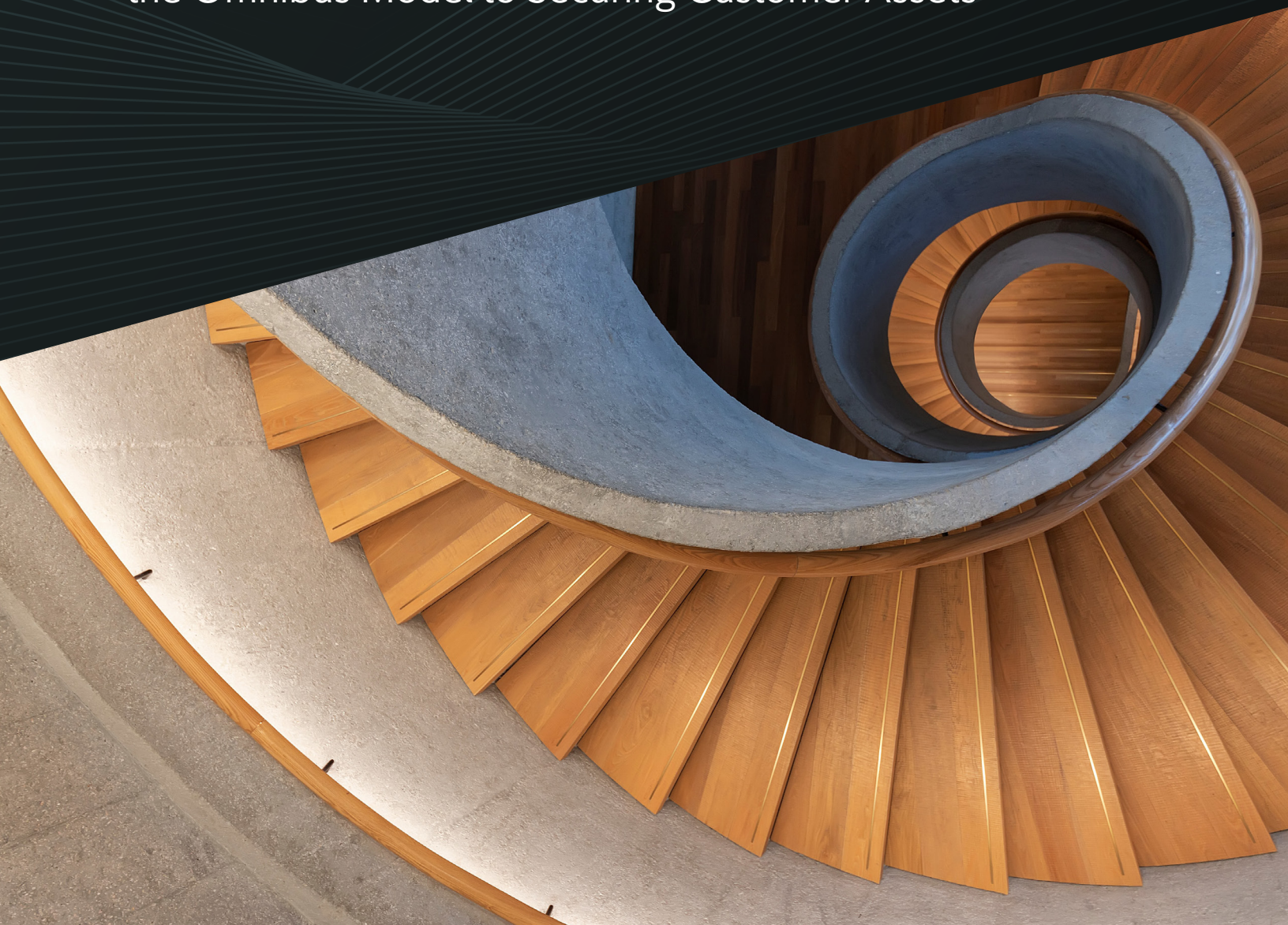
Fidelity DIGITAL ASSETS℠

AUGUST 2023

The Omnibus Model for Custody

How & Why Digital Asset Custodians Apply the Omnibus Model to Securing Customer Assets



Background

In January 2020, we described the origins of the omnibus custody model in traditional finance and its application to digital assets. Over three years later, the omnibus model remains a compelling and beneficial model for digital asset custodians (and investors). While the omnibus model has remained consistent, the digital asset market has evolved rapidly in recent years, with various innovations to custody models and technologies. While we encourage those seeking a detailed understanding of omnibus custody to read the earlier overview, we aim to reiterate many of the benefits of the omnibus model for digital asset custody below while contextualizing the approach within today's current digital asset market.

Introduction

Private key management is a critical component of investing directly in digital assets and choosing a custodian. Key management determines how digital assets, such as bitcoin and ether, are held and secured. The two most prominent models are omnibus[1] and segregated.

> In this piece, we provide an updated explanation of the omnibus custody model and explore how and why digital asset custodians may choose the omnibus model to secure customer assets.

Custody of Digital Assets

In the digital asset industry, custodians store digital assets in proprietary online (hot) and offline (cold) storage solutions instead of outsourcing custody to a depository. Digital asset custodians face an even greater responsibility than custodians of traditional assets to implement robust asset storage processes because digital assets are bearer instruments (like hard cash)–they cannot be recovered if lost or stolen.

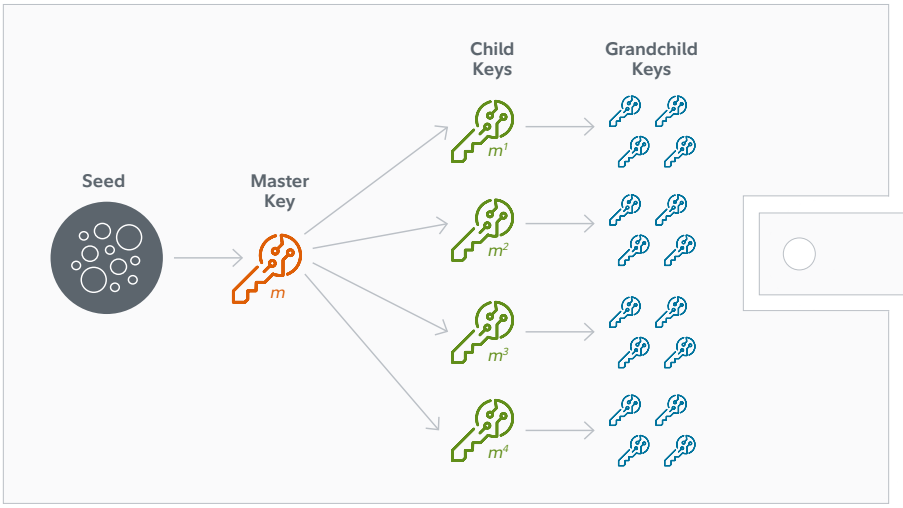
What is the Omnibus Model for Custody?

An omnibus[1] model combines clients' assets and spreads them across multiple digital asset private and public key pair groups and segregates funds at the books and records level. Conversely, we interpret a truly segregated model to be one that separates and accounts for client assets on-chain and in a books and records system, including in separate private and public key pair groups on-chain per client.

Under an omnibus model, the custodian establishes segregation at the books and records level in its systems to track assets held by each client, just as Depository Trust Company (DTC)[2] participants account for individuals and funds holding securities at the depository in the participants' names. Some traditional financial service providers have decades of experience with robust bookkeeping processes for maintaining segregation at the books and records level for traditional assets, which can then be extended to digital assets custody. Externally audited financial control environments and client statements provide additional assurance that funds are secure and data is accurate.

Custodians employing the omnibus model may use the hierarchical deterministic (HD) protocol to generate key pairs[3] and addresses that are maintained by the custodian in its name. The HD protocol was introduced in Bitcoin Improvement Proposal 32 (BIP32)[4] to simplify the process of generating, backing up, and organizing private and public key pairs in a tree-like structure.[5] Under the HD structure, master private keys and master public addresses are used to generate a near-infinite number of child keys that can generate their own child keys (see Figure 1).

Figure 1: HD Tree Structure



Source: The Evolution of Bitcoin Key Management

Note: Digital asset custodians may distribute assets across multiple key pairs, sub-accounts (child keys), and addresses to mitigate risk. When discussing digital asset custody, the term "omnibus" does not necessarily mean that all assets are held within a single key pair. In fact, client assets are commonly managed with multiple sets of key pairs to enhance overall security while maintaining the benefits of the omnibus model. Additionally, each individual blockchain address can be controlled by "multisignature" and require multiple private keys to send funds from a single address.

To generate a new master key pair, custodians often conduct a key ceremony. Key ceremonies are highly orchestrated processes that involve multiple stakeholders and can begin months in advance. Internal and independent external auditors may serve as witnesses during the ceremony to ensure that a custodian follows a secure, tamper-proof, rules-based process for generating master key pairs that will be used to store client funds.

The custodian may move assets within and between key pairs and across different storage environments to maintain a particular ratio of total assets in online (hot) and offline (cold) storage[6] or to limit the portion of funds within any key pair and/or address.

Why Use the Omnibus Model?

The omnibus model offers distinct operational, risk management, and security benefits for key generation and management, liquidity, transaction fees, and privacy to provide efficient, scalable, and secure digital asset storage.

Differences in key generation and management

The omnibus model may provide greater control of risk management by offering custodians the flexibility to manage key generation, replacement, and distribution of assets across different storage methods. By using an omnibus structure, custodians can control the number of key pairings they manage. Custodians can also establish a threshold for funds stored within each pairing. Custodians that offer clients absolute segregation would not be able to control or limit the number of key pairs that they manage or the way funds are distributed across key pairs, which we interpret as separate groups of master key pairs (online and offline) for each client.

A common misconception is that the omnibus model results in a "honeypot" of assets because omnibus custodians store assets under a single master key pair. In practice, omnibus custodians may have more groups of master key pairs than clients on the platform, where a group constitutes key pairs from the different storage environments (online to completely offline). For example, for simplicity's sake, consider an omnibus custodian that has a single client with $2 billion in assets. The custodian may choose to distribute the assets in $100 million tranches over 20 key pair groups (and divide each $100 million tranche further across the separate storage environments). Because omnibus custodians do not need to tie key pairs to clients, they can more effectively manage risk by using their discretion to decide how many key pair groups to generate and how to best distribute assets across them.

Under a segregated model, the custodian has less control over the process and risk parameters.

Omnibus vs. Segregated Model

	Omnibus	Segregated
Liquidity	Custodians can minimize online (hot) wallet exposure and simultaneously maintain a liquid position to meet trading or withdrawal needs in a timely manner. Additionally, when multiple clients request withdrawals, the custodian can minimize the number of transactions and visits required to move coins out of offline cold storage.	Digital assets are separated on a per-client basis rather than being shared by the platform. The custodian executes multiple separate coin transfers from offline-to-online storage—a complex process that requires more coordination of people and processes to constitute a key pair and extract the funds from an offline storage environment. Custodians *could* avoid much of this operational work by leaving more digital assets in hot storage, but this presents increased security risk.
Transaction Fees	More flexibility in managing fees using tools, such as aggregation and batching. Custodians determine the most efficient movement of coins between different storage environments, so there are fewer/lower on-chain transaction fees.	Maintaining strict segregation of wallets and funds means more transactions, and therefore, fees.
Privacy	Provide clients with enhanced privacy. Since coins are not transferred to absolutely segregated addresses, addresses cannot be linked to individual clients and address balances do not correspond to the exact value of individual client deposits.	Segregated addresses and identities are precisely linked, leaving digital money/transaction trails.

Impact on Liquidity

Segregated: Consider a scenario in which a custodian with segregated key pairs has 20 clients with $50,000 in assets each. Each client has a segregated wallet with 2% ($1,000) in online storage and 98% ($49,000) in offline storage. Three clients each instruct the custodian to withdraw $5,000 in assets. Given the segregated structure, the custodian cannot dip into another customer's online storage to complete the request. Thus, the custodian would have to execute three separate fund transfers ($3,000 per client) from offline-to-online storage—a complex process that requires more coordination of people and processes to constitute a key pair and extract the coins from an offline storage environment.

Omnibus: With an omnibus structure, custodians can minimize online (hot) wallet exposure and simultaneously maintain a liquid position to meet trading or withdrawal needs in a timely manner. Additionally, when multiple clients request withdrawals, the custodian can minimize the number of transactions and visits required to move coins out of offline cold storage.

Consider a hypothetical custodian with an omnibus model and the same risk parameters (2% of assets in online storage and 98% in offline storage) that receives the same instructions from three clients to withdraw $5,000 in assets each. The custodian would have $20,000 in online storage and $980,000 in offline storage. The custodian would be able to meet each client's withdrawal demands without touching funds in offline

storage at the time of withdrawal because they have more than the total withdrawal sum ($15,000) in omnibus online storage. After processing the client's request, the custodian could rebalance funds across the storage environments from assets of all clients per risk parameters.

Note: As mentioned above, under the omnibus model, the $20,000 may be distributed across *multiple* online storage key pairings so as not to create a single point of vulnerability—e.g., $5,000 across four key pairs. The difference is that the custodian that uses an omnibus model can access each of these four wallets to meet liquidity needs.

Transaction Fee Efficiencies

Custodians execute on-chain transactions as a part of their key management process (i.e., moving funds between different storage environments). Using omnibus wallets gives custodians more flexibility in managing fees using tools, such as aggregation and batching. Also, under the omnibus model, custodians determine the movement of funds between different storage environments, so they cover on-chain transaction fees.

Privacy

Omnibus models also provide clients with enhanced privacy. Since funds are not transferred to absolutely segregated addresses, addresses cannot be linked to individual clients and address balances do not correspond to the exact value of individual client deposits.

Appearance vs. Reality

Some perceived benefits from segregated wallets are often misinterpreted and clients need to perform due dilligence when choosing a custodian to understand exactly what segregated custody entails. There is no guarantee that assets are held by separate master private keys or that the custodian doesn't comingle other clients' assets at the books and records level.

The Introduction of Multiparty Computation

A recently developed model that's gained popularity lately is multiparty computation (MPC). MPC distributes private keys across multiple entities involved in a transaction or asset management. MPC ensures that no single party has complete access to multiple private keys or can manipulate the computation to learn new information. While quite a similar approach to the multisignature (which requires two distinct and separate signature authorizations to move funds from a wallet) signing process, MPC offers the simplicity of single on-blockchain cryptographic signature, but potentially with the enhanced security of multisignature. MPC ensures that a single key is never fully exposed in a single location.

MPC safeguards digital assets by using a combination of hardware and software security measures. While this model offers advantages including privacy, security, and verifiability, there are some challenges, such as complexity and trusted setup, that make MPC less accessible to noncryptography experts and can pose a potential vulnerability if not set up correctly by a trustworthy or properly secured third party. It is also worth noting that a key aspect of any custodian's services are the operational process and controls surrounding the technical custodial solution, including cyber and technical controls and the various audit functions needed to validate these controls. While MPC is undoubtedly an innovative technology, it still requires the broader operational elements that would complement both the omnibus and segregated wallet structure.

Furthermore, MPC has presented technical challenges when being used with certified Hardware Security Modules, and the underlying cryptographic algorithms are still new without the years of battle testing, expert code review, and official certifications as the cryptography underlying traditional financial services cybersecurity. As previously highlighted, similar to the segregated wallet model, MPC introduces technical complexities that may weaken or add unnecessary complexity to the operations surrounding the custodial solution.

Understanding the SEC Proposals for RIA Custody

Given recent industry events and the ongoing maturation of digital assets market participants, there is more emphasis than ever on the role of third-party custodians and the importance that they have for financial institutions and intermediaries. In February 2023, the SEC proposed an "Enhanced Safeguarding Rule for Registered Investment Advisers,"[7] which included additional guidance for digital assets. While this proposal does not offer RIAs any guidance on what specific custodial model (i.e., omnibus vs. segregated) to seek when enlisting a custodian, it may help to understand what regulators are seeking when defining a qualified custodian.

If approved, the SEC proposal would expand the scope of federal custody requirements by registered investment advisers to include digital assets, a change that would require some digital asset custodians, exchanges, and service providers to gain further regulatory approval. Notably, RIA-managed digital assets would have to be kept with qualified custodians, such as certain banks or broker-dealers, or institutions wishing to custody any digital assets would have to hold the bank charters or qualify as a registered broker-dealer, futures commission merchant, or a specific kind of trust or foreign financial institution.

While we await further guidance, intermediaries and institutions may choose to proactively activate some of the SEC's guidance, eliminating self-custody measures and enlisting a digital asset custodian that aligns with many of the attributes of a qualified custodian for traditional assets.

Conclusion

Finding the right custody solution for digital assets is essential for every individual or institutional investor. While some purists may prefer a segregated model, a robust omnibus model can simultaneously provide efficiency to digital asset custodians as well as enhanced risk management and security assurances to clients. A custodian using an omnibus model can distribute funds across multiple key pairs and addresses to avoid creating a proverbial "honeypot." However, not all omnibus and segregated models are created equal. Clients evaluating digital asset custodians should investigate the extent to which a custody solution is "omnibus" or "segregated" to get an accurate idea of the advantages and shortcomings of each structure.

1 The "omni" in omnibus means many and "bus" refers to businesses — many businesses.

2 Will Kenton. "Depository Trust Company (DTC)." November 2019 https://www.investopedia.com/terms/d/dtc.asp

3 A key pair refers to a private key and corresponding public key. The private key is used to spend funds (by creating a unique digital signature to sign each transaction) and the public key is used to receive funds. The private key must be kept secret to prevent funds from being compromised. The public key is used to generate public addresses that are shared to receive funds. A private key is often compared to a bank account pin that must be protected and a public key is referred to as a bank account number.

4 BIP stands for Bitcoin Improvement Proposal. It is a standard for proposing changes to Bitcoin or the BIP process. For a deeper overview of the BIP process, we suggest this piece by Bitcoin Magazine: What is a Bitcoin Improvement Proposal (BIP)?

5 Users can restore subsequent child public and private keys and corresponding addresses with a backup of the master private key.

6 Online storage is often referred to as "hot" storage and offline storage is referred to as "cold" storage.

7 https://www.sec.gov/news/press-release/2023-30

FDA LTD is registered with the Financial Conduct Authority under the U.K.'s Money Laundering Regulations. The Financial Ombudsman Service and the Financial Services Compensation Scheme do not apply to the cryptoasset activities carried on by FDA LTD.

To the extent this communication constitutes a financial promotion in the U.K., it is issued only to, or directed only at, persons who are: (i) investment professionals within the meaning of Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"); (ii) high net worth companies and certain other entities falling within Article 49 of the FPO; and (iii) any other persons to whom it may lawfully be communicated.

This information is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to local law or regulation. Persons accessing this information are required to inform themselves about and observe such restrictions.

Digital assets are speculative and highly volatile, can become illiquid at any time, and are for investors with a high-risk tolerance. Investors in digital assets could lose the entire value of their investment.

FDAS LLC and FDA LTD do not provide tax, legal, investment, or accounting advice. This material is not intended to provide, and should not be relied on, for tax, legal, or accounting advice. Tax laws and regulations are complex and subject to change. You should consult your own tax, legal, and accounting advisors before engaging in any transaction.

This material may be distributed by the following entities, none of whom offer direct exposure, nor provide clearing or custody for digital assets: Fidelity Distributors Company LLC ("FDC"), National Financial Services LLC ("NFS"), or Fidelity Brokerage Services LLC ("FBS"), none of whom offer digital assets nor provide clearing or custody of such assets. FDC, NFS, and FBS, and their representatives, may have a conflict of interest in the products or services mentioned in these materials because they have a financial interest in them, and receive compensation, directly or indirectly, in connection with the management, distribution, and/or servicing of these products or servicesFidelity Digital Assets and the Fidelity Digital Assets logo are service marks of FMR LLC.

1098628.3.0