COTW: Institutional Digital Asset Custody

As a bearer instrument with irreversible transactions, the importance of sound institutional custody for digital assets cannot be understated, especially as the number of digital assets proliferates and new institutions enter the space. We review institutional digital asset custody in this week's Chart of the Week.

The Importance of Crypto Custody: According to a recent survey by Nickel Digital, digital asset security is the top concern for institutional investors and wealth managers contemplating investing in digital assets. Underlying this is the fact that digital assets are bearer instruments and once made, transactions cannot be reversed. As such, a strong digital asset custody foundation is imperative for the continued adoption and potential ubiquity of digital assets. And, this importance should only grow in the future as the number of digital assets increases from the expanding use of blockchain technology and continued tokenization of real world assets. Enter digital asset custodians, who provide cryptocurrency storage and security solutions to enhance security, efficiency, and flexibility.

Crypto Custody Overview: Digital asset custodians don't actually custody digital assets, but rather store and secure the owner's cryptographic public and private keys, the latter of which enables the holder to sign digital asset transactions. Such keys are stored and managed in a customizable cryptocurrency wallet, which may be connected to the internet, known as a hot wallet, or physically isolated from the internet, known as a cold wallet. Hot wallets generally sacrifice security for greater speed, liquidity, and automation, while cold wallets are slower to execute on customer instructions and may require manual inputs to do so, but significantly lower the risk of unauthorized transfers. Institutions typically use a combination of both hot and cold wallets, and the pooling of assets can allow for a greater percentage of assets to be kept in cold storage. In addition, custodians may safeguard the keys on behalf of the institutional client or provide technology solutions enabling safe and efficient self-custody by the client itself. The former, known as a direct custodians, assume much more of the risk, offer top tier customer service to their typically smaller customer bases, are often subject to greater regulation, and may be required to be used by certain customer types (eg. US advisors must use a Qualified Custodian). However, they typically offer fewer assets and services/functionality, introduce counterparty risk, and may not be suitable for speed-based client strategies like high frequency trading. The latter, known as technology providers, introduce more risk as the client is ultimately responsible for maintaining their keys, though typically offer a broader array of assets, access to a greater breadth of

services such as more decentralized finance activities, and often have unique products such as a secure network of customers. Note there are several custodians that offer both direct custody and self-custody technology solutions. Custodians face a bevy of challenges, such as supporting an ever-expanding number of tokens, blockchains, and crypto activities (egs. airdrops, staking, governance, ect.), but bring security, reduced risks, and efficiency to institutions, who are also freed to focus on their core business.

Core Technology Solutions: Digital asset custodians use a variety of technology solutions and control procedures, which are often used in combination with one another and with proprietary solutions. These include:

- Hardware Security Module (HSM): A HSM is a hardened, tamper-resistant, lab-tested, government-certified physical device that secures cryptographic processes such as encryption, decryption, authentication, key management, and others. HSMs are not connected to a client's computer network or the internet, requiring physical access to the HSM to use the keys. For a transaction to occur, client instructions must be combined with the HSM. While difficult to breach, HSMs store keys in one place, constituting a single point of failure, and thus are focused more on key theft rather than fraudulent key usage, though configurations can require authorizations from multiple HSMs in order to sign the transaction.

- Multi-signature (Multisig): Multisig is the process of requiring multiple keys to authorize a digital asset transaction rather than a single signature from one key. Multisig usually requires a majority of the keys associated with an asset to sign the transaction, such as three of five, and may use signatures from different devices (one person signs using their HSM and their mobile phone) or from different parties. Multisig alleviates the single point of failure inherent in HSMs, but has some limitations. It requires varying implementations for different blockchains or may not be supported at all, cannot be changed once implemented, may introduce additional vulnerabilities such as with a poorly coded smart contract, can result in higher transaction fees, and may reveal information about its setup depending on the signature algorithm used.

- Multi-Party Computation (MPC): MPC is a process that splits a private key into key shares that can be distributed across multiple devices, prohibiting a hacker who acquires just one device from obtaining the full key (technically, the entire key is never fully together, even at its generation). MPC is flexible, allowing for multiple authorizers to sign a transaction, complex signing rules to be created, parameters to be changed post-creation, signer shares to be revoked without changing the key, and a mix of hot and cold wallets to be used. In addition, MPC generates a standard digital signature, so they are not only compatible with any blockchain and asset, but also don't reveal any information about the signers. However, despite the technology existing for decades, its practice for use in digital asset custody is newer and therefore less well-tested. Moreover, MPC providers may not be able to get insurance, as they are not fully in control of the private keys. Lastly, HSMs do not support MPC technology, removing a key piece of defense.

- Other: A variety of additional controls, policies, and workflows are instrumental in buttressing

digital asset security, depending on the set up and needs of the client. These include controlling physical access to devices, performing enhanced customer due diligence, whitelisting addresses, implementing transaction time delays, requiring two-factor authentication, acquiring insurance, and following best practices in key generation, rotation, and backup management.

The Business of Custody: The business of digital asset custodians are in many ways similar to those of traditional finance. Direct custodians earn revenue as a percentage of assets under custody (AUC), as well as revenue from other services such as trading and lending fees. Tech providers earn revenue by charging subscription and plan fees, as well from value added services. Digital asset custodians differentiate themselves based on the type of services offered, technology solutions employed, number of assets and activities supported, and level of regulatory oversight, among others. Custodians are under pressure to continually add support for more assets and blockchains, which often requires bespoke integrations and introduces reputational risks, especially for direct custodians, but helps to drive assets under custody. Custodians are also looking to add services to basic custody, trading and borrowing/lending, such as staking, wrapping, and governance participation, both in response to client demand and to drive additional revenue. When evaluating a particular crypto custody business, a traditional multiples analysis, such as enterprise value to AUC or enterprise value to revenue, may be used. In addition, earnings drivers should be assessed, which include both prospects for growth (egs. expected total industry AUC and expected market share) as well as for profitability (egs. value added services for additional cross sell/ pricing power; an evaluation of the competitive environment; scale economies). Liquidity and capital of the balance sheet should be assessed, especially for less regulated institutions. And lastly, catalysts and risks, both industry-wide and company-specific, should also be considered.

The Players: Custody solutions are administered by crypto-native specialized providers, traditional financial institutions, and cryptocurrency exchanges and prime brokers. In addition, security providers may focus on retail or institutional players, though some do both, such as hardware wallet manufacturers Ledger and Trezor or MetaMask with its institutional offering. Lastly, note that digital asset custody is much more fragmented compared to traditional financial custody. We show metrics on various custodians compiled by The Block in **Exhibit 1**, and provide brief overviews of a few select custodians below.

- Copper: Copper is a UK-domiciled digital asset custodian founded in 2018 by Dmitry Tokarev. Copper provides secure custody through its MPC-protected custodial architecture, supports cold, warm, hot and proxy layers, and ensures no single point of failure. Additionally, Copper allows clients to trade directly out of cold storage through its ClearLoop solution, to move assets instantly between 30+ top exchanges, and offers tight trading spreads through API-enabled RFQ/streaming. Copper is a FinCEN registered Money Services Business, is ISO 27001 and Cyber Essential Plus certified and registered, and offers crime insurance through Aon. Copper had $10b in AUC as of September, provides its services to over 400 clients, sees over $50b in monthly notional flow through its infrastructure, and supports over 400 digital assets.

- Anchorage Digital: Anchorage is a US-domiciled digital asset custodian founded in 2017 by Diogo Monica and Nathan McCauley. Anchorage offers customizable HSM-based solutions

that rely on biometric authentication, enhanced outlier detection, and hardware-enforced logic. Anchorage serves banks, market makers, funds, and miners with its services, including custody, trading, staking, governance, and financing. Anchorage is the first US federally-chartered digital asset bank in history and is a Qualified Custodian, allowing SEC-registered investment advisors to meet their obligations under federal law.

- Fireblocks: Fireblocks is a US-domiciled digital asset technology provider founded in 2018 by Michael Shaulov, Pavel Berengoltz, and Idan Ofrat. Fireblocks offers an enterprise-grade platform delivering a secure infrastructure for moving, storing, and issuing digital assets. Fireblocks serves exchanges, custodians, banks, trading desks, hedge funds and more using its patent-pending SGX and MPC technology. Its Fireblocks Network connects to all major exchanges, OTC desks, liquidity providers, and trading venues and offers instant settlement, fiat banking integration, API connectivity, and over 950 tokens and 30 supported protocols. Fireblocks is SOC 2 Type II certified and has a unique insurance policy that covers assets in storage and in transit.

- Qredo: Qredo is a blockchain-based financial markets infrastructure and product suite offering cross-chain liquidity and decentralized custody founded in 2018 by Anthony Foy and Brian Spector. Its layer two blockchain provides layer one interoperability and ultra-fast settlement, while its custody solution utilizes a decentralized, consensus-driven implementation of MPC to distribute private key shares to MPC nodes, decentralizing custody, eliminating counterparty risk, and removing the need for private keys. Additional institutional-grade infrastructure includes a decentralized communications platform, regulatory and compliance solutions, and API connectivity, which additionally facilitate compliant and efficient institutional digital asset participation.

Custody Predictions: The future of digital asset custody is intrinsically tied to the future of crypto, which given the influx of capital and talent and the many benefits crypto offers, is, we believe, in long-term secular expansion. Moreover, crypto custody has many levers for growth, both as a greater percentage of digital assets are custodied and as more digital assets are created through new blockchains and protocols, real world asset tokenization, and the continued success of new and existing categories like stablecoins and NFTs. Regulatory oversight is likely to increase, potentially around AML, licensing requirements, and securities definitions, though over the medium-term, this should encourage more institutional digital asset participation and increase digital asset custody demand. Custody fees will inevitably compress as new competition emerges from crypto-native startups, traditional financial institutions, and new exchange offerings, though there is still plenty of room to continue adding value-added services to push this out. And while new companies will form, we're also likely to see continued acquisitions in the space, perhaps by a large traditional finance custodian looking to jumpstart their business. Though late to the game, these traditional financial custodians should not yet be counted out given their enormous resources, regulated entity status, established trust, and existing client relationships. And, while large, regulated entities should thrive, decentralized implementations should as well, such as with Qredo's decentralized, consensus-driven implementation of MPC. Lastly, permissioned DeFi offerings should proliferate and provide institutional investors access to decentralized finance, such as with Aave Arc/Fireblocks, and offer yet another avenue for growth.

Exhibit 1: Digital Asset Custody Firms

Custodian	Custody Founded	Domicile	Type	Technology	Assets Supported	AUC, $b	AUC Date
Anchorage Digital	2017	US	Direct	HSM	74	Undiscl.	
Bakkt	2018	US	Direct	HSM, Multisig	2	Undiscl.	
Bitcoin Suisse	2017	Switzerland	Direct	Multisig	14	5	Nov '21
BitGo	2013	US	Hybrid	HSM, Multisig	400	64	Nov '21
Coinbase	2018	US	Direct	MPC	140	140	Sep '21
Copper	2018	UK	Direct	HSM, MPC	400	10	Sep '21
Fidelity Digital Assets	2019	US	Direct	Undisclosed	1	Undiscl.	
Fireblocks	2018	US	Tech Provider	MPC	1,500	NA	
Gemini	2019	US	Direct	HSM, MPC	74	30	Jun '21
Genesis	2020	US	Direct	MPC	20	Undiscl.	
Hex Trust	2018	Hong Kong	Hybrid	HSM, Undisclosed	100	2	Oct '21
Ledger	2019	France	Tech Provider	HSM	1,500	NA	
NYDIG	2017	US	Direct	Undisclosed	1	6	May '21
Qredo	2019	UK	Tech Provider	MPC	15	NA	
SEBA Bank	2018	Switzerland	Direct	HSM, Multisig	11	Undiscl.	
Silvergate	2020	US	Direct	Undisclosed	Undisclosed	11	Oct '21

Source: The Block Research, Company Websites, GSR

Author: Brian Rudick, Senior Strategist

Sources

[Fireblocks: Digital Asset Custody 101: Its Key Role in Expanding Cryptocurrencies]
[The Block: Institutional Custody for Digital Assets: A Primer]
[The Block: 2022 Digital Asset Outlook (Custody Section)]
[Unbound Security: Technical Whitepaper]
[Gemini: A Guide to Crypto Custody]

About GSR

GSR is a global leader in digital asset trading, market making, OTC derivatives, and investments. We operate in a culture of excellence and leverage our first-rate reputation, deep relationships and proprietary trading technology to move swiftly and capitalize on market opportunities.

GSR's experienced team brings together decades of institutional trading expertise, while our industry-leading proprietary technology stack anchors everything we do.

Our main service areas are: market making; proprietary and algorithmic trading; client execution; structured products; risk management solutions; and portfolio investments.

For more information or if we can help with anything, please see gsr.io or contact us at gsr@gsr.io.

Required Disclosures

This material is a product of the GSR Sales and Trading Department. It is not a product of a Research Department, not a research report, and not subject to all of the independence and disclosure standards applicable to research reports prepared pursuant to FINRA or CFTC research rules. This material is not independent of the Firm's proprietary interests, which may conflict with your interests. The Firm trades instruments discussed in this material for its own account. The author may have consulted with the Firm's traders and other personnel, who may have already traded based on the views expressed in this material, may trade contrary to the views expressed in this material, and may have positions in other instruments discussed herein. This material is intended only for institutional investors. Solely for purposes of the CFTC's rules and to the extent this material discusses derivatives, this material is a solicitation for entering into a derivatives transaction and should not be considered to be a derivatives research report.

This material is provided solely for informational purposes, is intended for your use only and does not constitute an offer or commitment, a solicitation of an offer or comment (except as noted for CFTC purposes), or any advice or recommendation, to enter into or conclude any transaction (whether on the indicative terms shown or otherwise), or to provide investment services in any state or country where such an offer or solicitation or provision would be illegal.

Information is based on sources considered to be reliable, but not guaranteed to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of the date of publication, and are subject to change without notice. Trading and investing in digital assets involves significant risks including price volatility and illiquidity and may not be suitable for all investors. GSR will not be liable whatsoever for any direct or consequential loss arising from the use of this Information. Copyright of this Information belongs to GSR. Neither this Information

nor any copy thereof may be taken or rented or redistributed, directly or indirectly, without prior written permission of GSR. Not a solicitation to U.S. Entities or individuals for securities in any form. If you are such an entity, you must close this page.