UNBOUND

WHERE SECURITY IS KEY

INSTITUTIONAL-GRADE CUSTODY:

SECURITY CONSIDERATIONS FOR DIGITAL ASSETS

TABLE OF CONTENTS

INTRODUCTION

In traditional financial markets, custodians are the trusted intermediaries between asset issuers and investors. They serve investor clients by facilitating their participation in financial markets and securing their asset ownership.

The incorporation of digital assets into the mainstream financial services industry (FIS) presents unique challenges. More than simply adopting a new type of asset into the market, digital asset adoption represents the fusion of two distinct and different worlds: the conservative, traditional, bureaucratic financial sector; and the iconoclastic, ever-changing, cutting-edge world of digital assets, tokenized assets, and cryptocurrencies.

Unbound Tech works with major global banks in the financial sector as well as the world's largest crypto-native institutions. This guide presents an amalgam of expertise from both worlds, in the hope that traditional financial sector professionals will gain a greater understanding of the unique challenges ahead in the institutional adoption of digital assets.

DIGITAL ASSET DIFFERENTIATORS:
What makes securing digital assets so difficult?

The evolution to dematerialized (fiat) securities and electronic book-entry settlements has expanded custodians' role to include not only physical asset protection but also secure management of digital records – and catapulted them into the world of cybersecurity best practices and IT infrastructure.

Now, custodians working with digital assets must understand the nuances of crypto assets, public key cryptography, and blockchain in order to build the best IT infrastructure for asset protection – and, ergo, to best serve clientele. We will explore the challenges of securing digital assets in this context below.

Blockchain: Fewer safety nets

The primary challenge of blockchain-based assets is the lack of ability to "roll back" asset transfers. Two properties of the digital asset landscape prevent rollbacks: the technology itself, and the frontier nature of tokenized asset regulation and normalization.

Fiat currencies are protected by several measures:

- Physical keys and credentials: a password to gain access to a bank account is a classic example of this (and physical keys to access a physical vault).
- Best practices in FIS, based on over 500 years' worth of standardized accounting practices which have become global standards.
- Mandatory Know-Your-Customer (KYC) processes.
- Mandatory Anti-Money-Laundering (AML) validation processes.
- The ability to roll back money transfers.
- Standards set and managed by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).
- Clearing and settlement processes.

Let's address these challenges, one by one.

Immutability Principle

Digital assets and blockchain data are keys by their very nature. With cryptocurrencies, the keys constitute the asset; this means that transactions cannot be rolled back – and one does not need to have physical access to the asset in order to steal it in a few keystrokes.

Due to the immutability principle that is inherent in the blockchain design, once a transaction is recorded, it cannot be rolled back; there are no do-overs. This presents issues relating to fraud and anti-money-laundering (AML) protection.

One misuse of a key is enough to lose it all; the malicious actor does not even need to have the key in his/her physical possession in order to gain ownership of the asset. This presents unique challenges in terms of protecting data and user privacy, considering that the decentralized ledger is available for the public to view (in the case of traditional cryptocurrencies).

Emerging market, fledgling standards

A bigger issue is the lack of standardization and regulation for digital assets, which are only now being considered "assets" in traditional financial forums.

While best practices for accounting have existed since the emergence of the ledger system some 500 years ago, a system based on physical asset storage, usage, and transfer also had different definitions in terms of what constitutes "ownership" – and certainly security.

With digital assets and their unique technological vulnerabilities, proper security and handling is critical not only to the future of the holders, but to the future of the industry itself.

In the meantime, the traditional financial world is redefining its standards to include digital assets – but based on the legal infrastructure of fiat. How do you secure an asset without centralized clearing/settlement processes and no Society for Worldwide Interbank Financial Telecommunication (SWIFT)?

The answer to this question is still being established – but regulation of digital assets demands that they adhere to traditional trappings, whether the technological framework exists or not. Ultimately, *institutions' ability to maintain high security standards* and formalized, professional SLAs will create the same pedigree of service going forward.

SECURING DIGITAL ASSETS:
Key management and Custody types

Types of cryptocurrency custody

There are 3 types of key management for digital asset tokens: **full custody, partial custody,** and **self-custody**. Each has differing implications in terms of key management – and, in practical terms, regulatory compliance.

Full custody

In full custody solutions, the entrusted institution holds all the asset keys and manages them – acting on the customer's behalf, without his/her direct involvement.

Partial custody

In partial custody solutions, the custodian holds part of the tokenized asset (keys or key shares), with the investor as an active participant in the signing process.

Partial custody solutions vary in terms of level of third-party involvement. Many of them offer additional safeguards which are difficult to build in-house, such as multi-party authentications and backup services.

From a regulatory perspective, partial custody providers may not be considered full custodians if they do not hold/control the majority of the assets being held.

Self-custody

In self-custody solutions, the investor holds the key shares and distributes them among his/her own devices and/or contacts; the custodial provider provides the technical framework for the investor to conduct his/her own key management and has no legal liability.

Custodians that offer their customers self-managed wallets build their own signing and security infrastructure from scratch.

Self-custody solutions present a problem in terms of compliance and regulation. Many regulations demand both a custodial service and a broker, i.e. a third party involved to audit transactions and ensure compliance.

Wallet types

Fiat custodians should also be aware of the different wallet types for storage and transfer of digital assets. Each wallet type presents unique business considerations; the entire spectrum constitutes a tradeoff between security and usability.

The details of each wallet type, and their place in this spectrum, are outlined in the chart below.

Cold Wallets	Warm Wallets	Hot Wallets
▪ Air-gapped, physical storage ▪ Offline approvers ▪ Business consideration: security	▪ Offline and online approvers ▪ Combination of offline/online storage ▪ Can vary in how transactions are conducted ▪ Business considerations: different trade-offs between perational efficiency, liquidity, and security	▪ Online, digital storage ▪ Online approvers ▪ Business consideration: liquidity

Digital asset custodians

Digital asset trading platforms and exchanges

As illustrated above, business considerations drive differing digital asset institutions toward different wallet types.

Traditional custodians generally follow best practices in the fiat world by sticking to "cold" wallets and physical storage; there are secure "warm" or partially-connected wallet solutions available which meet the same standards as a premium custody solution which are backed by, and installed with, cryptographic expertise.

REGULATIONS

Regulatory compliance requirements will vary from region to region, but there are a few common denominators for any successful custody solution:

- Account-based vault support – most custodial solutions require vaults for individual customers, to ensure the veracity of transactions being conducted by the account holder. (This contrasts with exchanges, for example, which often hold one vault per tokenized asset.)
- Segregation of authorities – defined roles for each approver and the separation of approving entities between separate people. This helps decrease probability of inside issues – for example, inside fraud, or inside attacks.
- Tamper proof auditing – while the specifics of how and when audits are conducted and which information is subject to auditing, any digital custody system requires automatic transaction logging. Cryptographic verification of approvers' identity, the assets being held, and any transactions therein ensures tamper-proof audit logs to withstand even the most rigorous of inspections.

We recommend that any custody provider review the applicability of fiat custodian laws to digital assets in their country or region.

CONCLUSION

Custodians accustomed to working with fiat or other traditional assets face significant challenges with incorporating digital assets into their portfolios. Potential adopters of digital assets into their custodial service offerings must attain a greater understanding of how blockchain-based assets work vis-à-vis ownership and transfer, different wallet types, and basic principles of key management and security.

We recommend that custodians carefully check their local regulations and best practices regarding safe asset storage before choosing a digital asset custody solution – and consider the role of their institution in the digital asset storage and transfer processes.

For more information on which features to consider for premium-grade, full-custody protection of digital assets, talk to one of our experts.

Schedule a 1:1 Demo

Unbound Tech

www.unboundtech.com | contact@unboundtech.com

Follow Us

UNBOUND

WHERE SECURITY IS KEY