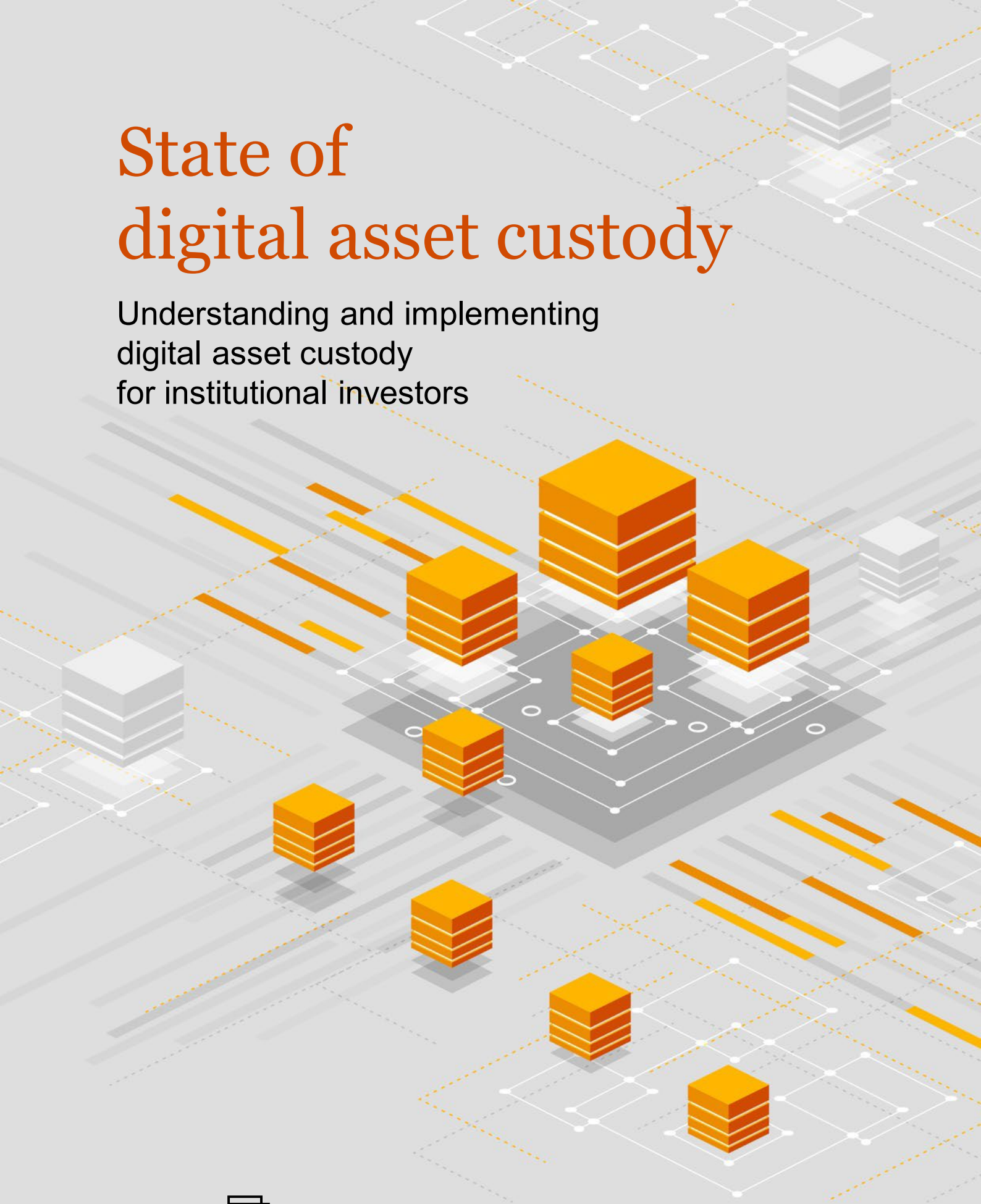
State of digital asset custody

Understanding and implementing
digital asset custody
for institutional investors



pwc

ASPEN DIGITAL

Notices

Readers are responsible for making their own independent assessment of the information in this document. This document: (a) is for general information purposes only and should not be used as a substitute for consultation with professional advisors, and (b) represents current market offerings and practices.

The information contained in this whitepaper is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of professional advice or service by PricewaterhouseCoopers Limited ("PwC") nor Aspen Digital. PwC and Aspen Digital have no obligation to update the information as regulation and practices change. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual client service team from PwC, Aspen Digital, or your other advisors.

The materials contained in this whitepaper were assembled on 16 June 2023 and were based on information available at that time.

Table of contents

Executive Summary

> 'Safekeeping of assets and ensuring they are segregated from client service providers' own (house) assets is a fundamental need. This has applied for many years in the traditional securities industry – so I am pleased to see that there are credible options available now in the digital assets ecosystem'
>
> Duncan Fitzgerald,
> Digital Assets & Web3 Co-Leader, PwC

> 'For institutional investors looking to allocate into digital assets, understanding the unique characteristics of custody solutions and providers compared with traditional assets is one of the biggest impediments when considering investment'
>
> Elliot Andrews,
> CEO, Aspen Digital

Since Bitcoin's inception in 2008, digital assets have emerged as an alternative asset class and gained significant attention from institutional investors. As digital asset adoption has surged, the need for institutional-grade digital asset custody for family offices, high-net-worth individuals (HNWIs) and external asset managers (EAMs) has also continued to grow. The PwC Aspen State of Digital Asset Custody report sheds light on the role of custody in enabling Asian institutional investors to grow and capture new opportunities in the digital asset ecosystem.

Institutions face key challenges in the safeguarding and transacting of digital assets, whether it be from operational complexity, security and reputational risks, or availability of insurance policies, among others. As the digital asset industry evolves, more institutions realise that self-custodial solutions have limitations in supporting the ongoing trading and operational needs of their growing digital asset portfolios. Many market participants have indicated that Asian institutional investors are increasingly seeking reliable, institution-grade digital asset custody options to safeguard both their existing digital asset holdings and new investment targets.

Digital asset custodians have expanded their role from the safekeeping of cryptocurrencies to helping clients navigate and participate in new business opportunities and asset classes, such as decentralised finance (DeFi), non-fungible tokens (NFTs), and metaverses.

In light of this evolving digital asset ecosystem, custodians worldwide are striving to enhance their technical capabilities and service offerings. This includes multi-party computation in transaction approvals and creating a custodial ecosystem that facilitates access to and the safeguarding of different types of digital assets – from NFT collectibles to staking and liquidity provision in DeFi protocols.

The ability to securely hold and access digital assets of all types is a core building block of digital asset strategies for Asian institutional investors. Our report introduces a multi-faceted approach to implementing a digital asset custody model that meets your institutional needs.

Section 1

Current state of digital asset custody

The digital asset industry has grown into a $1.2 trillion dollar market, reaching over $3 trillion at its peak in November 2021[1]. Bitcoin was the earliest digital asset, which appeared in 2008 as a peer-to-peer electronic currency built on the blockchain. Soon, technological advancements led to the creation of other blockchain protocols, including Ethereum, whose smart contract capabilities enabled developers to build thousands of decentralised applications.

The digital asset industry has evolved to over 8,000 cryptocurrencies[2] in 2023 and most institutions have tapped into the asset class by trading Bitcoin and Ethereum. One key difference between trading most financial instruments and digital assets lies in the process of custody. In the context of digital assets, custody refers to the process of safekeeping cryptographic private keys which are used to execute transactions on a blockchain network. Custodians of digital assets refer to any individual or entity who controls a blockchain wallet's private keys.

The need for digital asset custody has grown alongside industry development. Self-custodial solutions first emerged for retail investors after the Mt. Gox (a Bitcoin exchange) hack in 2014. The beginning of digital asset derivatives, marked by CME Group's launch of Bitcoin futures in late 2017, indicated the first wave of institutional interest in the growing asset class. However, self-custodial solutions were not capable of meeting institutional needs. With the increasing complexity of digital assets and the entrance of institutional investors into the space, digital asset custodians have been designed to sit at the intersection of the two.

Digital assets have evolved to include a vast range of products and sectors, such as stablecoins, non-fungible tokens, Layer-2 blockchains, gaming, liquid staking derivatives, oracles, and more. The private wealth sector, which includes family offices, HNWIs and EAMs, is becoming increasingly interested in this constantly evolving sector. As crypto products have grown more complex, custody solutions have had to rapidly advance their parameters and security.

The global digital asset custody market was valued at $447.9 billion in 2022[3]. With their growing interest in the market, private wealth sector participants are in search of reliable digital asset custody solutions. In particular, family offices, HNWIs and EAMs are looking for custody solutions that provide security and access to the broader digital asset ecosystem.

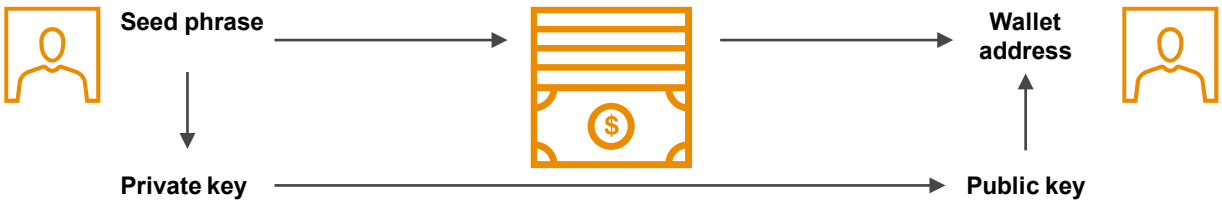
1. CoinGecko
2. CoinMarketCap
3. Proficient Market Insights, Digital Asset Custody Market Report 2023

How does a blockchain wallet work?

Firstly, it is essential to understand how a blockchain wallet works. This is a digital wallet that allows individuals and entities to manage their digital assets. There are four major components to a blockchain wallet:

1. A ‘seed phrase’ is crucial for restoring access to a wallet if it is lost, damaged or needs to be recovered for any other reason. It typically consists of 12 or more words that are randomly generated and serve as a master key to the wallet.
2. A ‘private key’ enables the owner of the wallet to control and access cryptocurrencies within the wallet. Loss of, or unauthorised access to, the private key can result in loss of access to the wallet and the cryptocurrencies stored in it.
3. A ‘public key’ serves as an address to receive cryptocurrencies from other users. It is commonly used in conjunction with a digital signature to verify the authenticity of transactions and to ensure that only the owner of the corresponding private key can spend the associated cryptocurrencies or assets in the wallet.
4. A ‘wallet address’ is a unique identifier used to send and receive cryptocurrencies. It is used by other users to send cryptocurrencies and other digital assets to the wallet. In addition, it is necessary to provide a sender with the correct wallet address when receiving cryptocurrencies to ensure that assets are properly credited to the intended wallet.

Figure 1: How a blockchain wallet works



What are the different types of wallets?

There are three major types of digital asset wallets: hot wallets, warm wallets, and cold wallets.

Hot wallets are designed to be constantly connected to the internet and ready for transactions in real time. They are suitable for frequent transactions, readily serving as a user interface for investors to buy, sell or swap their digital assets for day-to-day use.

Once created, hot wallets can be accessed by logging into a mobile app or through an internet browser extension. The private keys in the hot wallet allow users to initiate transactions, access the wallet and check wallet balances. While hot wallets are convenient for accessing funds on the go, they are more susceptible to hacks if the security of the private key is compromised.

A cold wallet protects your digital assets by holding your private key offline and is secured with a physical hardware wallet. As cold wallets are not connected to the internet and are safeguarded by a separate device from one's other electronics, such as a laptop or mobile phone, they are generally less susceptible to hacks.

The process of accessing funds that are held in a cold wallet is extremely manual, which is a security feature. Take hardware wallets as an example. Firstly, you must locate the hardware wallet, which is a physical device. Then, you must connect the device to a secure computer and open the hardware wallet by manually inputting the PIN code. Next, you must log into the computer and into the hard wallet's application, which allows you to see your crypto holdings in the wallet. In order to transfer any amount of crypto that is held in cold storage, you must input the address, the correct blockchain network, and the correct wallet address on the application. Then, you must confirm the transaction using the physical hardware wallet.

The transaction process of cold storage is vastly different from traditional finance, where an individual does not have to consider how to physically safeguard their assets and can leave that responsibility to their respective bank or custodian. Below are the steps to how transactions in cold wallets work:

Figure 2: How transactions in cold wallets work

How transactions in cold wallets work

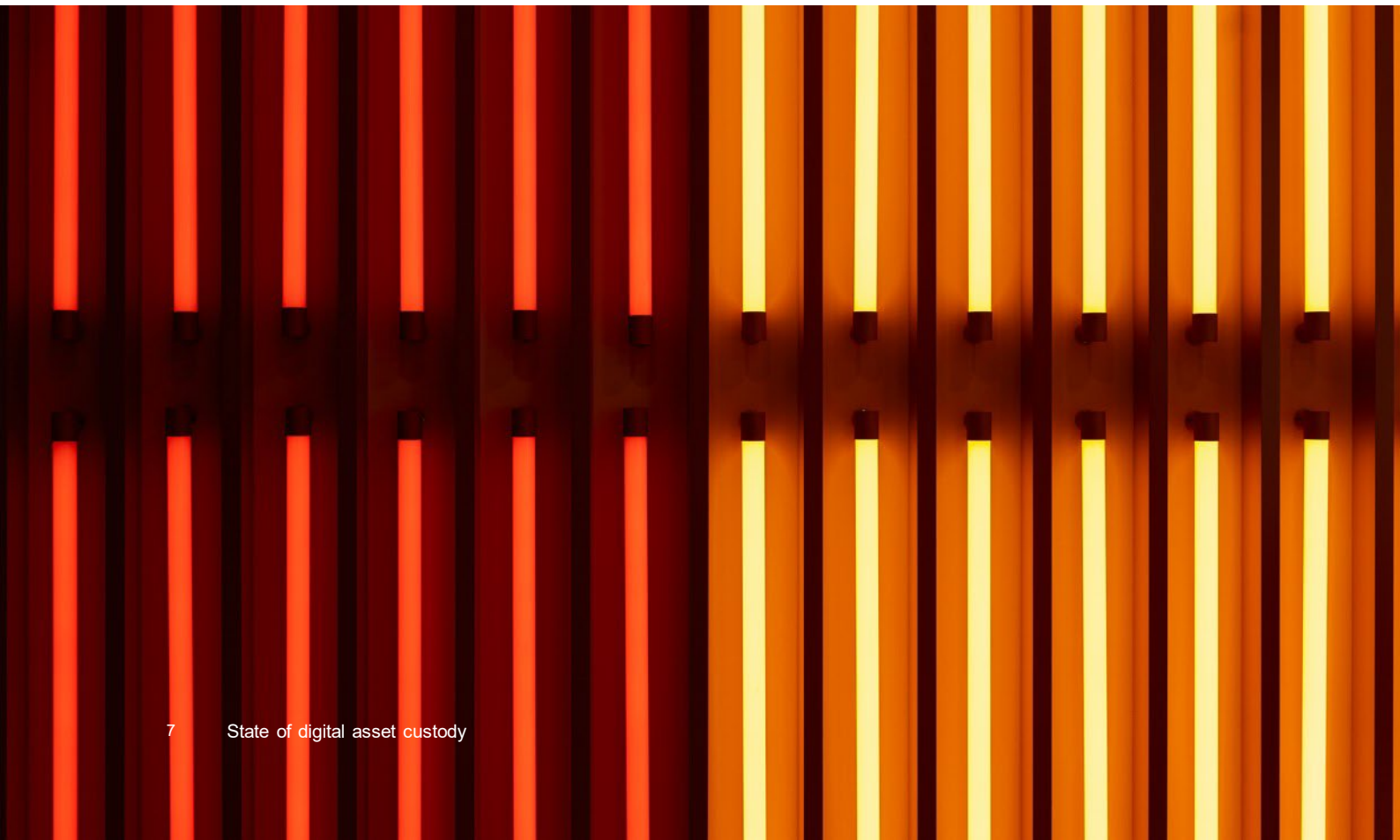
1. Connect hardware wallet to the computer by inputting the PIN code
2. Login to the hard wallet application in the computer
3. Initiate the transaction by inputting sending and receiving address and blockchain network
4. Confirm the transaction using the hardware wallet

To achieve a balance of security and efficiency, there are also warm wallets. A warm wallet is connected to the internet but, like a cold wallet, requires more human involvement to sign transactions. As a result, it offers the efficiency of a hot wallet but with an additional layer of security.

In a warm wallet, funds are held on a third party's downloadable software. There are also a variety of options to enforce governance layers for accessing funds, like multi-sig or multi-party computation.

Figure 3: Comparisons between hot, cold and warm wallets

	Hot wallet	Cold wallet	Warm wallet
Pros	• Usability • Convenience • Backup options • Variety of tokens accepted • Free	• Offline • Secure • Difficult to hack • Not vulnerable to regulation in certain jurisdictions • Ideal for long-term storage	• Efficient transaction processing • Secure • Automated • Variety of multi-party/MPC options
Cons	• Prone to hacks • Dependent on third parties (developers) • Possible for users to lose funds if service shuts down	• Human error • Prone to loss or theft (if you misplace your seed phrase) • Inconvenient	• Not fully offline • Dependent on third parties



The evolution of digital asset custody

Robust custody of assets provides investors with confidence in the traditional financial world. For digital assets, custody development first emerged from self-custody solutions, followed by digital asset custodians offering institutional-grade custody solutions.

Custody 1.0: Self-custody solutions

In the early days of digital assets, custody solutions were limited. There were self-custody wallets, such as hardware wallets, software wallets and paper wallets (physical printouts of public and private keys) available. With self-custody, individuals are solely responsible for managing their private keys to secure digital assets stored in their wallets.

It is also possible to hold digital assets with a third party, such as a centralised exchange. If you leave any cryptocurrency on an exchange, that is an example of asking someone else to look after your assets, as they hold the private keys. However, in some cases the client's assets have not been properly segregated from the exchange's own assets.

Exposure to hacking has also been a key risk. One of the earliest, most infamous incidents with a third-party "asset keeper" was Mt. Gox, a Tokyo-based Bitcoin exchange, which was hacked in 2014[4]. Hackers stole roughly 850,000 bitcoins from the exchange, the equivalent of $460 million today. The exchange filed for bankruptcy shortly after. This highlights the risks of trusting a third party to hold one's assets. But the alternative, self-custody, has risks as well, with numerous investors losing custody of their assets. For example, an estimated 20% of Bitcoin's supply has been lost forever[5], which is indicated by wallets that have not moved in over 10 years.

4. Bloomberg, Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss
5. The New York Times, Tens of billions worth of Bitcoin have been locked by people who forgot their key.

Custody 2.0: The beginning of institutional digital asset custody

By 2016, third-party custodians had begun offering cold storage solutions – private keys were stored in offline devices and in secure vaults. However, this did not cater to institutional needs, since accessing digital assets in cold storage involved significant human and manual operations. Institutions need high levels of security in addition to convenient access. As time went by, institutional demand for digital assets continued to grow. This was largely due to the launch of digital asset derivatives, such as Bitcoin Futures, by CME Group in December 2017[6]. Institutions' appetite for digital assets has grown alongside the demand for licensed and regulated digital asset custodians.

As a result of this, digital asset custodians have evolved to provide compliant and secure custody solutions specifically for institutions. Many adopted institutional-grade technologies such as hardware security modules (HSM), multi-party computations (MPC) and multi-signature (multi-sig) facilities. Custodians also began to offer institutional-grade controls, such as insurance coverage, compliance tools and customised transaction policies to meet the ongoing operational and security needs in digital asset custody. The number and variety of available options have thus increased to include self-custody through hot wallets and cold wallets, as well as third-party custody through the likes of centralised exchanges, exchange wallets, centralised and decentralised financial platforms, and institutional-grade custody providers. The latter are distinguished by the multi-party security and operational layers in place.

6. CME Group, CME Group Self-Certifies Bitcoin Futures to Launch Dec. 18

Custody 3.0: Digital asset custodians connect institutions to Web 3 ecosystem

From 'DeFi Summer' in 2020, to the booming metaverse and gaming sector in 2021, the digital asset ecosystem has grown significantly with the addition of new sectors. Going beyond trading digital assets, institutions started looking for flexible custody of their assets. Institutional-grade digital asset custodians needed to be one-stop shops for institutions accessing the widening use cases in Web 3, such as purchasing virtual land in the metaverse and investing in various DeFi protocols for purposes such as yield farming.

There is increasing demand for institutional-grade digital asset custody solutions among high-net-worth-individuals and family offices. One HNWI from Hong Kong says that the reliability of a digital asset custodian is more important than ever since self-custody has risks which are deemed too significant. The investor went on to say that, due to the pace at which digital assets change, he prefers putting his digital assets with an institutional-grade digital asset custodian.

Another HNWI from Hong Kong also mentioned that reliability, security and governance layers are extremely important now, which is why opting for an institutional-level solution is more suitable for her. Usability and ease of transferring assets within a secure ecosystem are also important.

Family offices have similar requirements. One Hong Kong-based family office founded by a property investor mentioned that they need a digital asset custodian that has proper governance layers in place while allowing reasonable mobility between multiple wallets, such as their cold wallet, hot wallet, and spot trading account. The Investment Director of the family office went on to say that they require multiple layers of security and some insurance surrounding the safekeeping of assets – whether by following institutional-grade procedures or otherwise – because they are starting to build a meaningful allocation into digital assets.

The current landscape of digital asset custody and how it differs from traditional custody solutions

The digital asset custody sector continues to evolve, with over 120 custody providers[7] as of April 2023. The landscape is classified into two main categories: third-party service providers and self-custody solutions.

Digital asset custodians and exchange-hosted wallets are key examples of third-party service providers.

While both parties have control of a user's private keys, exchange-hosted wallets are hot wallets that are more vulnerable to hacks and thefts. Digital asset custodians, on the other hand, can deliver fully managed custody services for institutions to trade digital assets. They also charge management fees to deliver custody services.

For non-custody solutions, users are solely responsible for safeguarding their digital assets, with the use of passwords and seed phrases. Examples include hardware and software wallets. Users cannot retrieve their digital assets if they have lost their seed phrases or physical devices for hardware wallets.

Figure 4: An overview of third-party custody

Third-party custody		
Categories	**Digital asset custodians**	**Exchange-hosted wallet**
Governance	Threshold Signature Scheme (MPC)	Policies set by crypto exchanges
Operations	24/7 institutional MPC with Robust Representational State Transfer Application Programming Interface (REST API), policy filters	Self
Management fee for custody services?	Yes	No
Risks	Counterparty risk	Cyber-attacks, regulatory risks, potential lack of segregation of client assets from the exchange's own assets

7. Blockdata: List of crypto custody providers

Figure 5: An overview of self-custody

Self-custody		
Categories	**Hardware wallet**	**Software wallet**
Governance	Seed phrase, password and physical device	Seed phrase and password
Operations	Self	Self
Management fee for custody services?	No	No
Risks	Loss of keys from improper storage	Loss of keys, cyber attacks

Instead of using self-custody solutions, most institutions prefer third-party custody service providers to fulfill their ongoing trading and operational needs related to digital assets. These include regulated custodians, trust-licensed custodians, technology service providers and hybrid custodians – a mixture of custodians and technology platforms.

Digital asset custodians manage clients' private key information, meaning that they have control and access to move clients' funds. As with traditional financial instruments, institutions look for licensed or regulated digital asset custodians to properly safeguard their assets. The definition of licensed and regulated custodians is different across jurisdictions. In general, trust-licensed custodians receive trust licenses and operate as trust companies or trust service providers.

Regulated custodians are further licensed to specifically serve in a digital asset and/or custody capacity – they adhere to additional regulatory requirements, such as regular auditing and monitoring, specific digital asset service provider requirements, and Anti-Money Laundering and Counter-Terrorist Financing procedures.

Technology service providers, on the other hand, provide underlying technology to let clients build their own custody solutions. Unlike digital asset custodians, technology service providers do not take custody of client assets and they are exempt from regulatory requirements. However, technology service providers allow institutions to control and access their own funds and implement security measures such as backup keys and insurance policies to mitigate potential risks.

Figure 6: An overview of digital asset custodians

	Regulated custodians	Trust-licensed custodians	Technology service providers	Hybrid custodians
Adhere to additional regulatory requirements?	Yes	No	Exempted	Case by case
Licensed?	Yes	Yes	No	Yes
Permission to move client funds?	Yes	Yes	No	Yes (for Custodians) No (for tech platform)
Examples	Anchorage Digital	Copper	Fireblocks	BitGo

For digital assets, control resides in the holder(s) of the private key, which allows one to execute transactions on the blockchain. As mentioned above, through multi-party computation, multi-signature, or other operational procedures, private keys can sometimes be split into shards among multiple individuals, removing unilateral access/control by a single person and having policies and controls in place to help avoid internal collusion. Some institutional custodians allow for custom asset transfer policies and governance, which are then automated and approved by necessary parties remotely. This means placing parameters on who is allowed to send assets, where they are allowed to send them, any maximum transfer amounts, frequency limits, and approvals.

In addition, some institutional-grade digital asset custodians can offer automatic authentication of deposit addresses, which mitigates the risk of loss of funds due to hacks, malicious internal actors, or human error.

This is important because it is easy to send digital assets to the wrong counterparty if a deposit address is misspelled or if there is an external or internal attack. Moreover, the loss of funds is irreversible on the blockchain, since it is a decentralised, immutable ledger. This explains why setting operational guardrails for transactions is important in digital asset custody.

In comparison, traditional financial services custodians participate in centralised clearance and settlement systems. Clients must trust traditional custodians with maintaining records and safekeeping of assets. Traditional custodians only deal with securities, including stocks and bonds, as well as commodities such as gold and silver. Only recently have certain custodian banks, such as BNY Mellon[8], started to consider building out digital asset custody solutions.

8. BNY Mellon, BNY Mellon Launches New Digital Asset Custody Platform

Section 2

Key developments for institutional investors

In this section, we explore digital asset custody's development in tandem with the cryptocurrency industry at large. As more investors enter the market – especially institutional investors, such as family offices and high-net-worth-individuals – the requirements for digital asset custody are evolving to fit their needs.

Ethereum Merge led to a huge institutional interest in staking

The recent Shanghai upgrade has marked Ethereum's transition from a Proof-of-Work to a Proof-of-Stake consensus mechanism. Institutional interest in Ethereum, as seen in total ETH deposited in the Ethereum network, rose to 23.9m[9] since Ethereum's Merge in September 2022 (13.7m Ether deposited). Institutions stake their Ether via decentralised staking pools or centralised third-party providers, such as cryptocurrency exchanges and digital asset custodians.

Decentralised staking pools are popular platforms among retail investors, as they allow users to directly participate in decentralised finance (DeFi) protocols. For instance, users can use staked assets for lending, trading and as collateral to generate extra returns. With the wide variety of DeFi products available, users need to manage an increasing number of private keys (for different blockchain protocols) and this may be inconvenient for family offices and external asset managers, given their time and resource constraints. A Hong Kong-based HNWI expressed his worries about learning to use decentralised staking pools. In particular, he struggled to learn the wrapping and unwrapping of assets, how to choose validators and the risks involved in participating in decentralised staking pools. A Head of Investments in a Singapore-based family office echoed this, adding that she is not familiar with risks such as 'slashing' and smart contract security.

9. Nansen, ETH Deposited

Figure 7: A comparison of decentralised and centralised staking providers

	Decentralised staking pool	Centralised staking service provider
How it works	Clients can manage their staking process or delegate a validator to do so	The service provider manages the staking process on behalf of clients
Pros	• Higher staking reward • Higher flexibility if you know how to manage your own private keys	• Simple to use • No technical knowledge required • Minimum requirement on the staking amount
Cons	• Lack of insurance policies • Need to trust the chosen validators • Smart contract risks	• Lower staking returns as customers pay staking fees to a service provider

Technology service providers gain traction among family offices in staking digital assets

Family offices and external asset managers are interested in digital asset staking and look for service providers that balance their needs between security, ease of use and product diversity. Technology service providers have emerged as a popular alternative, as they aim to provide an all-in-one service for digital asset staking. This not only includes the integration of digital asset staking providers, but other service providers in compliance, trading, fiat on- and off-ramp and tokenisation.

For family offices and investment funds, technology service providers allow them flexibility in staking participation, while offering security with built-in compliance infrastructure. A Hong Kong-based UHNWI praised the use of technology platforms in navigating the DeFi ecosystem. He highlighted that, compared to self-custody solutions, technology platforms have better security measures while offering a simple-to-use interface for implementing staking and yield farming strategies across DeFi protocols.

A Head of Investments for a Hong Kong-based family office shares a similar view, saying that approval limits and multiple authorisations built-in technology platforms add an extra layer of security when providing liquidity to DeFi protocols.

Institutions eye entry into non-fungible tokens and the metaverse

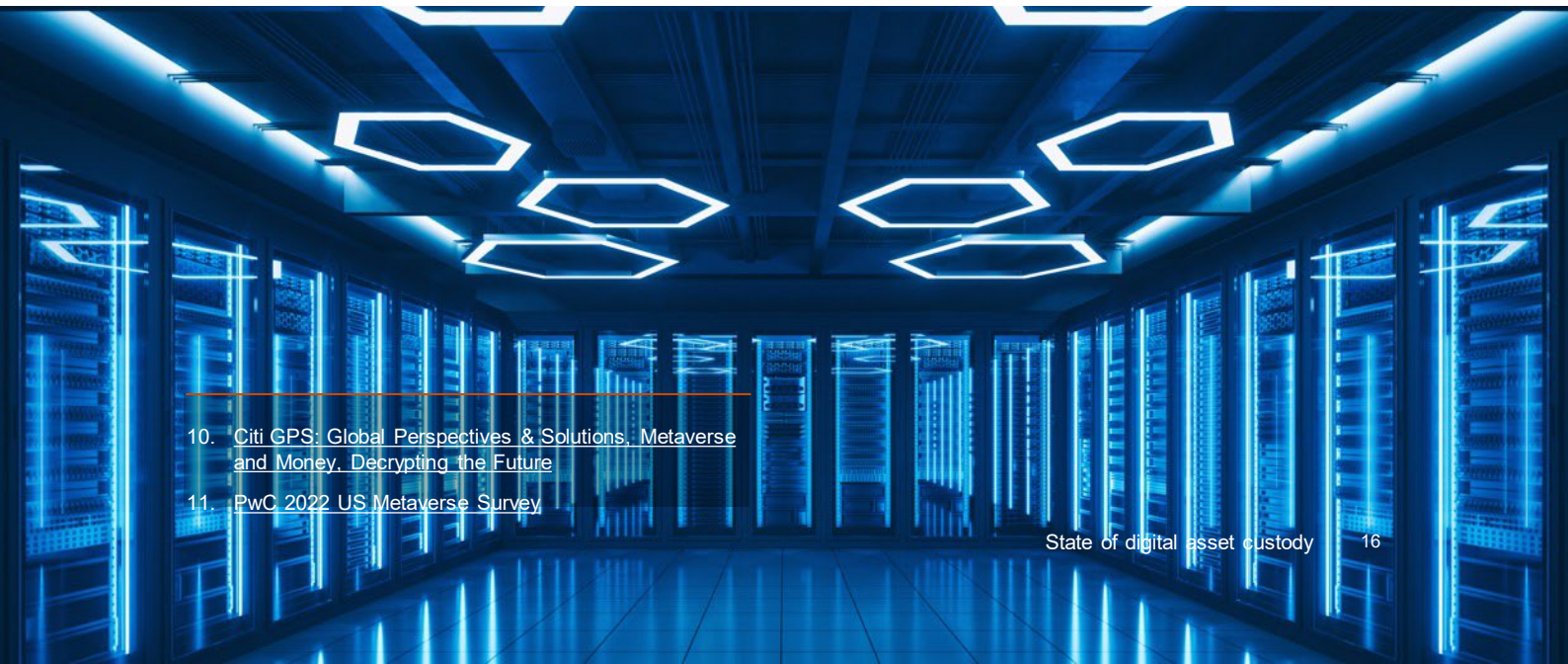
Non-fungible tokens have a huge potential to provide real business utility for institutions. This is attributable to their core properties: digital asset ownership protection and the ability to facilitate seamless value exchange. Household brands, such as Starbucks and Nike, have experimented with the use of NFTs to deepen customer engagement and explore new revenue streams.

The advent of NFTs is also accelerating metaverse developments, which are estimated to be a potential trillion-dollar market by 2030[10]. In PwC's 2022 Metaverse Survey[11], 82% of executives said they expect metaverse plans to be part of their business activities within three years. In addition, institutions are eyeing investment opportunities in well-known NFT collections and virtual land in the metaverse.

For traditional financial institutions initiating or accelerating their digital asset activities, the foundation is a strategy which includes custody. However, the majority of NFT custody services are offered by self-custody solutions. These are not user-friendly for institutions that are new to the digital asset industry.

A Chief Operating Officer from a Hong Kong-based family office highlighted his pain point in using self-custody solutions, such as the inconvenience of listing NFTs across different marketplaces and the complexity of managing private keys.

Third-party service providers are starting to launch NFT custody solutions for institutions. As opposed to self-custody solutions, these allow institutional clients to hold NFTs without managing private keys themselves. Apart from safekeeping NFTs for clients, service providers allow institutions to access various decentralised marketplaces and buy and sell NFTs directly. NFT custody solutions are in their infancy and most only support NFTs built using ERC-721 and RC-1155 protocols. A Hong Kong-based HNWI, who uses NFT custody services offered by a technology platform, said that the social recovery feature is extremely useful for recovering accounts without revealing one's private key information.



10. Citi GPS: Global Perspectives & Solutions, Metaverse and Money, Decrypting the Future
11. PwC 2022 US Metaverse Survey

Section 3

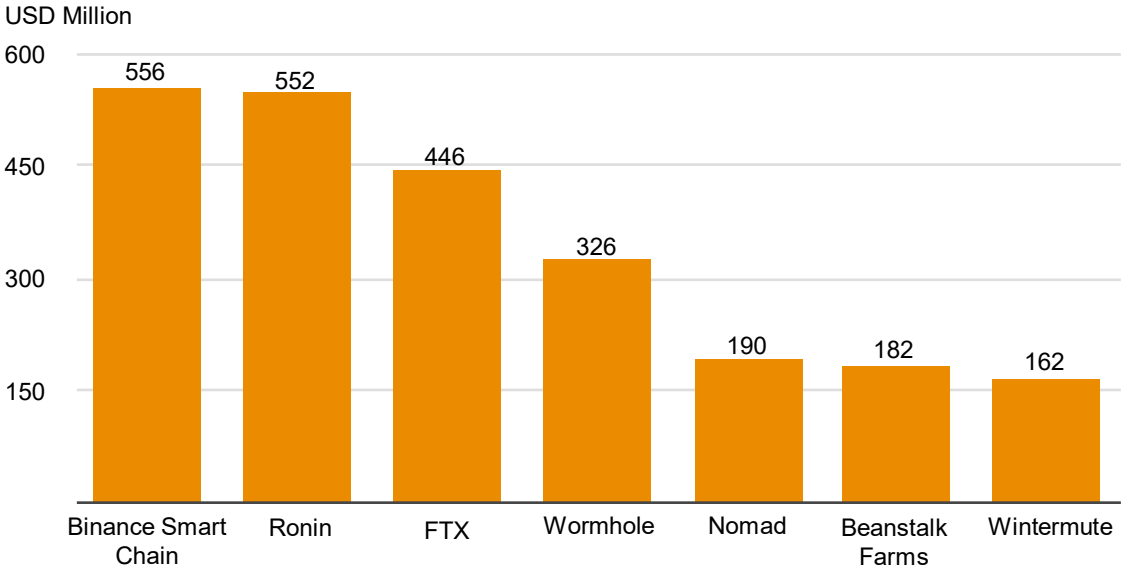
Key challenges of digital asset custody

#1 Security

The need for digital asset custody is often associated with high-profile cryptocurrency exchange hacks. In the early days, hackers targeted hot wallets of major cryptocurrency exchanges (e.g. Mt. Gox and Coincheck) in order to drain funds, causing millions of losses. While exchange-hosted wallets offer convenience when trading a variety of digital assets, users need to rely on the exchange's reputation and security infrastructure in safeguarding their funds.

As highlighted by FTX's collapse in 2022, an exchange's lack of appropriate governance, risk management and internal controls can lead to significant asset losses for customers. FTX filed for bankruptcy in November 2022 and has been charged with overleveraging and mishandling of customer funds. Institutions are increasingly looking to safeguard their assets through self-custody solutions or reputable digital asset custodians, rather than simply holding them with exchange platforms.

Figure 8: Largest digital asset hacks (2022)



Source: Decrypt

In using self-custody solutions, institutions often face challenges in protecting their private keys against unauthorised access or transactions. If private keys and their backups are compromised, their confidentiality, availability or integrity will be lost. When institutions lose control of digital assets, this may lead to a write-down of assets or the booking of additional liabilities on the organisation's balance sheet. The use of self-custody solutions has recently drawn controversies among some users. In May, Paris-based hardware wallet provider Ledger postponed the launch of subscription services to remotely back up user recovery keys due to fears that there was an avenue where private keys stored on hardware devices could be accessed remotely. Users have raised privacy and security concerns about how these hardware devices safeguard their private keys.

A Head of Investment of a Hong Kong-based family office said that the company is considering switching their digital assets from cold storage solutions to a digital asset custodian. As their digital portfolio grows, the family office is looking for custodians that provide a simple user interface to manage it more easily.

Digital asset custodians, on the other hand, aim to strike a balance between security and accessibility for institutions. This can be achieved by multi-party computation (MPC), which effectively divides the private keys and scatters sensitive key information across multiple locations. For institutions, the use of MPC avoids a single point of failure even if a certain part of a private key is exposed to unauthorised personnel.

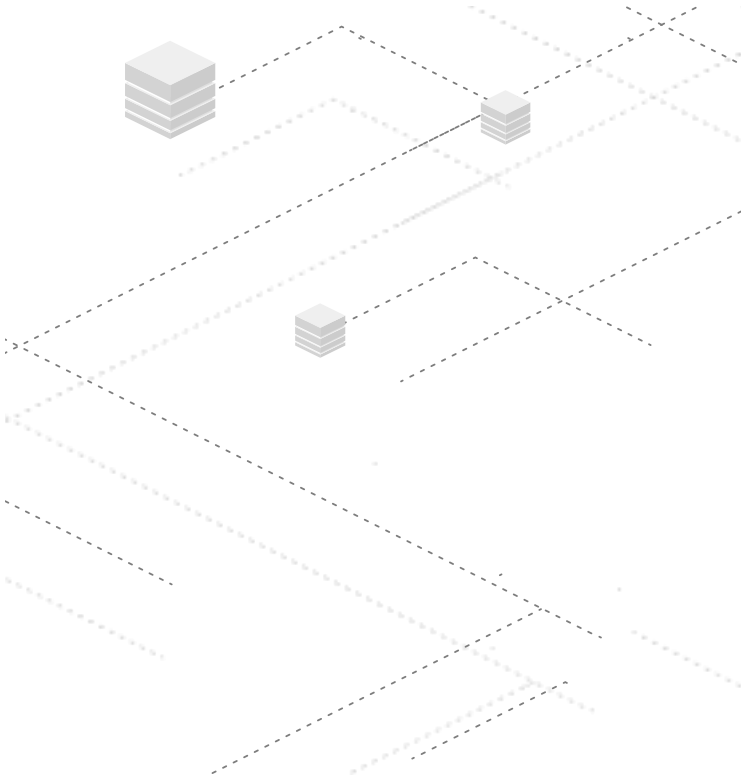
#2 Regulatory status

While recent legal developments worldwide have shown acceptance of digital assets, the regulation of digital asset custody is highly fragmented and needs further clarity. Many family offices and investment funds operate globally, and they face difficulties in choosing a digital asset custodian that is regulated across different jurisdictions.

As the digital asset industry develops, global standard-setters are attempting to offer regulatory clarity on digital asset custody. In the United States, the Securities and Exchange Commission (SEC) announced a proposed overhaul of the custody framework[12] for SEC-registered investment advisers, and this broadens the scope of digital assets. In particular, the SEC current Chair (Gary Gensler) stressed that most cryptocurrency exchanges do not meet the definition of qualified custodians for investment advisers. A Singapore-based UHNWI believes that SEC-registered investment advisers (RIA) will bring huge credibility to digital asset custodians, as clients expect custodians to be in full compliance with the SEC's RIA standard.

In the case of Europe, the Markets in Crypto-Assets Regulation (MiCA) introduced a licensing regime for crypto asset service providers (CASPs) who offer digital asset custody services. While the scope applies to entities trading asset-referenced tokens and utility tokens, it does not apply to non-fungible tokens – a sector that has seen growing custodial demand from family offices and investment funds.

> 'Our biggest concern is whether there is certainty over how digital assets are custodied, what the level of security is, and what the framework is in terms of operations. We have talked to many different custody providers, but those are the biggest hindrances.'
>
> An Investment Director from a single family office



12. Securities and Exchange Commission, Safeguarding Advisory Client Assets

#3 Sound insurance policy

Digital asset custody insurance is another level of assurance being adopted by custodians to provide a source of indemnification in the event of a loss of digital assets from client accounts.

Self-custody solutions do not offer insurance policies and users are not compensated for any loss of digital assets arising from negligence. In March 2023, the holder of CryptoPunk #685 intended to borrow money against this asset to purchase another NFT. However, the holder accidentally sent the NFT to a burn address and lost the NFT worth 77 ETH ($135k)[13].

While participants in the private wealth sector have limited experience in managing digital assets, having a sound insurance policy can protect them from human error and negligence. A Singapore-based UHNWI said that sound insurance policies are an important criterion in choosing digital asset custodians. In particular, when he participates in yield farming in DeFi protocols, insurance coverage can protect him from losses incurred by smart contract vulnerabilities.

> 'A comprehensive insurance policy is important for clients of digital asset custodians as it provides a safety net against unexpected events and helps to build trust in the security of their assets.'
>
> Ethan Tong
> Chief Investment Officer, Aspen Digital

Digital asset custodians and technology service providers have various insurance policies with different scopes of coverage. To evaluate the digital asset insurance coverage by custodians, one should consider the following criteria:

- What is the aggregate limit of the custodian's policy?
- Are client wallets segregated?
- Who are the insurers underwriting the policy?
- Does the policy cover theft of digital assets by outside parties?
- Does the policy cover insider theft? Insider theft by executives?
- Does the policy cover the loss/destruction of private keys caused by natural disasters?
- Does the policy cover losses incurred from software bugs?
- Is the coverage for cold wallets, hot wallets, both, or neither?
- What legal entities are covered by the insurance policy? Does this match the legal entity with which the customer has entered into a service agreement?
- Does the custodian or exchange allow you to purchase additional insurance of your own?

13. Cointelegraph, NFT investor accidentally burns $135K CryptoPunk trying to borrow money

Section 4

Selecting a custody model

The growth of the ecosystem and the widespread adoption of crypto-assets has enabled **new operators** to offer services that allow **institutional and private players** to access and operate in crypto markets and to safely keep and use their funds.

Customers & institutions

People or institutions interested in accessing the crypto market

Service provider

Financial operators offering a channel to crypto-asset markets

Crypto service provider

Crypto custody and execution services. The service provider can build its own solution or can decide to rely on external providers

Exchange

Place where it's possible to buy or sell on crypto market

Crypto market

Custody if the critical foundation for the rest of the digital asset ecosystem. Without appropriate custody, other digital asset activities — trading, staking, yield generation, asset management, borrowing and lending, derivatives, market making, issuance and insurance — could not exist. If recent market events have highlighted anything, it's the importance of how to address custody.

Digital asset custody is highly complex and technical and should not be taken lightly. Digital assets exist only as a code on a blockchain.

There are no traditional clearing houses and gatekeepers, transactions are irreversible, and investors are responsible for following their own transactions. In this new world, everyone is subject to risks and nuances that traditional custody tools, processes, vendors, and controls are probably not prepared to handle.

We recommend balancing operating effectiveness and efficiency with security by developing a strategy and model that addresses the critical challenges of digital asset custody.

Enforcing security in a world where a loss is irretrievable

In the digital asset space, if it's gone, it's gone for good. Blockchain transactions are irreversible, so if a digital asset is misplaced or stolen, there is likely no recourse. That makes security more important than ever. Besides up-to-date cyber defense, it is also critical to secure private keys: the strings of numbers and letters (like a password) that enable clients to access their digital assets.

If the user loses their private key, they will not be able to regain access to it through a central authority or request a new one. It is only possible to restore a private key if a suitable backup solution is in place. If a malicious actor gets hold of that key, they gain control over those assets.

Some of the biggest risks for users and their private keys are:

- **Confidentiality:** risk that unauthorised persons access private keys and backups. Anyone gaining unauthorised access can execute transactions and access the digital assets.
- **Availability:** risk that private keys and their backups will no longer be available, or at least not in a timely manner. If they are no longer available, it may be impossible to access the digital assets.
- **Integrity:** risk that private keys or their backups will be changed and rendered unreadable. If the integrity of the private keys and their backups is compromised, it may prove impossible to access the digital assets.

These major risks impact the main phases of a private key's life cycle:

- **Key ceremony:** Several risks exist during the key ceremony (when private keys are generated). For example, private keys may be viewed and copied during the generation process or while they are being transported to where they and their backups are ultimately kept. These attacks may be by persons directly involved in the process or by persons who gain access to selected technical components, e.g. a printer memory.
- **Key management:** In managing private keys and their backups, there is an inherent risk that they may be lost, stolen, or rendered no longer readable. There is also a risk of fraud if a clear division of responsibilities for the storage of private keys and backups is lacking or if the persons entrusted with controls and security fail to follow the necessary security protocols. The private keys and their backups, which should be stored in different locations, must always be protected against inappropriate access as well as physical interference or damage.
- **Transactions:** When initiating and approving transactions for digital assets, financial risks may arise if the control system is inadequately designed or if duties are insufficiently segregated. In the traditional world of banking, financial assets can sometimes be refunded in the event of error or fraud – but not in the blockchain world.

To address this threat, consider custody security measures and controls such as:

- Whole lifecycle private key management
- Suitable technology infrastructure
- Segregation of duties
- Limits on the number accounts that each key can access
- Maker/checker processes for transactions
- Asset segregation
- Identity and intent verification
- Strict transaction processing rules

It is important to keep in mind that these are just some of the measures required, and both the technology and the related threats are evolving quickly. You'll need to stay up to date on the latest in digital asset security.

Tailored compliance strategy to follow both new and old regulations

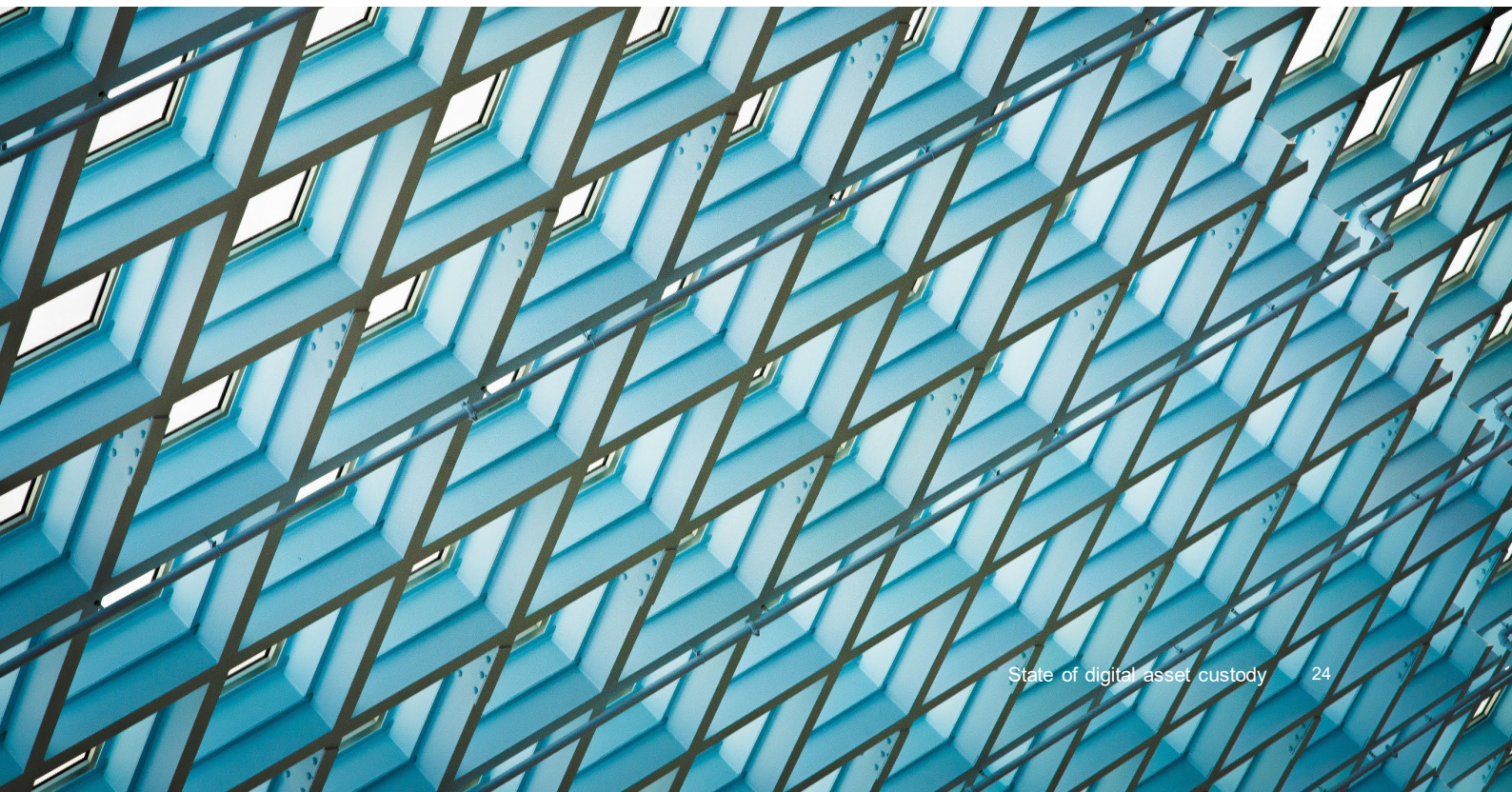
Digital assets are subject to both existing and evolving regulations. Users need to comply with Know Your Customer and Anti-Money Laundering (KYC/AML) measures, for one, as well as transaction monitoring and operational controls, and complaint and fraud processes, among others. Furthermore, new rules are being proposed all the time.

Traditional controls and software are probably not able to monitor blockchain activity for illicit behavior, so there is likely a need for new, specialised on-chain analytics software.
The right software can provide automated, configurable thresholds and alerts, establish transaction provenance, and perform forensic analysis. Many institutions use vendor and third-party services to support their compliance needs.

Should an institution seek an internal or external crypto custody solution?

This question is important both from a strategic and commercial angle. To build an internal solution requires the necessary knowledge and experience. On the other hand, if a third-party solution is used, then the task of custody can be delegated to a qualified third-party service provider. However, even when utilising a third-party custodian, it is important to remember that the user still bears the ultimate and associated responsibilities – especially for overall selection and management of vendors, own asset security measures and the holistic internal control system protecting digital assets.

To support these responsibilities, institutional-grade custody providers establish control reports to standards such as ISAE 3000/3402 and/or SOC 1 or 2 that can be used to assess and monitor the outsourced processes, risks, and controls.



Internal solution

If you decides to build a digital asset custody service from the ground up, there are potentially some big advantages. Proprietary software can help offer differentiated services and provide control over compliance and consumer protection.

This could both improve long-term profitability and help strengthen your brand for crypto services. But standing up a digital custody solution from scratch is costly and time consuming. This also introduces risks relating to any developmental or operational delays or mistakes.

Advantages	Disadvantages
• Proprietary software and infrastructure	• Large investment required
• Customisation and tailored features	• Complex technical capabilities and expertise required
• Full control	• Specialised resources to develop and maintain
	• High operating risk

External solution

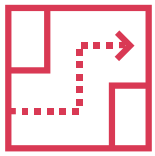
Working with an existing digital asset custodian can significantly cut costs and time to market. Depending on your contract, your service provider can also assume some budgetary and operational risks. However, they need to be relied upon for operations and it may be more difficult to differentiate your services in the market. As a user, you will still have to execute on compliance, both because regulators demand it and because – if there is an issue – it's the user's brand that may be impacted.

Advantages	Disadvantages
• Ready-made solutions	• Standardised service offerings and features
• Access to expertise, resources, and technology	• Reliance on others
• Less financial burden	

Typically, it is very difficult and time-consuming for non-blockchain native institutions to develop internal custody solutions. Almost all market participants (who are not custodian providers themselves) seek outside support to varying degrees. For institutional investors who are not providing services to end-users, the most efficient path to establishing a secure and operational custody model is to rely on third-party custody providers.

Suitable custodians can provide the technology and expertise that traditional institutions lack and provide a suite of digital asset services that allow the institution to focus on core business activities and investment strategy, while operational details are supported by a specialised vendor.

Custody model and vendor strategy



Strategise

Identify the suitable combination of custody service providers to best achieve business goals as well as mitigate and diversify risks.

Access to services

A combination of service providers might be required to access all desired service offerings, including:

- Access to certain markets or tokens
- Ability to custody certain types of assets

Diversification

Holding assets with multiple parties can lower concentration and counterparty risk.

Competitive pricing

Multiple vendor relationships can bring pricing transparency and additional quotations.

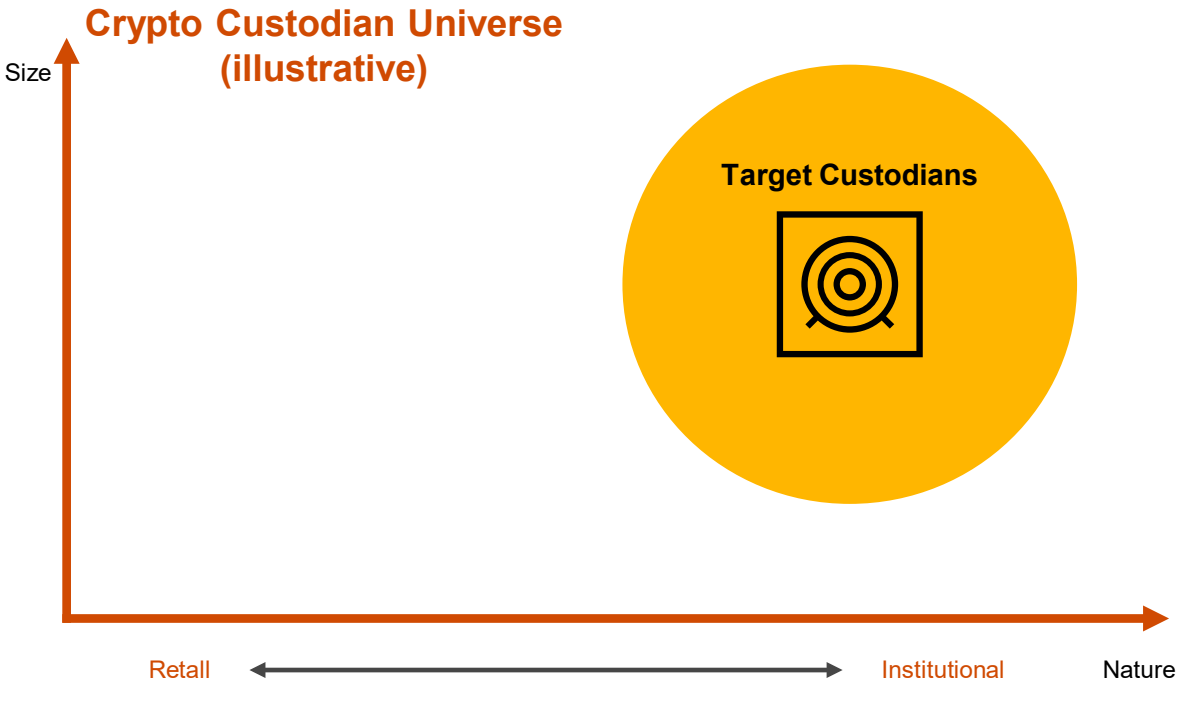
Compliance responsibilities

Compliance safeguards and programs operated by service providers can support your own compliance obligations.

Prior to selecting a specific custody provider(s), institutions should formalise their target custody model and supporting vendor strategies. As discussed above, an outsourced custody model is likely the most suitable option for institutional investors. However, there are still vendor strategy considerations relevant to the implementation of an outsource model. An institution should evaluate what functions and operations it would like to keep in house compared to what it would like to fully outsource to a third party. It should also consider the number of custody providers to engage with – while having only one third-party custodian will be the simplest operating model, engaging multiple custodians can potentially enable further advantages and safeguards.

Factors to look for in a custodian

While there is a large universe of providers and services that can help users hold digital assets, institutions should target custody providers that are large in scale and mature in their technology and operations.



Some important factors in identifying suitable custodians are:

Regulatory jurisdiction

The regulatory jurisdiction directly impacts the operation of custodians it supervises. Service providers who are under stronger regulatory regimes can usually be considered as more secure. **Regulatory jurisdiction can be an indicator of the strength of operational compliance.**

Operational history

Operational history is often the only publicly available information about the operations of an organisation. Incidents can relate to regulatory, reputational, cyber, or transformational (mergers and acquisitions) circumstances. Significant insight can be gained from the level and significance of past incidents, and how a vendor has responded to these. It is key to **consider the risk culture and governance structures** of a target vendor.

Service offerings

Target custody providers should be able to **offer services that meet your business requirements**. This could include: institutional grade asset custody, ability to custody various digital asset classes, operating in a mature regulated jurisdiction(s), access to trading and staking solutions, and high-quality reporting data (i.e. statements, confirmations, etc)

Costs/commercials

Custodian providers offer varying cost and fee structures and often adjust fees based on the magnitude of assets or transactions they will service for you. Providers also have different contractual terms, including liabilities and indemnities, service levels, and insurance coverage. **Commercial arrangements should fit strategy and business requirements.**

Public image and reputation

An organisation's public image is a key **reputational risk**. Publicly available adverse news, ultimate beneficial owners (UBOs), related and associated parties, as well as regulatory findings and sanctions should be reviewed.

Selection approach

Institutions should take a systematic and structured approach to the custodian selection process. It is important to narrow down the large array of existing providers in the current market to a group of suitable, qualified custodians that are fit for purpose. Utilising a defined and objective selection approach, along with potential assistance from experienced advisors, can enable you to effectively identify and evaluate the right custody provider(s) for your needs.

Some actions to consider adopting into your selection process are:

1. Map the market

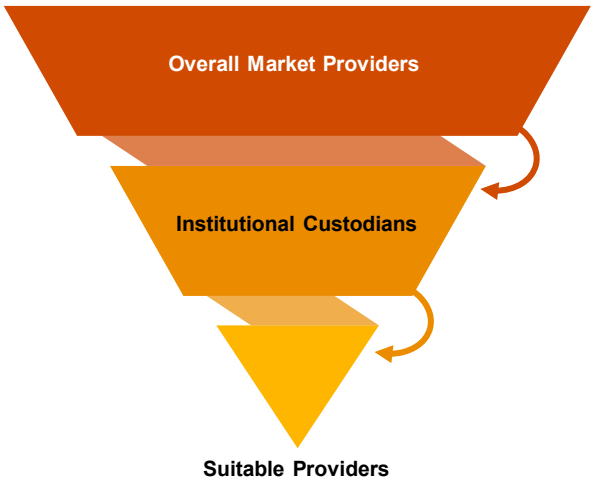
Market overview of the global service providers to understand which institutional providers would be suitable custody vendors. Institutions can apply the following illustrative considerations:

- Regulatory jurisdiction
- Operating history
- Service offerings
- Cost/commercials
- Reputation
- Existence of third-party assurance reports issued by a reputable organisation

As a result of this desktop overview, potential vendor candidates can be identified for further assessment.

2. Review criteria

Combine digital strategic goals, specific business requirements and potential SME advisor guidance to determine and define the detailed evaluation criteria to assess target custody vendors. Agree criteria with relevant stakeholders.



These assessment criteria can be used to evaluate the suitability of custodian providers and determine ultimate selection.

3. Define grading

Create an assessment grading system to evaluate how each vendor performs against the review criteria. Agree grading system with relevant stakeholders.

4. Perform review

Provide Requests for Proposals and an assessment questionnaire to target custody vendors. Engage in product demonstrations and Q&A sessions with target vendors. Apply the established assessment grading systems to vendors' responses and information provided.

Based on the evaluation results, determine the vendor(s) that differentiated themselves from the overall target pool.

5. Engage and onboard

Based on the evaluation results, engage selected vendors to determine commercial terms and services provided. Onboard and implement required processes and technology to operate vendor systems.

Key vendor evaluation considerations

Factors to assess when selecting a digital asset exchange

1. Reputation
- Reputation and background in the market
- Required experience, expertise, and quality
- Governance and controls environment

2. Custody and trade execution model
- Operational capabilities and controls
- Trade and order book execution, procedures
- Custody model and safeguards

3. Compliance
- Customer onboarding, KYC, and AML
- Compliance with regulation by jurisdiction
- Management of regulatory and compliance risk
- Previous and pending regulatory incidents
- Credentials and relevant certifications, licenses

4. IT & Cybersecurity
- API integration suitability
- Systems compatibility
- Cybersecurity measures and protections

8. Suitability of services
- Alignment with management's requirements
- Client asset safeguards in place and insurance coverage
- Business continuity (regulatory action, operational incident)
- Quality of services as compared to competitors

7. Commercials
- Contracting terms
- Completeness of services
- Rights and obligations

6. Ownership and legal
- Nature of legal structure
- Governing rule of law
- UBOs, Directors and Officers (PEPs, sanctions etc)
- Litigation and regulatory exposure

5. Financial stability
- Overall financial strength – indebtedness, solvency
- Financial strength of vendor's group /shareholder/UBO
- Viability of business model

Here are some illustrative factors that institutions should consider when evaluating custodian providers for ultimate selection.

Reputation

There are many custodians operating in the market. Consideration should be given to the reputation of the custodian based on their standing and background within the market.

Custody and trade execution model

Custodians can operate different models. Consideration should be given as to whether you need additional safeguards over the security of digital assets versus how quickly these assets can be traded. Some custodians operate a 'custody only' operation and therefore these need to be withdrawn and placed at an exchange venue to then trade. Some of the bigger exchanges offer both exchange and custody services to provide secure storage of digital assets tied with speedy access to these assets when they need to be traded.

Compliance

A custodian is an extension of your own business. Therefore, selecting a custodian with a robust compliance operation set-up will minimise potential reputational risks for your organisation. When researching a custodian it is important to look at the regulatory regime within which the custodian operates, whether there are any current or previous regulatory investigations involving the custodian and whether the custodian has obtained any relevant regulatory certifications or licences.

IT & Cybersecurity

Digital assets are inherently risky to hold. It is therefore important to understand the cybersecurity measures in place at a custodian. If hot storage access is required, then one should expect a custodian to have industrial grade security systems in place to protect assets. Even with the selection of cold storage, focus should be placed on where the cold storage is and who has access to that.

A further consideration is compatibility of the custody platform with a user's own systems. Some custodians will have developed APIs that allow a user's systems to interface directly with the custody system, whereas other will prefer a direct log in procedure. It is also important to consider what security features a custodian offers, for example multi-sig, which will reduce the risk of misappropriation of funds.

Suitability of services

A key consideration is whether the custodian's business model fits with the user's. Different organisations will have different requirements of their custodian.

Some providers only offer support for a small number of digital assets (e.g. only large-cap tokens). Others can offer support not only for cryptocurrencies, but other digital assets as well.

Some custodians will prioritise the safeguarding of assets in cold storage, which can slow down access to assets but give additional comfort that assets are secure until these are needed to be withdrawn. Other custodians will prioritise ease of access to assets in hot storage, which may lead to these being less secured but able to be extracted at a moment's notice.

Another key consideration is the business continuity arrangements that the custodian has in place. Custodians could cease to exist at any point and, therefore, any custodian that can allow you access to your assets without needing access to their platform could be advantageous.

Commercials

Each custodian will take fees for storing, depositing and withdrawing assets on their platform. Some custodians will be more expensive than others, depending on the services being offered. It is important to pay attention to the terms and conditions offered by custodians and, particularly, around the rights and obligations that they owe to their clients and what obligations a user has to their custodian. Some considerations will be who has the legal right to your assets in the event of a dispute or non-payment and the availability of services promised within the terms and conditions.

Ownership and legal

Users should understand the legal structure of any potential custodian to help determine which jurisdiction will have rule of law over the custodian. Jurisdictions can have very different approaches to the governance of digital assets, including hands on/off approaches and being favourable/unfavourable to digital.

Financial suitability

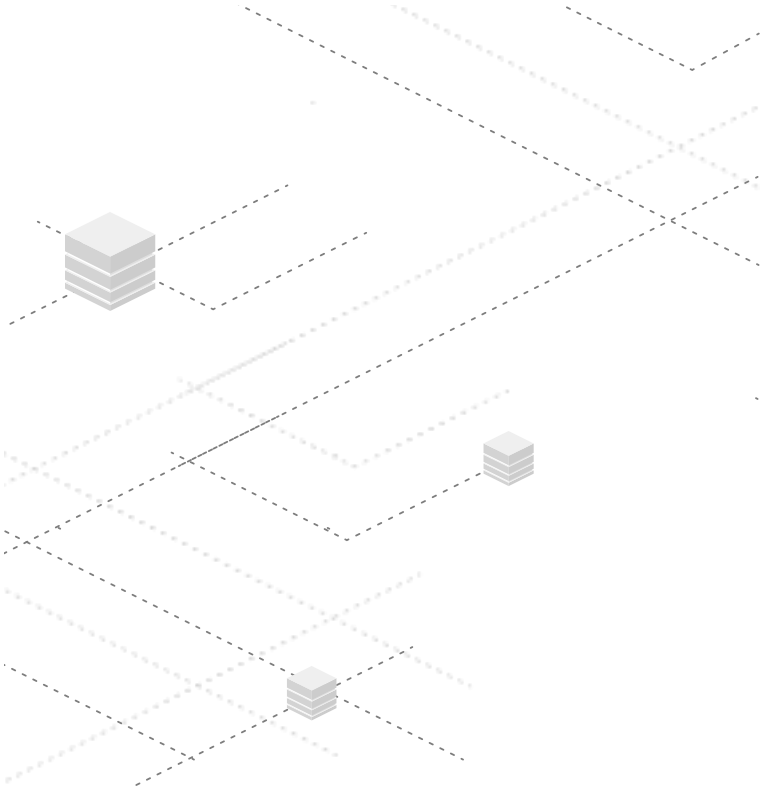
Assessment should be made as to the financial strength of a custodian. Should the custodian cease to exist, ease of access to assets will be key. Therefore, a custodian that is in good financial health, well-funded and with a viable business model will help ensure that there are minimal disruptions to its service.

Conclusions

The digital asset sector is continuing to experience rapid development and innovation. Particularly in Hong Kong, the market has been buoyed by the government's supportive stance in fostering a vibrant ecosystem for digital assets within the city. Institutional investors are being presented with a multitude of new opportunities that extend beyond the holding and trading of cryptocurrencies.

Digital asset custody is a key building block in any digital asset activity and interaction. In response to several collapses and market shocks, as well as more and more institutional parties entering the digital assets space, a flight to quality has occurred among market participants. There is an increased understanding and strong demand for institutional-grade custody solutions that will enable investors to pursue a wide spectrum of opportunities in a safe and controlled manner.

Institutional investors should undertake a systematic and informed approach to designing operating models and selecting the third-party providers that will custody their digital assets. Implementing the right digital asset custody solution could be the difference between successful investment opportunities seized and significant asset losses.



Glossary

Cold wallet: A wallet or device that keeps crypto private keys offline. Examples include a paper and hardware wallet.

Decentralised finance (DeFi) : An umbrella term that encompasses a range of financial services provided on public blockchains. This emerging ecosystem of financial technology products claims to be more open, inclusive, and transparent in relation to its accessibility, service offering, and transactions/operations (including fees charged).

Hardware security modules (HSM): Physical devices that perform major cryptographic operations, such as encryption, decryption, and key management.

Hot wallet: A blockchain wallet that allows users to access funds through a browser extension or mobile application and is thus connected to the internet. The keys of a hot wallet can either be self-custodied by an individual or through an entity such as an exchange, which makes the hot wallet non-custodial.

Liquid staking: Liquid staking is a software solution that enables users to enjoy staking rewards on proof of stake (PoS) networks such as Ethereum (staked tokens are typically locked-up) while also receiving a liquid staking token (LST) programmatically minted by the protocol. Liquid staking providers take user deposits, stake those tokens on behalf of users, and provide them with a receipt in the form of a LST, which is redeemable for the tokens they staked. This new LST can then be traded or used as collateral in DeFi protocols, thereby unlocking the liquidity of the staked assets.

Liquid staking derivatives : Derivatives that enable individuals to lock up small amounts of a cryptocurrency in exchange for the equivalent in a liquid staking derivative (LSD). Liquid staking derivatives can be used to invest in DeFi protocols.

Multi-Party Computation (MPC): A technology that splits a private key into “key shares” across multiple physical devices. MPC mitigates the risk of a single point of failure.

Multi-signature (multi-sig): A scheme that requires more than one authorised signature to process and approve a transaction. This differs from MPC in that its authorisation threshold, which is the threshold number of keys required to authorise each transaction, is fixed once it is defined.

Non-fungible tokens: Assets that are tokenised on the blockchain with a unique identifier, which proves one’s ownership and an asset’s authenticity.

Private key: A key that is used to execute transactions and manage digital assets. A private key enables the owner of the wallet to control and access cryptocurrencies within the wallet. Loss or unauthorised access to the private key can result in loss of access to the wallet and the cryptocurrencies stored in it.

Glossary

Proof-of-Stake: A consensus mechanism that selects validators in proportion to their quantity of holdings in the associated cryptocurrency to verify transactions and create a new block on a blockchain. This is done to avoid the computational cost of proof-of-work schemes.

Proof-of-Work: A consensus algorithm that involves solving a computationally challenging puzzle in order to verify a transaction and create a new block on a blockchain.

Public key: A key that is derived from the private key and is publicly shareable with others. It serves as an address to receive cryptocurrencies from other users.

Robust Representational State Transfer Application Programming Interface (REST API): A software style that was created to guide the architectural design and development of the World Wide Web.

Seed phrase: A sequence of random words required to access or recover cryptocurrencies in digital asset wallets. It is also known as a recovery phrase or mnemonic phrase.

Two-factor authentication (2FA): A security process that requires two forms of identification in order to access sensitive information. Examples of 2FA include security passcode and email authentication.

Wallet address: A unique identifier used to send and receive cryptocurrencies.

Warm wallet: A digital asset wallet that is connected to the internet but, like a cold wallet, requires more human involvement to sign transactions. As a result, it offers the efficiency of a hot wallet but with an additional layer of security.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We are a network of firms in 152 countries with more than 328,000 people who are committed to delivering quality in assurance, advisory and tax services.

Digital assets are a global financial services priority for PwC. Our global digital asset working group was established in 2017, with PwC Hong Kong as the main driver and centre of excellence. The PwC Global Digital Asset Team is composed of over 150 professionals active in over 25 countries, offering a one-stop shop solution for our clients across our multiple lines of service. We have already completed over 300 crypto client engagements in the past two years. We help both digital asset natives to institutionalise and traditional financial institutions and investors to enter into the digital asset universe, including entity setup and public company readiness, systems implementation, cybersecurity, internal controls and governance design, audit and attestation, corporate and personal tax, deals strategy and due diligence, and SFC licensing support.

For the latest information about PwC Hong Kong, please visit:
https://www.pwchk.com/en/about-us/about-us.html

Duncan Fitzgerald
Digital Assets & Web3 Co-Leader
duncan.fitzgerald@hk.pwc.com

Peter Brewin
Digital Assets & Web3 Co-Leader
p.brewin@hk.pwc.com

Lei Wang
Partner
lei.l.wang@hk.pwc.com

James Tao
Senior Manager
james.y.tao@hk.pwc.com

Matthew Hayes
Senior Manager
matthew.l.hayes@hk.pwc.com

Adrian Clevenot
Associate Director
adrian.a.clevenot@hk.pwc.com

About Aspen Digital

Aspen Digital is a full-service digital asset wealth-tech platform for wealth managers, family offices and HNWI. Backed by both blockchain and traditional investors including the Everest Ventures Group, TTB Partners, RIT Capital Partners (formerly Rothschild Investment Trust), Liberty City Ventures and Token Bay Capital they provide the technology and expertise to enable clients to build their digital asset portfolios.

Since inception, Aspen Digital has offered institutional-grade cold storage services that are MPC-based through Fireblocks.

For more information, please visit https://www.aspendigital.co/

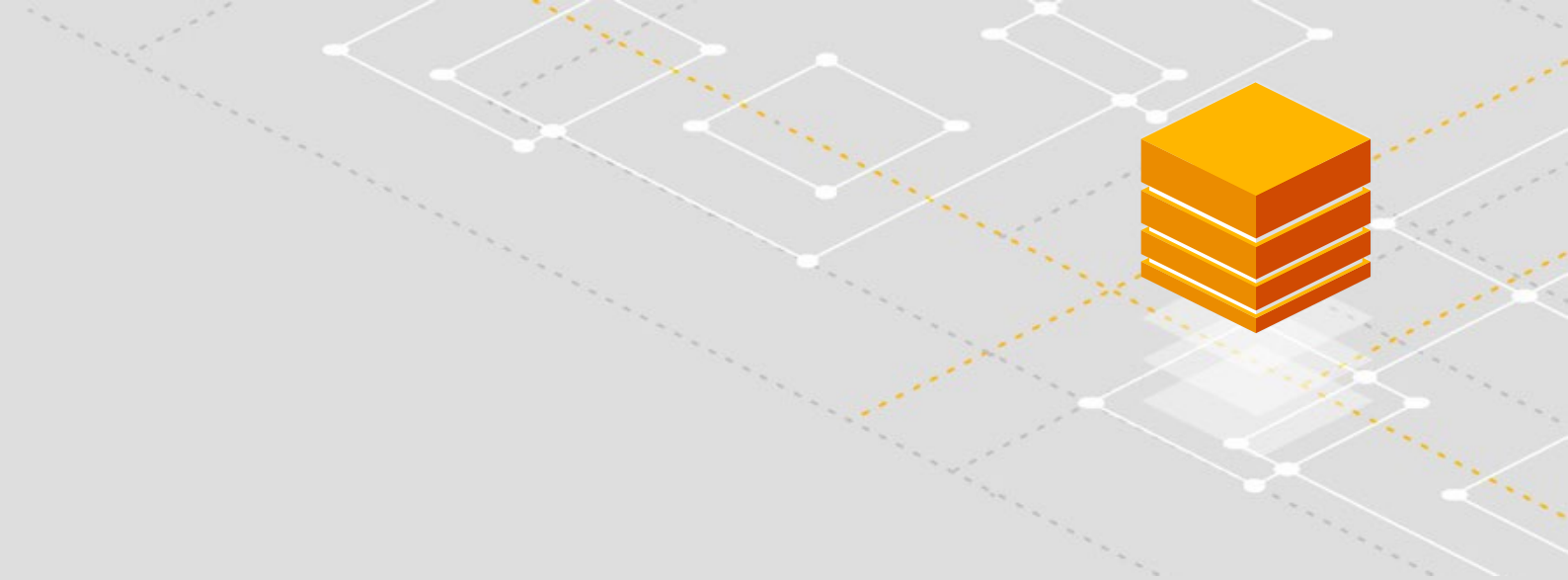
Elliot Andrews
Chief Executive Officer
elliotandrews@aspendigital.co

Ethan Tong
Co-founder and Chief Investment Officer
ethan@aspendigital.co

Matthew Lam
Head of Research
matthewlam@aspendigital.co

Amanda Xiang
Director of Business Development
amandaxiang@aspendigital.co

Arielle Lee
Associate
ariellelee@aspendigital.co



www.pwchk.com
www.aspendigital.co