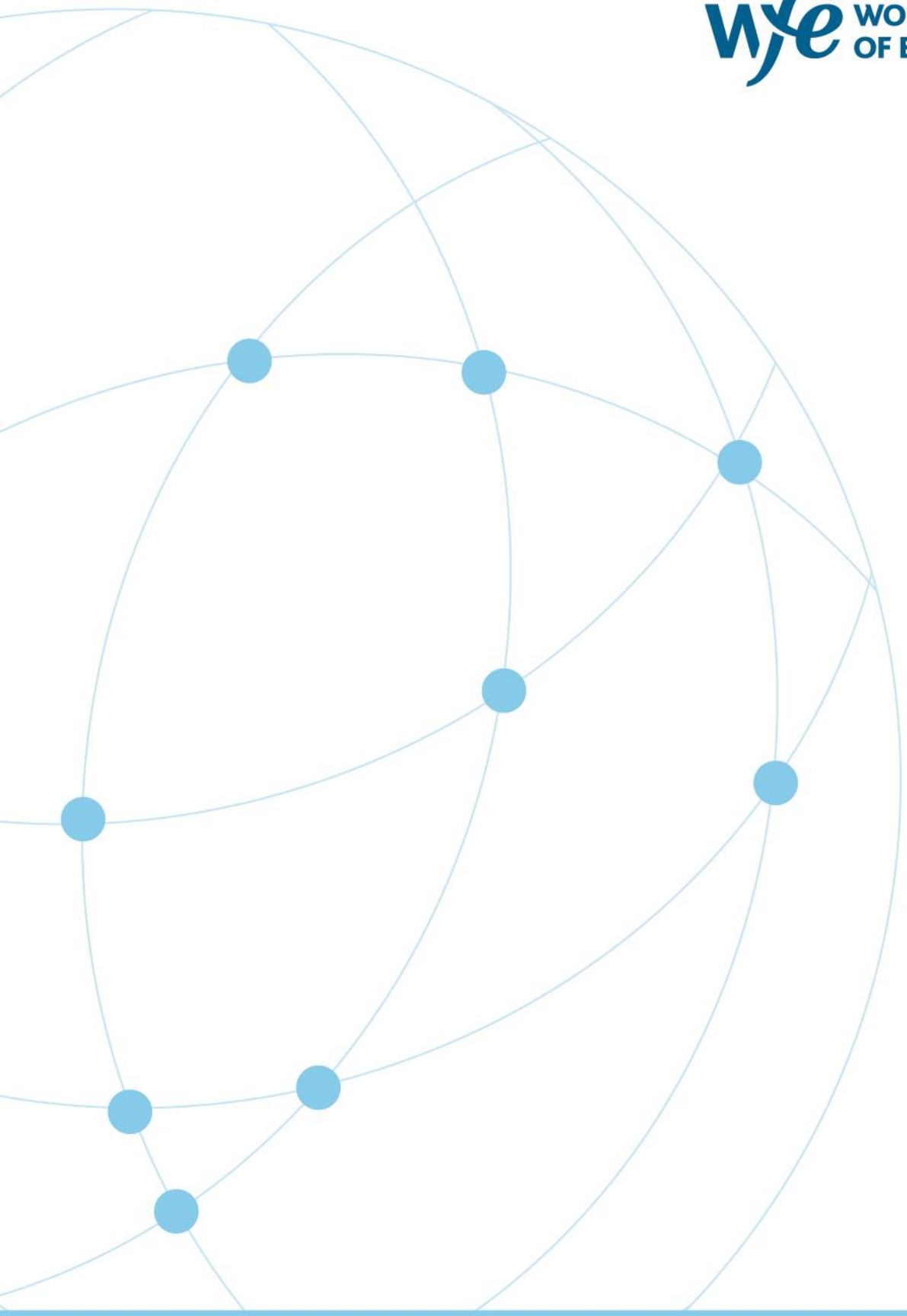
WORLD FEDERATION OF EXCHANGES



Crypto-Asset Custody: A Blueprint for Regulatory and Operational Excellence

28 August 2024

The global consensus is growing in favour of regulation for crypto-assets[1], driven by the growth of over 23,000 cryptocurrencies and daily trade volumes exceeding $275 billion on more than 400 platforms.[2] This rapid expansion in the crypto industry, coupled with high-profile collapses, has heightened the need for regulations aimed at protecting investors, ensuring market integrity, and preventing money laundering.

This paper, the latest from the World Federation of Exchanges examining crypto-assets, specifically addresses the critical issue of crypto-asset custody. This is a concern brought to the forefront by the FTX collapse and longstanding worries about insufficient custody controls in the crypto industry, which pose risks to both market integrity and investor protection.

Due to the lack of a well-defined regulatory framework for crypto-assets globally, the services offered by crypto custodial wallet providers can differ widely. There are regulated crypto custody providers, but the regulatory scheme differs from jurisdiction to jurisdiction, so a patchwork of crypto custody requirements is being created real-time and this causes problems. As a result, what is marketed as "crypto custody services" may not actually provide genuine custody, potentially placing it under a different legal category. This has significant implications for how a customer's assets are treated, especially during insolvency. This inconsistency is not necessarily due to deceptive practices by the service provider, though that could be an issue, but more often stems from legal ambiguities. This uncertainty makes traditional institutions reluctant to enter the crypto sector, thereby hindering market growth.

This paper looks at custody services in traditional financial services and compares them with custody services in crypto-markets trying to find lessons that crypto-custody providers can learn from traditional finance (TradFi) and traditional markets. It is intended to be a valuable resource for those looking to establish crypto-custody solutions. It is also intended as a useful blueprint for policymakers to use when developing regulation in keeping with the "same activity, same risk, same regulation" principle.

The paper concludes that crypto custody providers can:

- Consider segregating client assets to ensure they are protected in the event of a company's bankruptcy.
- Ensure client assets remain bankruptcy-remote, ie, separate from those of other persons, whether legal or natural.
- Address cyber risks through thoughtful technology architecture decisions and the operation of mature cyber security programmes
- Provide more than a place to hold or administer assets.
- Ensure that conflicts of interest are adequately managed and addressed.

[1] There are varying definitions for crypto-assets. For the purposes of this paper, a crypto-asset is:

- a type of private asset that depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value,
- and is not a tokenised version of a traditional asset.

The purpose of this definition is to include the largely unregulated sphere of DLT-based assets but exclude those assets that use DLT but are already regulated.

[2] https://www.nortonrosefulbright.com/en/knowledge/publications/10fba6f7/crypto-asset-regulation-in-hong-kong

- Manage all aspects of operational resilience across their support model.
- Disclose risks in a way that is clear and understandable, particularly for retail customers.
- Have adequate insurance and/or surety bonds and disclose these policies in clear understandable terms.
- Seek independent audits from reputable and credible auditors to provide an assessment of financial statements, process and controls.

What is Custody?

Custody is, in essence, a service consisting of holding, and usually administering, assets on behalf of third parties. Custody services exist in traditional financial services as a means to identify ownership, facilitate transfer and asset servicing and to securely hold assets to prevent theft or loss. In TradFi, custodians may hold equities, bonds, or other assets in electronic or physical form on behalf of end users.

Custody services have grown and evolved from their early inception in the 1940s[3] into sophisticated services that are no longer simply focused on holding and administering assets. The primary role of a custodian is to ensure secure holding and provide legal certainty over assets. This includes guaranteeing access rights and legal ownership.

Often, the custodian does more than provide asset protection and can manage accounts and transactions, service assets (e.g. dividend collection, ensure compliance with regulation, facilitate lending and manage settlement of transactions).[4]

Whilst custody has been a longstanding part of TradFi, market participants and regulators have recently converged on the value that custodians can offer to clients with crypto-assets – namely, certainty over what you are holding, certainty that you have access to it and legal rights over these assets. The existing marketplace for the institutional safekeeping of digital assets offers a variety of custody options. These options are delivered through diverse approaches and operational setups, leading to differences in how clients interact with, and lay claim to, the assets being safeguarded.

[3] See SEC Investment Advisers Act

[4] In traditional finance, managing the settlement ensuring that access rights of the asset, in Free of Payment (FoP) or both assets, in Delivery versus Payment (DvP), switch to the respective other party, most likely in the internal ledger of the custodian. For a crypto-native audience, this refers to ensuring the transaction is recognised by the consensus protocol of the underlying blockchain up to some definition of finality, which typically involves data being signed with the key controlling the assets that expresses a transfer of ownership on-chain.

Types of Custody Arrangements for Crypto-Assets

Self-Custody	Third-Party Custody
Also known as self-storage, self-custody involves holding crypto-assets directly by the owner, using a personal digital wallet. In this case, the owner is responsible for the safekeeping of their private keys, which are used to access and manage their assets. Self-custody gives an individual complete control of an asset. But with that control comes the risk that they lose or misplace their crypto-assets.	This setup involves a third-party service holding a user's private keys for a cryptocurrency wallet. Users can access their private keys through security measures or passwords provided by the platform. If users forget their password, recovery options are available. The third-party service is responsible for the safekeeping of the keys. However, in practice, many of these so-called third-party custody services are actually run by vertically integrated crypto-trading platforms, not independent third parties.
Hybrid Custody	
Hybrid custody is some combination of self-custody and third-party custody. For example, a typical hybrid custody solution allows users (owners) to retain exclusive control of private-keys and coins while the solution provider is granted limited access of private-keys, governed by some smart contracts. Users can still recover their crypto-assets even when they lose all of their private-keys using these limited access keys stored with the custody provider.	

Lessons from TradFi for Crypto-Asset Custody

The main reason that Bitcoin and other crypto-assets are run via a distributed ledger or blockchain is to address what Nakamoto called "the double spending problem." This is the risk that an individual could spend the same digital coin more than once. It is essentially a credit risk which is addressed in TradFi by clearing through a third party. To solve this problem Nakamoto "proposed a peer-to-peer network using proof-of-work to record a public history of transactions."[5] This is one of the reasons that has made cryptocurrencies so popular. However, crypto investors are often unaware of credit risks associated with custody. This is because they make the assumption that arrangements are similar to those in traditional finance, which is actually not the case most of the time.

Historically, custodial credit risk has been a concern in financial markets, notably with bank deposits and securities at broker-dealers. While traditional markets have mitigated these risks through regulatory measures and insurance, crypto-assets operate largely outside such protective frameworks. The absence of regulation amplifies the risk for crypto-trading platform users.

This next section of the paper looks at various risks to crypto-trading platform users, how these risks are addressed in traditional financial services and how custody can address these risks.

[5] https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

Segregation of Client Assets from Proprietary Assets: *Custody providers can consider segregating client assets to ensure they are protected in the event of a company's bankruptcy.*

Crypto-asset trading platforms often provide custodial services for digital wallets used by their clients. In this setup, clients hand over their private keys or the CTP would create wallets with their own private keys and the client would then transfer their assets into those wallets or buy assets against fiat at the CTP which are then deposited in such wallet. Therefore, the CTP and not the investor are in control of the crypto-asset for safekeeping. While there may be contractual restrictions on the CTPs use of these keys, they are ultimately under the exchange's control and can only be accessed by the client via the exchange's security measures.

CTPs could offer segregated accounts to ensure that client assets are not commingled with company assets or other users assets. This protects users if the CTP goes out of business but also protects users against the company using client assets for their own purposes.

As the next section will elaborate, if the CTP were to collapse, it is often unclear if the crypto-assets held by it —including any funds from non-custodial wallets temporarily held in a custodial manner— would be considered the CTP's property or the client's. In the worst possible outcome, clients wouldn't "own" the cryptocurrency; instead, they would be unsecured creditors, placing them at the back of the line for any potential reimbursement from the exchange's limited assets.

Bankruptcy Protections: *Closely linked to the above, custodians can ensure client assets remain bankruptcy remote and not recognised as part of the bankruptcy estate ensuring clients receive those assets back expeditiously independently of claims from secured or unsecured creditors and shareholders.*

In many jurisdictions there is still ambiguity in regard to how crypto-assets are treated legally. If a jurisdiction does not recognise crypto-assets as property, it is unlikely that crypto-asset owners can lay claim to their crypto-assets in an insolvency situation. Therefore, it is unclear how crypto-assets would be treated as part of bankruptcy proceedings and how those cases would proceed through local court systems before being repaid to clients.

This is not a universal situation. In some jurisdictions, legal and regulatory frameworks have been established to address these concerns. For instance, the Swiss Distributed Ledger Technology (DLT) law and the upcoming Zukunftsfinanzierungsgesetz in Germany have created clear legal frameworks for the segregation of crypto-assets in the event of bankruptcy. These laws ensure that in such jurisdictions, the assets held in custody would not automatically be considered the CTP's property in the event of its collapse. Instead, they provide mechanisms to treat these assets as separate from the exchange's property, offering better protection to the clients. Therefore, while the risk of clients being treated as unsecured creditors in the event of an exchange's collapse exists, it is not a universal conclusion and varies significantly depending on the jurisdiction.

We would urge policymakers to follow the Swiss and German lead but alternatively, similar to measures taken in TradFi, firms can take care to create legal structures that are 'bankruptcy remote.' This is where a legal structure is designed to minimise the risk that a specific entity or asset will be

drawn into bankruptcy proceedings if another related entity faces financial distress. The purpose of this is to protect certain assets (such as client assets) from the claims of creditors in the event of bankruptcy.

Cyber-security: *Crypto custody providers can address cyber risks with holding crypto-assets through thoughtful technology architecture decisions and the operation of mature cyber security programmes.*

As witnessed through the numerous cyber breaches plaguing the crypto industry[6], the risk of loss of client assets as a result of a cyber breach remains one of the pre-eminent risks for Crypto-Asset Trading Platforms (CTPs) and crypto-asset service providers. This is well reflected in the detailed requirements of existing regulatory frameworks in aligning towards well established cyber security standards such as ISO27000 and NIST. However, it should be recognised that the risk profile of crypto-asset service providers differs significantly given their business model, market infrastructure and choice of technology stack.

One of the natural reactions of individuals concerned with cyber-security or theft of their assets has been to trust no one but themselves and apply a self-custody solution. Private hacks can and still do occur, though the volumes hacked are dwarfed by hacks targeted at CeFi and DeFi platforms and protocols.[7] Much like keeping physical commodities or cash in a safe, there is a risk with self-custody services. If you lose your private keys, you will lose access to your crypto-assets.

WFE members are well-versed in servicing TradFi markets around the world, in particular, operating exchanges, clearing houses and central securities depositories. These business models generally operate across private networks to service their members. Therefore, these critical national infrastructure services are typically not internet facing providing dedicated networks for institutional players.

Whilst securing crypto assets is qualitatively different from the typical cyber security problems in the traditional world cyber security risks faced by crypto-asset service providers can be addressed by following the same principles that WFE members use to address these risks today in traditional markets. In particular, through thoughtful technology architecture decisions and the operation of mature cyber security programmes covering all of the same domains already established in ISO and NIST[8] standards.

Intermediaries providing hosted wallet services for the custody of client assets are implementing advanced security controls to ensure the secure movement of assets. These controls are structured to necessitate individual approvals from different operators within the organisation, enhancing protection against insider threats and collusion. The key aspect of these security measures is that they require multiple verifications for a transaction to proceed, ensuring that no single individual or group can unilaterally move assets. This approach is crucial in maintaining the integrity and security of asset

[6] See Molly White's timeline of events: https://web3isgoinggreat.com/
[7] https://go.chainalysis.com/2023-crypto-crime-report.html

transfers, with systems designed to prevent any asset movement on-chain without the necessary approvals.

Compliance Programmes: *Custody solutions in the crypto-assets space can, like their counterparts in TradFi, provide more than a place to hold or administer assets.*

For the crypto markets, compliance programmes provided by custody providers, combine both traditional market surveillance and fiat transaction monitoring with 'on-chain' analytics capabilities. As blockchain transactions are immutable (or irreversible) crypto-assets service providers, typically supported by a specialist on-chain analytics tool, are able to assess the risk of assets flowing into and out of their environment. This enables them to adhere to and enforce sanctions controls for known wallet addresses, entities, individuals or jurisdictions attempting to access those services.

Additionally crypto-assets service providers can analyse the transaction history for assets to view and assess the risks associated with 'funds' (in this case in the form of crypto assets) flowing from multiple transaction hops before arriving into the crypto-assets service providers environment. This allows platforms to manage assets that may have been the proceeds of crime (for instance acquired through a cyber hack) or passed through a mixer tool in an attempt to conceal the history of those assets. It should be noted that whilst inbound assets flowing into the crypto-trading platform (CTP) hosted wallets cannot be blocked they can be managed through crypto-assets service provider's[9] internal ledger effectively blocking access to assets flagged as sanctioned, terrorist financing or other high-risk categories. The Financial Action Taskforce (FATF) travel rule is particularly important in facilitating this.[10]

Conflicts of Interest Management: *Custody services should ensure that conflicts of interest are adequately managed and addressed. CTPs could also make use of third-party custodians or pursue legal separation where the equivalent is required in local regulations for TradFi.*

Crypto-asset trading platforms with vertically integrated business models have increasingly come under scrutiny with examples of CTPs issuing native coins, operating broker-dealer services, conducting proprietary trading, clearing and settlement activities and custody services. This model in an unregulated environment has proven fraught with hazards and lacking in necessary investor protection. There needs to be strong separations in place and no ambiguity for the bankruptcy remoteness of assets and professionalism of management. Adequate controls in the form of strong governance measures, ethical walls and policies and procedures addressing and - where possible - minimising potential conflicts of interest should be undertaken. Market structure, license and regulatory frameworks have evolved over centuries to address these exact risks, learning from market

[10] Under the crypto Travel Rule, CTPs must share customer information with each other when transferring crypto above a certain threshold. Information must include the following such that illicit actors can be traced:

1. Name and wallet address of the sender
2. Sender's physical address, national identity number, customer identity number, or date and place of birth
3. Name and wallet address of the recipient.

events that whilst technologically different are thematically identical. Where required for equivalents in TradFi, regulators and firms could require separate registration and regulatory frameworks.

Operational Resilience: *Custodians can manage all aspects of operational resilience across their support model, technology and cyber operations and third-party dependencies to ensure clients have access to their assets within custody at any point.*

Custodians, and indeed all crypto-asset service providers, should follow established practice for enterprise risk and operational resilience. For example, they should define and identify key business services and critical functions. After identifying these services and functions, custodians should set impact tolerances and risk metrics to try to forecast any possible disruptions.

Furthermore, those entities operating in the capacity of a bank or financial institution with fiduciary responsibility must ensure financial soundness and typically meet a regulatory capital requirement. These requirements may be tied to assets under custody, transmitted assets (movements on/off the platform) and wind-down needs sized to cover operating costs for a certain time period enabling a smooth wind-down and transition of client assets to an agreed alternative service provider should the custodian counterparty fail.

Clear Disclosure of Risks: *Custodians can disclose risks in a way that is clear and understandable, particularly for retail customers.*

The importance of adequate risk disclosures is an integral part of investor protection helping to educate investors to the risks of the asset class and operations of the custodian. The means by which custodians deliver their services to clients are all differentiated in some way with associated risks which need to be clearly articulated to potential and existing clients.

Other than gaining a clear understanding of how client assets are safeguarded (including the choice of wallet infrastructure, signing approach, etc.) some custodians may operate models with sub-custodians either performing part of the service (for example being used as a cold storage partner) or being the sole technology provider to that custodian. Often these details can be found in the fine print alongside important information such as investor protections in the instance of the custodian bankruptcy.

Insurance**:** *Custodians can have adequate insurance and/or surety bonds and disclose these policies in clear understandable terms.*

Insurance is an important part of the controls framework for custodians. It provides additional comfort that in the unfortunate instance of a loss, subject to determination of negligence, insurers may cover part or all of the value of those assets lost.

Custodians may be required by their regulators to place insurance and/or surety bonds as part of meeting licensing requirements. It should be noted that insurance policies held by custodians are typically not one-for-one covering all assets under custody as this is commercially unviable. However, given the significant role of these insurance policies in providing assurance to clients, greater

transparency is needed in this area. It would be beneficial for custodians to disclose more detailed information about their insurance policies, including the extent of coverage and the specific terms and conditions. Such transparency would help clients better understand the level of risk protection provided and make more informed decisions when selecting a custodian

Incumbent crypto native custodians have tended to use headline insurance cover limits as a key component of their marketing and sales materials often failing to disclose constraints of those policies – the types of events covered, those that are out of scope, the maximum single event cover etc.

Independent Audit: *Custodians can seek independent audits from reputable and credible auditors to provide an assessment of financial statements, process and controls.*

Many platforms have over the last year, announced their willingness to release audited Proof of Reserves (PoR) to provide transparency about company holdings and liquidity. However, it must be stated that PoR is not sufficient to prove solvency or that misuse of customer funds isn't taking place. PoR needs to be accompanied by Proof of Liabilities (PoL) that demonstrates the amount owed to depositors.

First, PoR may be gamed if just taken as a snapshot, as funds may be borrowed prior to the snapshot, and returned to their rightful owner after this. PoR must be fully audited and must involve the constant monitoring of blockchain addresses. This is addressable by requiring minimum standards (such as audits) for PoR across the industry, or taking snapshots simultaneously (ie, at the same timestamp) for all platforms.

Second, PoL are important to quantify total customer deposits, however, they do not highlight any off-chain or off-balance sheet liabilities, which may be hidden. Proper auditing by financial auditors could help to resolve this issue, though of course there are limits to what an audit can achieve. Therefore, proper regulation and supervision is needed as another pillar.

Independent audits can help to provide an objective and unbiased assessment of the accuracy, reliability, and transparency of financial statements, processes, controls, and other relevant information. Audits are not a panacea. We have seen examples in the past where auditors have either missed issues or been lied to by their clients. Nevertheless, they help to provide an extra layer of trust and credibility when undertaken by reputable, credible auditors.

CTPs could also publish their assets under custody (AUC). Regulators could request further access to AUC down to individual account level, i.e. the internal records of the CTP. CTPs could also disclose their on-chain wallets, like many do today. These could be reconciled to determine if the number of assets held on chain matches the number on internal records.

Conclusion

This document has examined key principles of the custody industry and highlighted its ongoing transformation in the digital realm. It aims to shed light on the significant distinctions between

traditional custody and digital asset custody for the purposes of developing more robust custody solutions going forward.

In summary, the proposed suggestions are that crypto custody providers can:

- Consider segregating client assets to ensure they are protected in the event of a company's bankruptcy.
- Ensure client assets remain bankruptcy-remote, ie, separate from those of other persons, whether legal or natural.
- Address cyber risks through thoughtful technology architecture decisions and the operation of mature cyber security programmes
- Provide more than a place to hold or administer assets.
- Ensure that conflicts of interest are adequately managed and addressed.
- Manage all aspects of operational resilience across their support model.
- Disclose risks in a way that is clear and understandable, particularly for retail customers.
- Have adequate insurance and/or surety bonds and disclose these policies in clear understandable terms.
- Seek independent audits from reputable and credible auditors to provide an assessment of financial statements, process and controls.

By examining the principles set out above, governments, regulators and industry participants can focus on the key issues relating to crypto-asset custody.

Background

Established in 1961, the WFE is the global industry association for exchanges and clearing houses. Headquartered in London, it represents the providers of over 250 pieces of market infrastructure, including standalone CCPs that are not part of exchange groups. Of our members, 36% are in Asia-Pacific, 43% in EMEA and 21% in the Americas. The WFE's 87 member CCPs and clearing services collectively ensure that risk takers post some $1.3 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. The exchanges covered by WFE data are home to over 55,000 listed companies, and the market capitalization of these entities is over $111tr; around $124tr in trading annually passes through WFE members (at end-2023).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back more than 40 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policy makers, regulators and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

James Auliffe, Manager, Regulatory Affairs: jauliffe@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

or

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org.