

Annex 3.1. Price Discovery in Tokenized Equities

1.1. Data Construction

The event-study framework uses firm-day observations for 5 traditional equities and their tokenized equivalents. The study uses data on 5-min windows from Bloomberg for traditional stocks and Allium for tokenized stocks, filtering for centralized exchanges due to better coverage. For each tokenized-traditional equity pair i and trading day d , construct the following prices:

$$p_{i,d,c-1}^E = \log(\text{traditional equity close on day } d - 1),$$

$$p_{i,d,c-1}^T = \log(\text{tokenized equity close on day } d - 1),$$

$$p_{i,d,-1}^T = \log(\text{tokenized equity price immediately before the open on day } d),$$

and

$$p_{i,d,h}^E = \log(\text{traditional equity price } h \text{ minutes after the open on day } d),$$

where $h \in \{0,5\}$.

Define the pre-open tokenized signal:

$$S_{i,d}^T = p_{i,d,-1}^T - p_{i,d,c-1}^T.$$

Define the traditional equity cumulative opening return:

$$R_{i,d}^E(h) = p_{i,d,h}^E - p_{i,d,c-1}^E.$$

The core prediction is that $R_{i,d}^E(h)$ should increase with $S_{i,d}^T$.

1.2. Main Regression

Estimate the following panel regression for each horizon h :

$$R_{i,d}^E(h) = \alpha_i + \tau_d + \beta_h S_{i,d}^T + \varepsilon_{i,d,h}.$$

Here, α_i are pair fixed effects, τ_d are date fixed effects. The coefficient of interest is β_h .

The null and alternative hypotheses are:

$$H_0: \beta_h = 0,$$

$$H_A: \beta_h > 0.$$

A stronger one-for-one incorporation hypothesis is:

$$H_0: \beta_5 = 1.$$

A result such as $\beta_5 = 0.80$ would imply that 80 percent of the overnight tokenized signal is reflected in the traditional equity price within five minutes of the regular market open.

Annex 3.2. A Framework for Assessing Financial Stability Risks from Tokenization

This annex presents the analytical framework underlying the tokenization risk matrix and explains how the matrix was developed. The framework maps the key features of tokenized financial markets to a range of financial stability risks they may directly generate or amplify.

The framework is organized around two dimensions. The first dimension consists of structural features and design choices that characterize tokenized financial markets. The structural features are organized around five broad layers. The first layer comprises the core technological features of tokenization, including distributed ledgers, programmability, composability, and atomic settlement. These are foundational characteristics that can affect financial assets throughout their lifecycle (Patel and others, forthcoming). The remaining layers reflect design choices across the full lifecycle of a tokenized asset, from issuance and trading to settlement, clearing, and cross-cycle financial functions such as collateral management.

The second dimension consists of a set of financial stability risk categories. The framework distinguishes between two broad categories of financial stability risks. The first comprises traditional financial vulnerabilities that have long been central to financial stability analysis, including liquidity stress and fire sales, contagion and interconnectedness, and leverage and procyclical deleveraging. The second comprises operational, governance, market-structure, and infrastructure risks associated with the technological and institutional arrangements that underpin tokenized markets. These risk categories were selected to capture both the familiar vulnerabilities that continue to characterize financial systems and the technology-related risks that feature prominently in the tokenization literature. While these risks are not new, tokenization can alter their relative importance and the mechanisms through which they materialize and propagate, making both sets of risks relevant for the assessment. Table 3.2.1 provides a more refined description of risks.

Annex Table 3.2.1. Description of Financial Stability Risks Used for the Risk Matrix

FINANCIAL STABILITY RISK LEGEND		
Code	Risk Name	Description
Liquidity	Liquidity, Runs, and Fire Sales Risk	Risk that investors rapidly redeem, withdraw, or sell assets, triggering liquidity strains, forced asset sales, price dislocations, and adverse feedback loops. Includes stablecoin runs, redemption pressures, liquidity mismatches, fire sales of reserve assets, and liquidity spirals. It also includes liquidity risk from fragmented structures.
Interconnectedness	Interconnectedness & Contagion Risk	Risk that shocks propagate across institutions, markets, infrastructures, or networks. Includes TradFi–ToFi linkages, cross-market spillovers, collateral linkages, counterparty exposures, interconnected protocols, and contagion through composability and common asset holdings.
Leverage	Leverage & Procyclical Deleveraging Risk	Risk that leverage amplifies shocks and leads to forced deleveraging. Includes collateral reuse, rehypothecation, margin calls, liquidations, collateral valuation shocks, collateral velocity, and leverage embedded in protocol interactions.
Operational	Operational, Technology & Governance Risk	Risk arising from failures of technology, operational processes, or governance arrangements. Includes smart-contract vulnerabilities, coding errors, cyber incidents, oracle failures, operational outages, governance failures, fraud, and human or process failures.
Infrastructure	Infrastructure & Market Risk	Risk arising from the organization and functioning of tokenized markets and infrastructures. Includes network fragmentation, interoperability failures, concentration in validators, custodians, cloud providers, oracle providers or tokenization platforms, settlement bottlenecks, and dependencies on critical market infrastructures.

A key feature of the framework is that it separates where risks originate from how they spread. For each feature, the framework distinguishes between primary channels through which risks are generated directly (solid circles in Table 3.2.2) and secondary channels through which existing risks are amplified or transmitted across markets and infrastructures (hollow circles in Table 3.2.2). The matrix deliberately focuses on the most direct and economically significant channels, so as to keep the matrix interpretable and its results tangible.

To provide a more balanced assessment, the framework was extended to incorporate mitigating mechanisms associated with the same features and design choices. These mitigating mechanisms (triangles in Table 3.2.2) capture ways in which tokenization may reduce specific risks. Consistent with the treatment of risks, each feature was linked to a single primary mitigation channel to preserve the interpretability of the framework and avoid overstating benefits.

The assignment of the linkages between features and risks relied primarily on staff judgment informed by an extensive literature review, outreach discussions, and analysis of tokenization use cases. Generative artificial intelligence tools were used as a research support and validation mechanism to challenge preliminary classifications, identify alternative interpretations, and test internal consistency across features. Final classifications were determined by staff and do not represent an automated output.

Annex Table 3.2.2 presents the full analytical framework used to develop the assessment. In addition to identifying direct and amplification risk channels as well as risk mitigants, the table provides a qualitative rationale describing the economic mechanism linking each feature to the relevant risk categories.

To facilitate presentation, the framework was reorganized around three dimensions: risk creation, risk amplification, and risk mitigation. Rather than mapping each tokenization feature directly to specific risk categories, the streamlined version retains the same tokenization features but groups their effects according to whether they directly generate risks, amplify existing vulnerabilities, or mitigate risk exposures. This approach highlights that a single feature can affect financial stability through multiple channels, creating trade-offs that depend on market design and implementation choices. The streamlined version is reported in the chapter (Table 3.1). The same rationale holds for each code.

Annex Table 3.2.2. Distribution of Risks in Tokenized Markets, Extended

Code	Features	Definition / Attribute	Risk Categories				Rationale	
			Traditional		Technology			
Core Features			Liquidity Risk, Runs & Fire Sales	Interconnectedness & Contagion Risk	Leverage & Procyclical	Operational, Technology &	Market Structure & Infrastructure Risk	
C1	DLT-based recordkeeping and transfer	Ownership and transfers are recorded on a shared distributed ledger rather than through traditional centralized registries.				○ ▲	●	DLT record-keeping produces high dependence on a shared market infrastructure and validator/network architecture. Outages or protocol failures can amplify operational risk. However, it can reduce operational risk by providing a shared and synchronized record of ownership and transactions, thus lowering reconciliation risk.
C2	Programmability	Rules governing issuance, transfer, settlement, collateral use, and corporate actions can be embedded and automatically executed.		○	○	● ▲		Automated code execution can create coding, governance, or execution failures, generating operational risk, while automated triggers can amplify contagion and deleveraging . However, well-designed smart contracts can reduce operational risk by reducing processing errors and legal ambiguity.
C3	Composability	Assets and applications can interact programmatically with other protocols, allowing assets to be combined, reused, or embedded in broader financial transactions.		●	○	○ ▲		Protocol linkages create direct contagion channels, and can amplify leverage , collateral reuse, and operational dependencies. However, it can reduce operational risk by lowering coordination frictions across applications and platforms.
C4	Atomicity	Linked transactions can be executed simultaneously, eliminating principal risk by ensuring that all legs settle together or not at all.	○	▲		●		Coordinated execution creates technology and settlement-execution dependencies, generating operational risk. It can amplify liquidity pressures by reducing timing flexibility in stressed conditions. However, near-instant settlement can reduce contagion risk by lowering counterparty exposures.
Issuance Design			Attribute					
I1	Nature of claim	Direct claim on underlying asset	●	○ ▲				Direct exposure to underlying asset liquidity and valuation can trigger redemption runs and fire sales . Contagion may arise through common asset holdings and market-wide price effects. A direct claim can reduce contagion risk by removing intermediary contagion channels.
		Claim on issuer-intermediary	○	●				Intermediated claims create dependency on the intermediary (issuing entity), creating direct contagion channels. Loss of confidence in the intermediary may trigger redemption runs .
I2	On/Off-chain dependence	Relies on off-chain assets or processes		●		○	▲	Off-chain links can transmit shocks between tokenized and traditional financial markets, increasing contagion risk. It may also introduce operational dependencies related to reconciliation, verification, custody, or legal enforceability. It can, however, reduce infrastructure dependence on the DLT architecture.
		Fully on-chain				○ ▲	●	On-chain processes concentrate dependencies on the underlying DLT network, validator mechanism, and governance framework, making market functioning increasingly reliant on the resilience of the underlying infrastructure . Failures in these arrangements can disrupt transaction processing and settlement, amplifying operational disruptions. However, a fully on-chain asset lifecycle can also reduce operational risk by eliminating reconciliation, verification, and coordination processes across on-chain and off-chain systems
I3	Access model	Permissionless				●	○ ▲	Open participation can heighten cyber, governance, and operational vulnerabilities, and amplify infrastructure coordination risks. At the same time, decentralized validation can reduce infrastructure concentration and single-point-of-failure risk.
		Permissioned	○	▲			●	Restricted access concentrates critical control of infrastructure and market functions in a limited set of participants. Segmentation across permissioned networks can fragment liquidity and impede its efficient redistribution during periods of stress. Restricted access may, however, reduce contagion risk by limiting participation and network connectivity.
I4	Governance structure	Decentralized governance				●	○	Distributed decision-making can complicate coordination and accountability, increasing governance and operational risk, with coordination risks for infrastructure .
		Centralized governance				○ ▲	●	Centralized governance creates infrastructure and service-provider concentration risk, with governance failures as a secondary risk channel. Clear accountability and rapid incident response can reduce operational risk by shortening remediation times.
I5	Oracle dependence	Yes		○		●		External data-feed failures or manipulation can create operational risk by disrupting valuation, execution, or settlement processes and can transmit shocks across linked protocols, increasing contagion risk.

Table continues...

Trading Structure		Attribute						
T1	Trading venue concentration	Single dominant venue	▲	○			●	Venue concentration creates single points of failure in trading infrastructure , and can amplify contagion across users and markets. Concentrated liquidity provision may, however, reduce liquidity risk by supporting market depth and price discovery.
		Multiple venues	○	●			▲	Trading across multiple venues increases operational complexity by requiring coordination across execution, settlement, and liquidity pools. Fragmentation can impair market depth and price discovery, amplifying liquidity risk and fire-sale dynamics. Multiple venues, however, can reduce infrastructure risk by limiting dependence on a single trading venue.
T2	Interoperability	Interoperable networks	▲	●			○	Cross-network links create direct contagion channels, while bridge or interoperability dependencies can amplify infrastructure risk. Interoperability can reduce liquidity risk by lowering frictions in asset transfers and collateral mobility.
		Siloed network	○	▲			●	Network silos fragment liquidity and settlement infrastructure , potentially amplifying liquidity strains. However, reduced connectivity can limit the transmission of shocks and lower contagion risk.
T3	Trading hours	Continuous (24/7)	○ ▲		○			Continuous trading can accelerate runs, margin calls, and liquidations, amplifying liquidity and deleveraging pressures. Continuous market access can reduce liquidity risk by allowing participants to access funding, rebalance positions, and respond to shocks as they occur.
T4	Investor access	Institutional only						No direct risk channel; risks arise through institutional investor specific features such as leverage or interconnectedness.
		Retail accessible	○	○				Retail access can amplify liquidity risk through run dynamics and increase contagion risk through common exposures, platform linkages, and synchronized investor behavior.
Settlement and Clearing		Attribute						
S1	Settlement finality	On-chain finality		○		○ ▲		Immediate finality can increase contagion risk through greater interconnectedness and interdependence as participants rely on immediate and irrevocable settlement. Reliance on DLT finality mechanisms can also amplify operational risk. At the same time, DLT-based settlement can reduce operational risk by lowering reconciliation needs.
		Reliance on legal or off-chain finality		▲		●		Legal or off-chain finality creates direct operational and legal uncertainty through reconciliation and enforceability gaps. However, established legal and CSD frameworks can reduce contagion risk through well-tested default-management and loss-allocation arrangements.
S2	Clearing structure	Bilateral clearing/settlement	○	●			▲	Direct bilateral exposures increase counterparty credit risks and create interconnectedness and contagion channels. Lower netting efficiency can increase liquidity needs. Reduced reliance on a central clearing entity can lower infrastructure concentration risk.
		Central clearing (or CCP-like model)	○ ▲				●	Central clearing concentrates clearing, netting, and risk-management functions in critical market infrastructure . By replacing bilateral credit exposures with margin and collateral requirements, central clearing may generate significant liquidity demands, particularly during periods of stress. However, multilateral netting and centralized risk management can reduce liquidity risk by lowering gross funding and collateral needs and limiting the propagation of bilateral defaults.
Financial Functions (cross-cutting)		Definition						
F1	Collateral mobility and reuse in tokenized finance	Tokenization enables collateral to move and be redeployed more easily across platforms, transactions, and financial applications.	▲	○	●			Tokenization can increase collateral portability, velocity, and reuse across platforms, supporting greater leverage and more complex collateral chains. Cross-platform collateral linkages can transmit shocks across markets and participants, increasing contagion risk. Higher collateral mobility can reduce liquidity risk in normal times by improving the availability and allocation of collateral across markets and counterparties.
F2	Programmable collateral and margining	Collateral management, margining, haircuts, and liquidation processes can be governed and automatically executed through programmable rules.	○ ▲		●			Programmable collateral and margining can automate margin calls and liquidations, increasing procyclical deleveraging risk. During stress, forced collateral sales or withdrawals may amplify liquidity pressures and fire-sale dynamics. Automated collateral management can reduce liquidity risk by improving collateral allocation and mobilization across counterparties and transactions, increasing collateral efficiency and reducing funding needs associated with fragmented collateral pools.

Notes: The table maps tokenization features and market-design choices to financial stability risks. ● indicates a primary (direct) risk-generating channel, where the feature can directly create or intensify a specific risk. ○ indicates a secondary (amplification) channel, where the feature can amplify or accelerate the transmission of an existing risk. ▲ indicates a mitigating channel, where the feature may reduce, absorb, or offset a specific risk. Features may affect multiple risk categories simultaneously through direct, amplification, and mitigating channels.

Annex 3.3. Examples of Specific Operational and Infrastructure Risks Related to Asset Tokenization

Annex Table 3.3.1. Definitions of Operational and Infrastructure Risk Categories

This table clarifies notions in the definition of operational and infrastructure risk categories as used in the matrix.

	Risk Category	Description
Operational and Cyber Risks	Smart-Contract Failure	Coding Bugs, logic failures, exploits, upgrade errors (many smart contracts can be modified through governance processes), admin-key misuse. For example, a tokenized real estate contract allows investors to trade tokens after a property sale, resulting in confusion over who is entitled to sale proceeds. Coding bugs can freeze or destroy assets instantly.
	Oracle Manipulation	The risk that the external data feeding a smart contract is deliberately altered, corrupted, or spoofed, causing the smart contract to execute incorrect actions. It can entail: i) price feed manipulation; ii) data source corruption; iii) oracle operator attack; iv) timing manipulation. Oracle manipulation risk is essentially valuation manipulation risk translated into code. Because smart contracts automatically act on oracle data, an incorrect or manipulated valuation can immediately affect trading, lending, collateral management, and investor payouts across the entire tokenized ecosystem.
	Bridge / Interoperability Failure	The risk that the infrastructure connecting different blockchains, tokenization platforms, or settlement systems fails, causing assets, cash, or information to become stuck, lost, duplicated, or transactions unable to settle. An example is asset lock-up risk when assets become inaccessible during transfer. If the bridge incorrectly records ownership—the same asset now appears to exist twice and can lead to disputes, overstatement of collateral, etc.
Infrastructure Risks	Recordkeeping Fragmentation	On-chain vs off-chain ledgers diverge, and ownership, transaction, and asset information becomes scattered across multiple blockchains, tokenization platforms, custodians, registrars, and traditional databases, making it difficult to establish a single, authoritative record of ownership and activity.
	Cryptographic risk related to keys, wallets	Owners lose access to, or unauthorized parties gain control over, the cryptographic credentials that establish ownership of tokenized assets. Unlike traditional securities, where ownership can often be restored through a broker or registrar, loss or theft of cryptographic keys may result in immediate and potentially irreversible loss of control over the asset. Assets continue to exist, but the investor may be unable to prove or exercise ownership rights.
	Cryptographic risk related to quantum computing	Risk that advances in computing, particularly quantum computing, could break the cryptographic algorithms that protect tokenized assets, wallets, digital signatures, and blockchain networks (see Wu 2005).