BLOCKZERO

Digital assets custody: An evolving landscape

January 2023

Authors:

Marie-Chantal Leduc

Sabrina McNeil

Kasyap Anand

Table of contents

Introduction: How an old mechanism became a new issue

Over the last few years, the digital asset market attracted a **growing number of investors.** The total market capitalization currently valued at $812B reached an all-time high of $3Tr in November 2021.

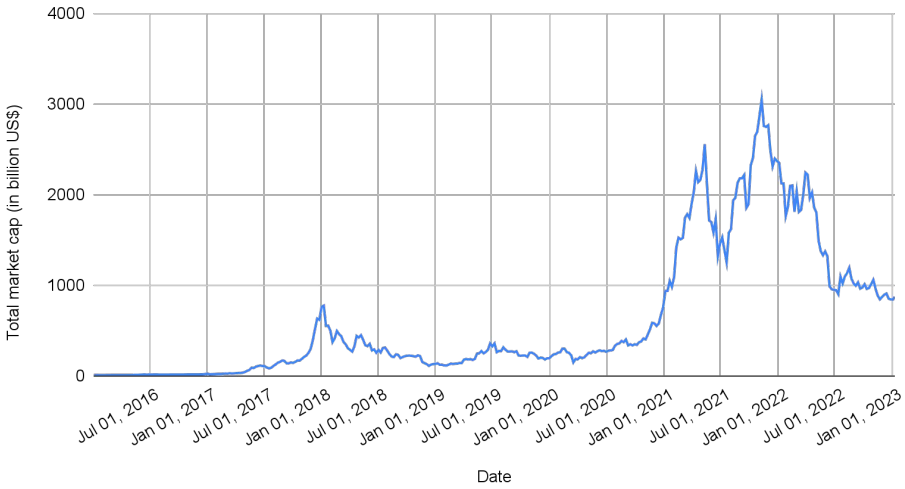
Yet, as with traditional assets and money, **investing or owning digital assets necessarily involves the storage and protection** of these assets, that is, custody. And what more, digital asset custody comes with a variety of choices, each with its own risk, advantages and implications.

The events that marked the digital assets space recently have emphasized **the relevance and importance of this core function** of the traditional financial infrastructure which has been around for ages.

Whether it be the collapse of Celsius or the scandals of FTX, the choice of custody method and of the type of custodian will **impact what happens to the assets when the worst case scenario materializes.**

It is one of the main question to be asked whenever contemplating investing in digital assets, be it Ethereum or Bitcoin, or tokenized assets like real estate tokens or gold tokens or NFTs.

Cryptocurrency market capitalization from 2016 to 2023 (in billion US$)



This article presents the key different custody options currently available to different types of investors, while exploring the fundamentals of custody to be thought of moving forward.

Sources: BlockZero analysis (2023); CoinMarketCap (2022), Statista (2023)

Digital assets custody in a nutshell

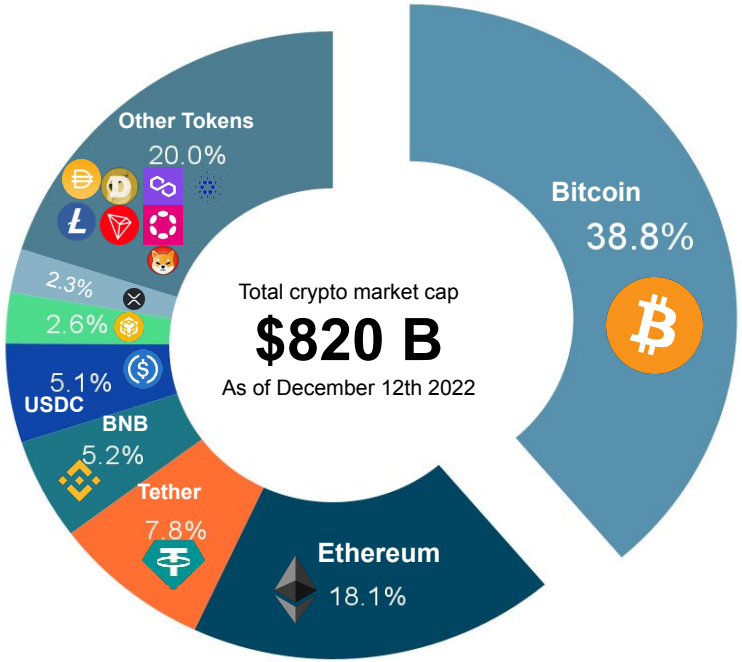
Digital asset custody: a critical infrastructure

In traditional finance, typically banks and other financial institutions custody customer assets, which means **they are responsible to safeguard that asset and prevent them from being stolen or lost.** Similar to traditional custody, digital asset custody is a general term that covers a variety of methods for storing and protecting digital assets, such as cryptocurrencies or Non-Fungible Tokens (NFTs), on behalf of their owners[1].

Both retail and institutional investors need to protect their digital assets in the same way they protect their cash, stocks and bonds. This type of custody is provided by crypto exchanges, dedicated custodians, self custody wallets and third party custody wallets. Whereas retail clients can choose their preferred method of custody, to some extent, in some jurisdictions such as Canada, institutional investors are required to store their assets with regulated third parties to ensure compliance with existing regulations and for effective risk management.

With the range of digital assets present in the market, including but not limited to cryptocurrencies, stablecoins, central bank digital currencies (CBDCs), NFTs, tokenized assets (gold, real estate, bonds…), there is an increasing need for digital asset custodians to protect consumers. In 2022, many investors and consumers have lost their assets due to the inherent risks of investing in crypto markets, but also the lack of vigilance towards their custodian. **This section introduces the range of digital assets custody options** and implications in terms of security.

Digital Asset custody could grow to a multi billion dollar industry [2]



Source: BlockZero analysis (2023); 1) Fireblocks (2022); 2) CoinMarketCap (2022)

Custodial vs non-custodial wallet: different IT / security risk exposure

At the core of digital asset custody is the concept of a wallet, which is the place where the owner's cryptographic keys are stored. Depending on the type of security selected for the cryptocurrency funds, users can select two categories of wallets services, such as non-custodial and custodial wallets services. A summary overview of each type of wallet service is provided below[1,2,3].

	Non-custodial wallet services	Custodial wallet services
Overview	Non-custodial wallets are also called "self-custody", meaning that investors and users have control over their private key. This allows the user to not trust a third-party custodian with their funds. However, the user must ensure that they do not lose their private key and guarantee the protection of their funds.	With the use of a custodial wallet, a third party has control over the private keys to access cryptocurrency funds. In this case, the user must trust the custodian to secure the funds and ensure they are available when needed.
Wallet backup	If the seed phrase (a random words used to access crypto or retrieve a wallet) is lost, the user loses his funds forever.	User has access to recovery options in case they lose access to their account.
KYC	No AML / KYC procedures are required.	AML / KYC procedures are needed.
Security risks	The user does not depend on a third-party, but he is personally vulnerable to thefts and errors on his own.	The user relies on a third-party which may be subject to hacking.
Common solutions	Browser-based exchange wallets or hardware wallets.	Web-based exchange wallets.
Examples	Electrum, Ledger, Trezor, Zengo, Binance Chain Wallet, Fireblocks, Metamask, Circle…	BitGo, Coinbase, Gemini, Kraken, Bakkt, Binance Custody…

Source: BlockZero analysis (2023); 1) Gemini (2021); 2) Linen (n.d.) 3) 101 blockchains(2022)

Different needs, different storage methods of digital asset custody and security

Depending on the wallet service chosen, three methods of storing cryptocurrency keys are available: Hot Wallet, Warm Wallet and Cold Wallet[1]. One may transition digital assets from hot to warm or cold wallet depending on trading needs. Some alternatives bring additional layers of security and functionality to cryptocurrency storage, such as multi-signature and smart contract wallets[2].

	Hot Wallet	Warm Wallet	Cold Wallet
Description	Two of three keys are held online and transactions can be signed instantly for the fastest possible access.	A hybrid solution developed to increase client-side efficiency with just one of the keys remaining online.	The ultimate protection takes all 3 distributed keys offline and accessible via optical air-gapping system.
Connected to Internet	✓	✓	✗
Fully offline	✗	✗	✓
Security	✗	✓	✓
Speed and efficiency	✓	✓	✗
Ease of trading/access	✓	✓	✗
Best for	High Frequency Transactions, Instant transfers	Arbitrage strategies, 24/7 access	Long only funds, Maximum security
Examples	BitGo, Coinbase, Binance Custody and chain wallet, Metamask, Circle…	Zengo, Fireblocks…	Ledger, Electrum, Trezor, Metamask, Circle…

BLOCKZERO

Source: BlockZero analysis (2023), 1) Deloitte (2020); 2) Fireblocks (2022)

Institutional investors needs are changing the landscape

Surge in institutional investors is creating new needs

Lately, number of institutional investors incorporated digital assets in their portfolio, which, in turn, drove the need for **ever more regulated and secure qualified custodian services** (see slide 9-10).

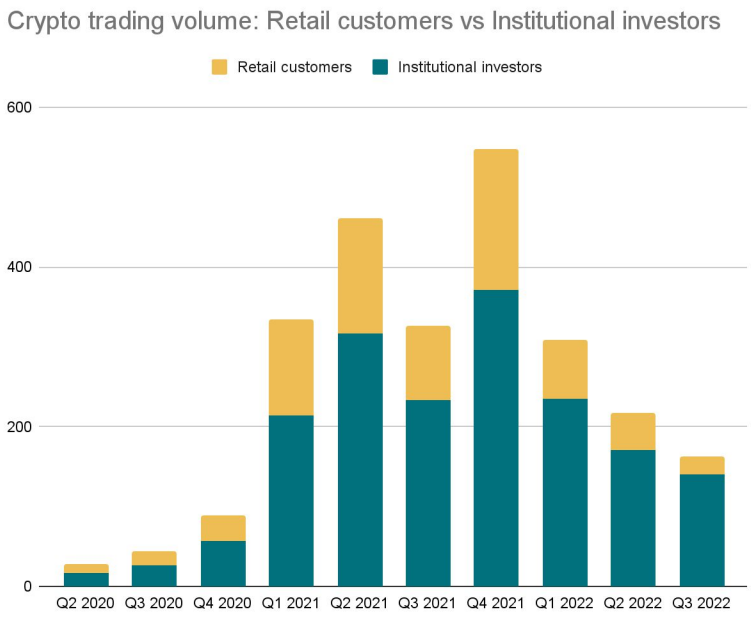
The increasing popularity and market cap of digital assets has spawned a number of custody solutions (see slide 11), resulting in a **dispatched, shifting and sometimes insecure landscape** which remind us the beginnings of the modern banking in the 19th century.

The appearance of confusion can worry institutional investors because it brings uncertainty (see slide 12). At the same time, after years of disbelief, their view of digital assets has turned to interest, fueled by the lure of higher returns and the underlying value of the technological innovations. Fulfilling their needs for the best customized solution has become a **strategic and sovereignty issue.**

Some north american custodians, qualified or not, like **Tetra**, **Knox**, **BitGo** or **Digivault** leverage institution-grade custody policy regulations to appeal to institutional investors. While continuously improving their service offering to meet evolving needs, there is still room for a competing offering - **Banks being one of them**.

Working to their advantage is the historical trust, built on their reputation (not without incidents) and the stringent and evolving regulations they must comply with. One may argue that their central role in the current financial system could **reassure the institutional investors** that their digital assets will be safely kept, thus driving adoption. It remains for these banks to build a robust infrastructure to efficiently manage this specific asset class. Although more easily said than done (see slide 14).

So it's not surprising to see more and more banks offering or announcing **new digital asset custody services to their clients** (see slide 13) - although they remain few. For now, retail customers are not allowed to sign up for these services, but for how long?



The volume of crypto transactions from institutional investors far exceeds that of retail clients

Source: BlockZero analysis (2023); CoinTelegraph (2022); Coinbase (2022)

Qualified custodian: What does it mean in Canada

According to the Canadian legislation [1]

There are three types of **Canadian Custodians**, all of which are considered qualified custodians:

- a **bank** listed in Schedule I, II or III of the Bank Act;
- a **trust company** that is incorporated under the laws of Canada and that has equity of not less than $10,000,000;
- an **investment dealer** that is permitted under the rules of IIROC to hold the cash and securities of a client or investment fund.

+

A **foreign custodian** is considered as qualified custodian if it is an entity - or an affiliate of an entity - that:

- is incorporated under the laws of a country, other than Canada;
- is regulated as a banking institution or trust company by the government of the country;
- has equity of not less than the equivalent of $100,000,000.

Canadian institutional investors must work with qualified custodians, even in the case of digital assets.

This requirement was issued by the **Canadian Securities Administrators** (CSA) - a grouping of all provincial and territorial securities regulators in Canada that acts to harmonise the regulation of Canadian capital markets - through National Instrument (NI) 31-103 which governs all registration requirements and exemptions. It is assisted by the Investment Industry Regulatory Organization of Canada (IIROC) who has quasi-judicial powers to enforce the law and take sanctions.

However, despite the requirement to use a Canadian custodian, NI 31-103 states that *"a **foreign custodian may be a custodian** of the cash or securities of the client or investment fund if a reasonable person would conclude, considering (...) the nature of the regulation and the sufficiency of the equity of the foreign custodian, that using the foreign custodian is more beneficial to the client or investment fund than using a Canadian custodian."*

This exemption allows any canadian institutional investor to entrust a foreign custodian with the custody of its assets (traditional or digital). As there is just one qualified custodian of digital assets in Canada, this explains why so many institutional investors turn to qualified US custodians.

Sources: BlockZero analysis (2023); 1) National Instrument 31-103 Registration Requirements, Exemptions And Ongoing Registrant Obligations.

Qualified custodian: What does it mean in the US

Institutional investors want to make sure their digital assets, as their traditional assets, are safe and **custodied by regulated method**.

In US, the Securities Exchange Commission (SEC) is a key regulator who has been active in the regulation of digital assets. As other regulators, it aims that the accounts holding these assets are safe and secure, that they exist there, and that they are custodied in a **qualified manner**. Which involves, by the law, the following requirements: details on how the assets are being held, detailed account statements, annual surprise exams...

This Custody Rule is designed, as elsewhere, *"**to protect client funds** or securities from being lost, misused, misappropriated or subject to investment advisers' financial reverses, including insolvency."*[1]

Some, like the non-qualified custodian Fireblocks, argued that this rule is **not adapted to the digital assets**, because their custody implies holding both the asset and the client's private key. So the qualified custodian Anchorage proposed, beyond the usual entities oversight, these technical requirements: proof of exclusive control of the asset, proof of its existence, highest hardware security standards, blockchain monitoring of custodied digital asset…

For now, the current law prevails. But this explains why some digital assets custodians are not qualified, but propose institutional-grade services.

According to the US legislation [1]

A **qualified custodian** maintains funds and securities of their clients either**:**

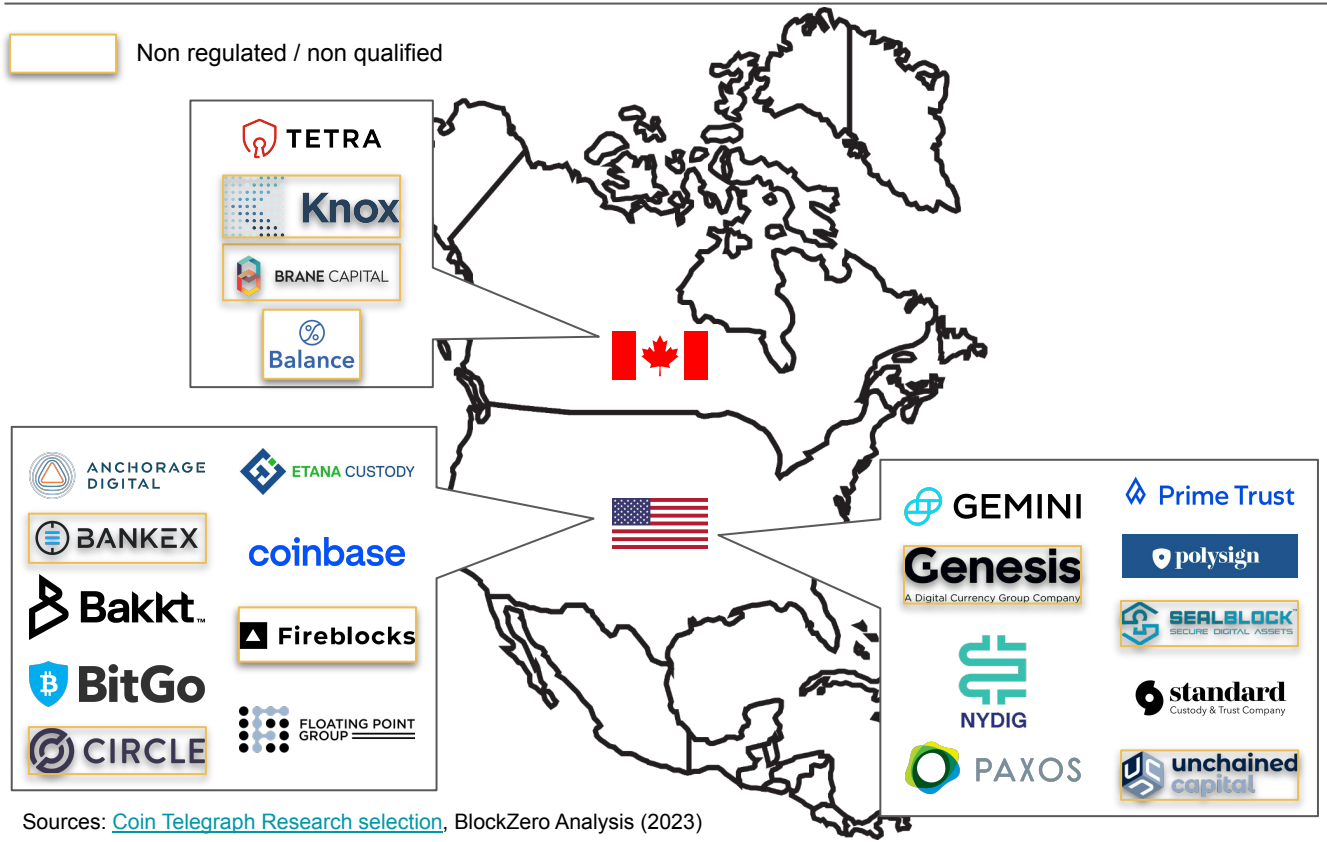
- In a separate account for each client under that client's name;
- In accounts that contain only clients' funds and securities, under your name as agent or trustee for the clients.

So a **qualified custodian** means:

- **A bank** or a savings association;
- **A broker-dealer** registered, holding the client assets in customer accounts;
- A future **commission merchant** registered, holding the client assets in customer accounts,;
- A **foreign financial institution** that customarily holds financial assets for its customers.

Sources: BlockZero analysis (2023); 1) Adoption of Rule 206(4)-2 Under the Investment Advisers Act of 1940, Investment Advisers Act Release No. 123 (Feb. 27, 1962).

North America's institutional grade custodians



Sources: Coin Telegraph Research selection, BlockZero Analysis (2023)

While there are many institutional-grade custodians in the United States (the main ones presented in the figure on the left), Canada has only four (Tetra, Knox, Balance and Brane Capital).

And although **Canada has been the 1st country to allow cryptoasset exchange-traded funds** (ETFs), and that regulation requires institutional investors to custody with regulated entities, preferably in Canada, **the ecosystem has lagged behind in providing qualified custody solutions**, such that many have chosen one of the many regulated US custodians to keep their digital assets safe

In fact, **Tetra** only gained regulatory approval as of 2021, and **it remains the only qualified custodian in Canada** [1].

Sources: BlockZero Analysis (2023;) Visual adapted from Cointelegraph Research (2022); 1) The Globe and Mail (2021)

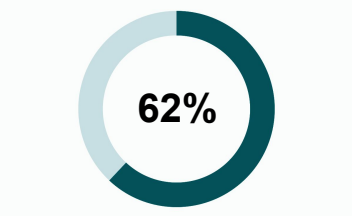
Growing demand from institutional investors is offering opportunities to banks

Yet, the recent collapses of major players abroad raised not only practical and security concerns, but sovereignty ones that may ultimately drive canadian investors' digital assets back home (see the diagram on the right).

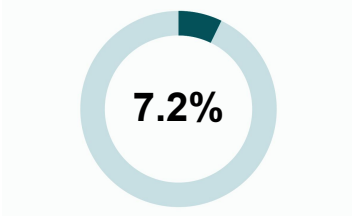
The timing of the recent partnership between 3iQ, Tetra and Coinbase - which aims at expanding the exchange-traded product ecosystem for digital assets in Canada - points in that direction. However, the supply will need to grow more to meet the expected growth in demand from institutions.

And as long-time qualified custodians, traditional banks are well-poised to capture at least some of this demand and respond to these concerns. According to the Bank for International Settlements (BIS), banks held over $100 trillion in all type of assets by 2022.

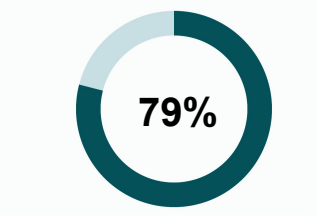
It is therefore no surprise to observe a growing number of banks offering custody services for digital assets as depicted on the following page.



Of institutional investors plan to hold or already hold digital assets

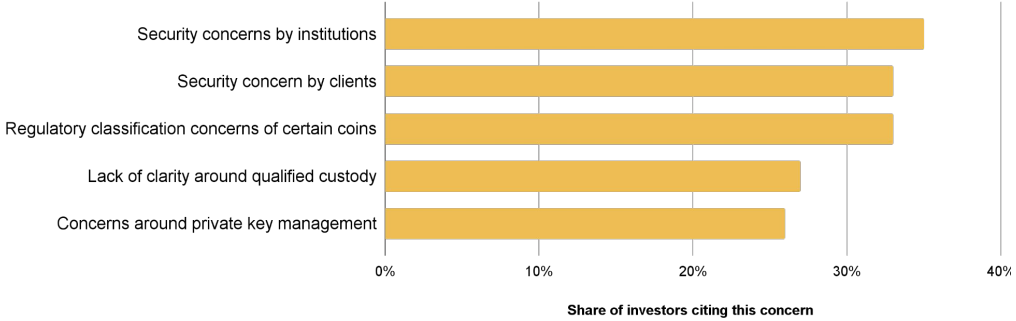


Of the bitcoin supply is held by institutional investors



Of Coinbase's daily trading are done by institutional investors

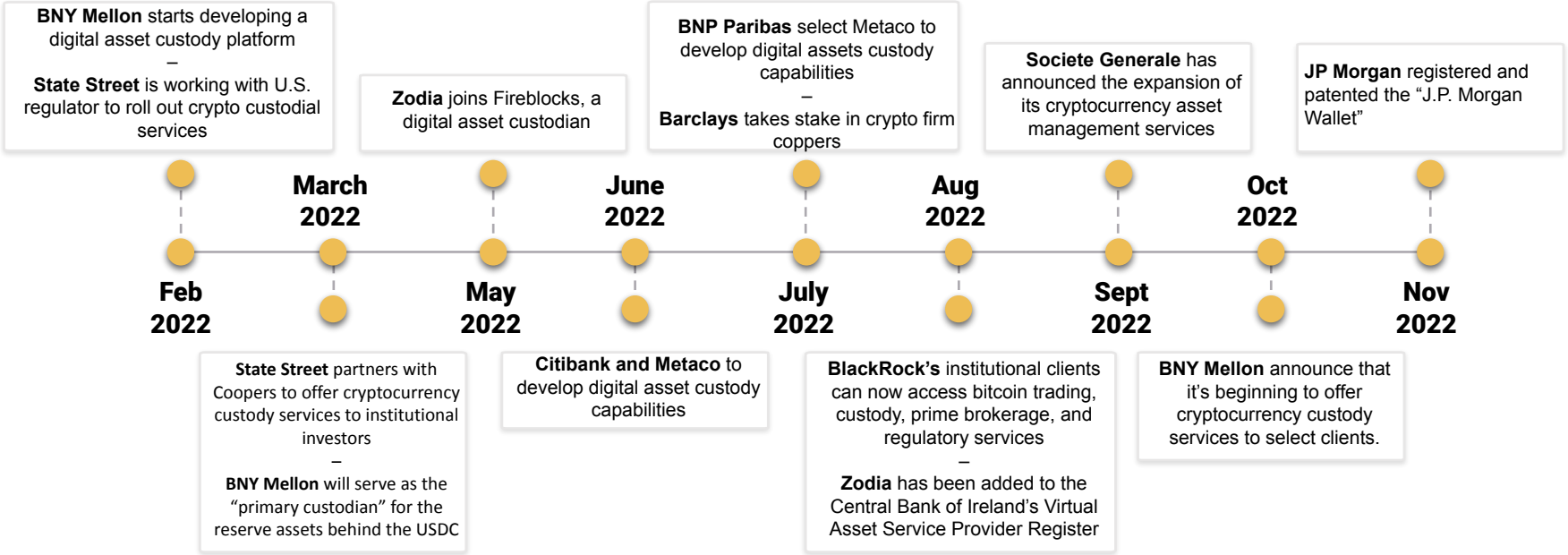
Obstacles to Investing in Digital Assets according to institutional investors (adapted from Fidelity Survey 2022)



Source: BlockZero analysis (2023); CoinTelegraph (2022): BIS (2022); Fidelity Institutional Investor Digital Asset Study (2022)

Outside Canada, banks are getting more and more involved in digital assets custody

Abroad, 2022 saw a large number of financial institutions announcing their entry into digital asset custody. To these announcements, one should add the proof-of-concept conducted in the recent months by the New York Fed to test the feasibility of digital currencies operating in a network of financial institutions. BNY Mellon, Citigroup, PNC, TD Bank, Truist, U.S. Bank and Wells Fargo are among the financial institutions participating, along with Mastercard and SWIFT.

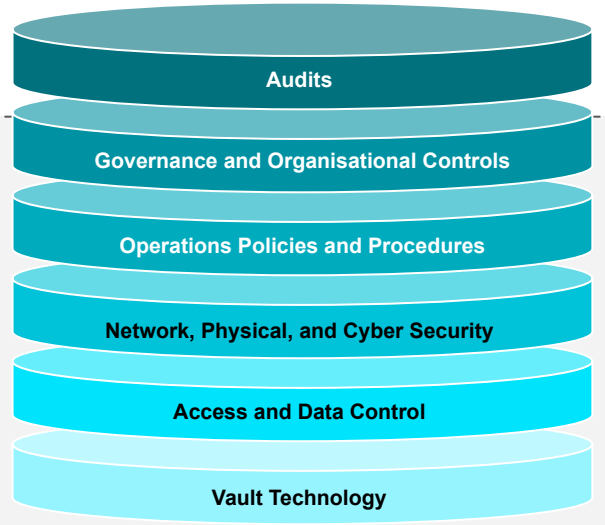


BLOCKZERO

Source: BlockZero analysis (2023); Visual adapted from Whitesight (2022

For banks, custody digital assets will require more than engineering

Adequately safeguarding digital assets, while enabling the full benefits that the underlying technology offers, including those of blockchain innovation, is a multi-layered process that extends beyond just technology (see governance model diagram below). While traditional banks have developed deep expertise in many of these areas, the regulation with regards to digital assets remains uncertain in some instances, while continuously evolving. Whether building in-house or partnering with a third-party, the technological developments the bank will require will go beyond the custodial assets and engineering needed for adequate integration of financial infrastructure.



Periodic internal and external audits to monitor compliance with regulations, internal policies and procedures and system controls supported by the client's auditing function and reporting (ie.Proof of reserves, SOC 1, SOC 2, etc.)

Governance mechanisms to monitor the operations and manage the systems, supported by the IT policies of the client

Policies and procedures that are compliant with KYC and AML transaction monitoring tools, processes, and systems to comply with regulations

Network, Physical, and Cyber Security: Stringent security to protect the custodian from physical, network and cyber attacks

Policies procedures and systems to adhere to regulations, internal policies and client contracts and the technology for the Data Center storage

Technology of the highest security and authenticity standards and non-disclosure throughout the lifecycle of a transaction, including key management, authentication methods, asset management, etc.

Further reinforced by below certifications: SOC 2 Type 1/2, ISO27001, ISO 27017, NIST lvl 3/4, NIST 800 - 53/57, ENISA

<u>Digital asset governance model</u>: multi-level controls are used to comply with the regulations and secure the custodial operations

BLOCKZERO

Source: BlockZero analysis (2023)

Final thoughts

Final thoughts

Custody is a **critical component of the current and future financial infrastructure** - digital or otherwise. Individuals and organizations will be faced with the choice of custody. Since the choice of custody type will need to be made, it becomes necessary for individuals as well as organizations or institutional investors to fully understand the different options available to them.

In order to make conscious and thoughtful choices, they will also need to **understand the regulatory requirements** in their region, their needs, their risk tolerance and the options available to them based on their various criteria.

Making conscious choices about the custody of digital assets will allow investors to better protect their assets, and could be **a key factor in introducing institutional investors to the digital asset market.**

49%

of institutional firms that purchase investment securities self custody some digital assets [1]

62%

of institutional firms that purchase investment securities say it is important for a custodian to be regulated [1]

Source: BlockZero analysis (2023); 1) Coalition Greenwich - Providing Digital Asset Services: An Institutional Infrastructure Roadmap (November 2022)

BLOCKZERO

Marie-Chantal Leduc

Director, BlockZero

mcleduc@blockzero.ca

Sabrina McNeil

Senior Consultant, BlockZero

sabrina.mcneil@blockzero.ca

Kasyap Anand

Senior Consultant, BlockZero

kasyap.anand@blockzero.ca

Address: Montreal, Quebec, Canada

LinkedIn: https://www.linkedin.com/company/b0

Website: https://www.blockzero.ca/

BlockZero Advisors is a boutique consulting firm specializing in digital assets & blockchain. We support companies and organizations in the public and para-public sector through their digital transformation.

Our mandates with players in the Canadian and international ecosystems allow us to have an up-to-date perspective on the evolution of the market, the value chain and the ecosystem of cryptocurrencies and digital assets, as well as the issues and risks specific to them and the regulatory environment that is evolving daily. In addition, strategic coaching for some of our clients leads us to work closely with Canadian regulators. In addition, our daily technology watch and market intelligence service ensures that we stay on top of the latest developments in the field.