



INSTITUTIONAL CUSTODY FOR DIGITAL ASSETS

A Primer



Institutional Custody for Digital Assets: A Primer

Introduction

Custody is at the heart of digital assets and blockchain technology, to the point where there is a common catchphrase: “not your keys not your coins”. Custody of digital assets is a foundational topic, and importantly one that greatly enhances the potential of the asset class as a whole. It is also a key property that differentiates it from all other asset classes. There is no controversy in making a bank deposit, or entrusting shares of a public company to your broker, but this changes completely when investing in and transacting with the growing number of digital assets.

What is it about digital assets that makes custody such a hot topic? In one word: Irreversibility. Unlike a fraudulent credit card transaction, a blockchain transaction cannot be reversed with a phone call to a bank or credit card provider. Reversing a blockchain transaction requires restructuring the entire blockchain. These events happen so rarely that when one does happen it sends waves across the entire industry. When trusting a custodian, be it an exchange or a specialized entity, you are trusting their security and reliability above all else. This is because if a breach ever happens, the stolen assets are nearly impossible to recover.

The most notorious example of this is the case of Mt. Gox which will be briefly described later on. However, as the industry has matured so too have its participants. Respected custodians have matured over a relatively short period of time providing sophisticated hardware and software, advanced technologies, and physical safeguards all working towards securing the assets of the growing number of institutional participants. More recently, a number of companies have taken a new approach to custody, rather than being a direct custodian of funds, they instead create tools to enable customers to establish custody themselves while relying on the support, technology, and security of these providers.

In this report, we will cover why custody is important, the technology that underpins both digital assets and their custody, explore the current state of institutional custody solutions, and compare some of the leading institutional custodians.

Institutional Custody for Digital Assets: A Primer

Commissioned by

Copper



Founded in 2018 by Dmitry Tokarev, Copper provides a gateway into the cryptoasset space for institutional investors by offering custody, prime brokerage, and settlements for over 400 digital assets across 45 exchanges. It is committed to providing flexible solutions for institutional investors that can adapt to the changing cryptoasset space, while enabling far greater transparency and control for asset managers.

Researched by



The Block Crypto, Inc. - The Block is an information services company founded in 2018. Its research arm, The Block Research, produces research content covering the digital assets, fintech and financial services industries.

Contact

The Block

Email: support@theblockcrypto.com

Twitter: [@TheBlock__](https://twitter.com/TheBlock__)

The Block Research

Email: research@theblockcrypto.com

Twitter: [@theblockres](https://twitter.com/theblockres)

Institutional Custody for Digital Assets: A Primer

Acknowledgements We would like to thank Copper for commissioning this research report, the support for which made its production possible. In addition, we thank everyone at The Block Research who helped with this report: Andrew Cahill and Larry Cermak for providing feedback.

We're also grateful to those that were willing to share their perspectives and be interviewed for this paper:

Tyler Kenyon - Chief Marketing Officer (Copper)

Fadi Aboualfa - Head of Research (Copper)

Jean-Michel Pailhon - VP Enterprise Solutions (Ledger)

Koichi Kano - Head of Digital Assets and Japan Business Development (SBI Digital Asset Holdings)

Alistair Heggie - Chief Operating Officer (SEBA Bank)

Paolo Guarnerio - Digital Custody Services Manager (SEBA Bank)

Finally, we thank our talented designer Aleksander Hamid.

Authors



Carlos Reyes

[Twitter](#)

[LinkedIn](#)

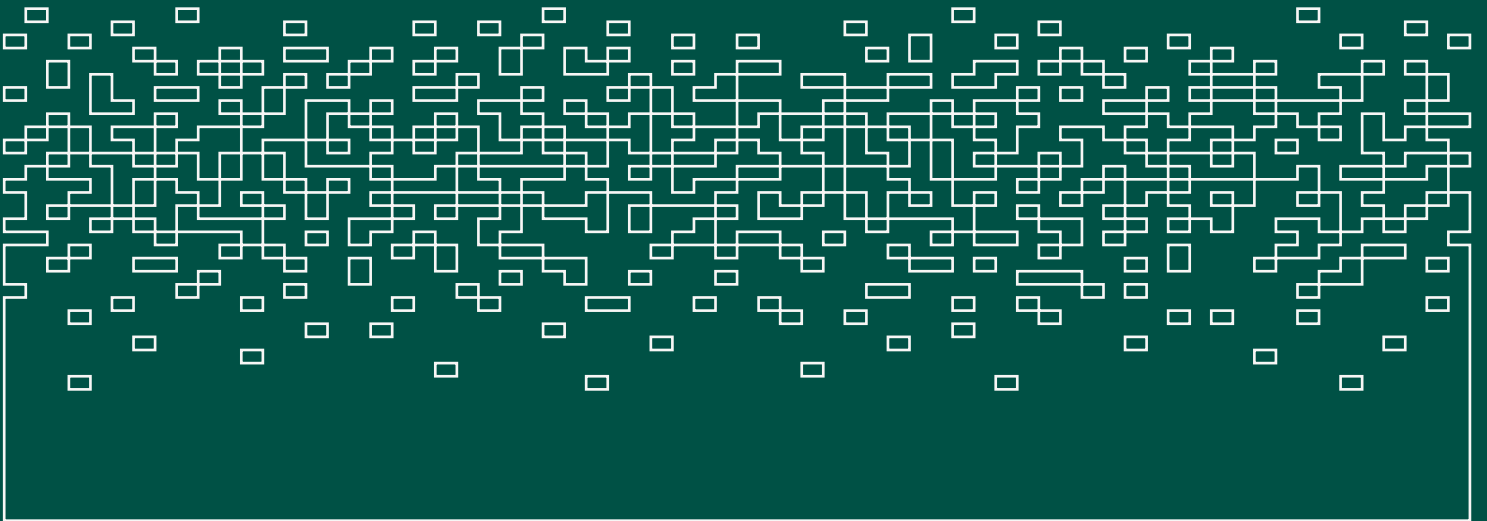
Institutional Custody for Digital Assets:

A Primer

Table of Contents	3	Introduction
	4	About
	5	Acknowledgements
	7	Chapter I: When Custody Goes Wrong, and When it Goes Right
	8	What Makes a Cryptoasset Custodian Different?
	16	Chapter II: Custody Taxonomy
	17	Public and Private Keys
	19	Hot and Cold Storage
	23	Custodian Solutions
	25	Categorizing Digital Asset Custody Firms
	30	Chapter III: The Current State of Institutional Custody Solutions
	31	Exchanges, Evolution into Custodians
	32	From Manufacturers to Technology Providers
	33	The Modern Custodial Industry
	36	Regulation and the Evolution of Services and Platform Providers
	41	Best Practices
	43	Chapter IV: Comparison of Institutional-Grade Custody Providers
	44	Operational Management
	50	Considerations on Custodian Offerings
	57	Conclusion

Institutional Custody for Digital Assets:
A Primer

I When Custody Goes Wrong, and When it Goes Right



Institutional Custody for Digital Assets: A Primer

Chapter I: When Custody Goes Wrong, and When It Goes Right

Custody is a double-edged sword, when done well it provides users with assets that cannot be stolen or confiscated, however occasionally it is the owners who are looking for a way to gain access to their own assets. It is not uncommon to hear stories of early Bitcoin adopters losing access to a hard drive or laptop containing their private keys to hundreds or thousands of Bitcoin. However in today's environment it would be quite rare for even a novice investor to commit such mistakes, due to the much higher awareness surrounding digital assets and the improved resources available to first time users.

Bad Management, Real Losses

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Programmer has two guesses left to access £175m bitcoin wallet

Stefan Thomas is not the first person to forget a password, but memory lapses are rarely so potentially costly



DeFi protocol bZx compromised again: \$55 million stolen in private key leak

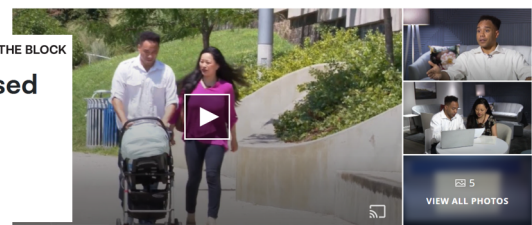
by Osato Avan-Nomayo
November 5, 2021, 11:49AM EDT · 1 min read

Man makes last-ditch effort to recover \$280 million in bitcoin he accidentally threw out

Bitcoin pros speculate over possible loss of \$2 billion crypto fortune after death of one large owner

DC family can't access \$5.8M cryptocurrency wallet & asks for help

by Scott Taylor/7News | Wednesday, July 21st 2021



Art & Yuki Williams Family Source: 7News

Source: The Block, The New York Times, The Guardian, CNBC, ABC 7News, Market Watch

The most infamous mishap regarding improper custody of digital assets happened in 2014 when Mt. Gox, the most popular Bitcoin exchange at the time, shut down and disclosed it had lost approximately 850,000 of its users' Bitcoin¹, the majority of which are still missing to this day. Much research and debate has surrounded the actual events that led to the loss of funds by Mt. Gox, however regardless of the exact details one thing is clear, Mt. Gox was not properly custodying the assets that had been entrusted to them by their users.

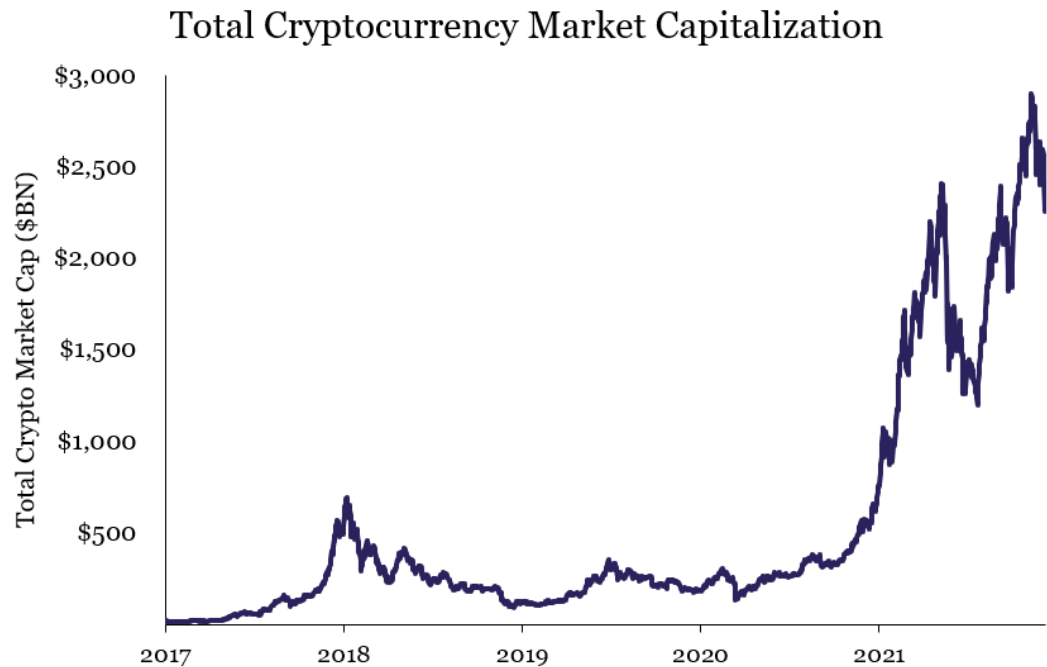
¹ [Mt. Gox files for bankruptcy as 850,000 bitcoins go missing](#). Los Angeles Times

Thankfully, the modern environment for digital assets is both much more sophisticated, and much more user friendly. However, it is important to remember the painful lessons learned by early adopters so that modern users and providers understand the importance of proper custody.

Unlike the peer-to-peer transactions and informal exchanges used by the earliest Bitcoin adopters, most modern users tend to go to well known and sophisticated centralized exchanges. Often these exchanges double as a custodian for users who chose not to withdraw their assets. There could be a number of reasons for a user to do this, perhaps the user is an active trader or is willing to trust their exchange while they learn how to use a private wallet.

Regardless of the reason, as the adoption of digital assets grows, so does the number of funds flowing into centralized exchanges. In response, many leading exchanges such as Coinbase and Gemini have begun offering sophisticated custody solutions as a stand-alone product. Some recent entrants into the digital asset space such as fintechs and neobanks typically do not allow their customers to withdraw their digital assets to external wallets, meaning that users have no choice but to rely on them as their custodian. These companies often rely on services offered by specialized digital asset companies to facilitate the trading and storage of their digital asset products. These offerings are also almost entirely directed at retail customers as this solution would be unacceptable for an institutional grade investor.

As the digital asset space continues to grow so too will the importance of custodians. While self custody is an incredibly important aspect of digital assets, it may not be the right answer for everyone, including institutional investors. Some firms may decide that the cost of building a solution in-house is too high, some may be required by regulators to utilize a custodian, and others may decide that an in-house solution with the support of a technology provider is the best solution in order to maintain their desired level of control. Regardless of the reason, custody is a foundational and necessary layer for digital assets upon which a number of other services can be built upon.



Source: Tradingview Dec 6th, 2021

What Makes a Cryptoasset Custodian Different?

As previously mentioned, a key differentiator of digital assets is the fact that transactions can only be reversed in extreme circumstances, and reversals become very notable and controversial events when it does happen. As the Mt. Gox case shows, once an attacker is able to complete a transaction it is nearly impossible for those funds to be recovered. Mt. Gox also highlights the importance of proper key management when securing digital assets. In more recent times DeFi hacks have served to illustrate a third major differentiator for digital assets and the networks they operate on. That of network and product risk. While these 3 risks are true of the asset category as a whole, custodians and this report will focus on private key management keeping in mind that this management is crucial as stolen assets are nearly impossible to recover.

For digital asset custodians and technology providers these risks mean that their security, procedures, and products must be constantly monitored, tested, and improved upon. These risks are further compounded as the number of supported blockchains increases over time. As will be discussed in detail further on, many custodians employ a range of advanced



techniques and technologies to reduce the likelihood of a successful attack or fraudulent transaction.

Standouts among these technologies are: multi-party computation (MPC), hardware security modules (HSM), and multi-signature (multisig) technology. Other highly effective security measures include two factor authentication (2FA), know your customer (KYC) policies, whitelisting, time delay policies, and access control, among others. While some of the measures mentioned are not necessarily technological innovations, such as KYC or access control, they highlight two key, non-technological, considerations when implementing proper custody: Regulations (as in the case of KYC), and proper implementation of policy (access control). They also highlight that while custodians and technology providers do provide a very high level of expertise and innovation, the human and regulatory elements must also be considered for a truly robust custodial solution.

While modern custodians have an impressive array of technologies, devices, knowledge, and best practices available to build their security, they also face the challenge of keeping up with the ever innovative digital asset space. Over the past 2-3 years there has been an explosion in the Decentralized Finance (DeFi) and Non-fungible Token (NFT) spaces. Typically interactions with these products function best and are designed around the assumption that every user will be using a private wallet. This is because the developers of these products often design around retail adoption, in line with the ethos that decentralized products should be available for all.

The best way to understand this concept is with examples; a DeFi contract may issue a token that is representative of the user's share of an asset pool or represents participation in a protocol. When minting NFTs the NFT is typically sent to the wallet that transferred funds to the minting application. In both cases the developers of these products have assumed an end user managing their funds independently.

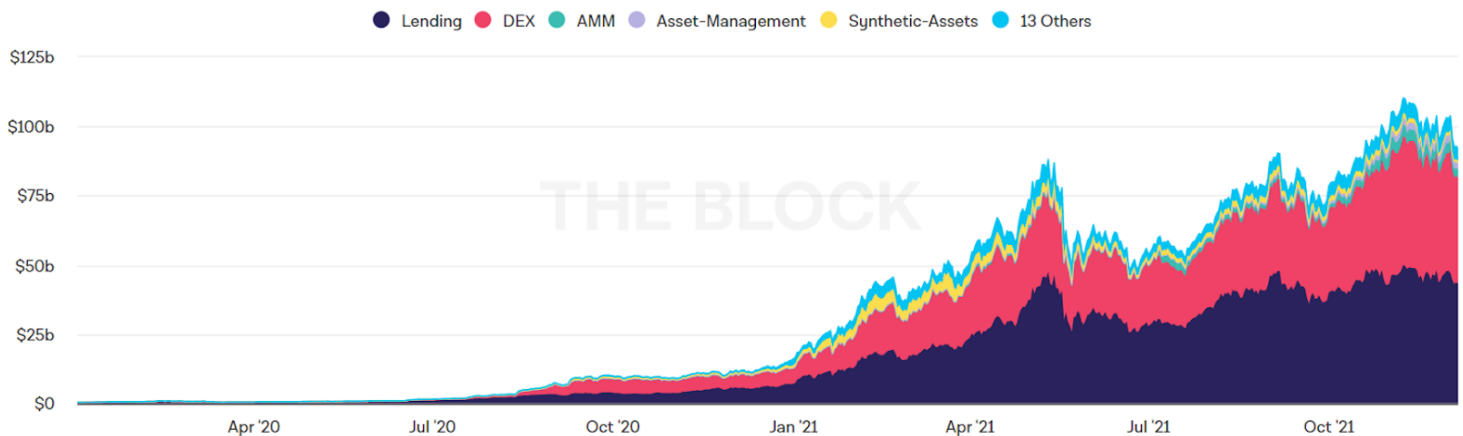
Institutional Custody for Digital Assets: A Primer

Chapter I: When Custody Goes Wrong, and When It Goes Right

Similarly, decentralized exchanges or DEXs, are designed around the assumption that a user will be trading from a private wallet. A recent innovation in DEXs is the automated market maker (AMM). An AMM allows for users to create liquidity for any asset rather than having to rely on a professional market maker. In exchange for providing liquidity users are rewarded with a share of trading fees proportional to the amount of assets contributed to the liquidity pool, and are often also provided other rewards in order to incentivize participation. These pools are vital to the growth of many modern DEXs and for newly launched protocols so they can incentivize adoption and provide liquidity to early adopters. The continued development of DEXs further differentiates cryptoassets from traditional assets as it allows for direct and indirect peer-to-peer transactions. For funds who actively participate in the DeFi space, being able to interact with products, retain ownership of their specialized tokens, and collect the rewards is vital.



Value Locked by Category (Net)



SOURCE: DEBANK
UPDATED: DEC 6, 2021

For a direct custodian, facilitating transactions to decentralized products requires the development of additional interfaces, policies, and infrastructures around the design of these products for every supported blockchain and must also consider any unique processes native to each blockchain. For many direct custodians, given they control customer private keys, they face reputational risk if a decentralized product exploit or failure were to

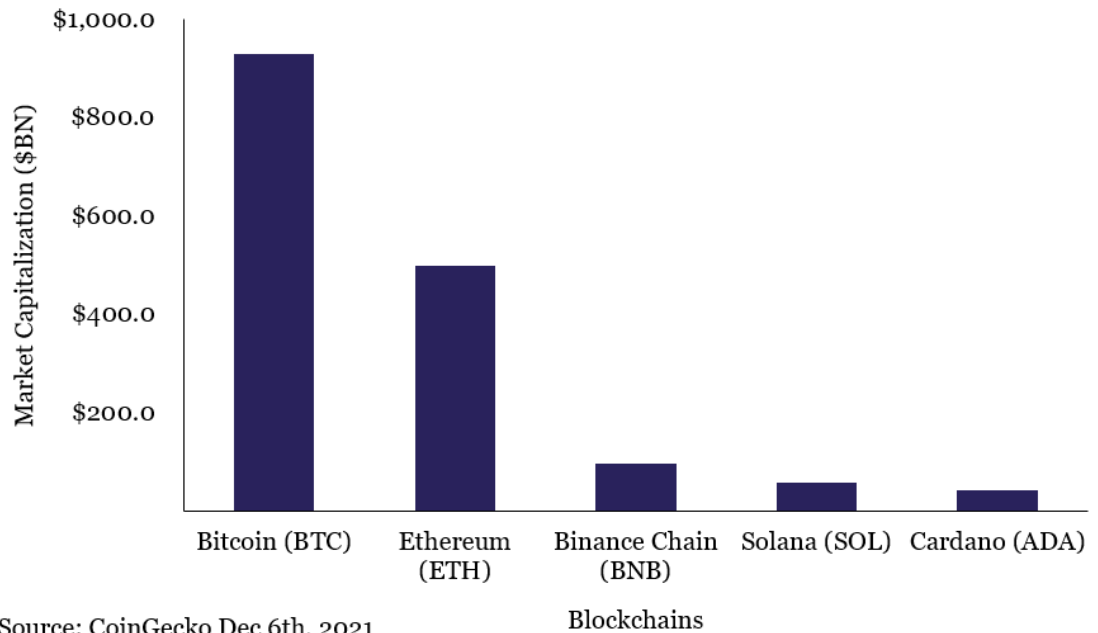
result in a loss of customer funds. Due to this risk, direct custodians who do offer access to decentralized products do so typically on a case by case basis.

Other policies that direct custodians can implement, such as pooling user funds into cold wallets, may further complicate the utilization of these protocols. Pooling user funds is a common action taken by digital asset exchanges which is also employed by a number of direct custodians. By pooling assets together a custodian or exchange is able to maintain a higher percentage of funds in more secure cold storage without negatively impacting their customers' liquidity due to also pooling the remaining funds into hot wallets enabling efficient trading and reliable withdrawals.

Technology providers can more easily meet the needs of customers who choose to actively interact with different types of decentralized products. This is because technology providers typically do not retain control of customers' private keys and do not restrict their interactions with decentralized products. They also face a lower reputational risk since customers bear all the risks of interacting with decentralized products and are also responsible for conducting appropriate research and risk evaluation.

Both direct custodians and technology providers have strong incentives to continue developing functionality for the growing number of decentralized products across multiple blockchains, namely strong and growing customer demand. Looking back, other earlier decentralized features and products such as staking and DEX trading presented their own challenges at the time. Early adopters of blockchains with staking rewards could not utilize custodian or exchange wallets, or even certain hardware wallets because they lacked the infrastructure to manage and distribute staking rewards to the appropriate accounts. For a period of time, only the officially developed wallets of newly launched blockchains were able to properly reward users for staking their coins. Since then nearly all exchanges, custodians, and hardware device manufacturers have been able to build the infrastructure necessary to distribute staking rewards, a crucial component for proof-of-stake blockchains and their users.

Top 5 Blockchains by Market Capitalization



Lastly, an important challenge for direct custodians and technology providers is multi chain management. Many of the most popular digital assets operate on their own blockchains and are not interoperable. For example Ethereum's native asset ETH and Ethereum based ERC-20 tokens cannot be stored on a Bitcoin wallet, however Bitcoin and Ethereum wallets can coexist on a single hardware device. As other blockchains such as Cardano, Solana, and Polkadot continue to gain in popularity, multi-chain considerations will only continue to grow as each blockchain operates in a different manner and may require further specialized technologies, policies, and knowledge in order to properly secure assets operating on newer blockchains. However, security is not the only concern when supporting additional blockchains. From a customer experience perspective, it is just as important to ensure that customers can easily manage the entire range of assets they choose to adopt.

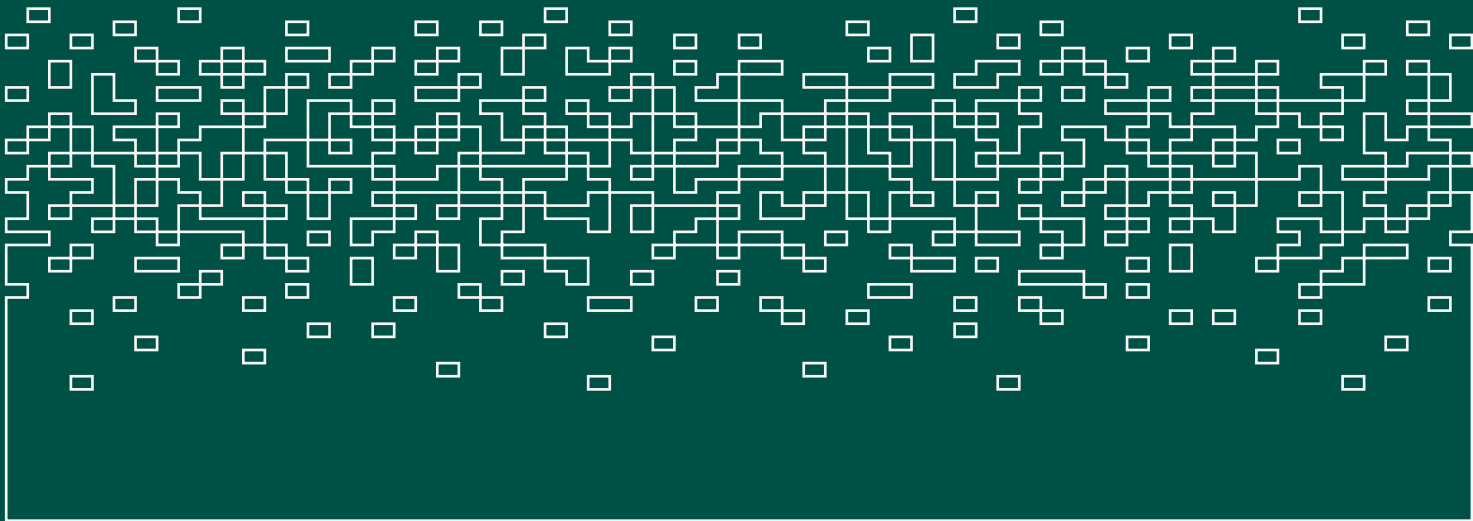
Though a seemingly straightforward point to those who are already experienced in the digital asset space, multi-chain considerations are a further differentiator from traditional assets. While a stock and bond are different financial instruments, a custodian would not need to take into account

any special technological considerations in order to custody both stocks and bonds. For digital asset custodians and technology providers this is the case given that multiple types of assets (security tokens and NFTs for example) can live on a single blockchain, and each blockchain has their own form of representing assets on that chain.

Any custodian or technology provider looking to attract users active in these innovative spaces must be able to solve for the challenges they present, and work towards continually enabling access and functionality to these products across multiple blockchains. Providing these kinds of solutions both enhances the experience of existing customers, and attracts new customers. Continuous development of these solutions will ultimately further broaden the total custodial market.

One final aspect that was highlighted by multiple custodians interviewed for this report is relationship building and the element of understanding between custodians/technology providers and their customers, including understanding the industries in which their customers operate. Customers rely on custodians to safeguard their funds, but importantly they are also relying on their compliance, standards, and ability to deliver products and technology that will not only enable their operations, but also enable the continued growth of the digital asset industry. Beyond this, custodians and technology providers also stressed the importance of knowing the business models, operating structures, and needs of their customers in order to develop and deliver products and technologies aligned with those needs.

II Custody Taxonomy



“Not your keys not your coins” is a phrase commonly heard in the digital asset space, but what exactly does it mean? Terms such as private and public keys, and hot and cold wallets are crucial for understanding what exactly the risks are with any form of digital asset custody. They are also important in understanding what risks are unique to custodians, what measures are in place to reduce these risks, and what advantages custodians offer to their customers.

Public and Private Keys

Cryptocurrencies use what is known as public-key cryptography. Mathematical functions derived from this technology such as elliptic curve multiplication, the basis of Bitcoin and Ethereum and many other blockchains' cryptography, are used to create a pair of public and private keys that control access to a user's cryptoassets. These mathematical functions are easy to calculate in one direction (multiplication), but nearly impossible to calculate in reverse (division). Thanks to this one way relationship, owners of private keys are able to create unforgeable digital signatures that can be validated against the public keys without revealing the private key.

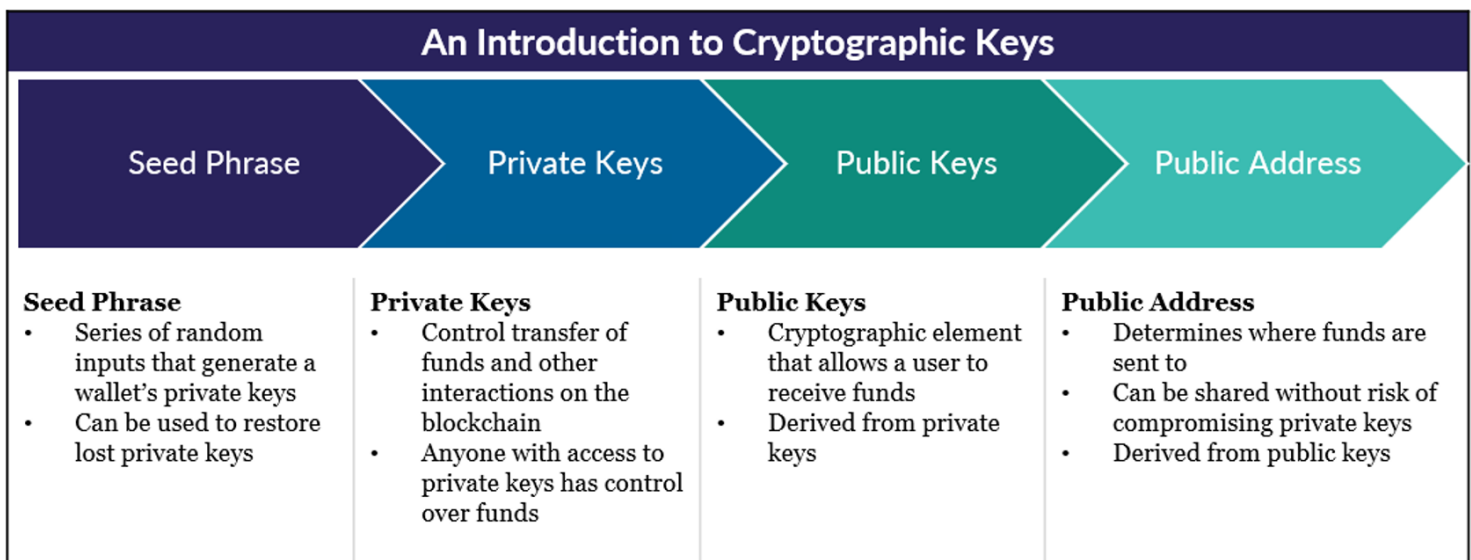
Private keys are the cryptographic element that allow a user to transfer funds or interact with products on the blockchain. Crucial to the proper management of private keys is how these are generated. Private keys are generated using random inputs such as the current time, mouse movements, or cryptographically secure random number generators. These inputs are referred to as seeds. Key generation is completely independent of the blockchain and can be done without connection to the internet, in fact generating keys offline is considered a basic security measure. Secure private key generation and protection is so important that most of the advanced techniques employed by direct custodians and technology providers are dedicated to this matter. Sophisticated forms of key generation and storage are discussed in the Operational Management section of this report.

Once the private key is generated a one way mathematical function, such as the previously mentioned elliptical multiplication, is utilized to generate the public key. Using a one way cryptographic hash function a pub-

lic address is generated from the public key. A single seed can generate an infinite number of private keys, which can then be used to generate an infinite number of public keys and public addresses.

Given the decentralized nature of the blockchain, a user can use their private keys from anywhere in the world and execute any transaction they wish. This power is among the main concerns with regards to entrusting a direct custodian with cryptoassets, given that in a strict technological sense, the custodian is the true owner of those assets especially if they are the only party with access to the private keys.

Public keys are the cryptographic element that allow a user to receive funds. Public keys are derived from private keys. A somewhat common misconception is that the public key is the public address, an understandable mistake since the public address is derived from the public key. Public addresses are the string of characters that we most commonly see when interacting with digital assets. Public addresses can be freely shared without risk of compromising a user's private keys. Public addresses may also point to programs or tokens on a blockchain, for example the public address 0xdAC17F958D2ee523a2206206994597C-13D831ec7 refers to the smart contract for the ERC-20 version of the Tether stablecoin.



Source: The Block Research

Hot and Cold Storage

Hot and cold storage options refer to a spectrum of accessibility for digital wallets. The common understanding of hot and cold wallets comes from the retail perspective, where hot wallets are connected to the internet for quick access to funds and cold wallets are typically specialized hardware devices that are kept offline and interact with the internet in an air gapped manner. When it comes to custodians and institutional users, hot and cold wallets are typically determined by the processes around access to the wallets since specialized hardware devices are always utilized even for hot wallets. Specialized hardware solutions are at the core of many institutional direct custodian and technology provider offers.

Whether it be through a direct custodian, or self-custody facilitated by a technology provider, transactions often require multiple authorizations. Broadly speaking, hot wallet transactions can be done entirely through software or with less authorizations when compared to cold storage transactions. Depending on the particular custodian, cold wallet transactions may require manual inputs from the custodian.

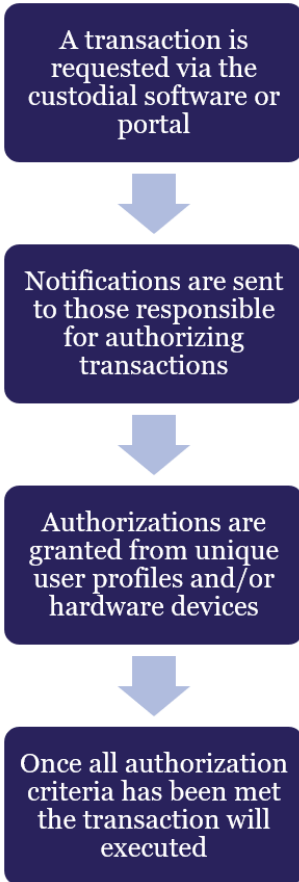
Hot wallets: For many retail users hot wallets are essential for interacting with decentralized products. The most popular kinds of hot wallets for this are desktop extension wallets. Notable fintechs such as PayPal and Robinhood which allow customers to purchase and store digital assets with them are also hot wallet providers. Browser extension wallet MetaMask is leveraging their popularity to enter the institutional space through their MetaMask Institutional product.

When it comes to institutional hot storage it is mostly defined around policy, permissions, and automation. While hot wallets are exposed to more threats than institutional cold wallets, an institutional grade hot wallet is still extremely secure. Specialized hardware devices are commonly used by custodians to heighten the security of their hot wallets, and it is not uncommon for technology providers to also provide their customers with specialized hardware. It is through this hardware that transactions are requested, authorized, and ultimately executed. A key differentiator between institutional hot and cold wallets is the degree of automation.

Institutional Custody for Digital Assets: A Primer

Chapter II: Custody Taxonomy

Institutional Hot Wallet Transaction Flow



Most hot wallet transactions can be executed through the custodial software or portal and the accompanying hardware, however cold wallet transactions often require additional manual interactions. A typical institutional grade hot wallet transaction flow is illustrated to the left.

Hot Wallet Vulnerabilities: Since hot wallets are characterized by their access to the internet, this presents attackers with a range of options when it comes to compromising user wallets in order to steal funds. Many commonly used techniques include: keyloggers, man in the middle attacks, phishing scams and attacks, clipboard malware, and other ways of compromising private keys. Despite the additional security added by institutional actors, hot wallets present attackers with a very enticing target that is both highly valuable and more vulnerable than cold wallets.

However, the targets of hot wallet attacks are usually exchanges and not institutional investors. This is because exchanges are much more visible and keep larger amounts of funds for liquidity in their hot wallets. Despite additional layers of security around their hot wallets, such as controlling physical access to devices, dedicated security teams, withdrawal policies such as email confirmation, whitelisting addresses, time delays, or enhanced KYC confirmations, exchange hacks continue to occur.

In September 2020, cryptocurrency exchange Kucoin had their hot wallets compromised in what resulted in the third largest exchange hack in history² only behind the Mt. Gox and Coincheck hacks. One of the containment measures taken by the Kucoin team after detecting the hack was to transfer all remaining hot wallet assets to their cold wallets. More recently, in August of 2021, Japanese exchange Liquid had their hot wallets compromised resulting in \$74M of assets stolen³.

Cold wallets: These are regarded as the safest option for storing digital assets. While cold wallets come in a variety of shapes and sizes and can use a number of software interfaces, all cold wallets are based on the same core concept: private keys are generated and stored offline at all times.

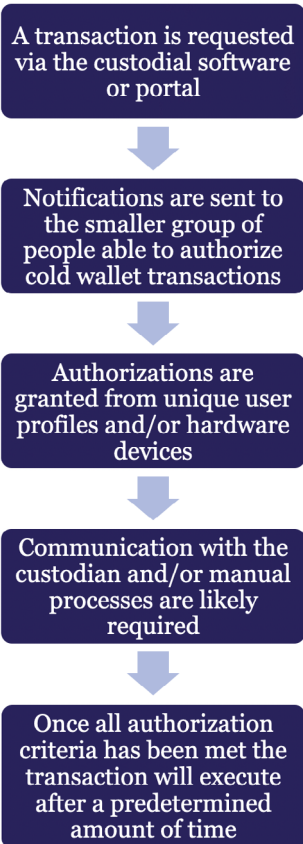
² [A look at the third largest exchange hack and its aftermath](#). The Block Research

³ [Japanese exchange Liquid hacked, hacker in possession of \\$74 million in crypto assets](#). The Block

Institutional Custody for Digital Assets: A Primer

Chapter II: Custody Taxonomy

Institutional Cold Wallet Transaction Flow



Cold wallets are intentionally designed to limit the amount of potential attacks directed on them. A typical hardware wallet contains within it a simple computer that has never been connected to the internet and does not have more than a few kilobytes of memory, only enough for basic functionalities and displaying data, but not enough for malicious software to be injected and executed. On these simple computers the private key is generated and stored, always isolated from the internet. Hardware wallets are capable of signing transactions and broadcasting them without exposing the private key in conjunction with software interfaces. Given their combination of security and ease of use, hardware wallets have become a mainstay of secure custody.

Due the wide range of security options that hardware wallets enable, and the flexibility in designing them, varying forms of hardware wallets can be found securing all levels of digital assets, from retail users to multi-billion dollar institutions. The most well known of these specialized solutions are hardware security modules (HSMs) which will be discussed in depth in the Operational Management section of this report.

One unique consideration for institutional cold wallets is that of key rotation. Key rotation is a process in which the current encryption key is retired and replaced by a newly generated one. This practice minimizes the risk of edge case scenarios such as key exhaustion or a data leak leading to loss of funds. Rotation every 90-180 days is common for highly sensitive keys such as those used by digital assets.

A potential disadvantage of cold wallets is that they are much slower in transaction execution by design. Viewing the typical institutional grade cold wallet transaction flow to the left, it is clear why cold wallets are typically not suitable for more active strategies.

For example, when executing trades on AMM based DEXs the trade will fail if the price has moved outside of the user's predetermined acceptable range. While this is typically the result of low gas fees resulting in a slow transaction, the time delay from attempting to trade from cold storage is also likely to lead to a failed transaction. This is why having both hot and cold storage is a fundamental need for most institutional investors.

The key differences between a cold and hot wallet transactions are that cold wallet transactions will typically:

- Have less people who can authorize them
- Require more authorizations
- Include a manual process
- Employ a time delay between when the transaction is confirmed and when the funds are actually moved

It is also important to note that not all hardware wallet solutions support all digital assets, this is especially true for assets that operate on newer blockchains. When selecting a custodian or technology provider it is important for prospective customers to understand which vendors are able to support the assets and blockchains they interact with.

Far from being a stagnant space, the hardware wallet industry itself is constantly evolving with Square recently announcing their plans to enter the space by developing a Bitcoin focused, multi-signature, mobile first, hardware wallet. Industry leaders Ledger and Trezor are also constantly improving on their hardware wallets and offer institutional solutions.

Cold Wallet Vulnerabilities: Given their offline nature, attacks on hardware wallets typically constitute physical attacks and exploits. Most of the known vulnerabilities around hardware wallets are discovered by white hat hackers who utilize responsible disclosure procedures to inform device manufacturers and the wider cybersecurity community. Hardware manufacturers will often place bounties on vulnerability discovery to further incentivize white hat hackers. Additionally, many institutional custodians and technology providers either contract or have in-house security teams dedicated to finding flaws in their operations for both their software and hardware, a practice known in the cybersecurity world as penetration testing.

Considering the high degree of difficulty in compromising hardware wallets, many attackers choose to instead focus on flaws in procedure by users or other parties involved. The information gathered by vendors such as names, emails, and addresses may be vulnerable to attacks. These

sorts of attacks have occurred and have resulted in targeted phishing campaigns against users who had their information leaked. Hardware wallets are also susceptible to unexpected events such as fires or floods damaging the device and the seed backup. Due to this risk direct custodians maintain physical devices and their backups in secure, geographically distant locations.

Custodian Solutions

With a more comprehensive understanding of some of the crucial and foundational aspects of digital asset ownership, it is easy to see why many novice, and even some advanced users find self custody to be difficult, tedious, and time consuming, or some mixture of these sentiments. While in the earliest days of Bitcoin there was no real alternative, with the advancement of technology, regulatory clarity, and most importantly the development of trusted institutional players, there now exists a number of trusted brokers, custodians, and technology providers. Custody focused firms range from those that only support Bitcoin, to those that support hundreds of digital assets through tokens standards. These players provide a wide range of services designed to cater to the needs of high value clients and institutions, and provide the necessary tools to directly or indirectly safeguard their customer's digital assets.

Custodians and technology providers also allow for a layer of innovation and customer service that is focused on their exact customer base. For example, some custodians have agreements with leading exchanges that allow their customers to access liquidity and execute trades against their custodied assets without transferring those assets out of the custodian and into the exchange reserves, and settlement of funds occurs on the custodian side. Other custodians stress the level of security around customer assets and include safeguards such as specialized devices or technologies, robust internal policies, or insurance for customers to protect them from a range of scenarios. Insurance provided by custodians is designed to protect customers from loss should failures happen despite proper management, for example in case of third party theft.

Institutional Custody for Digital Assets: A Primer

Chapter II: Custody Taxonomy



Source: The Block Research; Represents select industry participants and is not an exhaustive list.

Others such as custodial technology providers believe that users should be the ultimate keepers of their assets and instead provide the necessary technology to do so. They provide customers with specialized software and sometimes hardware as well so that institutions can secure their digital assets with the latest technology, without transferring ownership of their private keys.

One crucial component of innovation that separates institutional grade custodians from retail custody solutions is the ability to give clients options on the governance of their funds. By working with custodians and technology providers, companies have a much higher degree of control over who has access to funds, how many people are required to execute transactions, and maintain a record of who has interacted with funds among other features. If an institution relied only on mass market solutions such as hardware wallets they would be exposed to risks such as device malfunction or loss, or create a situation in which a single employee with access to the device could execute transactions without proper authorizations. These features and controls are crucial to effective institutional governance of large amounts of assets and help elevate digital assets as an asset class comparable to its more traditional counterparts.

It is also crucial to distinguish institutional custody focused firms from other firms which also deal with storing and transferring customer digital assets, such as exchanges and payment networks. While on a surface level all three deal with securing and facilitating actions such as trading, transferring assets, and borrowing and lending, operationally custody firms operate at a much higher level of security and efficiency. Institutional customers of custody firms are not only concerned with the security of their assets but also expect high grade performance in the execution of value added services such as prime trading from custodial storage.

However, it is important to remember that all players in the digital asset space still interact with the same public key cryptography previously discussed. Given that direct custodians are by nature third parties, practices around all aspects of private keys: generation, rotation, backup management, and access are all of the utmost importance. High caliber custodians have strict policies that enforce best practices around all aspects of key generation, maintenance, and recovery. Technology providers have several ways of aiding in the secure creation and maintenance of private keys, while still allowing for customers to retain sole access to their funds. Technologies that enable this, such as multi-party computation (MPC), are explored further on.

In the current digital asset environment, custodians also have a much more focused client base. They tend to have a low number of clients (under 100), but with every client being of a significant size (several million dollars in digital assets). This means that custodians can be extremely responsive to the needs of their clients. Oftentimes clients are able to request features and support directly from their custodian or software provider and tend to be accommodated as much as possible, though sometimes at additional cost.

Categorizing Digital Asset Custody Firms

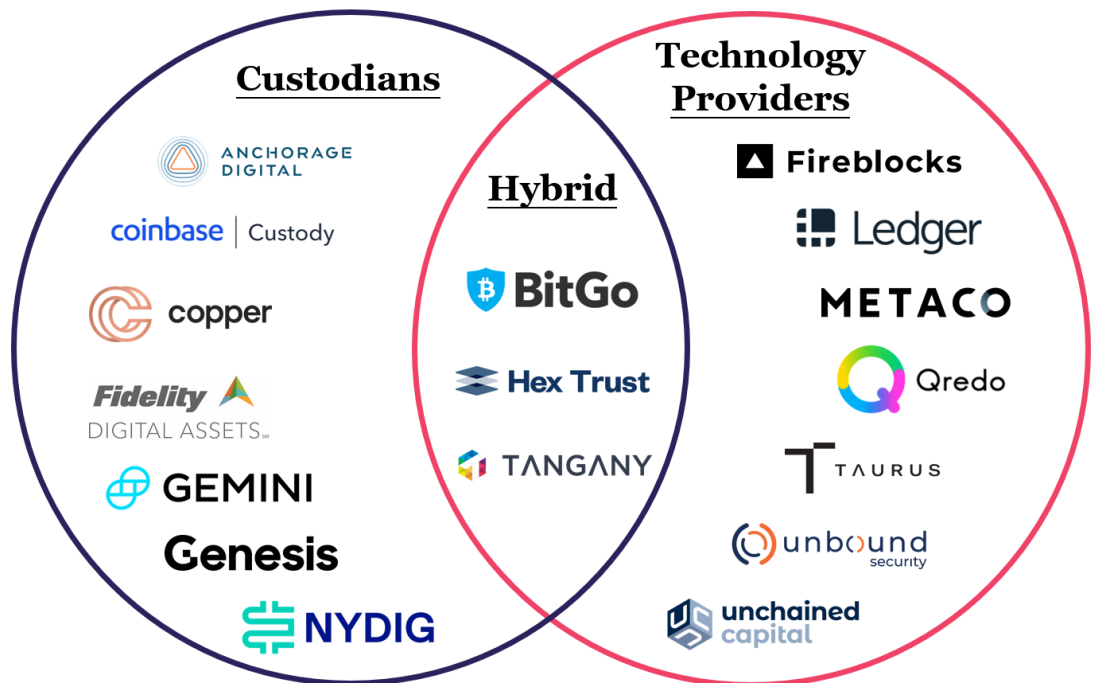
While the majority of digital asset custody firms focus on direct custody or acting as a technology provider, some companies bridge the gap and offer both direct custody and self custody products. Broadly speaking, institutional focused digital asset custody firms fall into one of three categories:

Direct Custodians: Directly secure the digital assets of others. They perform key management and assume the risks associated with the safe-keeping of assets.

Technology Providers: Provide software and hardware solutions that enable their customers to reliably self custody. These companies are more in line with software as a service (SaaS) or "platform as a service" (PaaS) models.

Hybrid: Providers that offer one of or both of the following:

- Both direct custody and self custody technology solutions.
- Products in which the customer and the custodian have shared custody over the funds. The custodian typically only utilizes their key(s) in case of emergency.



Source: The Block Research, Ledger Vault. Represents select industry participants and is not an exhaustive list.

Direct Custodians: Direct custodians are usually what first comes to mind when thinking of digital asset custodians. These companies retain full control over the private keys of the assets in their care. They typically operate by collecting a percentage fee based on the amount of assets under custody, other forms of revenue include trading fees and withdrawal fees, and revenue from other forms of value added services they provide.

A helpful way of understanding direct custodianship is to compare it to traditional outsourcing. Rather than the company building out its own infrastructure, hiring or training for specialized roles, and purchasing the hardware and software, a company chooses to hire a company that already is specialized in providing custodial services. By relying on a custodian the company saves on the upfront costs of creating an in-house solution for their digital assets, and may lower the barrier to entry for those institutions with a minor or long only position on digital assets. Furthermore some institutions are required by regulators to utilize a licenced custodian for the safeguarding of digital assets. For example, according to the Investment Advisers Act of 1940 advisers⁴ that have custody of client funds or securities are required to maintain those assets with broker-dealers, banks, or other qualified custodians. By utilizing a custodian, companies may reduce their internal risk and costs, and advisers reduce the risk of fraud by separating themselves from customer funds.

These benefits also allow institutions who are only just beginning to express interest in digital assets to enter the space in a lower risk manner. They are also able to justify a small allocation to digital assets without incurring the costs previously mentioned. For companies with small allocations or only just beginning to enter the space, building in-house may not only be more expensive, but may incur more risk if done incorrectly.

While there are certain clear benefits to operating with a licensed direct custodian, for certain firms this arrangement presents some disadvantages, such as balance sheet risk, compliance complications, or a desire to manage and control risk internally. For these firms the risk of trusting what are, from the perspective of multi-billion dollar institutions, "small fintech startups" is larger than the cost of investing into developing policies, hiring or training staff, and purchasing the necessary hardware and software. One provider of custodian grade software said that for clients who engage in high-frequency trading, or whose trading strategies often rely on execution speed, having their funds in a direct custodian would cause too much delay for their strategy to continue being effective.

⁴ Advisers refers to companies, including mutual funds, that engage primarily in investing, reinvesting, and trading in securities, and whose own securities are offered to the investing public.

From a regulatory perspective, while direct custodians may benefit from regulations that mandate institutions store their digital assets at regulated direct custodians, they may also be constrained in the services they are able to provide their customers. For example, in recent months the SEC and state regulators have been scrutinizing products that provide yield on user funds by lending the user's digital assets to other firms, a product custodians could offer either on their own or in partnerships with businesses that specialize in these products. In other countries regulators are increasingly concerned about their local financial institutions storing digital assets abroad, potentially limiting their ability to oversee and regulate these institutions.

Technology Providers: These companies offer a range of software and hardware solutions and services that allow for customers to secure their digital assets without transferring ownership of the private keys. Companies in this space look to differentiate themselves with the use of technology, a broader range of asset support, and unique features such as establishing a secure network of transactions among their customers. Direct custodians are sometimes also customers of technology providers and their software in combination with their own solutions. Typically technology providers operate by charging subscription and plan fees, as well as revenue from value added services.

A helpful way of viewing direct custodian services is to compare them to services such as Amazon Web Services. AWS provides the infrastructure necessary for companies to build a robust digital presence, but it does not mandate what the website is used for; shopping, entertainment, or corporate data can all be hosted on AWS servers. Using AWS also allows companies to offload many necessary tasks and hardware that once had to all be executed and maintained in-house if a company wanted to grow and maintain a strong digital presence. AWS serves as a tool that enables companies to grow their digital presence in a more focused and cost efficient way, while still maintaining full control over their data, strategy, and content.

In the same way that Netflix uses AWS for computing and storage so that the company can focus on production and customer acquisition, so too can a financial institution benefit from using software from a technology provider.

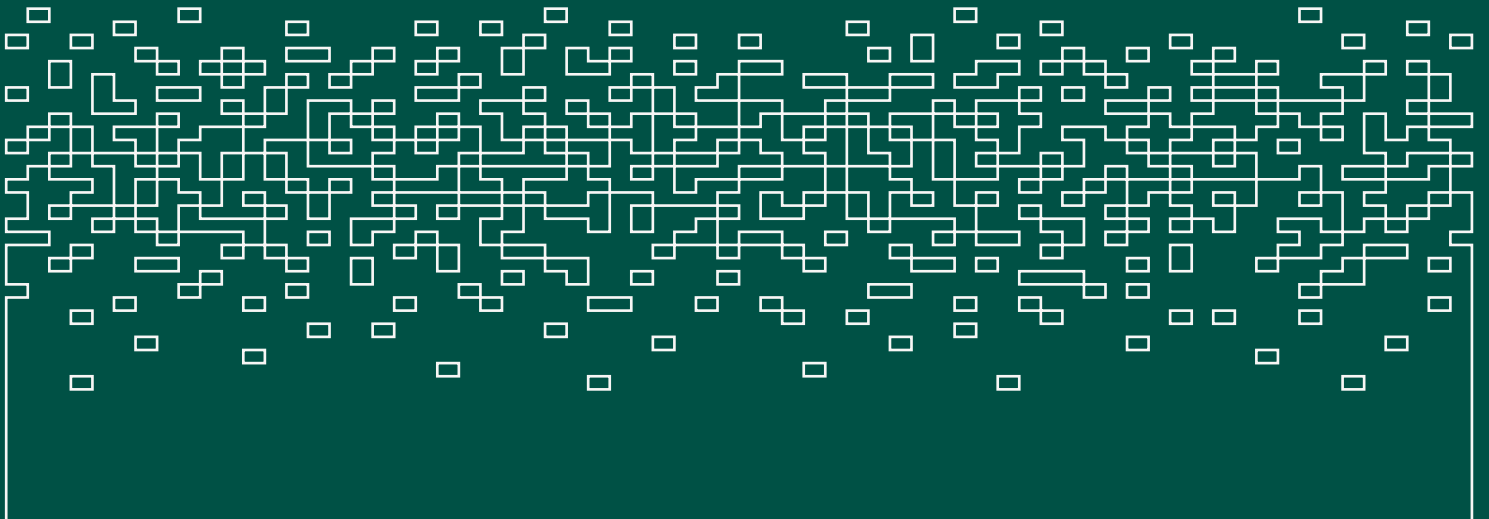
The software provided by these firms allows customers to have many of the same controls provided by a direct custodian, but without losing control of their assets. Customers can decide who has access to which funds or key shards, how many people are required to engage with funds, and log transactions made. More advanced functionality varies depending on the exact software provider, for example assisting in the creation of tax or other regulatory documentation, converting smart contract code into easily readable language, insurance, or secure ways for users to generate private keys without exposing the keys with the service provider.

While many of the products and services of technology providers are indeed impressive, there are also risks that must be accounted for. The largest of which is that, just as with other forms of self custody, the end customer bears the risk of properly maintaining and backing up their keys and/or key shards. One leading reason companies choose to utilize technology providers over direct custodians is the freedom to interact with decentralized products, however these products bear their own risks and utilizing the services of a technology provider does not affect the risk of a decentralized product.

Hybrid Providers: The majority of this category is simply companies that provide both direct custody and technology based solutions. However there is also a niche category of products and companies that specialize in a form of multisig enabled shared custody between the customer and the custodian. In these products the partner company typically only intervenes in order to help the customer regain access to their funds in case of emergency.

The majority of these products are offered only on single blockchains, if a customer wishes to employ this system across multiple blockchains they will most likely have two or more separate solutions, one for each chain. This structure is most useful to those who rarely make transactions and can follow the best practice of keeping their keys at separate locations, for example a mobile key on them, and a hardware wallet key in a secure location. Otherwise the user runs the risk of the majority of keys being compromised at the same time, in a house fire or flood for example.

III The Current State of Institutional Custody Solutions



Many of today's leading direct custodians developed the skills and technology necessary to do so from operating in the digital asset industry under mandates other than custody. Though they are industry leaders, they face many challenges from new companies dedicated to helping institutions self custody.

Exchanges, Evolution into Custodians

From the earliest days of Bitcoin many users much preferred unsophisticated personal storage over storing their Bitcoin on exchanges. A major catalyst in the spread of the phrase "not your keys, not your coin" and the overall mistrust of custodians, even licensed custodians, was the unreliability of early bitcoin exchanges, from poor security standards and frequent hacks, to outright scams and collapses.

Despite the poor state of many early exchanges, exchanges as a whole continued to be developed and improved upon. For the majority of users mining is not practical, or in the case of some institutional investors, may fall outside of their scope of operations. As more and more people began to adopt Bitcoin and other digital assets, so too did the amount of funds exchanges held on behalf of their customers and as liquidity necessary for daily operations. It is because of this that many early exchanges were also pioneers in the development of secure custody of digital assets. In fact some of today's leading custodians were also early digital asset exchanges.

Examples of these early exchanges and brokers that now offer high-grade custodial services among a suite of institutional offerings include: Coinbase, Gemini, and Genesis. Coinbase and Gemini were founded under a more straightforward exchange model and Genesis Trading began as an early Bitcoin OTC trading desk.

Crucial to their rapid development as institutional grade custodians has been the acquisition of existing custodian companies, all three custodians made acquisitions in 2021. The most recent acquisition was Coinbase's acquisition of Unbound Security in December 2021, in part for their multi-party computation (MPC) technology, a method of securely generating and distributing private key fragments without ever revealing the

entire key. Coinbase previously acquired Xapo's international business, a move that helped it cross the \$7 billion mark in assets under custody at the time of the deal in August 2019. In May 2021 Genesis Trading acquired London-based Vo1t notable for already possessing comprehensive security insurance at the time of acquisition. Finally, in June of 2021 Gemini acquired Shard X, namely for their MPC capabilities.

While industry leaders such as these have a clearly delineated distinction between their exchange and custody services, other exchanges have not taken these measures. Some exchanges offer staking rewards, interest payments, discounts or other incentives to encourage their users to retain their digital assets on their platform. While these exchanges will argue they are not custodians, they are also holding and securing funds on behalf of their customers.

From Manufacturers to Technology Providers

Another crucial innovation that helped lay the foundations of today's modern digital asset custody industry is the creation of the hardware wallet. Hardware wallets rendered paper wallets obsolete thanks to their ideal mix of security and ease of use. Both leading hardware manufacturers, Ledger and Trezor, have come to develop services that enable enterprise and institutional clients to secure their digital assets through a suite of specialized software and hardware offerings.

As both hardware and software manufacturers, both companies have created deeply integrated ecosystems designed to function seamlessly with their own hardware. Ledger, for example, has created what they call the Personal Secure Device which is linked to a particular user within a company and is used to authorize transactions. These solutions are tailored around the heightened needs of enterprise users, such as reporting and recordkeeping capabilities, the need for multiple secure devices, and more advanced ways of ensuring access, distribution, and recovery of vital data such as seed phrases.

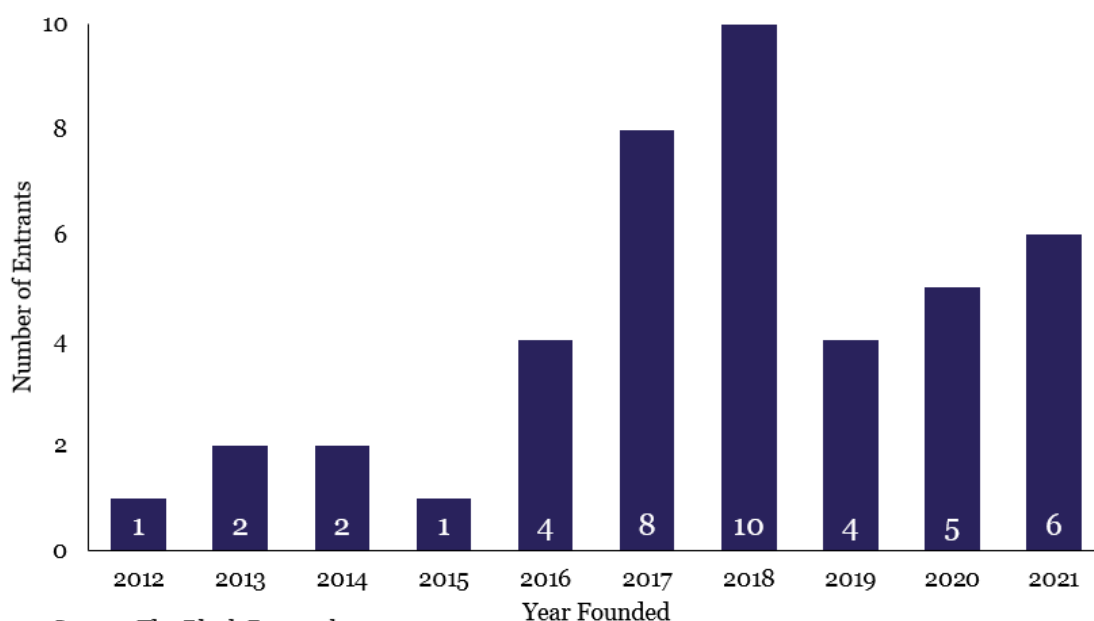
While both companies offer institutional services, Ledger has taken a more aggressive approach in growing this side of their business, with themselves and their customers often highlighting the \$150M insurance

included as part of the offering as a key differentiator for their service. This and other insurance offerings will be discussed in more detail further on. Though they do not disclose how many assets are secured via their enterprise offering, Ledger has stated that their customers range from institutions storing \$5M - \$10M in digital assets all the way to direct custodians who utilize their software with these making the top end of the customer spectrum ranging from \$2B - \$5B in assets under custody.

The Modern Custodial Industry

While the evolution of early participants into sophisticated custodians is noteworthy, it is important to remember how young this segment of the digital asset industry truly is. The majority of firms dedicated to the safeguarding of digital assets were founded in 2017 and 2018 which coincided with the significant appreciation of digital assets during those years. Even the companies previously mentioned did not enter the institutional custody space until many years after their founding. Coinbase founded in 2012, and Gemini and Ledger, both founded in 2014, did not create their dedicated institutional custodial offerings until 2018, 2019, and 2019 respectively.























Institutional Focused Custody Providers for Digital Assets (Year Founded)



Source: The Block Research

Institutional Custody for Digital Assets: A Primer

Chapter III: The Current State of Institutional Custody Solutions

Select Custodian M&A Activity			
Announced Date	Target	Acquirer	Amount (\$MM)
August-19	 xapo.*		\$55
January-20			Undisclosed
February-20			Undisclosed
April-20			Undisclosed
May-20			Undisclosed
January-21			Undisclosed
March-21			\$200 (Estimated)
May-21			\$1,200
June-21			Undisclosed
November-21			\$115
December-21			Undisclosed

*Coinbase acquired Xapo's institutional businesses only

Source: The Block Research, Company Press Releases

While many attention grabbing acquisitions in 2020 and 2021 came from the DeFi, infrastructure, and other payment and financial services spaces, there were also many high profile acquisitions and investments in the institutional custody space. The most notable acquisitions in 2021 have been PayPal's acquisition of Curv for an estimated \$200M, and Galaxy Digital's acquisition of BitGo for \$1.2B marking it as one of the largest acquisitions in the entire digital asset space to date. The rapid development, investment into, and acquisition of companies in the digital space shows that custody is a crucial foundational layer for businesses who invest and participate in the digital asset space, and wish to develop and offer increasingly sophisticated products.

One example of this is the acquisition of Israeli custodian GK8 by Celsius Network, a self-described "Centralized Finance" (CeFi) platform, for \$155M. Celsius and platforms like it offer customers returns on their deposits and aggregate them in order to generate a return via

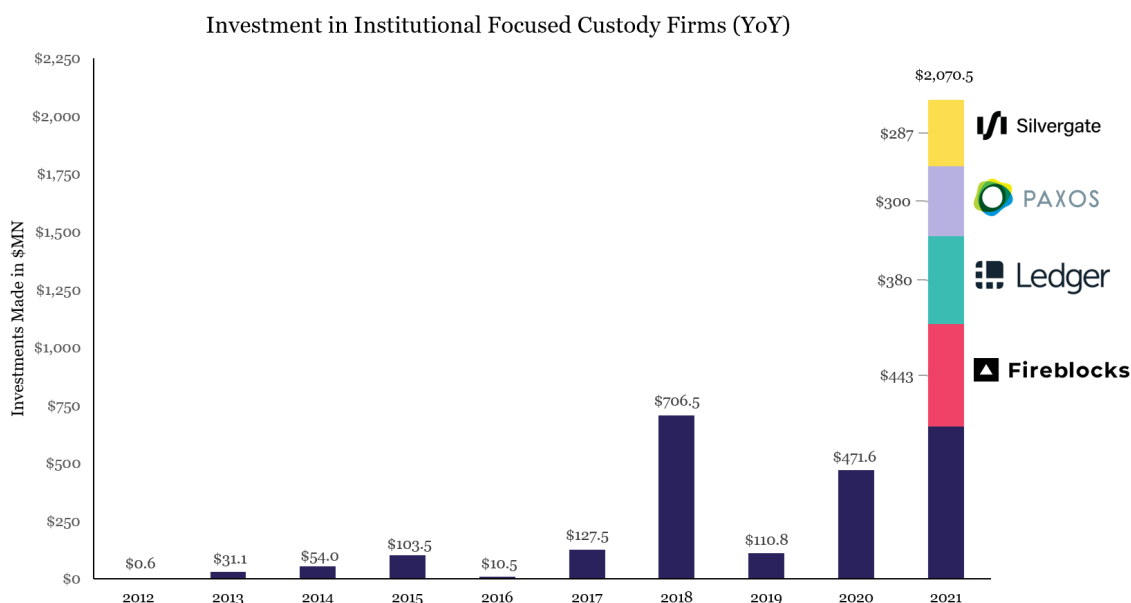
activities such as lending to trading firms, market makers, and exchanges. Other CeFi platforms rely on direct custody services and technology providers to safeguard customer funds. These platforms gather billions of dollars in user funds and are among the largest dollar value custody customers.

Acquisitions will continue to play an important role in the custodian industry. Both PayPal and Galaxy Digital stated that among their reasons for acquiring Curv and BitGo respectively, were their hard to find talent, strong technology, and intangible assets such as experience and customer relationships necessary for success. These are all aspects of successful custodians that require not only financial resources, but also a significant amount of time to be developed. For companies looking to jumpstart their development in the digital asset space, and looking to

bring the custody of their (or their clients') digital assets in-house, acquisitions are a logical investment to make.

Acquisitions from custodian businesses themselves have also been seen as these firms seek to strengthen their offerings. Acquisitions by Coinbase, Gemini, and Genesis Trading have already been mentioned. Other notable acquisitions in the space include Anchorage's acquisition of Merkel Data for their risk and data solutions, NYDIG's acquisition of crypto data firm Digital Assets Data, and BitGo's acquisition of Harbor and Lumia for their security token and reporting capabilities respectively before being acquired itself.

Fundraising: The growth in interest in digital asset custody is not only coming from institutional customers or larger players looking to acquire specialized firms. A significant amount of capital has also gone to investing into growing digital custodian firms especially in late 2020 and 2021. While Ledger had the single largest investment figure raising \$380M for their Series C, Fireblocks had a higher combined total, raising \$443M for their Series C and Series D both in 2021. Though not a fundraising event, Coinbase's IPO marked a landmark moment for digital assets as the exchange listed on the NASDAQ at a valuation of \$65.3B.



Source: The Block Research, Company Press Releases

One notable investment was that of the Swiss Stock Exchange into Custodigit, a digital asset provider offering a number of services including direct custody of assets, in December 2020. Though the amount of the investment was not disclosed, it is notable nonetheless that the third largest exchange organization in Europe is investing in the digital asset space. The Swiss Stock Exchange is not the only regulated stock exchange to delve into the digital asset space. For example Börse Stuttgart, the second largest stock exchange in Germany, founded Blocknox GmbH in August 2018 as a subsidiary specializing in the custody of digital assets on an escrow basis.

Regulation and the Evolution of Services and Platform Providers

An ever present and ever evolving topic in the digital asset industry, regulations have also had their hand in shaping the industry of institutional custody. As previously mentioned, certain types of institutions, such as investment advisers, are required by regulators to keep assets secured by a qualified custodian. However, in the current geopolitical landscape where data is being seen as an increasingly valuable commodity, some regulators may take action to ensure they have sufficient oversight over their local financial institutions and their transactions.

Should these regulatory trends continue, it is likely that direct custodians with an international presence will be required to further increase their compliance and licensing in each country they operate. It is also likely that these kinds of regulatory actions will encourage the creation of more local custodian institutions focused on servicing their national market. It is also possible that governments will create a regulatory environment to benefit their local institutions.

When it comes to technology providers, the effect of regulatory decisions is less direct given that they are not directly protecting customer funds. Many of a custodian's typical regulatory burdens such as KYC and AML enforcement are the customer's responsibility not the technology providers'. Regulatory decisions surrounding data transmission and storage more often affect technology providers. Countries may also enact regulation to encourage both direct custodians and technology providers to establish

legal entities in countries which they expand their services into so that regulators may have more insight into the financial operations they facilitate.

Many features common to both direct custodians and technology providers are highly requested because they not only help ensure customer safety, but also help clients remain compliant in their own operations. The most commonly seen features of this type include detailed transaction reporting, insurance, and policy and governance features, such as requiring multiple authorizers to a transaction, both provide security and help ensure customers remain compliant.

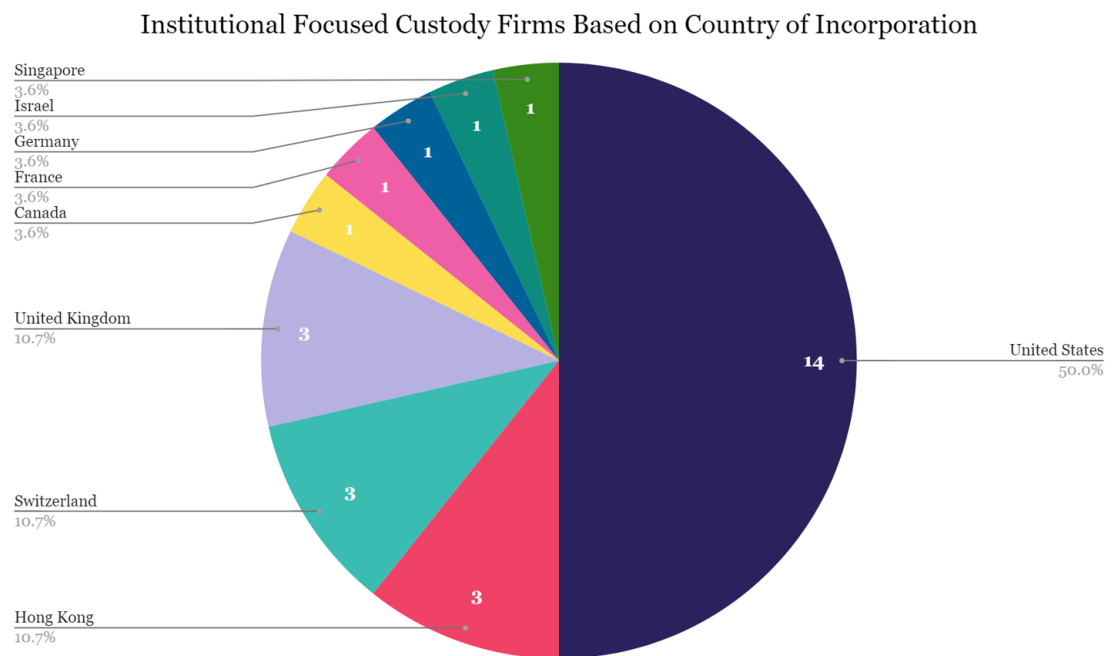
This section will explore the regulatory conditions in The United States, Japan, and Switzerland as they are geographically distant regions with key roles in the development of digital assets, custody, and technology, and have a range of sophisticated offerings for institutional grade investors. Though the U. S. is a global leader in digital assets, and their regulatory decisions greatly influence other regulators, their regulatory approach has also been criticized by some. Japan and Switzerland provide clear examples of how regulators in other leading digital asset jurisdictions are approaching the many regulatory challenges this new asset class presents.

The Regulatory Environment in The United States

Though the majority of institutional custodians offer their services to clients around the world, companies incorporated in the United States made up half of institutional focused custodian companies in 2020. Not only is the U.S. the largest economy on the planet, but is also a global leader in digital assets with many custodians, exchanges, brokers, developers, investors and more being based in or originating from the United States. It is no wonder that any regulatory decision (or even regulator's statements) makes headlines.

However many industry leaders have long been critical of the U.S. for what they call a lack of clarity and more recently "regulation by litigation". These critics state that regulators are choosing to punish actors in the space without providing clarity on where the regulatory boundaries lie. For example, while many treat stablecoins as a cash equivalent, the

IRS classifies stablecoins as property. Critics believe that the lack of clarity will lead to good actors being punished since they are the ones most likely to be responsive and invest resources in regulatory discussions and defending against litigation, but bad actors will simply continue ignoring regulators. More recently critics have stated concerns that the lack of regulatory clarity will lead to industry brain drain as entrepreneurs leave the U.S. in favor of other regions where regulations are not only clearer, but also friendlier. Countries praised for their friendlier, more comprehensive, or simply clearer regulations include Japan and Switzerland among others.



Source: The Block Research

Due to the fragmented nature of regulators in the U.S. and the fact that digital assets encompass a wide range of assets with a variety of purposes (security tokens, NFTs, governance tokens, utility tokens and more), it is not always clear which regulatory entity has jurisdiction over digital assets. A common example is that if a token behaves as a commodity or as a derivative, then it should fall under the jurisdiction of the Commodity Futures Trading Commission (CFTC), however tokens such as security tokens, most often intended to behave similarly to stocks, would fall under the purview of the Securities and Exchange Commission (SEC).

For custodians one particularly relevant regulatory entity is the Office of

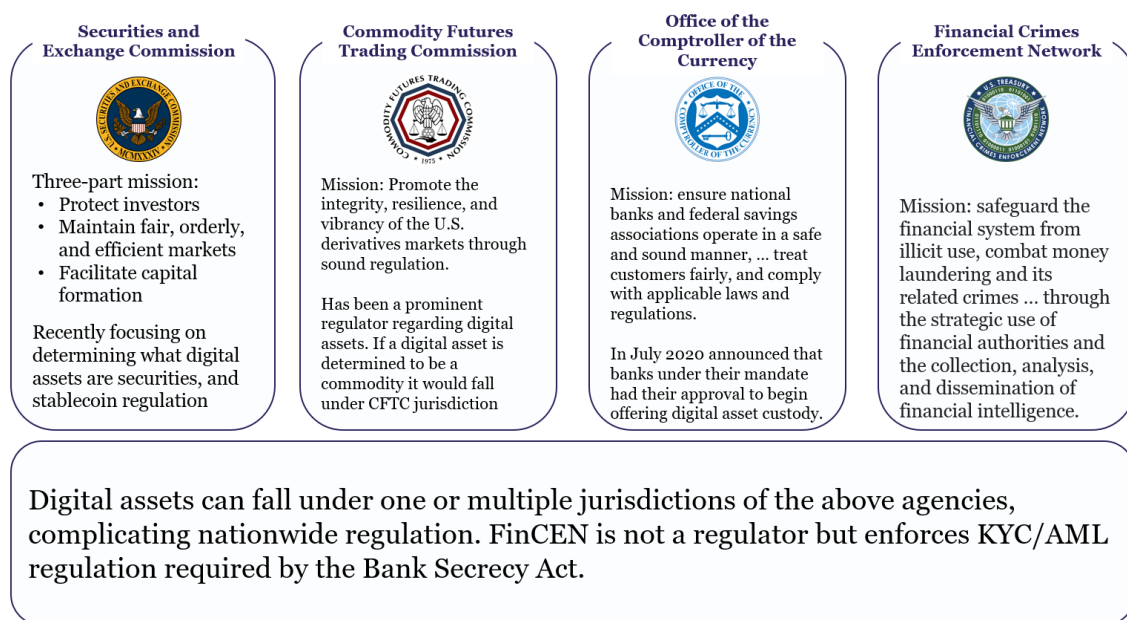
Institutional Custody for Digital Assets: A Primer

Chapter III: The Current State of Institutional Custody Solutions

the Comptroller of the Currency (OCC). The OCC is mandated with chartering and regulating all national banks and federally licensed foreign banks in the country. In July of 2020 the OCC announced that banks under their mandate now had their approval to begin offering digital asset custody. While this opened the door for traditional banking institutions to begin competing with “crypto first” custodians, very few banks have taken this step as of writing. One notable bank who has taken this step is BNY Mellon who announced the creation of their Digital Asset unit in February of 2021.

Finally, some important regulatory mandates such as Know Your Customer (KYC) and Anti Money Laundering (AML) requirements are part of the Bank Secrecy Act, which is enforced by the Financial Crimes Enforcement Network (FinCEN). States also play a prominent role in U.S. regulations as they can emit state licenses and other regulations or prosecute bad actors independently from federal authorities.

Relevant Regulatory Agencies in the United States for Digital Assets and Custodians



Source: The Block Research, Regulator's Websites

Looking to the future, upcoming regulatory decisions such as those surrounding stablecoins, other digital assets, and digital asset service providers may impact what assets custody focused firms can provide support for. These regulations may also affect value added products such as lend-

ing, and custody firms may be forced to alter how they operate. They may be unable to provide lending or other services to customers based on where the client is located, or may be unable to provide services altogether.

Given the diverse nature of digital assets combined with the numerous regulatory and enforcement agencies that exist in the U.S. the lack of clarity surrounding digital assets begins to make more sense. That said, when it comes to regulatory decision making, the majority of leaders, businesses, and investors in the U.S. are paying closest attention to the decisions of the SEC.

Key Facts:

- The Financial Market Supervisory Authority (FINMA) is Switzerland's financial regulatory authority. It is responsible for the supervision of banks, security dealers, exchanges, and the broader financial markets. This includes the issuance of banking licenses.
- Swiss law continues to develop. The first proper law regarding distributed ledger technology, the "DLT Act" was approved in 2020, but provisions concerning ledger-based securities only came into effect in February of 2021.

Regulatory Environment in Switzerland

With its long history in banking, financial services, and asset custody it is no surprise that Switzerland has also emerged as a leader in digital asset custody and banking. Switzerland, specifically Canton Zug, is also the home of many prominent ecosystem foundations including: the Ethereum Foundation, the Cardano Foundation, the Web3 Foundation (Polkadot), and the Tezos Foundation, among others.

Switzerland is also the home of a number of digital assets companies providing a wide range of services, including custody. When it comes to government licensing many of these providers are still in the application stage. However a few key licences have been granted to institutions who operate in the custody space. SEBA Bank and Sygnum were the first digital asset custodians to receive a FINMA banking license. SEBA bank is currently the only digital asset institution to obtain a Collective Investment Schemes Act (CISA) license in Switzerland. This license allows for SEBA Bank to offer digital custody services for Swiss domiciled mutual funds.

Traditional banking institutions have also begun to offer digital asset services to their customers, though this is usually on a per request basis as these institutions are only now beginning to develop their digital asset teams and custody capabilities. Some banks who have begun to build out these capabilities include Julius Bär, BBVA's Swiss entity, and private bank Vontobel. However, one traditional bank who has already launched their digital asset ser-

vices is InCore which acts as a payment gateway for the exchange Kraken.

Key Facts:

- The Financial Services Agency (FSA) is the main regulatory body
- After changes in the last few years, Custodians are now regulated in the same manner as exchanges even if they do not offer exchange services

Regulatory Environment in Japan

Though initially quite heavy handed due to the turbulent past digital assets have had in Japan⁵, the country has taken a more open approach over the last few years. One interviewee noted that since Japan has been at the forefront of digital assets with a number of important regulatory decisions, the overall regulatory picture in Japan is quite clear.

With regards to custodians in Japan, the largest recent regulatory shift has been the change to regulate them in the same manner as exchanges, even if they do not offer exchange services. This shift in categorization was seemingly done in order to bring custodians more in line with Know Your Customer (KYC) and Anti Money Laundering (AML) regulations already required of exchanges.

For custodians this means they are required to create and maintain identity and transaction records for their customers for a minimum of 7 years, report suspicious transactions and any transaction exceeding 30M Yen (approx. \$270,000) in either crypto or fiat to the Ministry of Finance. The Payment Services Act also enforces the use of “reliable methods” to secure customer funds, and places an upper limit to the percentage of funds an exchange may maintain in their hot wallets. This specific act was implemented to heighten the security of Japanese exchanges since many users, especially retail users, may rely on them for storage.

Best Practices

Though oftentimes not a result of direct regulations, throughout our interviews certain best practices were recurring answers to questions around institutional adoption of digital assets and utilization of both direct custodians and technology providers. These best practices have come about as a mix of security, transparency, favorable corporate structure, and impor-

⁵ The Mt. Gox bankruptcy has had a notable impact on regulations even outside of digital assets. It presented Japanese regulators with the rare case of a bankrupt enterprise's assets, recovered Bitcoin, being worth more than the initial bankruptcy claim due to Bitcoin's appreciation. User security has since become a top issue for Japanese regulators.

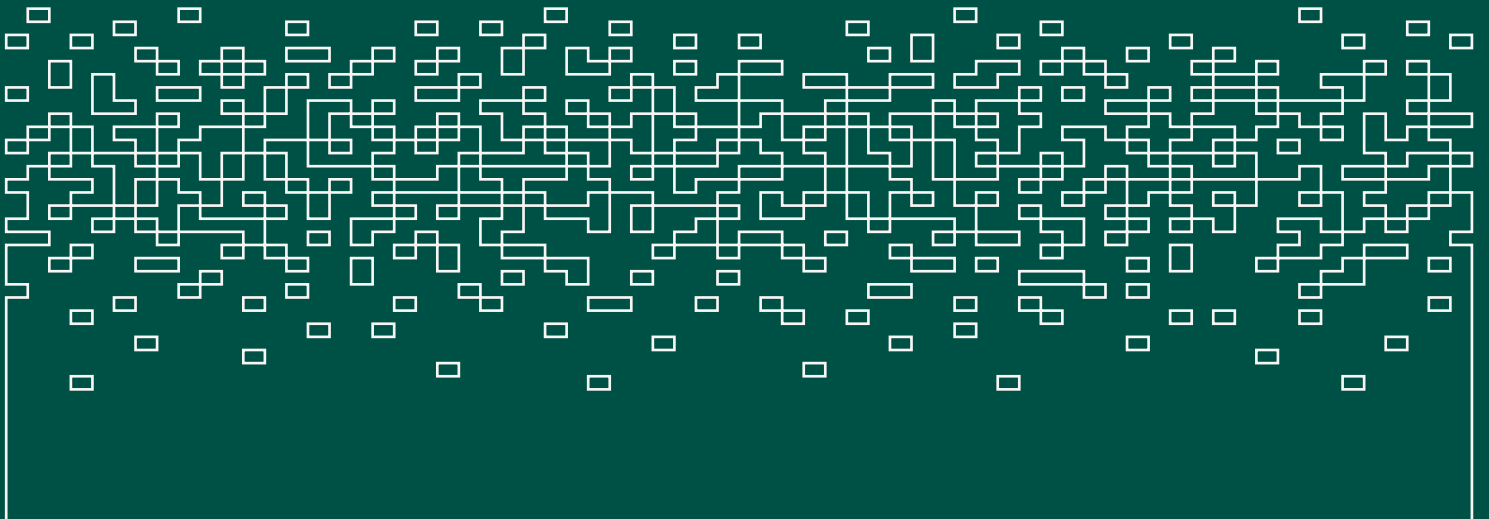
tantly provide institutional customers with a counterparty that meets the expectations carried over from the traditional financial world.

These best practices often include:

- Creating standalone businesses to exclusively handle custody.
 - This is separate from creating standalone business entities to service specific markets and better comply with those markets' regulatory requirements.
- Matching or even exceeding policies expected of traditional custodians regarding fund and risk management, access to hardware and software, recordkeeping, reporting, and KYC/AML compliance. These actions are also in line with regulatory requirements and help custodians obtain relevant licensing or approval.
- Higher client involvement. Given how new this asset class is to most investors, custody providers often act as knowledge sources for their clients when it comes to understanding how digital assets work or explaining how customer funds will be kept secure. Some examples of this include:
 - Setting up customer devices and providing training on proper usage of them
 - Ensuring customers understand the technologies and other components such as physical and cyber security that all work together to secure funds
 - Explaining specialized processes such as key generation ceremonies
- Rapid development in response to feedback, customer demand, and developments in the digital asset industry. DeFi integrations, for example, are a response to both industry development and client demand for access to these new products.
- Reporting standards such as SOC II, ISO 27001, third party audits or attestations of operations and/or funds, and regular security evaluations such as penetration testing all provide further confidence in a custodian's operations.

This section will cover in detail certain operational and technological details

IV Comparison of Institutional-Grade Custody Providers



of direct custodians and technology providers. It will also cover unique features of certain companies and products that these companies highlight in order to differentiate themselves from their competitors. These include: insurance, key generation, hardware support, customizability, and ease of use among others. Finally this section will present a comparison of leading custody providers, and key items for institutions to consider when selecting a custody provider for themselves.

Operational Management

It goes without saying that institutional custodians manage funds in a much more sophisticated manner than the majority of individual users, however the exact mechanisms of how this is achieved is not often understood even by institutions. There are a number of advanced techniques used to both securely generate and store the private keys which ultimately have control over digital assets. While every custodian optimizes for security and client needs in their own way, there are a number of areas of overlap. The following are the leading technologies utilized by custodians to help secure and manage access to digital assets.

Hardware Security Module: Often referred to simply as HSM, a hardware security module is a special piece of hardware that protects and stores digital keys, performs encryption, decryption, authentication, and other cryptographic functions. These modules are specially designed to be tamper-proof and isolated from external systems and the internet. HSMs are used across all industries where digital security is crucial, from securing medical hardware to protecting against piracy in online streaming, as well as in the traditional financial industry.

While a retail hardware wallet matches the strict definition of an HSM in that it is a specialized piece of hardware that encrypts and authorizes transactions, and exists (mostly) disconnected from other systems and the internet, it is not what institutional custodians refer to when discussing HSMs. When speaking of HSMs in the institutional custody space, this term refers to robust and highly specialized hardware, often custom built and running custom built software and operating systems. These more robust HSMs can serve multiple purposes for the custody of digital assets,

they can generate and store private keys as well as generate and sign transactions at high throughput.

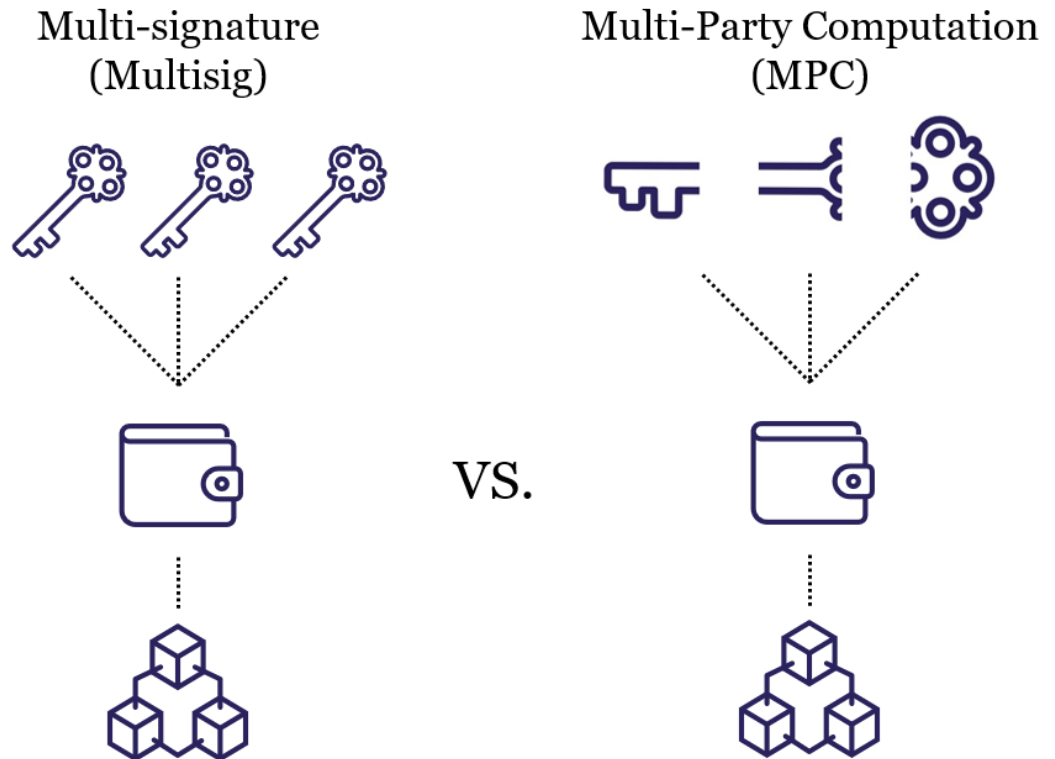
HSM implementations can be quite capital intensive with high variable costs, especially with a rapidly growing client base. Two noteworthy areas of cost are the requirement for physical access and the cost of new hardware. Since HSMs are hardware based solutions they require physical access by specialized engineers for deployment, maintenance, upgrading, and configuration. Along with this, scaling hardware is typically more expensive than scaling software due to the costs associated with purchasing, shipping, and installation.

Multi-Signature: often referred to as multisig, it is a system in which multiple keys are required to sign a digital asset transaction. These signatures can be from different devices, e.g. one person signing from their mobile device and from a hardware wallet, or they can be multiple keys held by multiple parties. This second system forms the minority of hybrid custody providers and is used by companies such as Keys.Casa, Unchained Capital, Gnosis Safe, and others.

Multisig takes a modified form when used in the institutional custodian space. Multisig is often implemented more as a policy and asset management feature than a strictly technical and security solution. Given that it is nearly impossible to reverse a blockchain transaction, institutional investors in digital assets often implement multisignature policies to ensure that no single individual in a company could conduct transactions. An additional benefit of a policy based implementation of multisig is that it can be applied to any digital asset supported by the custodian rather than utilizing a different multisig solution for every blockchain of interest as is the case with a traditional technological implementation.

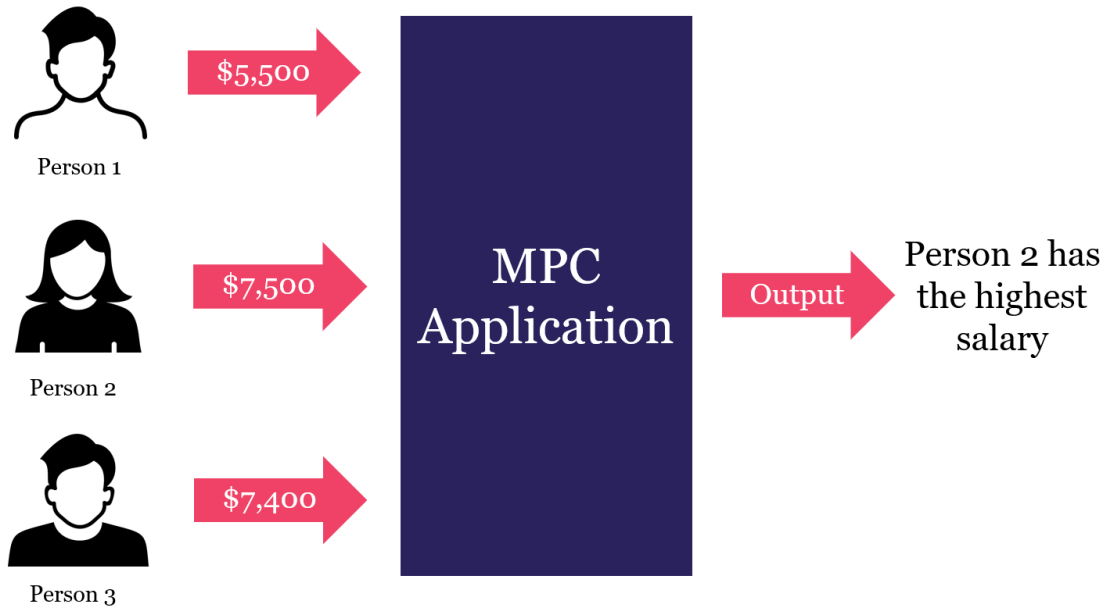
Multisig implementations can be entirely software based or also include hardware components for added security. Multisig can be designed to require a majority share for a transaction (3 of 5), a totality (5 of 5), and more advanced services can offer custom solutions. For example the Chief Investment Officer must be a signer on a transaction above a certain size overriding the simple majority rule, but the CIO cannot execute a

transaction without other signers.



Multi-Party Computation: While Multi-Party Computation or MPC has existed for decades, it has only begun to be applied to the field of digital assets in recent years. The main concept of MPC is that inputs can be taken from multiple sources to create a desired output, without the individual inputs being revealed to other participants. A simplified example can help illustrate the basic mechanisms of MPC.

Three coworkers would like to know who has the highest salary without revealing how much they earn. Each one of them can secretly input their salary into an MPC application which will output that person 2 has the highest salary, but the other two participants do not know how much this person makes or the difference between their own salaries and the salary of this person.



Building on this example, let's instead say that the three people wished to know their average salary. In order for each person's information to be kept private each person's salary is split into three shares of scrambled, but relevant, data. These shares are then randomly distributed to each of the participants. While the information each participant holds is individually useless they can still combine their shares to determine the correct sum of their total salaries in order to find their correct average.

MPC Shares of Data			
	Person 1	Person 2	Person 3
Share 1	\$8,381.00	-\$5,499.00	\$351.00
Share 2	-\$4,913.00	-\$10,042.00	\$27.00
Share 3	\$2,032.00	\$23,041.00	\$7,022.00
Sum	\$5,500.00	\$7,500.00	\$7,400.00

The previous table shows the scrambled data of each participant before being randomly distributed. While each person's shares sum to their respective salaries, once the data is randomly distributed it becomes impossible for an individual outside the group to determine a specific person's salary. Even for those within the group, if simply given the 9 shares of data, they would have a very hard time finding the 3 shares that correspond to their individual salary. As this process is scaled up to utilize more inputs, more sophisticated data obfuscation, and generate more data shares, it becomes impossible to determine inputs even for participants.

While MPC can be utilized in a number of fields and applications, there are a number of key benefits when it comes to the secure custody of digital assets. The main way in which MPC technology is implemented by custodians and technology providers is in secure key generation. MPC allows for private key shards to be generated, distributed, and used to produce signatures without the private key ever having existed as a whole. This is in contrast to other methods of sharding keys wherein the private key is first made and then divided and distributed. This crucial difference has led to a growing number of institutional custodians adopting MPC technology, stating that it is a superior form of multisignature technology.

The largest benefit to generating private keys in this manner is that there is never a single point of failure in the lifespan of that private key. These key shards can then be utilized under a similar governance policy as previously described, in which all key shards or a predetermined number of them, must sign in order to approve a transaction.

However MPC, like any other technology, has limitations and tradeoffs. Without proper accompanying software, MPC can provide less accountability than a multisig system. This is because MPC key shards combine to form a single signature, from which it is impossible to determine the individual parts, as opposed to the M of N individual signatures that make up a multisig transaction. If for example 2 employees colluded to execute a fraudulent 2-of-3 MPC transaction it would be impossible to determine who signed from the transaction alone. Other criticisms of MPC include the frequent use of proprietary methods which make it difficult to inde-

















pendently verify their security, and the lack of HSMs which support MPC. However it is important to note that Intel Software Guard Extension or SGX does support MPC implementations, but also that SGX is different from a traditional HSM. Intel SGX is a form of hardware based encryption wherein security instructions are directly built into the CPU to create secure enclaves for data.

Policies and Other Safeguards: There are of course a number of policies and safeguards implemented by custodians and technology providers to ensure the safety of their customers and their assets. Some commonly implemented policies and safeguards include:

- Policies around which types of transactions may be carried out automatically and which transactions must be done manually. For example, removing funds from cold storage often includes one or more manual processes.
- Policies around which types of transactions require human touchpoint verification such as a video call. These policies are often customized to match customer needs, but two common triggers are transactions over a predetermined amount or to remove funds from cold storage.
- Policies around how private key backups are stored, encrypted, and maintained, and in what form (physical vs digital).
 - These backups can also be further fragmented and encrypted and stored in geographically separate locations for additional security.
- Some custodians and technology providers develop specialized hardware for their clients in order to provide an additional layer of security when executing transactions.
 - These devices may also have custom software with features such as displaying transaction data in human readable form.
- Some custodians and technology providers create secure transaction channels for their customers to transact with each other with low friction within that particular provider's environment.

Considerations on Custodian Offerings

When it comes to comparing custodian and technology provider offerings it is important to identify which aspects of the provider and their offerings are the most important for an institution, as well as what strategies the institution wishes to employ and what forms of risks they wish to minimize. These considerations can range from support of a specific asset, to the underlying technology securing the assets, to counterparty risk.

Overview of Institutional Focused Digital Asset Custody Firms						
Custodian / Technology Provider	Founded	Domicile	Direct / Technology Provider / Hybrid	Technologies Used	Assets Supported	Assets Under Custody (\$BN)
 ANCHORAGE DIGITAL	2017	U.S.	Direct	HSM	74	Undisclosed
 bakkt	2018	U.S.	Direct	HSM, Multisig	Bitcoin, Ether (Announced)	Undisclosed
 Bitcoin Suisse	2017 (Custody)	Switzerland	Direct	Multisig	14+	>\$5 (Nov-21)
 BitGo	2013	U.S.	Hybrid	HSM, Multisig	400+	>\$64 (Nov-21)
 coinbase	2018 (Custody)	U.S.	Direct	MPC	140+	>\$140 (Sept-21)
 copper	2018	U.K.	Direct	HSM, MPC	400+	>\$10 (Sept-21)
 Fidelity DIGITAL ASSETS	2019 (Custody)	U.S.	Direct	Undisclosed	Bitcoin	Undisclosed
 Fireblocks	2018	U.S.	Technology Provider	MPC	1,500+	-
 GEMINI	2019 (Custody)	U.S.	Direct	HSM, MPC	74	>\$30 (Jun-21)
 Genesis	2020 (Custody)	U.S.	Direct	MPC	20+	Undisclosed
 Hex Trust	2018	Hong Kong	Hybrid	HSM, Undisclosed*	100+ and NFTs	>\$2 (Oct-21)
 Ledger	2019 (Custody)	France	Technology Provider	HSM	1,500+	-
 NYDIG	2017	U.S.	Direct	Undisclosed	Bitcoin**	>\$6 (May-21)
 Qredo	2019	U.K.	Technology Provider	MPC	15	-
 SEBA BANK <small>Banking Partner for the New Economy</small>	2018	Switzerland	Direct	HSM, Multisig	11	Undisclosed
 Silvergate	2020 (Custody)	U.S.	Direct	Undisclosed	Bitcoin and others***	>\$11 (Oct-21)

Source: The Block Research, Company Press Releases, Interviews, SEC Filings, FDIC Filings, Corporate Websites. Not an exhaustive list of custodial offerings.

* Hex Trust utilizes ZeroKey, a proprietary technology, and does not disclose if it is multisig or MPC based

** NYDIG Officially only supports Bitcoins, however sources including an investor have stated that NYDIG supports 4 additional digital assets

*** Silvergate does not publicly disclose their full list of supported assets

Asset Support: While the number of digital assets continues to grow daily, custodians take a measured approach in supporting assets and blockchains. Asset support by direct custodians and technology providers can range from Bitcoin only (typically seen in heavily regulated direct custodians) to hundreds or thousands of assets enabled through the support of token standards, the most prominent of which is Ethereum's ERC-20 token standard. From the provider's perspective the technical challenges of supporting new assets mostly occur when new blockchains are being added to their service offerings, once support is enabled adding token support for that blockchain is comparatively straightforward.

When deciding to add support for a new asset or blockchains custodians tend to broadly look for the following characteristics:

- Liquidity
- Compliance and/or regulatory clarity
- Development history and capacity
- Decentralization, validators, and network stability
- Reputational risk in case of enabling/supporting a problematic asset

Direct custodians tend to be more conservative in their asset support, with a number of custodians backed by large financial institutions such as Bakkt, Fidelity Digital Asset Holdings, and Silvergate backing only Bitcoin, or Bitcoin and a very limited number of additional assets. Technology providers on the other hand are more flexible in enabling support of additional digital assets given that end users bear many of the risks associated with newer digital assets. For technology providers the major decision is developing the necessary infrastructure to support an additional blockchain.

Technologies Used: With the continuous development of new technologies it is important to understand the benefits and limitations of them and how they interact with other aspects of a digital asset strategy. In particular it is important to understand how a custody firm's use of HSM, MPC, multisig, and other technologies affect client side operations, especially when self custodizing through a technology provider.

For companies who choose to utilize a direct custodian the impact of technologies on their operations is much smaller than in the past. Previously institutions would have to purchase digital assets first and then transfer them to a direct custodian and because of this had to account for some degree of self custody in their operations. However today many leading direct custodians now offer trading and brokerage services to assist their clients in purchasing digital assets through them and immediately secure newly purchased assets.

However for those who choose to self custody the choice of provider and their technological strategy has real operational implications. For example, if choosing to utilize a multisig solution a company may create one or more additional “backup” keys to mitigate the risk of losing a key; companies may even entrust backup key(s) to their technology provider if the provider allows for it. Another operational consideration is that of complementary devices such as specialized hardware provided by the company. Learning how to correctly use and secure devices supplied by a technology provider is also a crucial operational task that may even require training by the technology provider.

Unique Solutions/Offerings: As competition in the custodial landscape increases along with the level of customer sophistication, many custodians have developed unique solutions and products to distinguish themselves. Some standouts in unique products include:

- **Copper Clear Loop:** Allows for customer assets in custody to be utilized for trading on centralized exchanges with balance changes settled afterwards
- **Fireblocks Digital Asset Transfer Network:** Connects customers with each other, and with exchanges and protocols allowing rebalancing across exchanges and instant settlements among customers
- **Silvergate Exchange Network (SEN):** Enables clients to send U.S. dollars 24/7 to other clients. Participating in the SEN requires an active

banking relationship with Silvergate

- **Bakkt Futures & Options:** Bakkt is also the provider of Bitcoin Futures and Options derivatives. Futures are physically settled monthly contracts for bitcoin held in the Bakkt Warehouse
- **SEBA Bank Tokenization:** Offers customers asset tokenization and storage of their newly created tokens. Examples of assets that SEBA tokenizes include: equity, debt, precious metals, commodities, fine art, and copyrights among others

Internal Investment Strategy: Though custodians are constantly innovating and offering additional ways of interacting with decentralized products, there are differences in the ability to execute certain strategies depending on the provider. While trading through centralized exchanges is facilitated by both direct custodians and technology providers, utilizing decentralized exchanges and other decentralized products is typically easier to achieve through a technology provider.

Broadly speaking, firms that are actively engaging in DeFi and other decentralized products will likely prefer to rely on technology providers. On the other hand, institutions looking for prime brokerage services, structured products, derivatives and other sophisticated financial services will likely choose to engage with direct custodians. Firms that are heavily regulated or offer structured products of their own are likely to be compelled to use direct custodians who have qualified custodian certifications.

Long-Term Vision: Just as it is important to understand the company's internal investment strategy before selecting a custody provider, it is also vital to understand the provider's long-term goals and vision. Some companies have explicit goals, for example catering to a certain type of institutions such as banks or hedge funds, or providing specialized services around a narrow selection of products such as derivatives or retirement accounts. Other custodial firms may be part of a larger company that has goals beyond securing digital assets, while this is not a negative, some companies may prefer selecting a counterparty that is highly specialized in securing digital assets. Though not as directly impactful as asset sup-

port or technologies used, having long-term vision and goal alignment with a custodial provider adds an intangible layer of value and understanding between the customer and custodial firm.

Counterparty and Other Risks: While custodians and technology providers go to great lengths to ensure the security of their products and services, counterparty risk is still worth consideration. From the perspective of multi-billion dollar institutions many custodial providers are simply startups. When evaluating from this perspective the clear approach would be to engage with custodians who have a high degree of experience and knowledge regarding digital assets, or those who have institutional backgrounds themselves and understand exactly how to cater to institutions like themselves.

Other risk considerations also apply to utilizing newer technologies such as MPC. While the technology is impressive and well understood in applications outside of digital assets, entrusting billions of dollars in digital assets to recently adopted technology does carry risk. Many custodians who focus on this highest level of institutional customers such as BitGo, Bakkt, and Ledger choose to utilize technologies that are better understood such as HSM and multisig. Finally the regulatory risk of the specific assets being custodied is important to consider as well. Many traditional finance backed custodians carry only Bitcoin or Bitcoin and a limited selection of other assets with clearer regulatory standing, but complement their limited assets with sophisticated and regulated offerings such as options, futures, and retirement account offerings.

Insurance: Insurance provided by custodians is a topic that can be easily misunderstood. The first point worth highlighting is that under current regulatory circumstances digital assets are not covered by FDIC or other forms of government insurance in other nations. Custodians negotiate their insurance offerings directly with their counterparties, and given the novelty and unique risks of digital assets, the majority of digital asset insurance plans are custom made. Second, many of these insurance plans are very detailed in what they do and do not cover for example while one company's insurance plan may cover transactions on its network between clients, another company may only provide coverage while assets are in cold storage, and

still other policies may focus on theft by employees or third parties. Given that digital asset insurance is incredibly new and developed on a case by case basis it is vital that companies looking to utilize a custodian or technology provider clearly understand what is covered by a particular insurance offering. Detailed information about these policies is not publicly disclosed, and should be provided to customers as part of the sales and onboarding process. Some companies do publicly provide basic details regarding their insurance plans, here are two examples of custodian and technology provider insurance:

- BitGo: All customers have a \$100m policy for assets held in BitGo's qualified custody at BitGo Trust where all private keys are held by BitGo Trust or BitGo, Inc. and are covered in the event of:
 - Third-party hacks of cold-storage environment
 - Copying or theft of private keys
 - Dishonest acts by BitGo employees
 - Loss of key material due to natural disasters

BitGo also offers the option to purchase additional insurance upon request.

- Ledger: Provides a \$150m crime insurance program which covers:
 - Third-party theft of the master seed and private keys following a physical breach of a hardware security module in a secure data center.
 - Secure transmissions of the master seed fragments as part of the client onboarding.
 - Insider Ledger employee theft caused by collusion.

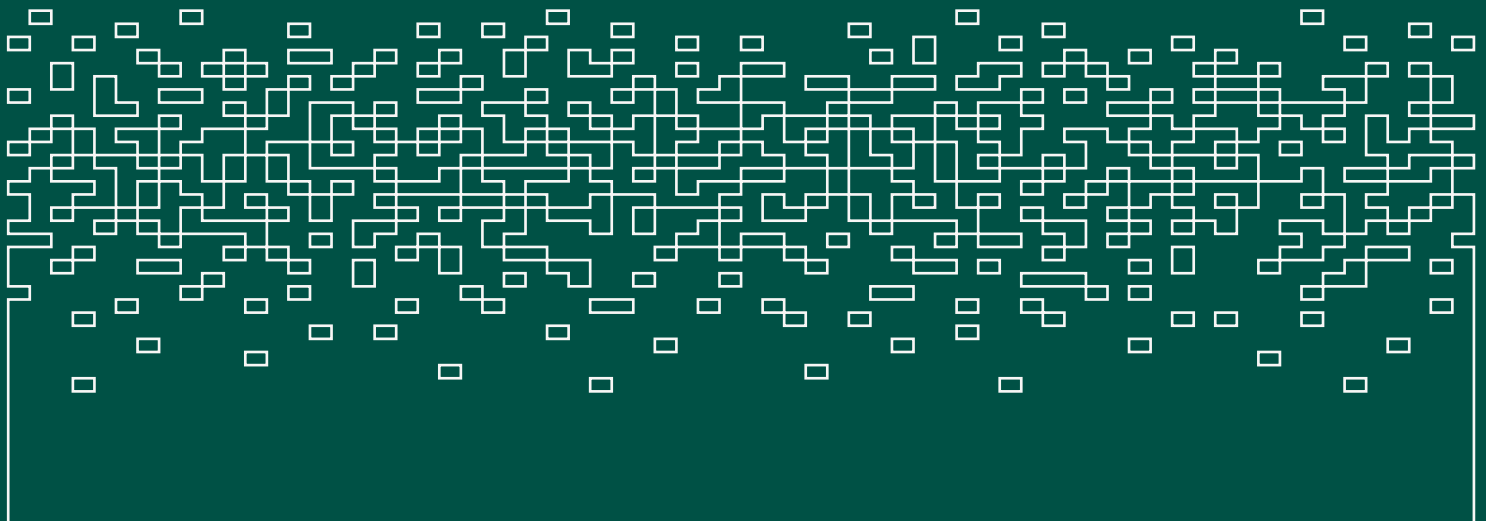
As these examples lay out, custodian insurance plans often have very specific coverage conditions and vary in policy size. Custodians such as BitGo, Coinbase, and Bakkt also give customers the option to purchase additional coverage.

Regulatory Considerations: These considerations apply to both the custodian and the institution looking to custody assets. From the custodian's perspective this includes items such as relevant regulatory licensing, especially for direct custodians, proper corporate structure, reporting requirements, and proper creation of international entities.

From the perspective of the institution, their own regulatory requirements may disqualify certain forms of custody solutions for them. For example, they may be required by regulations to utilize qualified custodians, or may have geographic restrictions on where their assets may be secured. Institutions may also face other forms of internal limitations such as ESG committees favoring Proof-of-Stake blockchains over Proof-of-Work blockchains. During an interview, one custodian mentioned that third party auditors may reject an audit request based on how custody is structured. If third party auditing is important for regulatory compliance, companies should consult with auditors who specialize in digital asset audits to understand which forms of custody structures comply with their auditing standards.

Having a clear internal understanding of what assets and strategies both align with company goals and are compliant is crucial for selecting the appropriate custodian or technology provider that can enable the secure execution of that strategy.

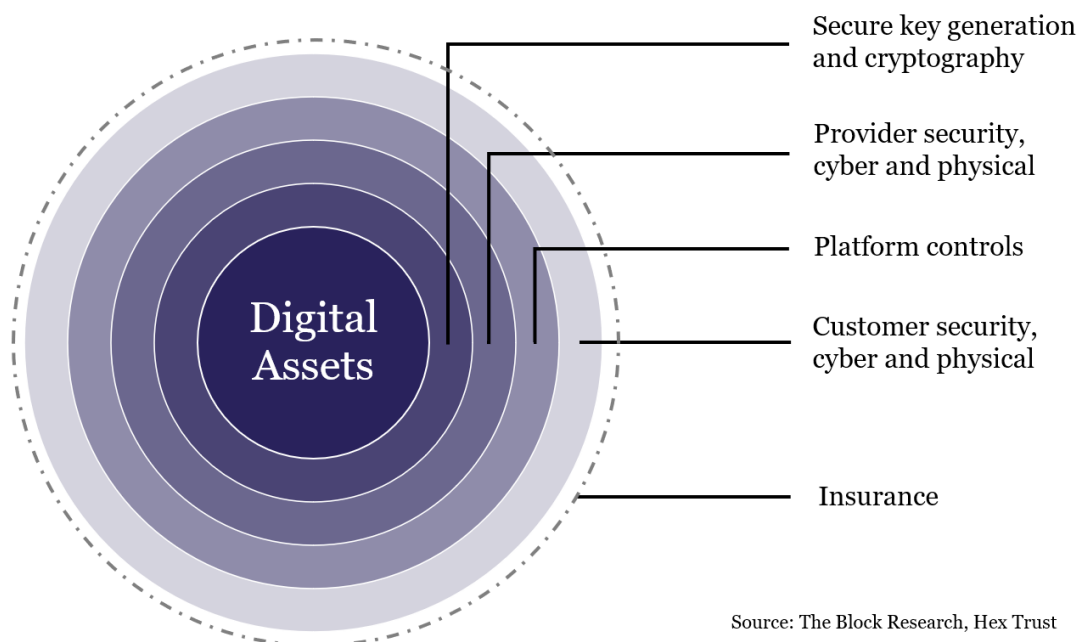
Conclusion



Like nearly all facets of the digital asset industry, custody has taken major strides towards maturity, especially at the institutional levels. While it is not a topic that is given as much attention as it deserves, custody of digital assets is a foundational layer of the asset class. Custodial solutions will continue to grow in importance as sophisticated services such as prime brokerage, lending, derivatives, and others continue to be built utilizing institutional custodial services.

Custody is not a single technology or strategy, it is a multilayered combination of physical and digital security, process, design, policy implementation, and matching customer needs with the right tools and services. This multilayered approach highlights the rapid development of custody from homemade paper wallets to a growing multi-billion dollar industry.

Layers to Securing Digital Assets for Institutions



Regardless of whether firms choose to rely on a direct custodian or utilize the services of a technology provider, these companies provide increasingly valuable services for the growing number of institutions in the digital asset space. The choice between direct custody or self custody is one that will change from company to company, and a choice that has real implica-

Institutional Custody for Digital Assets: Conclusion

A Primer

tions for the technology and methods utilized as well as the internal procedures and operations of companies active in the digital asset space.

The growing number of sophisticated institutions entering the space and utilizing increasingly advanced products has been enabled in large part by the technological advances of the custodial industry. In only a few years, the topic of digital asset custody has gone from basic software on laptops and cumbersome paper wallets, to a rapidly growing multibillion dollar industry in which traditional financial juggernauts are the ones struggling to keep up. It is in part due to the rapid sophistication of the industry that the next stage of digital asset custody is likely to be a continuation of rapid investments and acquisitions from more traditional financial institutions as they seek to keep pace with the rapid growth of digital assets.

Regardless, custodians will have to continue rapidly developing and implementing solutions as there will not only be continued growth in the number of decentralized products, but also in the number of assets that will be digitized. Though many institutions are currently focusing on entering the DeFi space, the explosive growth of NFTs is creating an entire new segment of digital assets that will require specialized custodial solutions. Furthermore, the potential of digitization is so great that it has not only captured the attention of companies like Microsoft and Adidas, but has also led to the renaming of Facebook to Meta, a reference to the metaverse, a reality that blurs the lines between physical and digital. Some custodial firms are already looking ahead to this increasingly digitized future and building out solutions to secure both digital first assets as well as assets that have digital representations through means such as tokenization. As our world and our assets continue to be digitized, being able to secure the ownership of our digital assets will continue to be one of the most important topics in the industry.

© 2021 The Block Crypto, Inc. All Rights Reserved. This report is provided for informational purposes only. It is not offered or intended to be used as legal, tax, investment, financial, or other advice.

