the ValueExchange

AMCC Crypto Crisis Workshop

Under the leadership of

CIRO · OCRI

Canadian Investment Regulatory Organization

Organisme canadien de réglementation des investissements

IOSCO

Contents

1. Executive Summary

On Friday October 10th, 2025, IOSCO hosted a workshop in London gathering securities regulators from around the world alongside global digital asset industry leaders. The objective and sentiment was clear – to **understand the threat that digital assets pose as a present-tense risk to global securities markets, and to consider the best means available for securities regulators to coordinate and manage this risk.**

With cryptocurrency growth climbing over 172% year on year and with USD 4.22 trillion in issued value[i], the question for regulators and industry leaders has fundamentally shifted from *if* a crisis will occur to *how* we manage the instability already inside our ecosystem. Following the FTX 'crypto Lehman moment' in 2022 (where over USD 8 billion of customer funds disappeared), the six hundred stablecoin de-pegging incidents logged in 2023 are not merely a warning sign. They are active failures demonstrating systemic vulnerability today.

In the face of these risks, core questions now arise for securities markets around the world. Does each market have asset safety rules and settlement finality that are applicable for digital assets? Do the regulatory and legal frameworks exist to recover digital assets and to ensure investors retain access and rights to their assets in the event of another crypto-exchange or custodian failure? How are markets ensuring equivalence across multiple regulatory units around the world? The pace and growth of digital assets means that these questions must have answers.

Understanding that the digital asset risk management dialogue must evolve immediately, IOSCO's workshop was timely and showed the unity between the industry and regulators to get this right. Participants recognized that there will be more questions than answers but observed the following key points:

In the face of growing holdings of offshore-issued digital assets, global coordination is not optional; it is the only viable path to stability.

Lessons from Lehman, Silicon Valley Bank, and from the 2022 fund crises stand out as highly relevant precedents for understanding digital asset risk, providing clear precedent on questions of asset segregation, custody risk and liquidity risk.

Actors in traditional finance (TradFi), decentralised finance (DeFi) and regulators all need to acknowledge the current risk and seek to partner with the regulators – no one constituency has the answers.

Regulators must move beyond jurisdictional constraints to build a cohesive global perimeter.

Most importantly there was a sense to seize the opportunity. As holdings of digital assets grow rapidly, the benefits that they are delivering to individuals and organisations around the world are evolving fast. As today's markets reinvent themselves, digital assets provide a rare opportunity to set a high, unified bar for supervision, policy alignment, and information sharing, ensuring the shared challenges of this technology are met with a shared, robust defence.

2. Digital assets today:
Why is this already material?

Crypto assets are very much now part of our eco-system and the digital asset landscape is no longer a future theme we should be watching out for. With over 7% of the world's population holding digital assets today, the sector has surpassed a significant threshold for materiality.

This leads to a fundamental question - how are digital assets treated in your market? What exactly do we define as digital assets and who in your markets are holding and transacting in them today?

This section provides some core context and background to these important points.

a. 7% of the world's population is already holding crypto-assets

Three types of digital assets were discussed – all are material and growing exponentially in value and investor reach.

Depth of digital asset markets

Cryptocurrencies	Stablecoins	Tokenised securities
+172% YoY (2023/2024)	+22% YoY (2023/2024)	+80% YoY (2024/2025)
$4.22T in issued value (o/w Bitcoin is 56%)		
562 million holders	**$291B** in issuance	
6.8% of global population	**192M** holders	**$33.07B** in issuance
18,000+ coins in issuance	**$8.9T** turnover	**413,439** holders
$245B in custody by Coinbase Institutional	**22%** annual growth rate (to 2024)	**$8.4B** in US Treasuries

I. Cryptocurrencies

Characteristics

Decentralized, not issued, or controlled by any central authority, government or regulator. Most use a public blockchain that records every transaction. Advanced encryption techniques are used to secure transactions and control the creation of new units.

Scale

Today, 7% of the world's population is holding a digital asset. With over USD 4 trillion in crypto-asset holdings today, all questions of materiality are already in the distant past – particularly given that holdings are growing by 172% year-on-year (2023/2024). Whilst there are over 18,000 cryptocurrency coins in issuance today, 50% of holdings are in Bitcoin, and over USD 245 billion of these assets are held in custody by Coinbase Institutional.

Risks

It is not uncommon for a cryptocurrency's price to swing 10-20% or more in a single day, or to lose over 90% of its value in a bear market. Recent examples (such as FTX) have highlighted the credit risks that cryptocurrency exchanges can create for investors, adding to network risks from 'forks' and other events.

II. Stablecoins

Characteristics

Designed to have a stable value, a stablecoin is "pegged" (or tied) to the value of a specific, stable asset. The entire purpose of a stablecoin is to offer the benefits of a cryptocurrency (fast, global, 24/7 transactions) without the extreme price risk. There are 3 types of stablecoins:

Fiat-collateralized

Most common (e.g. Circle USDC or Tether USDT) they are 100% backed by a 1-to-1 peg with a fiat currency and high quality, liquid assets (e.g. USD fiat cash or US Treasury bills).

Crypto-collateralized

Decentralized, backed by a "vault" of other cryptocurrencies (like Ethereum) in a smart contract. These coins are often over-collateralized to protect against volatility.

Algorithmic

The most complex and riskiest, with no collateral backing. These coins maintain their peg using only algorithms and smart contracts and hence imply significant credit risk.

Scale

With USD 291 billion issued and held by 192 million people, stablecoins also demonstrate significant scale. Stablecoins facilitate USD 8.9 trillion in market turnover today (which is greater than the total US repo market at USD 7 trillion) – although over 90% of this turnover is as the funding or cash leg for Defi transactions. Growing by a fifth each year (2023/2024), stablecoins are gaining widespread acceptance, with leading coins such as USDC starting to enter the institutional arena.

Risks

As with cryptocurrencies, material failures have occurred with stablecoins – most notably with TerraUSD (UST), which collapsed in 2022 when its algorithm failed, wiping out over USD 40 billion. As stablecoin holdings have grown, so have market efforts to regulate stablecoins across leading global jurisdictions.

III. Tokenized Securities

Characteristics

Merging traditional finance and blockchain technology, a tokenized security is a digital representation of a traditional financial asset that is issued and managed on a blockchain. It is a digital title of ownership that is subject to all the same laws as the traditional asset. If you own the token, you have a legal claim on the underlying security.

Scale

A much smaller asset class today, USD 33 billion have been issued and held by 413 thousand (largely institutional) investors. However, tokenized securities are growing fast by over 80% (2024/2025), driven by leading use cases in tokenised bonds (as collateral by Broadridge DLR or JPMorgan's Kinexys, for example), funds (e.g. Blackrock's BUIDL) and equities (e.g. by RobinHood or TradeRepublic).

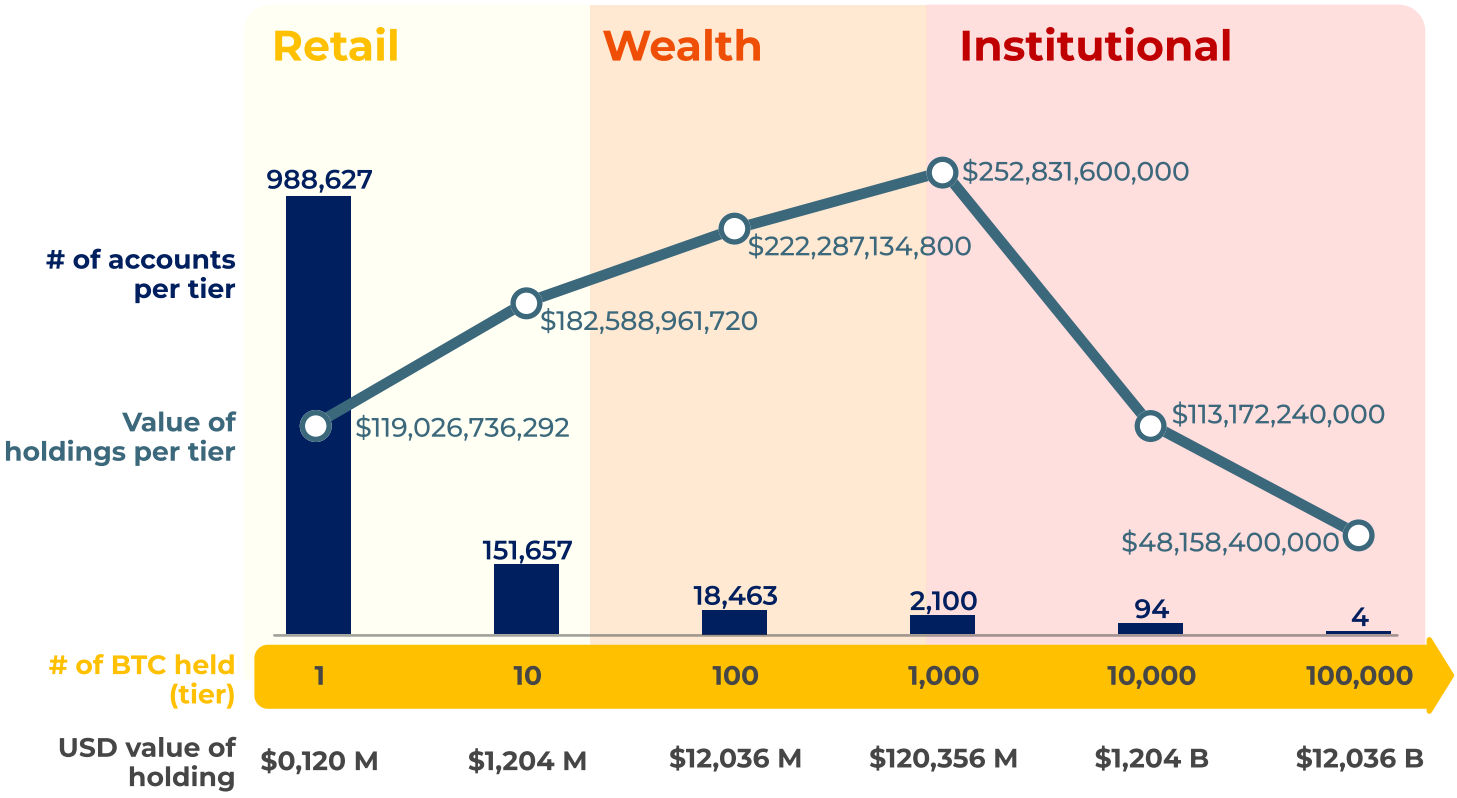
Risks

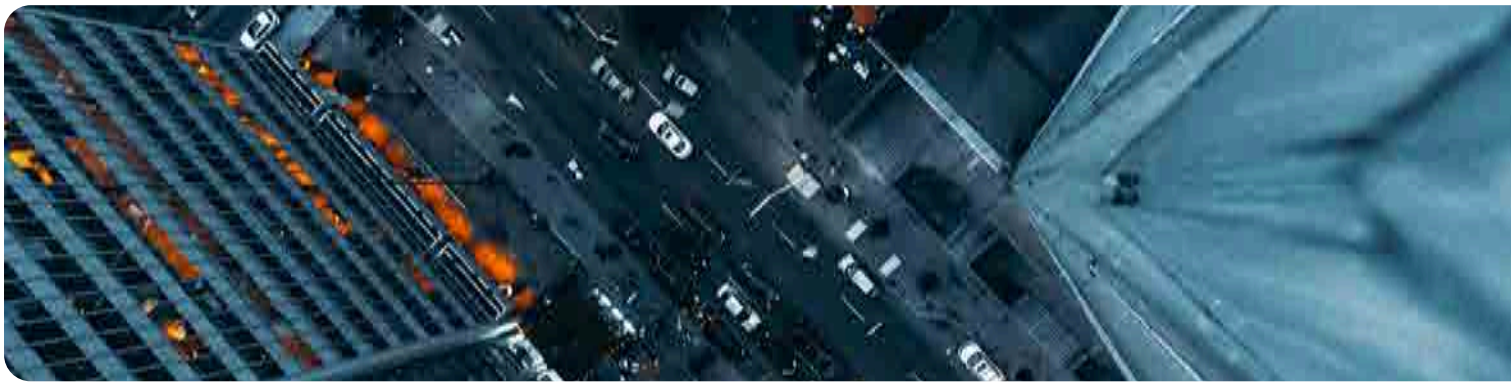
Although tokenised assets exist on-chain, the main risks that they entail are in the failure of the link between the on-chain token and the off-chain asset. As such, the risks of tokenized securities are parallel to those of traditional securities: liquidity risks, fraud, and custodian failure – although new risks such as oracle risk (where the smart contract receives the wrong price, for example, resulting in wrongful liquidation of billions of dollars in collateral) are now entering the risk agenda.

b. Cryptocurrencies are not about just retail investors any more

Whilst almost one million wallets now hold bitcoins, cryptocurrencies are no longer a purely retail play. With over USD 410 billion in bitcoins held by institutional firms (i.e. those with over USD 120 million in assets), the impact of cryptocurrencies is starting to be felt across the trading floors of the world's regulated securities houses. And outside of the trading floor, crypto-assets are beginning to underpin capital financing and balance sheet management for global financial institutions – creating a new string of dependencies that need careful evaluation and risk management. Cryptocurrencies are starting to need institutional levels of scrutiny.

Today's Bitcoin holdings





c. Digital assets: Already material in your market

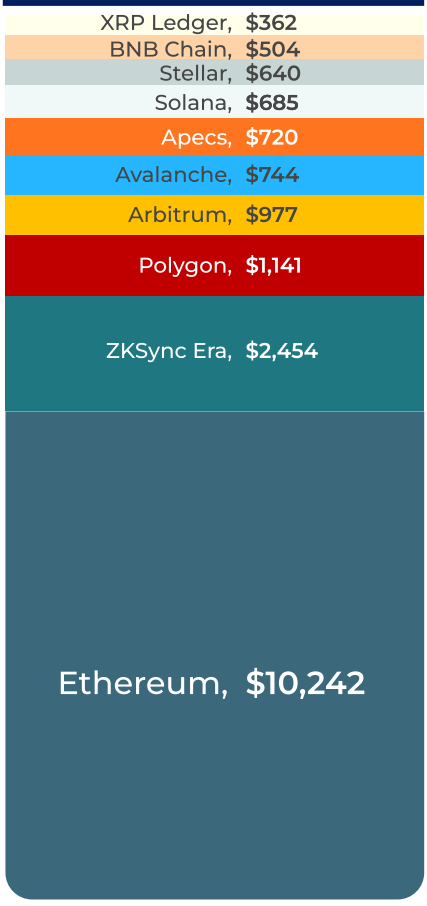
These holdings are also not just accumulating in a far distant land. Material levels of crypto holdings are also growing in every recognisable market, meaning that no regulator and no industry operator should think that they are exempt from the above risks.

Where and how digital assets are held

Where in the world?

Ranking	Country
01	India
02	Nigeria
03	Indonesia
04	USA
05	Vietnam
06	Ukraine
07	Russia
08	Philippines
09	Pakistan
10	Brazil
11	Turkey
12	UK
13	Venezuela
14	Mexico
15	Argentina
16	Thailand
17	Cambodia
18	S. Korea
19	China
20	Canada

On which public chains?



Value of assets on chain (USDm)

Where else?

Canton network
USD 6 T

R3 Corda
USD 7 T

Hyperledger, Quorum?

Importantly, these assets reside on a large number of blockchain networks, many of which are entirely new to many regulators and risk managers. Of these, Ethereum stands out as the biggest, publicly accessible chain for digital asset liquidity – although other new networks are evolving and growing quickly. In parallel, private and public-permissioned networks (or Layer 2 networks) are also gaining widespread adoption as regulated firms look to optimise both investor reach and network risks as part of their daily operations.

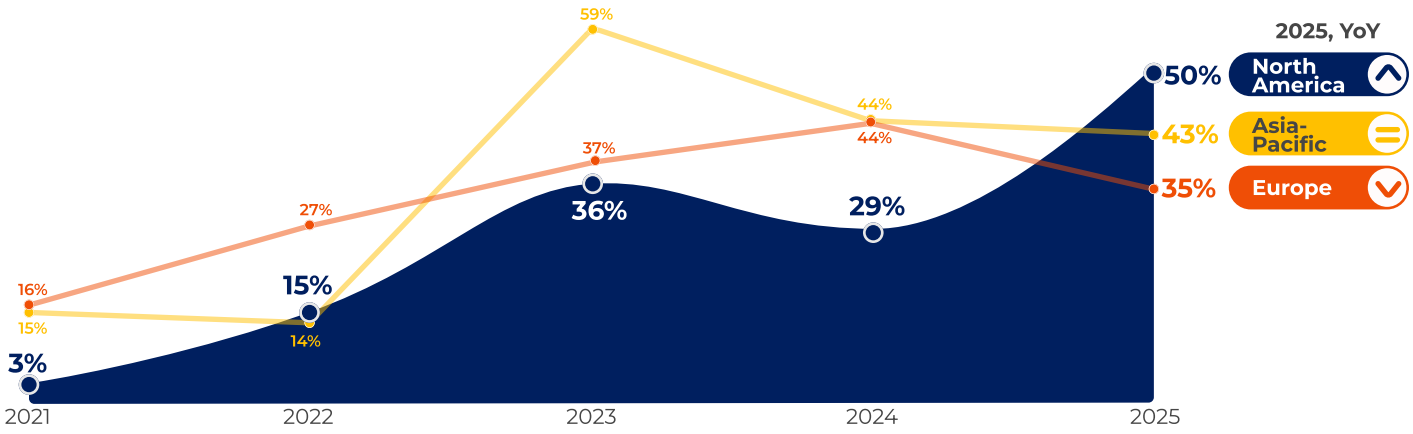
Aside from the physical challenge of evaluating and managing multiple networks, this range of public and private blockchains also creates a new due diligence risk for firms, which we expand on in the scenario sections below. Network and chain risk are new competencies that market operators and regulators quickly need to master, if they are to properly manage the risks that these networks pose for their regulated institutions.

d. Where is the momentum?

Where in the world are these digital assets being issued? Progress varies greatly around the globe with regions at different stages of the crypto asset journey – but the USA stands out above all others in investment, engagement and in the speed of asset issuance today.

Having gone from the 'crypto winter' to the forefront of growth, the US is moving extremely fast today, propelled by the GENIUS Act, the CLARITY Act and other developments that continue in 2025. Whilst the average firm spend on digital assets and DLT in 2025 is USD 2.2 million per annum, North American firms are spending over 200% more than their global counterparts today – with 29% of firms in North America investing over USD 10 million in digital assets in 2025.

Regional use of digital assets



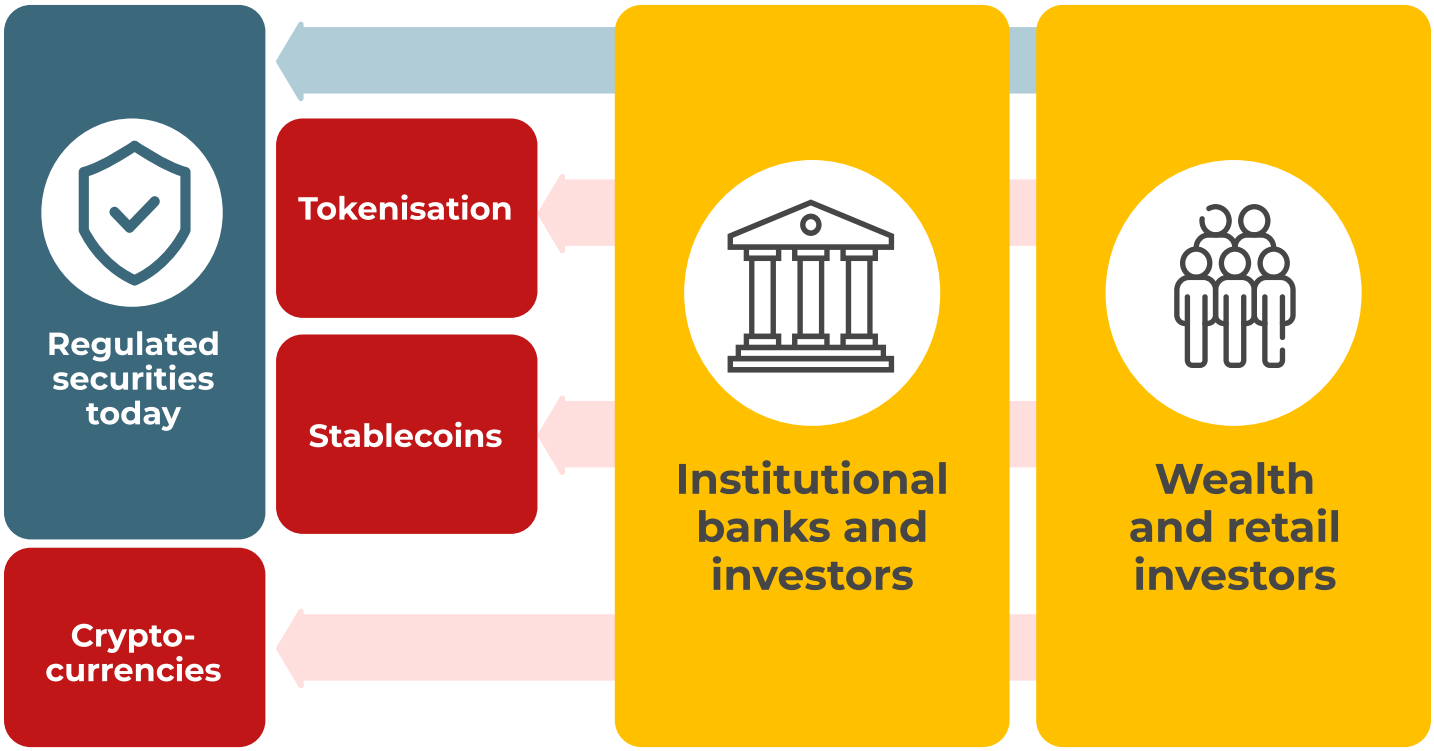
For global regulators, this means that they need to pay close attention - what happens in the US will ultimately impact their jurisdiction both in terms of market frameworks to be scaled but also in terms of growing holdings of US-issued assets on their local balance sheets.

e. Digital assets are reshaping regulated securities markets

What does this growth mean for the world's regulated capital markets? In many markets, regulated securities are already taking their place alongside these digital assets as core parts of financial market ecosystems.

Historically, regulated securities houses have provided wealth and retail investors with access to regulated securities (either directly or indirectly). Today, many of these same firms are (or will soon be) providing access to cryptocurrencies and digital assets alongside traditional assets – as part of their wealth management, retail brokerage or even institutional offerings. Growing holdings of crypto ETFs, futures, options or other products – not to mention direct holdings of cryptocurrencies, stablecoins and tokenised securities are all evidence that these digital assets are making their way onto the 'shelves' of global investors – creating a present-tense, grass-roots risk that warrants careful attention.

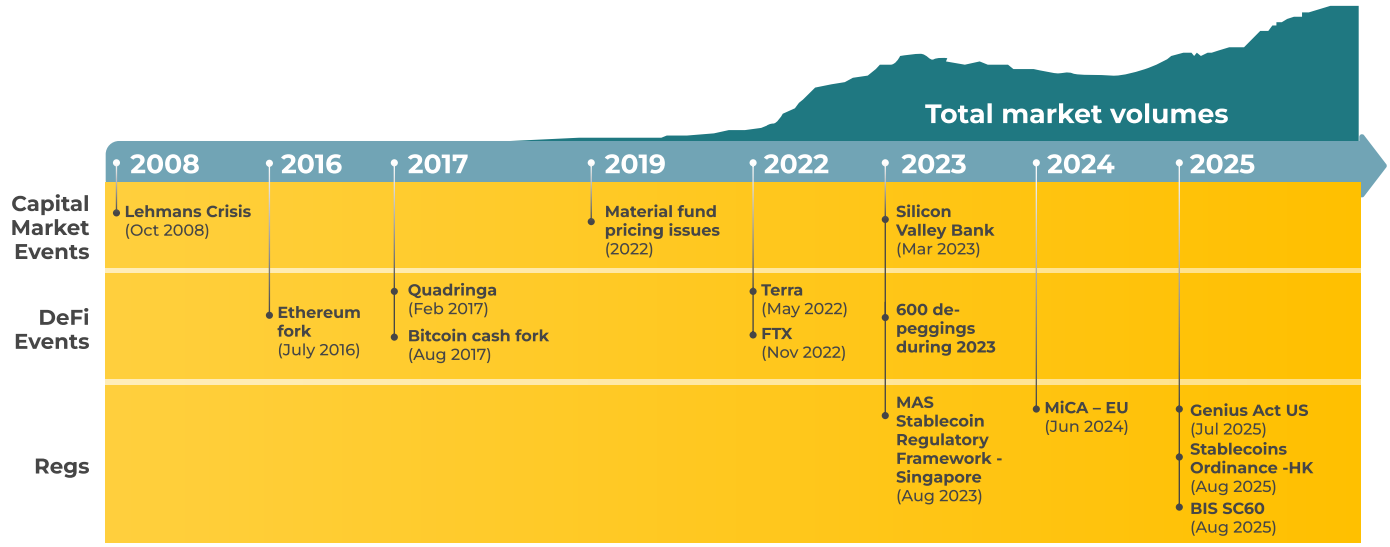
The transformation of investor access



f. Managing digital asset risk: leveraging decades of experience

Whilst digital assets may use new terms and technology, the questions that they pose are, in many cases, unchanged from traditional finance. To safely manage the risks that digital assets present, organisations can draw on extensive precedents from the traditional securities world in order to balance market innovation and investor protection in a digital world. Ultimately, it's the same questions with different answers.

Where assets are held



Of these precedents, Lehman Brothers (2008), the material fund pricing issues / UK LDI crisis (Liability Driven Investment) (2022) and Silicon Valley Bank (2023) all stand out as relevant. Each event offers a distinct and crucial lesson for regulators designing rules for digital assets:

Lehman Brothers

A TradFi systemic crisis. The problem was extreme leverage and opacity of true asset holdings. Lehman held complex, hard-to-value subprime mortgage assets on its books. The firm failed when their value collapsed and, in the global financial crisis that followed, new scrutiny was placed on asset safety, segregation and valuation methodology.

UK LDI Crisis

A TradFi liquidity crisis. The problem was hidden leverage (via derivatives) in "safe" pension funds, which, when triggered by a market shock, created massive, simultaneous margin calls. This forced a 'panic sale' of safe assets (UK GILTS), exposed a schism between the timing of liquidating liabilities and assets on both sides of the balance sheet. Delays in the conversion of (bond) assets into cash created a spiral that required central bank intervention - the perfect case study for the risks inherent in any asset backed token today.

Silicon Valley Bank

A modern TradFi crisis. The problem was a classic 'bank run,' but accelerated by technology. SVB had a fundamental asset-liability mismatch i.e. holding long-term bonds that lost value as interest rates rose. Its highly networked tech- depositors caught wind, and a panic ensued via social media and chat groups causing a digital run that drained the bank in hours, not days.

In parallel, the evolving DeFi world has also seen a growing body of precedents, most notably in the FTX and Terra crises of 2022:

FTX

A crypto-native crisis. The problem was fraud and a total lack of corporate controls. FTX secretly co-mingled customer funds with its sister trading firm and used its own illiquid, self-created token as collateral for loans. This is a classic conflict of interest and fraud.

Terra (UST/LUNA) Collapse

A crypto-native algorithmic failure. The problem was a flawed design. An algorithmic UST stablecoin was not backed by real dollars, but by a volatile sister token (LUNA) via a financial algorithm. When a market panic hit, holders rushed to sell UST, which forced the algorithm to mint trillions of new LUNA tokens to try and prop it up. This spiral sent the price of both tokens to virtually zero in days.

With the acceleration of all forms of digital assets, it is essential that we learn from these events now before holdings become even more material and to prevent more client assets from being lost.

g. Looking ahead: New forms of digital asset regulation

The safe management of digital asset risk is not a new consideration – and there is an equally fast-growing community of regulatory jurisdictions today who are taking steps to provide rules frameworks today. These include:

The United States

The GENIUS Act creates a robust federal framework for stablecoin issuers mandating 1-to-1 backing with high-quality liquid assets, monthly audits and attestations of those reserves directly addressing the risks we saw with the Terra/LUNA collapse.

MAS Stablecoin Framework

Creating an "MAS-regulated stablecoin" label for issuers who meet strict requirements aiming to make stablecoins a trusted digital medium of exchange.

The European Union

The EU passed its landmark Markets in Crypto-Assets (MiCA) framework creating a single, harmonised rulebook for all 27 member states, providing legal certainty for stablecoin issuers and crypto-asset service providers (CASPs).

Hong Kong's Stablecoin Ordinance

Provides regulatory clarity for the safe issuance and management of asset-backed stablecoins, with the aim of supporting a growing ecosystem of commercially-backed stablecoins.

Other regions have moved quickly to create their own bespoke regimes. These include the UK (building its own post-MiCA framework), Japan (which was one of the first to regulate exchanges), and UAE. These regions have clear rules for how exchanges and custodians must operate.

In addition, many more countries (such as South Africa, etc.) are starting to impose new registration requirements on cryptocurrency firms, as a first step in identifying the key players in their local, digital asset ecosystems.

Underpinning many of these regimes is the work of international institutions such as the Bank for International Settlements – whose "DIS55: Cryptoasset exposures" rules provide essential clarity on due diligence and accounting treatment for different forms of digital asset.

3. Crisis Scenarios

If digital asset risks are already material and immediate, then how are regulators and firms meant to identify, scope and prepare critical risk scenarios across global jurisdictions?

In order to provide a clear and actionable set of working considerations, the AMCC group focused on three core risk scenarios as the starting point for an in-depth evaluation of scope, core considerations and potential regulatory responses. These scenarios were:

01

Physical access

The impact of digital assets becoming physically unavailable, due either to network constraints, smart contract hacking or real-world access limitations

02

Issuer risk

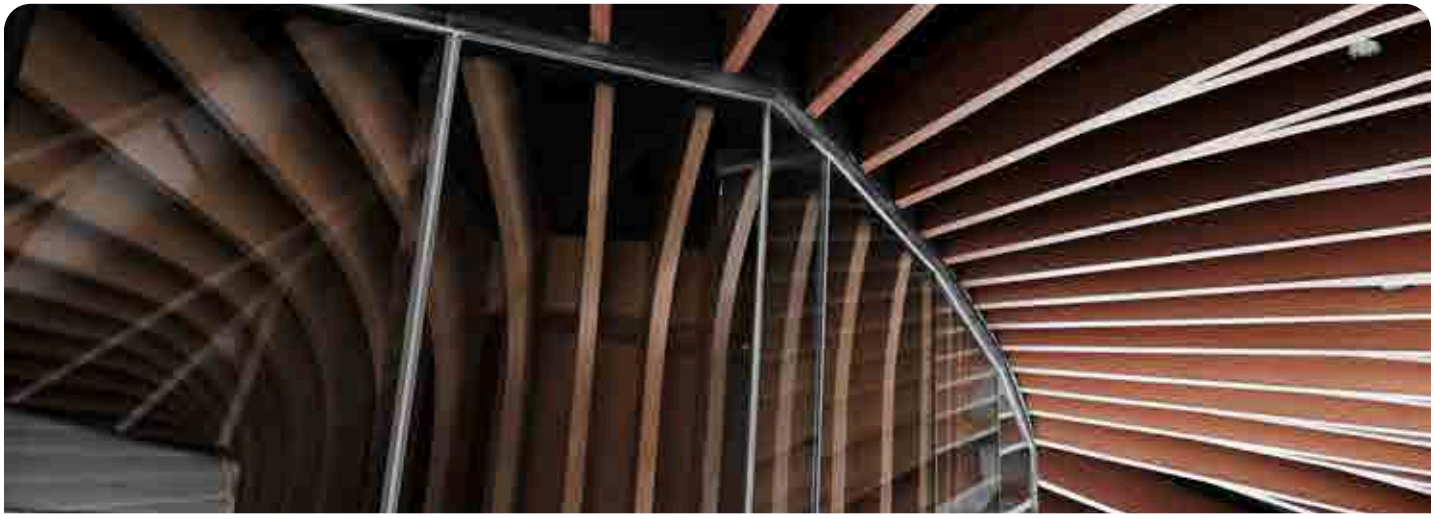
The impact of a stablecoin failure and the consequences of a major unwinding

03

Safe-keeping risk

The impact of a default / bankruptcy of a digital asset custodian entity

Each of these risk scenarios was discussed during an open discussion that included representatives of regulated financial institutions (whose daily experience in traditional and digital assets helped to frame the core, practical considerations at play) and securities regulators (who were then able to provide their own context in terms of how each scenario could be managed at a market level). These discussions were moderated by Suzanne Lasrado (Vice-President, Strategy & Innovation and Member Services at CIRO) and by Barnaby Nelson (CEO, the ValueExchange).



Physical access

The impact of digital assets becoming physically unavailable, due either to network constraints, smart contract hacking or real-world access limitations.

a. Defining the challenge: Multi-layered risk

The core issue discussed by the industry and regulatory representatives was the potential for a failure within the digital asset ecosystem stemming from a malicious attack; an unexpected outage of a foundational blockchain network (L1); or a specific smart contract built upon it.

The following scenarios were discussed:

Network-level failure / Fork

When a blockchain's software or rules are momentarily disrupted, creating two asynchronous sets of records – that then need to be reconciled for the chain to continue to function.

51% attack

Where a single party's control of more than 50% of a cryptocurrency's network computing power allows them to cheat the system and become the single source of truth.

Physical unavailability

The inability of investors and participants to access their assets on chain due to real-world events such as a large-scale power or telecommunications outage.

Smart Contract Exploitation

A vulnerability in a smart contract's code could be exploited, leading to the draining of funds or manipulation of its functions.

Physical and Digital Access Control

The deprivation of access to private keys through sophisticated hacking, simple operational errors or theft (e.g. a bank heist).

The impact of such events is not confined to the crypto-native world. Any one of these events has direct, knock-on consequences into the world of traditional finance (TradFi) through digital assets held as tokens (e.g. by corporate treasuries holding digital assets) or through derivative and structured products that hold digital asset underlyings (e.g. ETFs or structured notes).

In addition to the simple (opportunity) cost of lost trading opportunities throughout the duration of any outage, the repercussions are multi-faceted and include the following:

Fund pricing issues

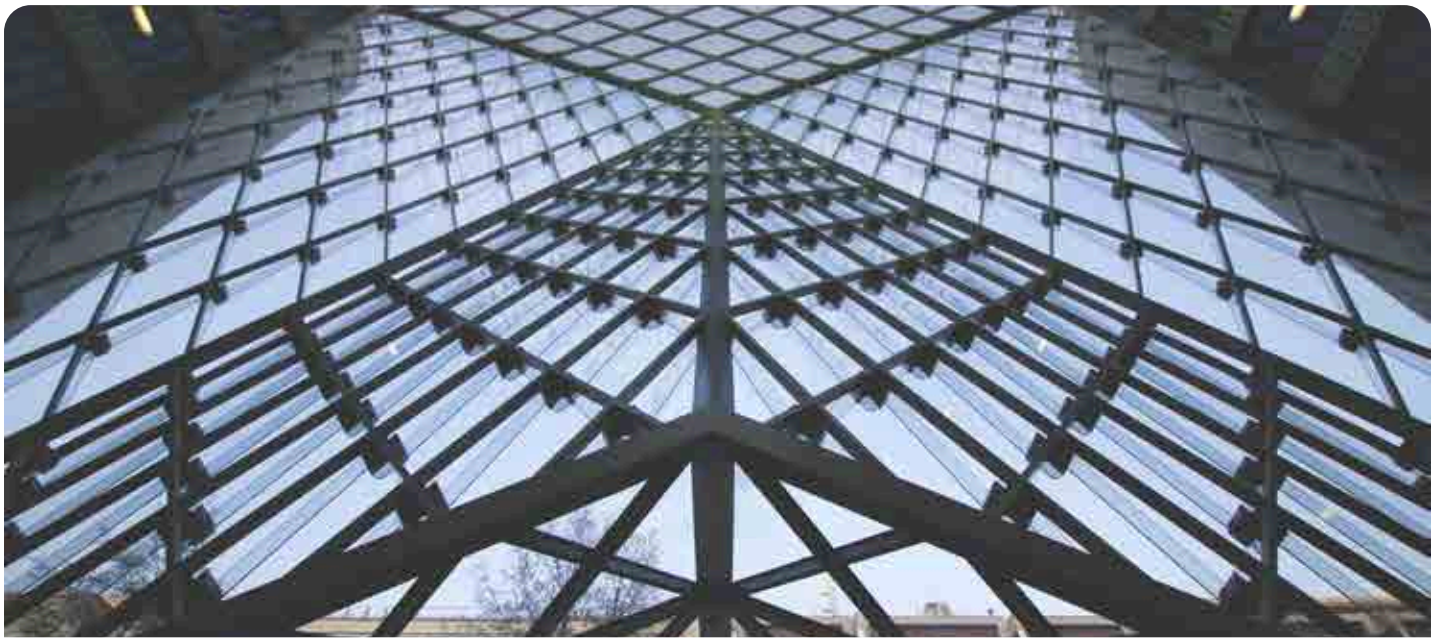
TradFi funds holding the compromised asset would have to immediately write down the value of any digital assets held in this scenario to $0. This would cause the NAV to crash, triggering a "run" by investors, which would force the fund to sell its traditional assets to meet redemptions.

Funding and collateral issues

If the compromised digital asset was being used as collateral for a TradFi loan, the collateral would instantly vanish. This would force the lender to issue a massive margin call, creating a ‘black hole’ on its own balance sheet and forcing the borrower to sell all other assets to cover the debt.

Settlement and operational failure

If the compromised asset is a stablecoin or tokenized security used in the wider TradFi settlement chain, its failure would cause all in-flight transactions to freeze. Which would create an operational gridlock, where trades fail to settle and counterparties are left without their money or their assets.



b. The industry perspective: A new level of due diligence

> "This is due diligence 101

Industry participants from banking, exchanges, and digital asset firms framed the problem as a complex operational resilience challenge that blends existing frameworks with new risk considerations. Whilst traditional risk management principles provide valuable clarity on playbooks, they can fail to consider the nuances of the DeFi technology, the roles of the different actors in a decentralised ecosystem and hence the threat that needs to be managed.

Key considerations:

The "Ghostbusters" issue

In the event of a network issue on a public chain, who are you going to call? In short, when something goes wrong e.g. you get hacked, you send funds to the wrong address, or a protocol fails, there is no entity or central authority to call for help. In essence you are trusting a 'code' to hold your money with no recourse, no reversibility and no authority to authorise special measures (e.g. in the event of a fork).

In this context, a crucial distinction was made between the nature of the counterparties in the chain. Centralised finance ("CeFi") entities, such as Coinbase, operate as regulated intermediaries with 'traditional' controls and are hence reachable. By contrast, truly decentralised finance ("DeFi") structures operate via autonomous code and hence have no central operator.

The physical custody parallel

With over 90% of crypto currencies held off chain in cold storage, the challenge of securing digital assets was compared to the physical custody of gold. And there is commonality. While cold storage effectively shields crypto assets from online hacks, it introduces significant physical vulnerabilities; the hardware wallet or paper backup can be lost, stolen, or destroyed. Critically, security becomes entirely dependent on the user safeguarding their private keys or recovery phrase.

But there are also differences. Gold is a tangible and bulky physical asset and not entirely portable (although theft has been possible). Crypto keys are not. If both the device and these crucial backup credentials are lost or forgotten, the funds are permanently and irretrievably gone as there is no central authority for recovery. Without careful procedures, the cold storage solution itself, or its single backup, can inadvertently become a single point of failure if not managed with sufficient diligence and potentially redundant backups.

Security flaws

Smart contracts automatically handle valuable assets based on code. But what if there is a security flaw? A newly discovered bug in a live smart contract creates an immediate, critical emergency. It's a race against time for attackers to exploit it versus developers trying to mitigate the damage. The creators will have ‘zero days’ to fix it before it can be exploited, leading to potentially widespread damage (data breaches, system crashes, asset theft). As with the gold parallel, these risks are similar to "zero-day" risks in traditional software, where developers maintain rigorous code audits, identify bugs, and coordinate launches carefully in order to minimise their security risks.

Liability in a decentralised world

Underpinning all of the above risks is the core issue with decentralised finance: the ambiguity of liability. If a decentralised network fails, there is no single entity to sue or hold accountable. Attempts have been made in the past to identify or target programmers or individuals who have been closest to the above issues, but little global consistency has so far emerged on the treatment of this issue.

c. The regulator's perspective: Applying a framework to an ever-moving target

Regulators approached the issue from the standpoint of financial stability, consumer protection, and market integrity. Their primary challenge is adapting time-tested regulatory principles to a technology that was explicitly designed to operate outside of traditional frameworks.

Key challenges and regulatory approach:

Accountability is paramount

Regulators firmly believe that "nothing happens without human intervention." Even in DeFi, there are individuals or groups who write the code, govern the protocol, and hold significant influence. The regulatory task is to identify these points of control and hold them accountable.

Regulating the on-ramps and off-ramps

The current strategy focuses on regulating the CeFi firms that act as gateways between the traditional and digital asset worlds. These firms have legal incorporation, physical locations, and identifiable leadership, making them subject to existing regulatory oversight (e.g. operational resilience, custody rules).

Proportionality and materiality

Regulators acknowledge that not all digital asset activities pose a systemic risk. The principle of proportionality is key: a small, immaterial protocol should not be subject to the same stringent standards as a systemically important one. The challenge lies in establishing clear criteria for what constitutes "materiality."

The moral compass

Failures like FTX were cited as being rooted not in technology, but in a "lack of a moral compass" and fundamental governance failures. Regulation aims to enforce a baseline of ethical behaviour, proper risk management, and accountability that technology alone cannot provide.

A collective action problem

Crypto is inherently global and cross-border. No single regulator can effectively oversee the entire ecosystem. This necessitates deep international cooperation through bodies like IOSCO and the FSB to create a consistent global framework and prevent bad actors from moving to jurisdictions with weaker rules.

d. Building solutions: Cooperating to shape a resilient future

> **Firms have to participate in the governance of networks**

Ensuring the stability of the financial system in the face of these new risks requires a concerted and collaborative effort.

The following follow-ups were recommended:

I. Strengthen Industry-Regulator dialogue

The need to deepen the collaboration between the industry and regulators is clear. There is a shared need to develop clear standards for operational resilience, risk management, and due diligence when using decentralised networks. This includes defining clear criteria for the materiality of different protocols.

This goes beyond periodic consultations to establishing standing public-private working groups. The immediate goal should be to co-create practical, actionable standards for due diligence. For example, this could result in a shared framework for assessing the operational and governance risks of a specific L1 network. This should include factors like validator decentralisation, developer community robustness, and the clarity of its fork resolution process.

A key output must be a common understanding and methodology for defining the materiality of a protocol, establishing clear and tiered thresholds (based on total value locked, transaction volume, or interconnectedness). This would trigger heightened supervisory expectations and clear guidelines to innovate and operate within.

II. Establish clear frameworks for accountability

Policymakers and legislators must work to clarify legal liability in the event of a network or smart contract failure. While regulating code is impractical, frameworks should focus on the accountability of the developers, founders, and governance bodies who exercise effective control.

While the code itself is neutral, the individuals and entities that develop, deploy, and govern protocols are not. Future legal and regulatory frameworks should provide clear tests for identifying definitive control (i.e. looking at who holds significant voting power via governance tokens, who has the exclusive ability to propose protocol upgrades, and who profits disproportionately from its operation).

Going further, whilst a technology may not be regulated, the entities using it are. Therefore, if a decentralised network fails, the liability should also fall to the regulated firms using the technology. To ensure an effective liability protocol is in place, and to help firms protect their clients (and themselves), the industry and regulators should unite to define a decentralized due-diligence regime.

Holding these parties to a standard of care, similar to that of traditional financial market infrastructure operators, is a necessary step to ensure someone is responsible when things go wrong.

III. Promote international regulatory consistency

A fragmented regulatory landscape creates weak links that can be exploited and lead to systemic contagion. Given the borderless nature of digital assets, preventing systemic risk requires moving beyond high-level principles to concrete implementation.

National regulators must accelerate their work through international bodies such as IOSCO and the FSB to harmonize rules in order to ensure that recommendations are translated into consistent, binding rules across major financial centres. The ambition must be to prevent a "race to the bottom" where risky activities migrate to the weakest regulatory environments.

Formal information-sharing agreements and cross-border resolution plans for major digital asset firms and protocols that operate globally should also be established.

IV. Invest in education and capacity building

Both industry and supervisory bodies need to continuously invest in their technical understanding of the technology. This will enable firms to conduct better due diligence and allow regulators to create effective, technology-neutral rules that focus on outcomes rather than prescribing solutions.

To create effective, technology-neutral regulation, supervisors need deep technical expertise embedded within their teams. This means hiring blockchain analysts and cryptographers and establishing continuous training programs and reverse-mentoring opportunities with industry experts.

For the industry, this means ensuring that risk, compliance, and legal teams have a sophisticated understanding of the technology they are using, enabling them to challenge assumptions and conduct meaningful due diligence, rather than simply relying on the assertions of technology teams.

V. Release planning / due diligence

Whilst code should be accepted as commonplace, any new code, any modification to a code should be subjected to rigorous audits. Bugs will need to be detected by developers not by hackers. This is unnegotiable to prevent any flaws leading to instant, irreversible theft. The audit and patching process is crucial preventative risk management technique to avoid catastrophic financial losses.

VI. Innovate to strengthen risk frameworks

Whilst the industry (and regulators) can lean into TradFi for solutions it should not be shackled to past best practices. For example, the industry should continue to challenge itself to move beyond existing ‘cold storage’ protocols to highly sophisticated solutions like Multi-Party Computation (MPC), where a private key is never assembled in one place, thus eliminating a single point of failure.

VII. Formalize crisis management protocols

The theoretical risk of a failure must be met with practical preparation. Just as in traditional finance, the industry and regulators should jointly design and conduct market-wide crisis simulation exercises.

These drills must test specific, plausible scenarios, such as a major stablecoin de-pegging or a contentious L1 fork occurring during a major margin cycle to identify and close gaps in communication and resolution procedures before a real crisis occurs.

The goal is to create a clear playbook that answers critical questions in real-time: Who communicates with whom? What is the process for pausing trading or settlement? How is a definitive version of a ledger agreed upon? These exercises will reveal gaps in coordination and communication that can be fixed before a real-world crisis forces the issue.

VIII. Business continuity

Firms should ensure unwavering business continuity plans are in place which should cater for:

Redundancy
Running their own network nodes to 'back-up' and maintain a copy of the ledger. Therefore, in the event your node fails, no data is lost because other nodes still have a copy of the history and continue to run the network.

Contingency planning
Establishing clear business continuity plans to 'rollback' the ledger (or reorganization / reorg) or where the community agrees to revert the blockchain to a state before the failure (like restoring from a backup), or activating a pre-designated alternative system, which might be a backup ledger, a new 'forked' version of the blockchain, or even traditional off-chain records, to restore ownership and continue operations.

Real-time monitoring
Continuously monitoring on-chain events to detect and react to anomalies before they escalate.

02 Issuer risk

The impact of a stablecoin de-pegging / failure

a. Defining the challenge

While the total stablecoin market cap stands at USD 291 billion it remains a fraction of the USD 9.6 trillion daily foreign exchange market.

While de-pegging events are frequent, they have so far been minor and manageable. However, as the market grows, so does the potential for a significant failure to cause ripple effects across broader financial markets challenging investor and issuer confidence.

But important distinctions need to be drawn between algorithmic and asset back stablecoins:

Algorithmic stablecoins

Low holdings, largely speculative and very high volumes of de-peggings (but ultimately low impact). In this case the risk is largely speculative. “It’s natural to have dislocations. These are the natural course of business”

Asset backed stablecoins

High value, high impact but asset backed. In this case the risk is widespread - but more focused on the short-term considerations of an unwinding event.

The central challenge facing the global financial ecosystem, therefore, is how to manage the risk of a systemically important, asset-backed stablecoin de-pegging or failure.

As highlighted in Scenario 1, the extended impacts of this type of failure can be extensive – stretching well beyond the individual users of stablecoins for their DeFi trading, into the institutional capital markets. With growing volumes of corporate treasuries holding stablecoins as stores of value, the concentration risk on a small number of issuers is growing every day. And as we highlighted above, the risk to the liquidity of the global financial system of lost value can be immediate and widespread – impacting traditional finance transactions, counterparties and account holders.

But what does (or should) managing a de-pegging event look like in practice? In practice it is an exercise in trust and confidence. A stablecoin de-pegging shatters confidence. It can trigger ‘panic selling’ and chaos leading to mass liquidations of loans. Liquidity from trading pools drain. And fear can spread to other stablecoins resulting in an even broader crypto market sell-off. Centralized exchanges may halt trading, trapping funds, while crypto firms holding the failed stablecoin can face insolvency.

b. The industry perspective: Operational hurdles that undermine product design

> **"A stablecoin de-pegging transfers credit risk into liquidity risk**

For industry participants, the starting point is that stablecoins present a fully asset-backed (and therefore safe and resilient) form of digital cash – and one that can be left to unwind or regulate in an orderly fashion during periods of stress.

Yet upon closer inspection, the core risk in stablecoins is how to manage the operational dependencies that link these digital assets to the world's traditional financial markets – and which create a potential domino effect in times of market stress.

Dependence on TradFi infrastructure

The stability of stablecoins is deeply intertwined with the traditional banking system. The shutdowns of Silicon Valley Bank, Signature, and Silvergate highlighted this vulnerability – where the failure of digital infrastructures forced firms to fallback to slower (traditional) settlement systems. In the event of a network or platform failure, the transfer of volumes and processing over to legacy infrastructures can trigger operational (load-related) limitations that then manifest in significant processing delays, manual processing requirements and exponentially more risk.

Evolving data maturity

The ideal first step in ensuring investor confidence is in providing clear and transparent market data – with which investors can manage their risks. The challenge today is that the rapidly evolving stablecoin ecosystem lacks the mature, standardised data needed for effective risk management. This creates significant blind spots for the industry (and regulators) and makes it hard to accurately gauge critical risks like reserve quality or volumes. During a time of stress, this lack of transparency can undermine investor confidence and allow contagion and liquidations to cascade unexpectedly.

Dependence on TradFi markets

If these (or other triggers of) stress were to then overflow into a run on the stablecoin, then further risks quickly become apparent. Whilst the world's leading stablecoins might be 100% asset backed, the assets held by a coin issuer have widely varying degrees of liquidity. Cash might be instantly transferrable during a stablecoin run or failure, but cash reserves often make up only a portion of stablecoin reserves. The remaining reserve assets (most often government bonds or short term papers) can only be transacted based on traditional settlement cycles that run into days – with specialists anticipating that it would take up to a week to fully divest all securities holdings held by a stablecoin issuer.

Bankruptcy costs

Stablecoins are backed by assets to 100% of the issued value. But in a failure, there would be additional insolvency costs (e.g. through legal and recovery proceedings) – which risk depleting the value of cash and assets available for redemptions. In essence, once insolvency costs are accounted for, the true asset backing of a stablecoin is in fact <100%. So, who doesn't get their share? If there isn't enough left after those costs (and any reserve losses) are covered, it's the stablecoin holders who bear the final shortfall, receiving less than the $1 per coin they expected.

Concentration risk

Over-reliance on one or a few dominant stablecoins, for a fledgling asset class, and industry, is difficult to avoid and even more difficult to manage. Given the highly concentrated nature of today's stablecoin market (where two coins make up over 85% of issuance), the failure of a stablecoin creates systemic contagion, triggering mass liquidations and a widespread liquidity crunch. This could be a chain reaction that erodes trust in the asset class, forces market-wide asset selling, leads to business failures for exposed firms, and attracts intense regulatory scrutiny, destabilizing the entire ecosystem.

Identifying the end customer

Stablecoin holders using self-custody wallets (as opposed to those using independent custodian entities) are essentially unidentifiable. This creates numerous threats: regulators can't easily track illicit funds (AML/CFT risk), investors have no recourse if funds are lost or stolen. During periods of normal market function, this makes the monitoring of systemic financial risks harder and obscures tax compliance is. In the event of a default, this same challenge can make it impossible for issuers to even know who to deliver liquidation proceeds to. Essentially, anonymity undermines crime prevention, financial oversight and consumer safety.

Put together, these considerations raise three questions:

1. In the context of the SVB crisis, can stablecoin liquidity be managed fast enough during times of stress to provide continuing liquidity to its holders?
2. If a run were to occur on a stablecoin, how would the issuer categorise its holders? Who would get instant access to cash reserves and what would happen to those slower to react, for whom only securities holdings remain as reserves? How long would they have to wait for their cash?
3. How can stablecoin issuers maintain market confidence to the level where investors are fully confident in their ability to redeem their stablecoins on a 1:1 ratio at all times – so that the above scenarios never become a reality?

c. The regulator's perspective: Systemic and jurisdictional complexities

Regulators are focused on the bigger picture: maintaining financial stability, protecting consumers, and creating a consistent framework for borderless technology.

Regulatory fragmentation

A primary challenge is the fragmented global regulatory landscape. How to manage a stablecoin when the issuer is domiciled in one country while its user base resides in a different regulatory environment? This creates substantial cross-border challenges, including potential rule conflicts, difficulties in supervision and enforcement, and the risk that consumers fall outside the direct protection and oversight of their home regulators. While international bodies like the IMF, FSB, and IOSCO have issued high-level standards, these need to be adapted locally, which is difficult for countries with less regulatory capacity.

Systemic risk

Stablecoins are increasingly systemically important, with combined US Treasury reserves now comparable to major sovereign holders like Norway. A sudden, large-scale sell-off of these reserves could significantly disrupt Treasury market liquidity and yields – triggering a host of unforeseen consequences for Central Banks. Regulatory frameworks are needed to monitor the growing influence on sovereign debt markets (such as the size, composition, and potential market impact). Coherent and coordinated regulatory approaches to monitoring and crisis management are needed across jurisdictions to mitigate potential instability.

Insolvency and resolution

A major unresolved issue is the lack of a harmonized global approach to a stablecoin issuer's failure. Key questions remain around:

Asset segregation
Uncertainty exists whether reserve assets are legally ring-fenced from the issuer's other debts across different jurisdictions. And if they are, will they be sufficient after insolvency costs and potential losses?

Identifying end-users
It's difficult to verify and distribute remaining funds fairly to all holders, especially those using anonymous self-custody wallets versus known exchange users or custody account holders.

Cross-border recovery
No standard process exists for coordinating asset seizure and distribution across multiple countries, leading to potential legal conflicts and unequal treatment of holders based on location.

Redeem or transfer

Should stablecoin holders even expect to receive fiat cash in the event of a default – or should they perhaps receive entitlements to new, substitute coins? Swapping to another coin keeps users in the digital ecosystem and might be faster - but usually locks in significant losses immediately, and doesn't solve the underlying value shortfall. Fiat Redemption, on the other hand, aligns with the stablecoin's $1 promise, fits existing (slow, costly) insolvency laws, but requires forces users out of the digital ecosystem and likely provides less than $1 back after costs.

There is no clear, global, framework which defines which option holders should get, meaning that the path taken during a stablecoin failure would likely be decided ad-hoc by courts, regulators, and insolvency practitioners based on the specific circumstances (jurisdiction, issuer structure, reserve status). The lack of a defined framework creates major uncertainty for holders, leaving them guessing whether to cut losses quickly via a swap (potentially at a loss) or wait for a slow, potentially partial, fiat payout through a complex legal process.

Covering a 24/7 day

Crypto's non-stop markets present an oversight and operational challenge for those anchored in the world of traditional finance. In an always-on world, how can regulators continually oversee the smooth functioning of a market – and how can participants manage margin calls, exceptions and escalations on a round-the-clock basis? With key personnel often unavailable outside standard banking hours, the risks of processing issues immediately escalating into liquidity is very real. A major shift in TradFi's operational norms and risk management infrastructure are needed before digital liquidity can be safely managed.

d. Building solutions: Preventing and recovering from failure

To address these challenges, the discussion highlighted actions for both the industry and regulators, aimed at preventing a de-pegging event and, if one occurs, ensuring a swift and orderly recovery. The following follow-ups are recommended:

I. Prevention: Building a resilient ecosystem

Proactive measures are crucial to building market confidence and preventing catastrophic failures. Together, the industry and regulators play a crucial role.

Enhance due diligence and risk management

Regulators must require the industry to move beyond simple reliance on an issuer's brand and conduct deep, ongoing due diligence. This involves a "traditional counterparty analysis" that scrutinizes the issuer's reserve composition, redemption processes, and operational SLAs. This must be paired with establishing robust counterparty risk limits and dynamically applying haircuts to mitigate emerging risks.

Mandate and enhance transparency

Regulators must continue to enhance standards for regular audits of stablecoin reserves. A critical step is forcing the market to transition from simple "attestations" to full, independent audits. This should be supplemented by implementing real-time reporting mechanisms for reserve holdings to build market confidence.

Manage concentration risk

Investors should limit their exposure to any single DeFi protocol or exchange or become heavily reliant on one stablecoin. Liquid reserves against non-stable assets (like BTC, ETH, or fiat) should be encouraged.

Guarantee universal redemption

Regulators should compel issuers to provide non-discriminatory 1:1 redemption rights, removing contractual loopholes, and secure formal agreements with liquidity providers for stress periods.

Drive secure institutional integration and leverage blockchain efficiencies:

Industry leaders should actively pilot and adopt regulated stablecoins for institutional treasury management and payment settlements. In simple terms, robust frameworks specifically designed to manage the unique liquidity and operational risks inherent in digital assets and 24/7 markets should be established.

Investment in tokenization infrastructure and supporting processes that enable instant, 24/7 settlement should be championed. By embracing these technologies, institutions can leverage blockchain's core strength - transparency for real-time risk management and streamlined operations. Ultimately reducing dependency on less efficient, slower-moving traditional fiat rails will unlock significant operational gains and smoother crypto markets.

Establish clear, coordinated global regulatory frameworks and systemic risk management:

Implement clear national rules

Regulators should roll out standardised frameworks (e.g., EU MiCA, US GENIUS Act) covering compliance, transparency, collateral haircuts, and liquidity management to build institutional trust and asset safety.

Foster international cooperation

Regulators should develop concrete information-sharing agreements, such as the IOSCI MOU and coordination mechanisms between global regulators for consistent supervision and preventing regulatory arbitrage.

Monitor systemic footprint

Investors and regulators should actively track the scale and impact of their stablecoin reserves, particularly large holdings in sovereign debt markets.

Coordinate macroprudential policy

Regulators should develop coordinated policies to mitigate potential instability caused by sudden, large-scale outflows from stablecoin reserves impacting traditional markets.

II. Recovery: Protecting investors and the economy

In the event of a failure, a clear and coordinated plan is needed to protect investors and contain economic damage.

Be operationally prepared for failure

While regulation sets the framework, the industry must be operationally prepared for a failure. This includes having robust contingency plans for banking holidays and settlement delays, ensuring redemption processes do not grind to a halt during a crisis. Cooperation with insolvency authorities would be critical.

Develop clear insolvency and resolution frameworks

This is one of the most significant and unresolved challenges. Global regulators must urgently develop specific insolvency regimes for stablecoin issuers. This framework must prioritize:

Asset segregation
Establishing clear protocols to ensure stablecoin reserves are distinctly separated from the issuer's operational funds to protect customer assets.

Customer identification
Implementing robust customer identification (AML/KYC) measures. This is critical for accurately tracking ownership and efficiently processing claims during a resolution.

Cross-border recovery
Creating mechanisms that allow for coordinated regulatory responses and asset repatriation. This is vital to overcome the complexities of differing national insolvency laws.

Provide technical assistance for global harmonization

International bodies, especially the IMF, should provide country-level support to help nations align their local laws with international standards. This technical assistance is crucial for countries with less developed regulatory capacity to avoid creating gaps and fragmentation that could be exploited.

Establish and enhance crisis response protocols

Regulators should establish clear protocols for cooperation during a crisis. This includes enhancing existing multilateral agreements (like the IOSCO MMOU) to be more effective for crisis response and cross-border supervision, especially since emergency liquidity assistance mechanisms are typically available only to banks, not stablecoin issuers.

03 Safe-keeping event

The default / bankruptcy of a custodian entity

a. Defining the challenge: Protecting client assets in a crypto crisis

Following the "crypto winter" and high-profile failures such as FTX, the fundamental challenge for the industry and regulators alike is to establish a robust global framework that protects client assets in the event of a custodian's default or bankruptcy.

Drawing lessons from TradFi crises such as the Lehman Brothers and MF Global collapses, the ambition must be to ensure that client assets are clearly identifiable, legally segregated, and can be promptly returned to their rightful owners, irrespective of the underlying technology. This requires addressing issues of legal uncertainty across jurisdictions, new market structures with inherent conflicts of interest, and the unique operational risks associated with digital assets to establish a global framework for the safekeeping of crypto-assets and stablecoins.

b. The industry perspective: Learning lessons from past crises

> **"Where is the omnibus account?**

The outcomes and experiences of past financial crises are directly applicable to the digital asset space, even if the technology is different.

Putting experience into action

The collapses of Lehman Brothers and MF Global provided critical lessons which should be applied in the context of digital assets.

The primary challenge during the Lehman crisis was locating assets due to siloed systems and a lack of clear, reconciled records of ownership. It took years to resolve entitlements.

This highlighted the need for sophisticated record keeping, robust reconciliation and clear lines of ownership.

The MF Global case was different; it was a case of fraud where funds were illegally taken from segregated accounts proving that even with contractual and operational segregation, a safety net is required to protect against malicious actors.

In the case of digital asset safety, the importance of real-time record keeping and of the safe-guards that this can provide is paramount. The industry has learned that the speed of resolution is critical, noting the FTX wind-up was significantly faster (3 years) than Lehman's (17 years). The use of on-chain, atomically settleable stablecoins based on pre-funding or instant-settlement models (versus traditional T+2 settlement cycles), have had a clear role remove ambiguity in the trade cycle and in facilitating much improved record keeping.

Asset segregation

A key focus is on how asset segregation principles apply in a digital custody arena. A major challenge has been the lack of a trustworthy bench of counterparties for settlement, custody, and hedging. That these same parties (or others) then operate omnibus accounts creates new issues in obscuring direct proof of ownership for the end client and creating grey-areas that then acquire critical importance during defaults. The omnibus accounts need to be either fully disclosed or avoided at all steps of the digital trade cycle if asset safety is to be maximised.

Wrappers versus security risk

A critical part of asset recovery is understanding the holder's claim to the asset. In a tokenised assets context, key nuances are emerging – pitting ‘wrapped’ tokens against fully ‘on chain’ assets. Wrapped tokens represent a complete claim on the issuer/custodian for the underlying asset – but they imply a counterparty (default) risk against the issuer of the token. If that issuer is not the same entity as the issuer of the underlying asset then there is an additional layer of counterparty risk in the token (versus the traditional asset) – and if the wrapper fails, holders become unsecured creditors. This differs fundamentally from ‘on chain’ assets where tokens representing a direct, legally enforceable claim on the asset itself (most often because the tokenisation has been done by a regulated financial market infrastructure).

The Basel Committee's cryptoasset standard (SCO60/d579) explicitly addresses this distinction. In cases where the token represents the “same asset, same risk” as the underlying asset (in this case Group 1a assets), the Risk Weighted Asset treatment of the token is the same as the underlying (e.g. 0-4%). However, any token that fails to match the behaviour of the underlying asset against a number of requirements (i.e. Group 1b assets) requires a Risk Weighted Asset treatment of 1250%.

Due diligence remains paramount

The fundamental rules of due diligence have not changed. Investors and clients must understand their service provider, how they are regulated, where they are regulated, and how client assets are held. The distinction between property rights and contract rights is crucial. The focus should not be on the technology itself but on the underlying principles of asset safety, control, and reconciliation.

New levels of limit and counterparty management

Atomic settlement is an opportunity to be seized, it enables new levels of limit management allowing for more dynamic, real-time control over counterparty risk. But this needs to be clearly understood and firm's risk frameworks need to reflect the evolution and not stand still.

The need for settlement finality

A key concern the industry today is where is settlement finality?

> **"In the traditional world we have DVP, we know the jurisdiction where settlement takes place. We know when cash goes out and secs come in that it simultaneous, it is final and irrevocable. In a permissionless environment what is settlement finality?**

Again, this was a key learning from the Lehman crisis when trades were unilaterally cancelled, adding to the risk and scale of the default. And it is by no means clear cut. Whilst code-level finality seems to be assured (based on the trade being practically irreversible by the network's consensus rules) legal finality (unconditional and protected by law from being unwound or 'kicked back,' especially in the event of a counterparty's insolvency) does not exist in the DeFi permissionless world. This remains a critical risk for the industry.

The need to define the trusted counterparties

Unlike CeFi where assets are held by regulated, centralized platforms functioning as Qualified Custodians, the very nature of true DeFi means there is no central intermediary. There is no legally recognized 'Qualified Custodian'. Because true DeFi protocols do not meet the legal definition of a QC, regulated institutional investors (e.g., banks, wealth managers) are often legally blocked from placing client assets directly into these protocols, severely limiting DeFi's integration with the traditional financial system which remains a hurdle for mainstream institutional adoption.

c. The regulator's perspective: Adapting Existing Regulatory Regimes

Regulators acknowledged the applicability of existing frameworks but highlighted the new challenges and risks introduced by crypto-assets and their market structure.

Putting experience into action

Post Lehman regulations, such as the UK's CASS regime (Client Assets Sourcebook), were created to protect client assets and were successfully tested by the MF Global failure. These principles still apply, but they need to be adapted. While the rules for traditional registered assets are well-understood, the treatment of cryptographic keys and achieving settlement finality in a permissionless environment are less clear. Regulators are considering whether dedicated regulatory divisions are needed for crypto-assets, similar to those for payments and client assets.

Preventing conflicts of interest in new market structures

A primary concern is the emergence of new, vertically integrated business models where a single entity acts as the exchange, custodian, and trader. This concentration of functions creates significant conflicts of interest and removes the checks and balances inherent in traditional market structures, which have intermediated brokerage and custody protections.

The failures of FTX and MF Global, where client funds were misused, were viewed as fraud. The risk was amplified by this integrated structure. A global regulatory protocol is therefore required to define conflict of interests with standards to be applied for each function undertaken (issuer / exchange / trader and custodian).

Global systemic risk and jurisdictional challenges

Regulating entities that are centralised but operate globally presents a major challenge. The principles for resolving a firm like Lehman Brothers were broadly similar in the key jurisdictions (UK and US), but the same cannot be said for a digital asset firm operating across many legal systems with varying approaches to property law. Furthermore, digital asset markets are often more concentrated than traditional ones, creating single points of failure. This raises the question of whether GSIB style requirements are appropriate. However, regulators noted a key difference: GSIB requirements focus on capital and liquidity, whereas for custody, the focus should be on qualitative measures like controls and operational risk capability.

The core principle of asset return

There is a foundational legal principle that if a custodian fails, the assets should be returned to their rightful owners. The law must be clear that holding an asset for a client means it belongs to that client, not the custodian. The challenge is ensuring this principle can be enforced in practice, particularly when dealing with complex, multi-party claims in the digital asset ecosystem. Regulators must not be blinded by the technology and need to ensure they understand the risks to enforce these core principles, focusing supervisory efforts on firms with lower resources and questionable ethics who are most likely to cause harm.

d. Building solutions: Prioritizing asset safety

To protect against the default or bankruptcy of a crypto-asset custodian, multi-faceted and globally coordinated effort is required – a partnership between the industry and regulators:

I. Establish international legal certainty

Move beyond ambiguity by creating a clear, internationally recognised legal framework for digital assets. This requires global bodies like UNIDROIT, IOSCO, the FSB in partnership with national legislators, to:

Define property rights
Formally establish that crypto assets held in custody are the property of the client, not the custodian, and are therefore not part of the custodian's estate in bankruptcy.

Harmonise conflict-of-laws rules
Develop and adopt clear rules to determine which jurisdiction's law applies to cross-border digital asset transactions and holdings, preventing legal disputes and uncertainty during insolvency proceedings.

Create clear asset taxonomy
Legally classify different types of tokens (e.g., as securities, commodities, or payment instruments) to ensure they fall under the correct regulatory and resolution regimes.

II. Mandate structural separation of functions

To eliminate inherent conflicts of interest and prevent the misuse of client funds, regulators must introduce and enforce a clear separation between core market functions. This includes:

Requiring separate legal entities
Mandate that custody, exchange, and proprietary trading activities are conducted in distinct, separately capitalised legal entities with independent governance and boards.

Prohibiting commingling of assets
Implement strict prohibitions on the commingling of client assets with the firm's own assets (house assets) and on the sharing of capital or liquidity between the segregated business lines.

Enforcing full transparency
Require firms to provide clients with clear and unambiguous disclosures about their corporate structure and the legal protections afforded to their assets.

III. Modernise and adapt client asset rules

Regulators globally must update existing client asset protection regimes (e.g., CASS, SEC Rule 15c3-3) with specific provisions for digital assets. Key modernisations should include:

Standards for private key management
Mandate robust technical standards for the secure generation, storage, and use of private keys, and audited disaster recovery protocols.

Rules for on-chain segregation
Define clear requirements for how client assets are segregated on blockchain, whether through individually managed addresses or omnibus accounts, and mandate that omnibus structures are supported by meticulous and auditable daily off-chain record-keeping.

Legal definition of settlement finality
Establish a clear legal definition for when an on-chain transaction is considered final and irrevocable, providing certainty for market participants and insolvency practitioners.

IV. Promote and formalise industry standardisation

Regulators should actively encourage and guide industry-led initiatives to create common standards that enhance safety and interoperability. This includes:

Standardised custody agreements
Develop common legal templates for custody agreements that clearly outline the rights and protections of clients, ensuring a consistent and high standard across the industry globally.

Technical interoperability standards
Promote the creation of common technical standards for token issuance and communication protocols between market participants to reduce operational risk and avoid fragmentation.

Eradicating misleading practices
Work to eliminate opaque practices like "asset wrapping," where a client's direct claim on an asset is replaced by a less secure contractual claim against a service provider.

4. Taking this discussion local

While this paper address global issues and themes for the industry and regulators alike, there is an opportunity now for market authorities, infrastructures and participants to work together to apply these principles to their own local markets – so that the above considerations can be tailored to specific market needs and risks unique to their environments.

To support this, we would be pleased to support or assist in your running similar workshops in your own jurisdiction.

Following the same broad framework as this London workshop, this discussion would encourage local markets to consider the following steps:

01 **Establishing clear frameworks for accountability of digital assets**: Making the roles and responsibilities of digital assets transparent across the security lifecycle

02 **Promoting international, regulatory consistency** in asset treatment, due diligence / disclosure requirements, and jurisdictional coverage

03 **Mandating and enhancing transparency** in digital asset issuer and exchange entity structures, digital asset structures, asset segregation procedures and settlement finality

04 **Driving standardisation** in digital asset definitions, standardised custody agreements and interoperability standards

05 **Managing concentration risk** and monitoring systemically important digital asset issuers, exchanges and counterparties

06 **Formalizing crisis management protocols** across the local industry (and in partnership with key issuance jurisdictions)

07 **Investing in education** and capacity building

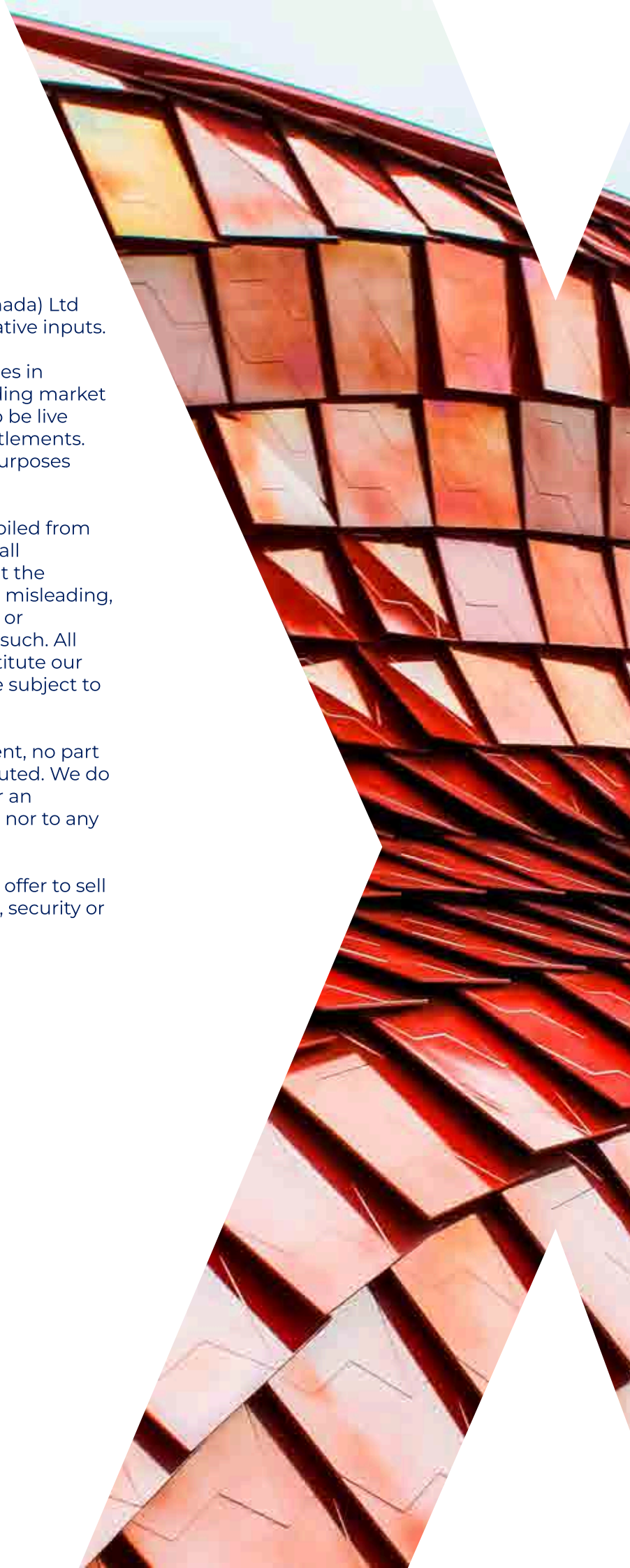
08 **Championing the adoption of digital assets** to build real-time infrastructures that can deliver meaningful benefits to issuers and investors

With 7% of the world's population now engaged on this topic, now is the time to build a safe, coherent and complementary global digital asset ecosystem that maximises investor safety. There is a clear need for formal global regulatory engagement to develop worldwide policy development which IOSCO is well-placed to lead on.

5. Participants and support

The above discussions were led and supported by the following industry specialists, whose valuable time in preparing for and attending the AMCC London workshop is greatly appreciated:

Luciana Pereira Costa	B3
Jochen Mielke de Lima	B3
Matthieu Herbeau	Banque de France
John Siena	BBH
Julien Clausse	BNP Paribas
Pete Elkins	Coinbase
Alan Leung	Coinbase
Scott Bauguess	Coinbase
Caroline Tarnok	Coinbase
Rick Schonberg	Coinbase
Boon Hiong Chan	Deutsche Bank
Kelly Matheson	Digital Asset
Chris Zuehlke	DRW
Nico Di Gabriele	ECB
Jane Moore	FCA / CER
Rostin Benham	Georgetown University
Matthew McDermot	Goldman Sachs
Richard Stobo	IMF



This report has been prepared by The VX (Canada) Ltd and draws on a range of statistical and qualitative inputs.

Quantitative analysis of cost structures and fees in Europe have been added to interviews of leading market practitioners who are either live or are soon to be live using a centralised platform for European settlements. The information is provided for information purposes only.

All findings contained herein have been compiled from sources believed to be reliable, but, although all reasonable care has been taken to ensure that the information contained herein is not untrue or misleading, we make no representation that it is accurate or complete and it should not be relied upon as such. All opinions and estimates included herein constitute our judgment as at the date of this report and are subject to change without notice.

Unless we provide express prior written consent, no part of this report should be reproduced or distributed. We do not accept any liability if this report is used for an alternative purpose from which it is intended, nor to any third party in respect of this report.

This document must not be considered as an offer to sell or a solicitation of an offer to buy any product, security or service.

the ValueExchange

Under the leadership of

CIRO · OCRI

Canadian Investment Regulatory Organization

Organisme canadien de réglementation des investissements

IOSCO