

An Evaluation of Digital Asset Custody Solutions

RESEARCHED BY



THE BLOCK Research

COMMISSIONED BY



Fireblocks

Commissioned By

Fireblocks

Fireblocks is an enterprise-grade platform delivering a secure infrastructure for moving, storing, and issuing digital assets. Fireblocks enables exchanges, lending desks, custodians, banks, trading desks, and hedge funds to securely scale digital asset operations through the Fireblocks Network and MPC-CMP based Wallet Infrastructure. Fireblocks serves over 650 financial institutions, has secured the transfer of over two trillion in digital assets, and has a unique insurance policy that covers assets in storage & transit. For more information, please visit www.fireblocks.com.

Researched By

THE BLOCK Research

The Block is an information services company founded in 2018. Its research arm, The Block Research, produces research content that covers the digital asset, fintech and financial services industries.

Contact

Research Email: research@theblockcrypto.com

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

Author

Andrew Cahill, Research Analyst

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

Introduction

Fraudulent credit card transactions can be reversed or disputed with a call to the bank or credit card provider.

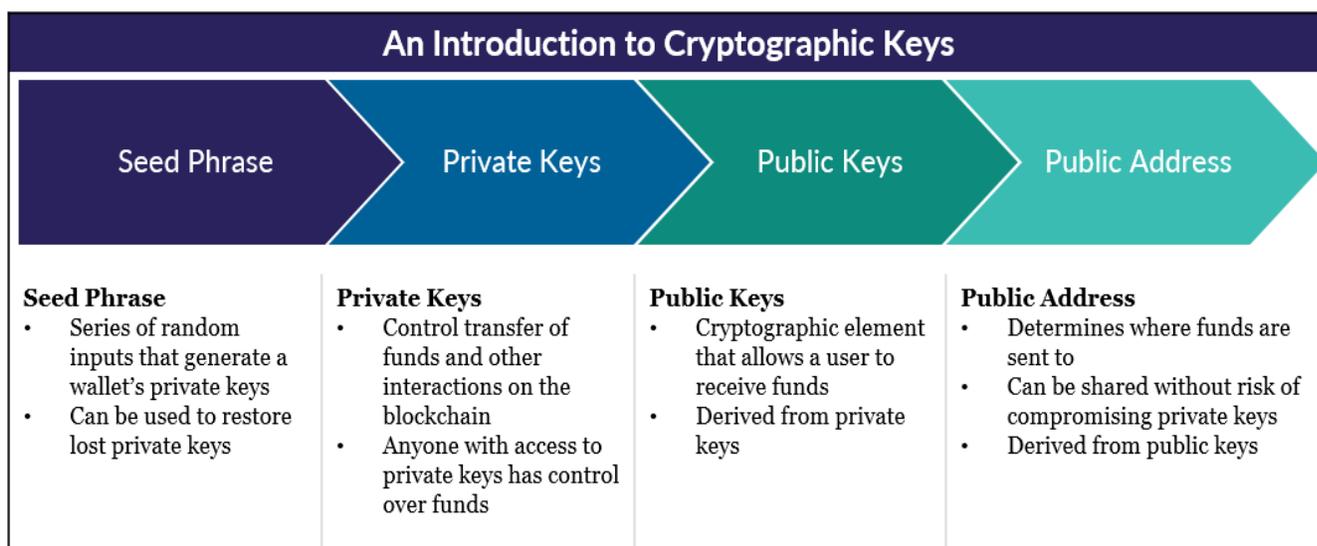
The same cannot be said for digital assets transactions.

There is no “bitcoin customer service department” to contact to dispute the validity of a bitcoin transaction. Once digital assets are transferred from one party to another, transactions are final and immutable. Only in extremely rare circumstances are blockchains modified such that previously finalized transactions are invalidated.

Hence, placing controls on how digital assets are stored and how transactions can be effected, also known as “digital assets custody” is an important consideration for operators in the digital assets industry.

How is Custody Managed?

The storage and transfer of digital assets are operationalized by cryptographic key management.



Source: The Block Research

Public keys are just that: public. They map to a **public address**, which is a string of alphanumeric characters that can theoretically be used by anyone to send funds to the individuals or entities in control of the public address.

Private keys are just that: private. They are derived from **seed phrases** and also map to public addresses. But importantly, control over private keys is synonymous with control over the digital assets that reside at these public addresses. If you control the private keys, you control the assets

“Your keys, your bitcoin. Not your keys, not your bitcoin.” - Andreas Antonopoulos, Tech Entrepreneur & Bitcoin Advocate

Accordingly, how private keys are managed matters... a lot.

All stakeholders in the digital assets industry, regardless of whether or not they are aware of it, are exposed to some degree of risk when it comes to managing private keys. When private keys are poorly managed, bad things happen.

Poor Private Key Management in Action

INSIDER SEARCH MARKET MOVERS BUSINESS 03:03:2021 00:38 AM

A man who says he threw away a hard drive loaded with 7,500 bitcoins in 2013 is offering his city \$70 million to dig it up from the dump

The Inside Story of Mt. Gox, Bitcoin's \$460 Million Disaster
Tokyo-based bitcoin exchange Mt. Gox filed for bankruptcy last week, saying hackers had stolen the equivalent of \$460 million from its online coffers. The news rocked the bitcoin world, and it could even bring down the much-hyped digital currency.

OH BUSINESS Markets Tech Media Business Value

\$530 million cryptocurrency heist may be biggest ever
by Daniel Graham @CNBTech
January 01, 2020 12:50 AM ET
A cryptocurrency exchange in Japan is coming under government scrutiny after it said hackers stole \$530 million from its users.

THE BLOCK
JUST IN | EXCHANGES

Japanese exchange Liquid hacked, hacker in possession of \$74 million in crypto assets
by Wolfe Zhao
August 18, 2021, 11:59PM EDT · 1 min read
Download PDF / Print

The Washington Post
After founder's sudden death, cryptocurrency exchange can't access \$190 million in holdings
By Taylor Telford
February 4, 2019

Scenes from the landfill in Newport, Wales, where Howells' hard drive is thought to be located. BBC News

Source: The Block, Business Insider, The Washington Post, Wired, CNN Business

Custodians vs. Technology Providers

Given the easily quantifiable financial risks and the significant reputational risks associated with key management, a diverse landscape of digital asset custody solution providers has emerged. Operators in the landscape can broadly be classified as custodians, technology providers, and hybrid operators.

Custodians perform key management and assume the risk associated with safekeeping assets. These firms are regulated financial institutions that, in the United States, are typically licensed under state banking regulations.

Example: Coinbase Custody, a subsidiary of Coinbase, holds a Limited Purpose Trust Charter and is overseen by the New York Department of Financial Services (“NYDFS”), New York State’s insurance and banking regulator. This grants Coinbase the ability to directly safekeep customer funds. Nonetheless, it precludes the company from functioning as a fractional reserve bank (i.e., loaning out funds that it holds under custody).

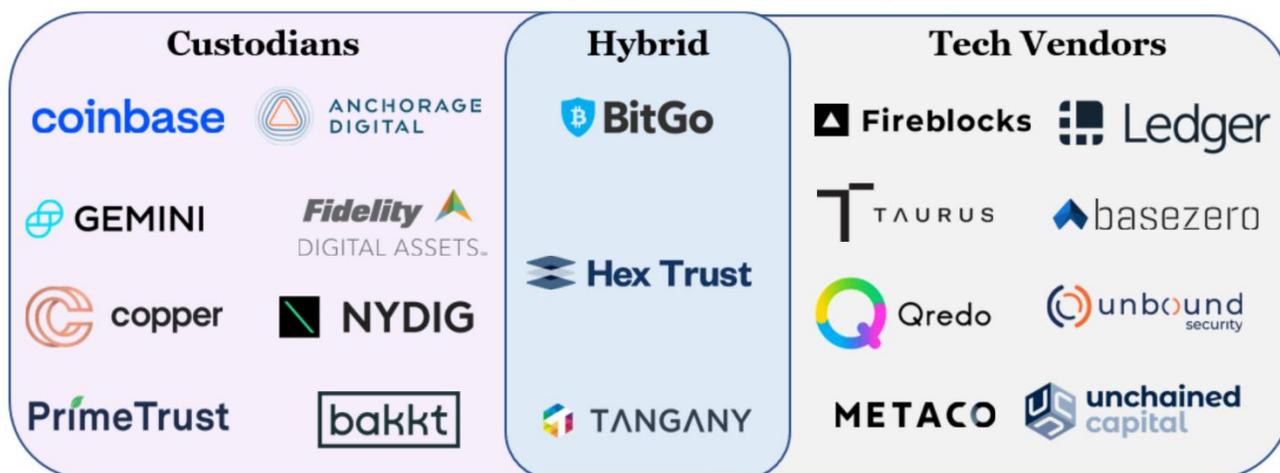
Technology providers provide computer software and hardware solutions that enable their customers to establish custody of their own assets.

Example: Fireblocks, a technology provider, provides MPC-CMP custody technology solutions, tokenization, and settlement network services to institutions. Prime Trust, a custody firm chartered in Nevada, is one example of a regulated custodian that leverages technology solutions provided by Fireblocks to safekeep client assets.

Hybrid providers provide custody solutions and also function as tech providers in providing solutions enabling companies to establish custody over their own assets.

Example: BitGo’s subsidiary, BitGo New York Trust Company LLC, holds a Limited Purpose Trust Charter and is regulated by NYDFS. Additionally, BitGo provides Self-Managed Custody Services which grants its customers full control over their custody operations.

The Custody Provider Landscape



Trust Custodians or Partner with Tech Vendors

Source: The Block Research, Ledger

Security, accessibility, and even the insurance policies that institutional custodians maintain are all important considerations for operators (Exchanges, OTC Trading Desks, Hedge Funds, High Net Worth Individuals, etc.) requiring custody solutions.

But before examining the differences between service offerings, these operators face a more existential question:

“Do we outsource the safekeeping of our business and/or client assets to a custodian (i.e., sub-custody)? Or do we partner with a technology provider to safekeep assets internally (i.e., directly custody)?”

Sub-Custody vs Direct Custody

For traditional financial assets, outsourcing custody operations to a third party is the ‘modus operandi’ for essentially all firms that deal in securities.

As displayed in the table below, four major banks based in the United States, sub-custody the vast majority of all traditional financial assets and support thousands of individual businesses with their securities safekeeping, settlement, and reporting needs.

Traditional Bank Assets Under Custody ⁽¹⁾		
Bank	Domicile	Assets (\$TN)
 BNY MELLON	U.S.	\$45.0 (Jun-21)
 STATE STREET	U.S.	\$42.6 (Jun-21)
JPMORGAN CHASE & CO.	U.S.	\$29.1 (Dec-20)
 citi	U.S.	\$28.5 (Mar-21)
 Northern Trust	U.S.	\$14.8 (Mar-21)
 BNP PARIBAS	France	\$16.1 (Mar -21)
 MUFG	U.K.	\$12.9 (Jun-21)

Source: The Block Research, Company Press Releases, OCC, AssetServicingTimes; (1) Includes assets under custody and/or administration

Reasons for this consolidation include fierce price competition that has favored larger players as they realize economies of scale. Given the size and value of assets and securities held by custodians, entities securing traditional financial assets tend to be large, well-capitalized, and reputable firms.

For digital assets, the custody landscape is highly fragmented across a number of providers. While certain providers, such as Coinbase, have emerged as leaders over the past ~10 years, the industry is still in its early stages and, to date, consolidations have been limited.

Crypto Firms Offering Custody Overview ⁽¹⁾					
Company	Domicile	Custodied Assets (\$BN) ⁽¹⁾	Company	Domicile	Custodied Assets (\$BN) ⁽¹⁾
 coinbase	U.S.	~\$100 (Jun-21)	 ANCHORAGE DIGITAL	U.S.	Undisclosed
 BitGo	U.S.	~\$40 (May-21)	 bakkt	U.S.	Undisclosed
 GEMINI	U.S.	~\$30 (May-21)	 Fidelity DIGITAL ASSETS.	U.S.	Undisclosed
 KINGDOM TRUST	U.S.	~\$12 (May-21)	 Genesis	U.S.	Undisclosed
 NYDIG	U.S.	~\$7 (May-21)	 FirstDigital	Hong Kong	Undisclosed
 Bitcoin Suisse	Switzerland	~\$3 (Mar-21)	 PrimeTrust	U.S.	Undisclosed
 Hex Trust	Hong Kong	~\$1 (Mar-21)	 OSL THE TRUSTED DIGITAL ASSET PLATFORM	Hong Kong	Undisclosed
 copper	U.K.	Undisclosed	 SEBA BANK	Switzerland	Undisclosed

Source: The Block Research, Company Websites, Press Releases & Financial Statements; (1) Represents select providers and is not an exhaustive list

The decision of whether to outsource digital assets custody to a third party, such as the digital assets custodians listed above, or to retain custody in-house has emerged as an important consideration for digital assets companies. It has far-reaching operational, risk management, and regulatory and compliance implications for these firms and their customers alike.

Operations

Securing digital assets requires diligence across multiple fronts. Generally speaking, custody solutions have two main goals:

- 1) Securely storing assets through private key management or MPC technology
I.e., How do you prevent malicious actors from gaining control over the ability to sign transactions?

2) Providing for the safe transfer and settlement of digital assets
I.e., Once someone has the ability to sign transactions, how do you minimize attack vectors and ensure no errors are made when sending assets to another counterparty?

1) Securing Assets: Transaction Signing Power, Cold Wallets vs Hot Wallets, and MPC technology

Transaction Signing Power

Who holds private keys determines who can digitally sign and effect transactions on the blockchain and ultimately who assumes the risks associated with securing digital assets.

While transaction signing arrangements can have layers of complexity, digital assets firms that outsource custody operations (i.e., go sub-custody route) grant custodians the ability to sign transactions on their behalf. Service level agreements typically govern relationships between firms and their sub-custodians and outline when customers can withdraw funds and how long it will take the custodian to perform withdrawals. Under these arrangements, custodians assume the risk associated with securing assets.

Digital assets firms that partner with custody tech vendors, ultimately retain control over the signing capability for transactions. Hence, while these firms employ the software and hardware solutions provided by technology firms, they devise their own governance mechanisms detailing who at their firms can sign transactions and what conditions need to be met for transactions to be effected. Under these arrangements, digital assets firms retain the risk associated with securing their own assets.

Second to who can actually sign transactions, which types of wallets (i.e., cold vs hot) that private keys are stored on, is an important security consideration.

Cold Wallets

For cold wallets, private keys that sign transactions are held offline and never come into contact with an online server. Hence, the security of assets in cold wallets is primarily a function of the controls and physical security of the offline computer hardware where keys are stored (or in some cases the physical paper that keys are printed on).

While some custodians commingle funds to expedite withdrawals, retrieving digital assets stored in cold wallets is not too dissimilar from accessing gold bars

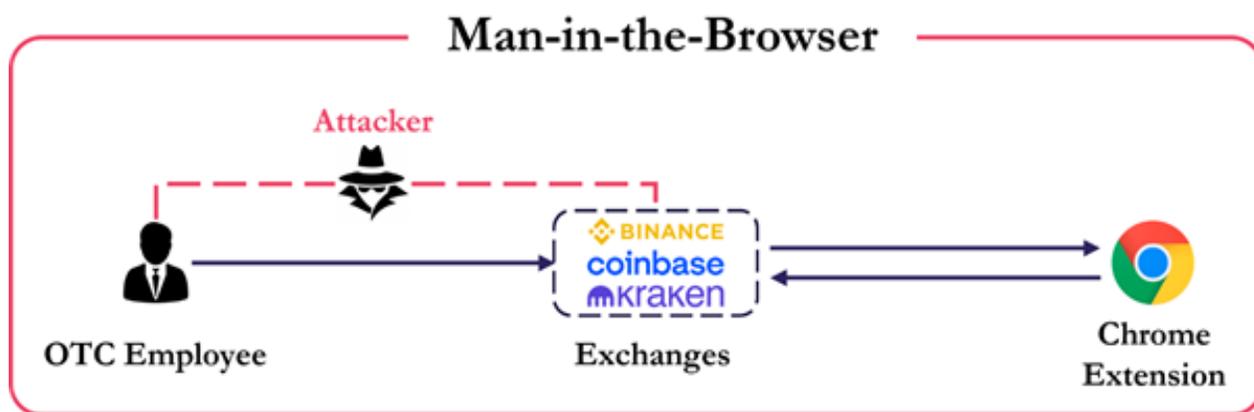
stored in a safe. Depending on the security mechanisms of the firms relying on cold storage, governance policies in which multiple individuals are required to gather in a vault to collectively unlock hardware storing private keys, or biometric scans are examples of some of the authentication processes required to access funds held in cold wallets.

Hot Wallets

For hot wallets, the keys signing transactions are held online and transactions can be effected without having to physically access hardware devices. This provides many benefits for operators as it enables them to more easily transfer funds to other counterparties on a timely basis. But it also introduces a new array of web-based attack vectors as private keys are hosted online.

For example, when keys are stored online, a “Man-in-the-Browser” attack, such as the one depicted below becomes a new attack vector.

Example: In late 2020. A hacker stole 370,000 NXM (worth ~\$8MM) from DeFi project Nexus Mutual by exploiting the web-based hot wallet (Meta Mask) that its CEO was using. The hacker infected the project’s CEO’s computer with malware and installed a modified, malicious chrome extension which ultimately tricked the CEO into signing a transaction that transferred funds into the attacker’s own address.



Given these risks associated with hosting a single private key in an environment that is connected to the internet, several solutions (i.e., multi-signature wallets, and MPC) that eliminate these single points of failure risks have emerged.

Technology Providers and Multi-Party Computation (MPC)

MPC is a popular solution that technology firms provide to digital assets operators enabling them to custody their assets. Rather than private keys being generated during wallet creation or transaction signing, MPC produces encrypted shards that, when combined, ultimately constitute a private key capable of signing transactions. With MPC, parties independently compute their part of the private key share to produce a signature without revealing their share to other parties. Accordingly, the private key is never formed in one place, and MPC shards are typically spread across multiple decision makers within or across organizations.

Ultimately, the security of MPC-based solutions is ultimately a function of governance processes. If MPC shards are truly distributed across organizations that do not share servers or computer infrastructure, the risk of funds being compromised in a hack is essentially eliminated as no one entity has access to the entire key. On the other hand, an MPC implementation whereby all shards are stored on one vulnerable server could still result in a single point of failure and higher risk of attack.

While MPC theory has been around since the 1980s, there has been significant innovation in the digital assets space the past few years. For example, MPC-CMP, an open-source algorithm released by Fireblocks in 2020, builds on prior MPC implementations to bring performance and security enhancements compared to earlier protocols

MPC-CMP reduces the number of requisite communication rounds found in previous MPC algorithms (typically 6 – 9 rounds) to 1 round thus allowing transactions to be signed ~8X faster. It allows for key shares to be refreshed in minutes-long intervals, thus reducing the amount of time that a malicious actor would have to steal all the key shards before shares are refreshed. And finally, it allows for more flexible hot and cold key signing mechanisms whereby at least one key shard can be stored offline and still used for signing.

Notably, unlike sub-custody arrangements whereby digital assets companies are exposed to the risk of custodian insolvency, in the unlikely event that a custody tech provider were to go out of business, companies relying on their solutions would still be able to recover their funds.

So, who is in charge of securing digital assets (sub vs direct custody), where signing material is stored (cold vs hot wallets), and what technology operators are using to manage keys (single key vs multi-sig vs MPC (and its different implementations)) are all important considerations for digital assets operators.

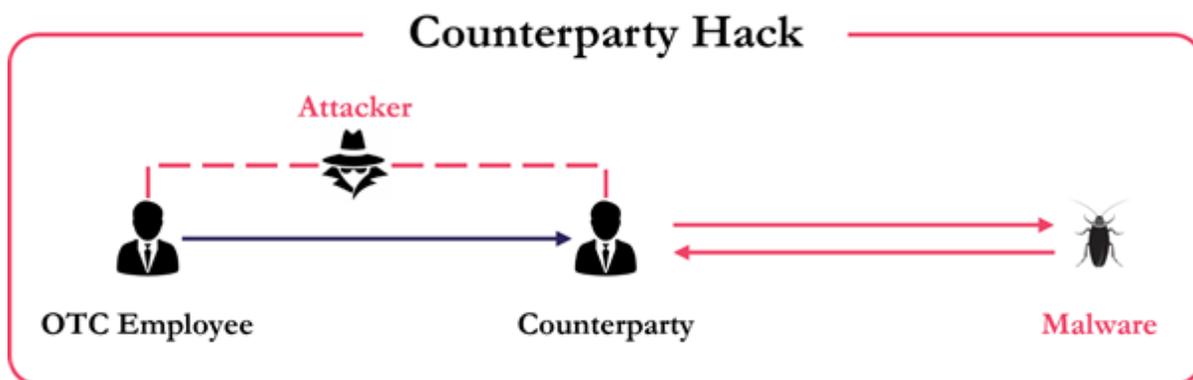
But security does not stop there.

2) Transferring and Settling Assets

As digital assets are settled on a peer-to-peer basis, there is no clearinghouse that establishes trust between counterparties. This peer-to-peer nature eliminates many of the costs that accrue when middlemen establish trust between counterparties. But it also adds a new element of risk whereby digital assets operators need to exercise diligence and caution when effecting irreversible transactions.

“One of the biggest fears that we have in trading crypto is sending coins to a wallet that isn’t in use anymore...or is the wrong wallet or maybe we copy and pasted something wrong. That’s one of the biggest concerns that everyone in crypto has”
- Delfos Machado, Managing Director at Dunamis Trading

For example, consider what can happen when a digital assets counterparty wants to send funds to an OTC desk. Even if the employee of an OTC desk sends this counterparty the correct deposit address on a secure messaging service, an attacker can still interfere by deploying malware onto the counterparty’s system to change this deposit address and divert the funds to its own personal wallet.



Hence, digital assets custody not only requires controls surrounding how assets are secured, but also safeguards on how transfers are operationalized. Technology providers are providing solutions that seek to mitigate many of these settlement risks by automating many of the processes around address input and management.

Example: Technology provider Fireblocks’s Digital Asset Transfer Network (Fireblocks Network) connects counterparties on its platforms with major OTC trading desks and exchanges. The network authenticates counterparties within the network such that public addresses do not need to be manually input when sending funds to other counterparties.

In addition to these services that automate and reduce the risks associated with

transferring assets, custodians are devising solutions that eliminate the need to remove assets from cold storage and transfer them to other liquidity venues such as exchanges (which to date have been some of the biggest “honey pots” for hackers).

Example: Using Copper, a U.K.-based custodian’s ClearLoop network, participants can delegate assets that are held under custody at Copper to a third party such as an exchange, while never removing the assets from cold storage. Thus, operators no longer need to entrust their funds to third-party exchanges (mitigates the security and settlement risks) and can also improve capital efficiency by not pre-funding exchange accounts.

Risk Management: Insurance and Control Testing

While digital assets and blockchain technology are lauded for their “trustless” nature, trust remains a critical component of custody. In the case of traditional financial assets custody, large and reputable firms with big balance sheets and long histories of successful safekeeping of client assets have won the trust of thousands of firms.

Given the nascent stage of the digital asset industry, the overall size and longevity of digital assets custodians pales in comparison to that of the largest traditional financial firms.

Example: Coinbase, which is likely the largest digital assets custodian by assets under custody, was founded in 2012 and custodies ~\$100 billion in assets. The largest custodian for traditional financial assets, BNY Mellon, was founded in 1874 and has custodied trillions of dollars of assets for decades.

To mitigate some of these uncertainties that come with not only safekeeping an entirely novel asset class, but also the relatively limited track record of operators, insurance and control testing have emerged as popular offerings.

Insurance and Control Testing

Traditional, fiat-denominated bank deposits in the United States are backstopped by The Federal Deposit Insurance Corporation (FDIC), an independent government agency created by Congress to instill trust and confidence in the banking system. Accordingly, depositors are guaranteed their money (up to \$250K per depositor) even in the event that the bank they hold their deposits at becomes insolvent.

The same cannot be said for digital assets custodians. Even as it relates to federally chartered custodians, such as Anchorage Digital, the digital assets that it holds under custody are not backstopped by FDIC insurance. Accordingly, the risk management policies and operational processes followed by digital assets custodians can be an important consideration.

While custodians are not required by law to maintain insurance, they typically maintain policies that cover a small portion of their total assets under custody thus providing a degree of protection to their customers.

The two main insurance policies held by custodians today are specie and crime policies. Specie policies focus on physical damage or loss (employee misuse or theft) of private keys in cold storage. Crime policies are broader in scope and cover internal and external fraud, including electronic theft which would extend to hot wallets. Coverage for hot wallet exposures is significantly more expensive than coverage for cold storage alone.

Example: Coinbase carries an annually renewed commercial crime policy that carries a \$320MM limit (per-incident and overall), with Coinbase Global as the named insured.

Recently, some custodians have started offering customers options to be named as “loss payee” so as to provide increased assurances of the security of their individual funds as opposed to general, company-wide policies such as Coinbase’s crime policy which typically only cover a portion of their funds.

Example: In March 2021, BitGo announced a \$700MM insurance program for assets held in its cold storage. Of this \$700MM, \$100MM is held in BitGo’s name as the insured and available to all customers. The remaining \$600MM is available to its customers on a “loss payee” basis whereby individual customers, rather than BitGo, would be entitled to payment in the event that the insured, BitGo, were to make a claim.

Finally, technology providers and custodians periodically undergo audits and control testing performed by independent audit firms and cybersecurity companies. Two of the more common audits are SOC 1 (“System and Organization Controls”) which is focused on financial reporting processes, and SOC 2 which assesses the effectiveness of security controls and compliance processes. Additionally, many providers undergo simulated cyber-attacks on systems, also referred to as penetration tests, to expose any potential weaknesses in security architecture.

Regulatory Compliance for Custody Providers

Globally, the regulatory landscape for digital assets is highly fragmented. To date, the United States, Switzerland, and Hong Kong have emerged as popular domiciles for some of the industry's largest custodians.

Historically, entities in the United States that custody digital assets are chartered as banking institutions at the state level. In some instances, bank charters eliminate the need for custodians to obtain a separate state money transmitter license which is typically required to be obtained by any digital assets companies that fall under the State's individual definition of a Money Services Business ("MSB"). Under these state banking licenses, custodians are also required to comply with federal Anti-Money Laundering ("AML") regulations and put in place the appropriate policies and procedures such as Know Your Customer ("KYC") processes. In the United States, these regulations fall under the Bank Secrecy Act ("BSA") which is administered by The Financial Crimes Enforcement Network (FinCEN), a bureau of the United States Department of the Treasury.

At the federal level, The Office of the Comptroller of the Currency (OCC), an independent bureau within the United States Department of the Treasury, published an interpretive letter in July 2020 authorizing national banks regulated by the agency to custody digital assets on behalf of their clients. Accordingly, a slew of traditional financial firms including custodian banks are well underway researching digital assets custody and some have already begun offering digital asset custody services to their customers.

As technology providers do not transact in digital assets, they are not subject to money transmitter and/or banking regulation. Nonetheless, several firms provide integrations with on-chain forensics and transaction monitoring firms such as Chainalysis and Elliptic, to help their customers meet compliance requirements.

Which solution is right?

Whether a firm's needs are best met by outsourcing custody of assets to a third-party custodian or by partnering with a technology provider and retaining custody over their own assets will ultimately depend on their individual circumstances.

For example, for passive digital asset fund managers (e.g., Grayscale, Bitwise) that stockpile one or few assets and issue securities against them, sub-custody solutions that rely heavily on cold storage remain popular solutions. These companies have minimal needs to withdraw assets, rarely conduct complex trading strategies, and generally speaking do not participate in yield generating opportunities and staking. Hence, entrusting assets to a third-party custodian

that places assets in cold storage does not preclude them from servicing their customers.

On the other hand, for more active digital assets market participants, such as hedge funds and fintech companies, outsourcing custody to a third party could prevent them from appropriately servicing their customers. Accordingly, partnering with technology vendors has become an increasingly popular trend these firms that has enabled them to be flexible and rapidly adapt to the evolving digital assets landscape.

By retaining custody over their own assets, these firms can withdraw, deposit, and transfer assets on a 24/7 basis and avoid the “closed loop” nature of some sub-custody relationships whereby they would be required to trade through their sub-custodian’s venue. This could be a critical factor for allowing them to rapidly and opportunistically deploy capital in the fast-moving digital assets market – an action that could be severely limited if they outsourced custody to a third party that needed to be contacted to retrieve assets from cold storage.

Additionally, many firms that retain custody over their assets have benefited from easier access to investment and yield generating opportunities accessible in decentralized finance (DeFi) markets and staking. Leading technology providers have built out integrations to DeFi protocols such as Compound (a decentralized lending protocol) as early as November 2020. This has granted their customers access to yield generating opportunities without having to transfer assets to web-based browser extension wallets.

Outlook

While custody in the traditional financial landscape is highly concentrated amongst a few top providers, the digital assets custody landscape remains highly fragmented across both regulated financial institutions and technology providers who are competing within their respective niches.

The world’s largest traditional financial institutions and custodian banks are well underway with researching digital assets custody, and deployments of their own solutions are already hitting the market.

Institutional Interest in Digital Assets Custody

REUTERS
BANKS MARCH 18, 2021 / 8:04 AM / UPDATED 7 MONTHS AGO

BNY Mellon invests in cryptocurrency storage firm Fireblocks

By Reuters Staff 2 MIN READ

Bloomberg
Cybersecurity
Cowen to Offer Crypto Custody to Hedge Funds and Asset Managers

By Jennifer Surane + Follow
May 13, 2021, 7:00 AM EDT

- It promises 'institutional-grade' custody in new partnership
- Wall Street is warming up to holding clients' cryptocurrency

Business
US Bank Launches Crypto Custody With NYDIG Backing

The service will support private funds holding BTC, BCH and LTC, with an ETH option in the works, a source told CoinDesk.

By Danny Nelson · Oct 5, 2021 at 125 pm EDT · Updated Oct 5, 2021 at 2:07 pm EDT

CNBC
MARKETS
State Street is creating a dedicated cryptocurrency division

PUBLISHED THU, JUN 10 2021-9:53 AM EDT

Tanya Machael
@TANAMAC

TECH
PayPal is acquiring crypto security company Curv, for less than \$200 million

PUBLISHED MON, MAR 8 2021-9:41 AM EST | UPDATED MON, MAR 8 2021-2:25 PM EST

Jessica Berezovsky
@JBREZOVSKY

Source: The Block, Reuters, Bloomberg, CoinDesk, CNBC

In March of this year, the world's largest custodian, BNY Mellon invested in Fireblocks's \$133MM Series C fundraise and is working with the institution on a custody solution. And in October, US Bank, the fifth-largest banking institution in the United States, launched crypto custody services in a partnership with NYDIG.

Over the short term, there are several factors that make rapid consolidation with the industry due to the entrance of these major players unlikely. It will take significant time and resources for traditional firms to develop custody platforms and the related products and services that firms rely on (i.e., digital asset prime brokerage services). Switching costs make it unlikely that incumbents will swiftly adopt solutions pioneered by traditional institutional players. And finally, firms that have already developed and are realizing the benefits of leveraging their own custody solutions, are unlikely to move to a sub-custody model.

Over the long-term, tens and eventually hundreds of trillions of dollars' worth of value will likely be tokenized into liquid, fungible and non-fungible blockchain-based assets. All signs point to traditional financial firms, incumbent digital assets custodians, and technology providers all playing an important role in this rapidly evolving and competitive market.