while broader adoption remains early.

The Bank for International Settlements, in its G20 report on tokenisation, defines the shift precisely: tokenisation generates digital representations of assets on a programmable platform, one with an execution environment that can run smart contracts to update a common ledger, and realising its benefits "will require sound governance and risk management." A white paper by J.P. Morgan and the MIT Digital Currency Initiative on programmability in commercial banking reinforces the point: the application of programmable logic to payments and settlement is no longer experimental, it is operational.

> *Yet as the adoption conversation has advanced, the governance conversation has not kept pace.*

Most institutions approach blockchain security through the same lens they use for any technology deployment: custody solutions protect assets, transaction monitoring detects anomalies, AML frameworks screen for illicit activity. These are necessary controls. But they operate around the blockchain, not within the logic that powers it.

Consider what happens when a bank deploys a tokenized deposit. A smart contract is written, tested, and deployed to a blockchain network. Once deployed, this contract governs the issuance, transfer, and redemption of that deposit. It defines who can hold the token, under what conditions transfers are permitted, and how governance decisions such as pausing or upgrading the contract are executed.

The contract is, in a very real sense, **the operational policy of that financial product**, expressed in code rather than in a policy document.

This is not a distant scenario. J.P. Morgan's Kinexys platform has processed over $1.5 trillion in notional value since inception, and in May 2025 completed a cross-chain delivery-versus-payment test settling tokenized U.S. Treasuries against USD deposits across permissioned and public blockchain environments. In January 2026, Lloyds Banking Group completed what it described as the UK's first public blockchain transaction using tokenized deposits, including the first gilt purchase settled through tokenized deposits on the Canton Network.

Deutsche Börse Group signed an agreement with Société Générale-FORGE to integrate its MiCA-compliant stablecoins as payment and settlement instruments within Clearstream infrastructure. A joint report by Bain & Company and Kinexys documents how tokenization platforms represent investor portfolios as smart contracts containing both records of ownership and the programmable rules for updating those records.

The governance question is no longer hypothetical. The code is already in production.

In traditional banking, operational policies are subject to continuous governance: they are reviewed, updated, tested against evolving risk environments, and audited regularly. The smart contract that performs an equivalent function typically receives a point-in-time security audit before deployment, and then very little structured governance thereafter. If the contract is immutable, there is no opportunity to patch it. If it is upgradeable, the upgrade mechanism itself becomes a critical governance surface that few institutions have formalized processes to manage.

The scale of the exposure is already visible. Across the broader Web3 ecosystem, over $3.3 billion was lost in security incidents in 2025, an increase of 37 percent year over year, according to CertiK. The structural pattern is consistent: most exploits occur not at the point of initial deployment, but in the operational window between reviews, when code is live and active governance is absent. These are not failures of intent. They are failures of governance architecture.

This is the governance gap. It is not a technology gap. It is a gap in the institutional control architecture that has not yet adapted to the reality that financial logic is now programmable.

Exhibit 1: Governance Evolution in Financial Infrastructure

Traditional Finance Governance	Programmable Finance Governance
• Policy committees and approval chains	• Smart contracts as operational policy
• Manual process checkpoints	• Automated, immutable execution
• Periodic compliance audits	• Code lifecycle management
• Human-interpretable procedures	• Machine-executable business logic
• Static risk assessment frameworks	• Continuous posture monitoring

Note: The transition from process-based to code-based governance does not eliminate the need for institutional oversight. It changes the object of that oversight from human procedures to executable logic and the infrastructure surrounding it.

3. Where Controls Must Move

In a traditional banking environment, controls sit around processes. Segregation of duties ensures no single individual can authorize a transaction end-to-end. Compliance reviews occur before product launches. Internal audit examines whether processes were followed according to documented procedures.

In a programmable environment, the equivalent controls need to sit inside the executable logic itself, and in the lifecycle management of that logic from development through deployment through operation. This is a structural shift, not an incremental one.

It requires institutions to govern three dimensions that they have not historically managed as a unified discipline.

3.1 Pre-Deployment Assurance

Before a smart contract goes live, the institution needs confidence not only that the code is free from technical vulnerabilities, but that the business logic encoded in the contract accurately reflects the intended operational policy. A reentrancy vulnerability is a code defect. A token transfer rule that does not enforce the intended compliance constraints is a governance failure. Both must be caught before deployment, because in many blockchain architectures, there is no second chance.

3.2 Deployment Integrity

The process of moving code from a development environment to a live blockchain involves wallet interactions, signing workflows, and in many cases multi-signature governance structures. Each step introduces risk. A misconfigured deployment script or a compromised signing key can result in a contract that behaves differently from what was tested, or that is controlled by the wrong parties. Institutions accustomed to change management processes for traditional software deployments need equivalent, and arguably more rigorous, processes for on-chain deployment.

3.3 Continuous Posture

Once deployed, the smart contract and its surrounding infrastructure exist in an environment that evolves independently of the institution. New vulnerabilities are discovered in the programming languages and frameworks used to build the contract. The blockchain network itself may undergo protocol changes. Third-party dependencies, such as oracles or bridge contracts, introduce risks that were not present at the time of the original security assessment.

Without continuous monitoring of the security posture of deployed contracts and their dependencies, institutions operate with a snapshot of assurance that degrades over time. Continuous posture in this context means continuous assessment, inventory, and risk visibility across the contract lifecycle, not transaction monitoring or payment security.

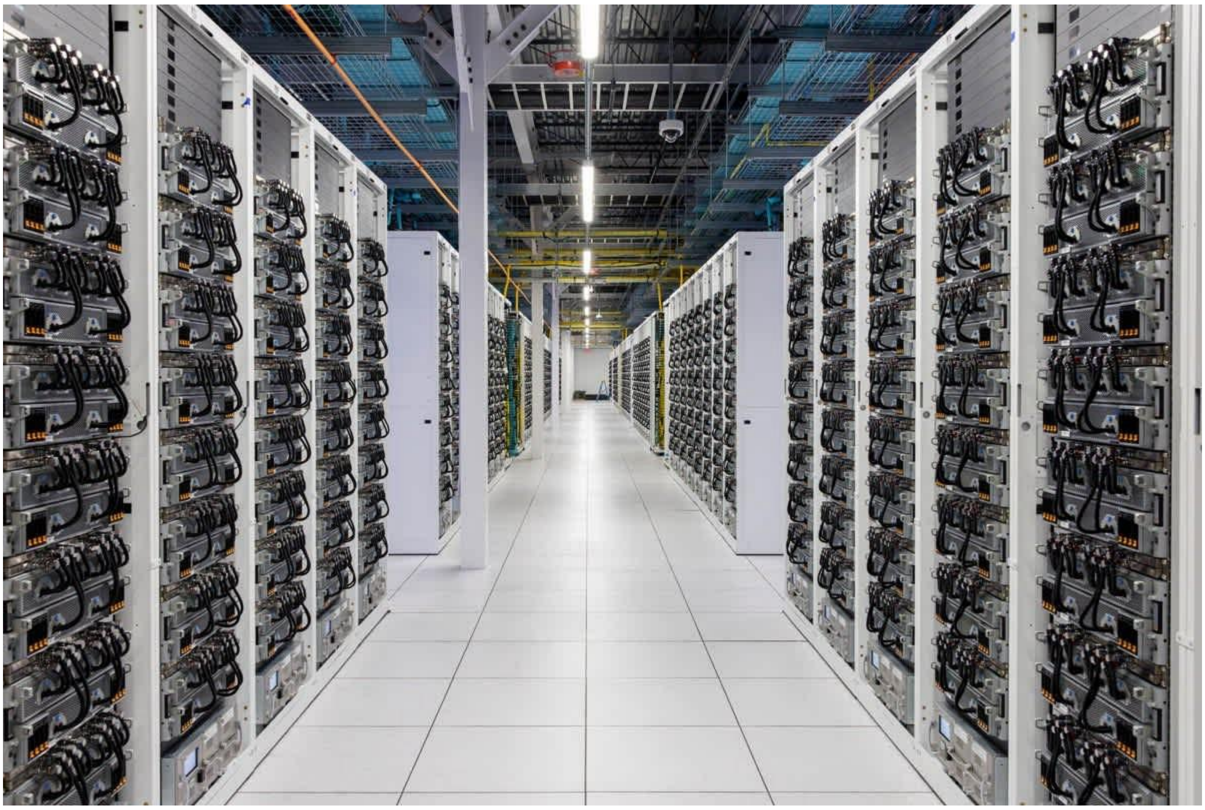
Security posture management adapted to smart contract infrastructure is emerging as one operational framework through which institutions can maintain continuous governance and control over programmable financial systems, extending established posture management disciplines into a new infrastructure layer.

Exhibit 2: Smart Contract Lifecycle Governance

Development → **Deployment** → **Operations**

Development	Deployment	Operations
• Code review and testing	• Key management	• Continuous monitoring
• Business logic validation	• Signing governance	• Dependency risk tracking
• Security audit	• Multi-signature controls	• Protocol change assessment
• Vulnerability assessment	• Deployment integrity checks	• Posture management
• Standards compliance	• Configuration verification	• Evidence and reporting

Note: Each phase represents a distinct governance surface. Institutional control must span all three phases as a unified discipline, not as isolated checkpoints. The operational phase, where most governance gaps currently exist, requires continuous rather than periodic oversight.



4. The Cloud Governance Parallel

This challenge is not without precedent. When enterprises migrated from on-premises infrastructure to cloud computing, they encountered an analogous governance gap. Traditional security models assumed a perimeter: assets were inside the network, threats were outside, and controls sat at the boundary. Cloud computing dissolved that perimeter. Infrastructure became programmable, dynamic, and distributed across providers.

The institutional response was the emergence of Security Posture Management as a discipline. Cloud Security Posture Management (CSPM) provided continuous visibility into cloud configurations, detecting misconfigurations and compliance drift before they became incidents. Application Security Posture Management (ASPM) extended this into the software development lifecycle, integrating security assessment into CI/CD pipelines so that vulnerabilities were identified during development rather than after deployment.

These disciplines are now standard practice across enterprise security. Industry analysts and major cybersecurity providers classify posture management as essential infrastructure, and chief information security officers increasingly operate with a posture-first mindset. The question is no longer whether to implement posture management for cloud environments, but how comprehensively.

The parallel to Web3 is direct. The emergence of Web3 Security Posture Management (W3SPM) as a governance discipline reflects the same structural logic that produced CSPM and ASPM: when infrastructure becomes programmable, institutions require continuous visibility into the security and configuration state of that infrastructure.

Blockchain introduces programmability into financial infrastructure in the same way cloud introduced programmability into computing infrastructure. When infrastructure becomes programmable, governance must move closer to the code. The existing posture management frameworks, built for SaaS, cloud-native applications, and traditional data environments, do not cover the Web3 layer: smart contracts, cross-chain logic, validator infrastructure, decentralized storage, and blockchain-specific deployment patterns.

The institutional need is the same: continuous, automated visibility into the security and governance posture of programmable systems, integrated into the development and deployment lifecycle rather than applied as a periodic checkpoint after the fact.

Exhibit 3: Infrastructure Transition Pattern

	Legacy Model		Programmable Infrastructure		Governance Response
Technology Precedent	On-Premises Infrastructure	→	Cloud Infrastructure	→	**CSPM / ASPM**
Financial Infrastructure	Traditional Banking Systems	→	Programmable Finance	→	**Web3 Security Posture Management**

Note: The vertical alignment of the two rows illustrates the structural parallel. In both cases, when infrastructure becomes programmable, governance must shift from periodic review to continuous posture management. The arrows represent qualitative transitions in infrastructure complexity, not a timeline.

5. The Regulatory Dimension: A Transatlantic Convergence

This governance gap is not merely a matter of best practice. Regulators across major financial jurisdictions are converging, from different directions and at different speeds, on the same structural expectation: institutions deploying blockchain-based financial products must demonstrate continuous operational governance over the technology that powers them.

5.1 MiCA (European Union)

MiCA, the EU's Markets in Crypto-Assets regulation, is now fully operational: its stablecoin titles (covering asset-referenced tokens and e-money tokens) applied from 30 June 2024, with the broader regime applicable from 30 December 2024. MiCA establishes requirements for token issuers that include operational resilience, governance arrangements, and risk management.

While MiCA does not prescribe specific technical controls for smart contracts, it creates an environment in which regulators will increasingly ask: what assurance do you have that the code governing your digital asset products is secure, correctly implemented, and continuously monitored?

5.2 DORA (European Union)

DORA, the Digital Operational Resilience Act, applicable from 17 January 2025, is more explicit. It requires financial entities to implement continuous monitoring and testing of their ICT systems, including third-party dependencies. For institutions whose ICT systems now include smart contracts deployed on public or permissioned blockchains, the DORA requirements imply a level of continuous governance that point-in-time audits cannot satisfy.

5.3 FINMA (Switzerland)

In Switzerland, FINMA has moved further than most regulators in connecting code-level assurance to supervisory expectations. Its DLT trading facility framework, operationalized in 2025 with the licensing of BX Digital AG, requires operators using public blockchain settlement infrastructure to contain operational risks through technical checks including, in FINMA's own phrasing, "checking the source code used by smart contracts."

FINMA's 2024 guidance on stablecoins, its 2026 guidance on custody of crypto-based assets, and the proposed new licensing categories for payment instrument institutions and crypto-institutions all point in the same direction: code-level governance is becoming a regulatory surface, not merely a technical best practice.

5.4 GENIUS Act (United States)

In the United States, the GENIUS Act, signed into law on 18 July 2025, establishes the first comprehensive federal framework for payment stablecoins. It requires issuers to meet licensing, reserve, and operational standards under the oversight of the OCC, FDIC, or state regulators. The OCC's 2026 proposed rulemaking makes this operational dimension concrete: prospective stablecoin issuers must demonstrate governance structures, technology infrastructure, and risk controls as part of their application.

When the code underlying a payment stablecoin is itself the operational infrastructure, the governance of that code becomes inseparable from the licensing requirement.

5.5 ECB Collateral Signal

A further structural signal: in January 2026, the European Central Bank announced that the Eurosystem will accept marketable assets issued in central securities depositories using DLT-based services as eligible collateral for Eurosystem credit operations, effective 30 March 2026, with exploration of expansion to assets issued and settled entirely on DLT networks. Once DLT-issued assets connect to central bank operations, governance expectations around operational resilience and control evidence rise accordingly.

5.6 Practical Implications

The practical implication for treasury and payments professionals is significant. Across the EU, Switzerland, and the United States, the regulatory direction is consistent: institutions that can demonstrate continuous security posture across their blockchain deployments will be better positioned for regulatory examinations, auditor inquiries, and the kind of enterprise risk reporting that boards increasingly expect.

Institutions relying solely on a pre-deployment audit conducted months ago will find it increasingly difficult to demonstrate the ongoing operational resilience that regulators on both sides of the Atlantic now require. Posture management tools can support compliance by generating evidence and traceability, but they do not replace governance decisions, legal interpretation, or supervisory dialogue.

6. What Institutional Control Must Become

The path forward is not to abandon the governance principles that have served institutional banking. It is to extend them into a new execution environment.

This means treating smart contracts with the same lifecycle governance that institutions apply to any critical operational system: continuous assessment, change management, dependency monitoring, and documented assurance that can withstand regulatory scrutiny. It means embedding security posture management into the development and deployment pipelines for blockchain-based products, so that governance is proactive rather than retrospective.

Emerging operational frameworks designed for Web3-specific infrastructure are beginning to operationalize this approach, extending posture management disciplines to smart contract systems, deployment workflows, and cross-chain dependencies.

And it means building internal capabilities, or selecting partners, that understand the specific risk characteristics of programmable finance: the immutability constraint, the composability risk of interconnected contracts, and the unique attack surfaces that Web3 introduces.

When institutions like J.P. Morgan, Lloyds Banking Group, Société Générale-FORGE, and Deutsche Börse are building production-grade smart contract infrastructure, the partners and service providers supporting that infrastructure must meet the same standard of continuous governance. This is distinct from custody, transaction monitoring, or payment security. Code-level posture management occupies its own governance layer, one that complements but does not replace the controls institutions already operate.

For CISOs and compliance leaders, this represents an expansion of scope rather than a departure from existing practice. The discipline of security posture management is proven. The question is whether institutions will extend it to cover the programmable finance layer before the governance gap creates consequences, or after.

For treasury and payments professionals, the implication is equally clear. As tokenized deposits, stablecoin integrations, and smart contract-based settlement become operational components of cash management and payments infrastructure, the security and governance of the underlying code is no longer someone else's problem. It is a direct input to operational risk, regulatory compliance, and fiduciary responsibility.

As financial products increasingly operate through executable smart contract systems, institutions are no longer only governing processes and organizations, but the financial logic embedded directly within their infrastructure.

Exhibit 4: Governance Layers in Programmable Finance

Board and Risk Governance	Strategic oversight, risk appetite, regulatory accountability
Operational Processes	Compliance reviews, change management, audit, reporting
Technology Infrastructure	Networks, cloud, databases, APIs, identity management
Executable Financial Logic (Smart Contracts)	Tokenized deposits, programmable settlement, automated compliance, on-chain governance

▲ *New governance surface introduced by programmable finance*

Note: Traditional institutional governance addresses the upper three layers. Programmable finance introduces a fourth layer at the base of the stack: executable financial logic embedded in smart contracts. This layer requires its own governance discipline because the code, once deployed, operates autonomously within the infrastructure and directly determines the behavior of financial products.

> *The institutions that move early to formalize code-level governance for their blockchain deployments will not simply be better governed. They will be better positioned to scale. Because in every infrastructure transition where systems became programmable, the institutions that governed the new layer first were the ones that scaled fastest. Programmable finance is unlikely to be different.*

About the Author

Olivier Laurette is a Senior Executive at Dedge Security, where he works on the security and governance challenges associated with smart contract infrastructure in institutional financial environments. His work focuses on the intersection of digital assets, regulatory frameworks, and operational risk management for blockchain-based financial systems and the institutional adoption of programmable financial infrastructure.

He previously advised more than 40 organizations across Europe on crypto compliance, market integrity, licensing processes, and institutional digital asset operating models, supporting regulated financial actors as they integrated emerging blockchain technologies into existing governance and risk frameworks.

He is an active member of INATBA, the Crypto Valley Association, and Letzblock.

linkedin.com/in/olivier-laurette
dedgesecurity.com

Institutional and Regulatory Sources

BIS G20 Tokenisation Report

Governance thesis anchor: "will require sound governance and risk management"

Full report: https://www.bis.org/cpmi/publ/d225.pdf
Landing page: https://www.bis.org/cpmi/publ/d225.htm
Press release: https://www.bis.org/press/p241021.htm

FINMA: BX Digital DLT Trading Facility

Source code checking reference, March 2025

Press release: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/

Lloyds Banking Group: Tokenised Deposits

UK's first public blockchain transaction, January 2026

Press release: https://www.lloydsbankinggroup.com/assets/pdfs/media/press-releases/2026-press-releases/lloyds/07.01.2026-lloyds-tokenisation.pdf

Deutsche Börse / SG-FORGE: CoinVertible Integration

MiCA-compliant stablecoin settlement, November 2025

Deutsche Börse press release: https://www.deutsche-boerse.com/dbg-en/media/news-stories/press-releases/Deutsche-B-rse-Group-Partners-with-Leading-European-Stablecoin-Issuer-Societe-Generale-FORGE-4804012
SG-FORGE announcement: https://www.sgforge.com/deutsche-borse-group-partners-with-sg-forge/

J.P. Morgan Kinexys: Cross-Chain DvP Test

Tokenized U.S. Treasuries, May 2025

Newsroom: https://www.jpmorgan.com/payments/newsroom/kinexys-chainlink-ondo-tokenized-asset-test

ECB: DLT Collateral Acceptance

Eurosystem collateral from 30 March 2026

Press release:
https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260127_1~a946167ce1.en.html

— End of Report —