



crypto.com

Safeguarding Your Crypto Assets

An Overview of Custody Solutions for
Institutions and Individuals

April 2022

Research and Insights



Research Analyst
Alan Lee



Head of Research and Insights
Henry Hon PhD, CFA

Research Intern
Bowen Liu

RESEARCH DISCLAIMER

The information in this report is provided as general commentary by [Crypto.com](https://crypto.com) and its affiliates, and does not constitute any financial, investment, legal, tax, or any other advice. This report is not intended to offer or recommend any access to products and/or services. The views expressed herein are based solely on information available publicly, internal data, or information from other reliable sources believed to be true.

While we endeavour to publish and maintain accurate information, we do not guarantee the accuracy, completeness, or usefulness of any information in this report nor do we adopt nor endorse, nor are we responsible for, the accuracy or reliability of any information submitted by other parties. This report includes projections, forecasts, and other predictive statements that represent [Crypto.com](https://crypto.com)'s assumptions and expectations in light of currently available information. Such projections and forecasts are made based on industry trends, circumstances, and factors involving risks, variables, and uncertainties. Opinions expressed herein are our current opinions as of the date appearing in this report only.

No representations or warranties have been made to the recipients as to the accuracy or completeness of the information, statements, opinions, or matters (express or implied) arising out of, contained in, or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) that may arise from any person acting on any information and opinions contained in this report or any information made available in connection with any further enquiries, notwithstanding any negligence, default, or lack of care, is disclaimed.

This report is not meant for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of [Crypto.com](https://crypto.com) in any form is prohibited except with the written permission of [Crypto.com](https://crypto.com). This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of, or located in a jurisdiction, where such distribution or use would be contrary to applicable law or that would subject [Crypto.com](https://crypto.com) and/or its affiliates to any registration or licensing requirement.

The brands and the logos appearing in this report are registered trademarks of their respective owners.

Contents

| | |
|---|-----------|
| Executive Summary | 4 |
| 1. Introduction | 6 |
| 1.1 Overview | 6 |
| 1.2 Motivations | 7 |
| 1.3 Genre | 8 |
| 1.3.1 Self-Custody Solutions | 8 |
| 1.3.2 Hosted Solutions | 9 |
| 1.4 Potential Challenges & Risks | 10 |
| 2. Institutional Custody Solutions | 12 |
| 2.1 High-Level Comparisons | 12 |
| 2.2 Selected Big Players | 13 |
| 2.2.1 BitGo | 13 |
| 2.2.2 MetaMask Institutional | 14 |
| 2.2.3 Fidelity | 15 |
| 2.2.4 Coinbase Custody | 16 |
| 2.2.5 Fireblocks | 16 |
| 2.3 Fundraising Rounds | 17 |
| 3. Self-Custody Solutions | 20 |
| 3.1 Security Features | 20 |
| 3.2 Hot Storage Wallets | 21 |
| 3.2.1 Types of Hot Storage | 21 |
| 3.2.2 Hot Wallet Basics | 22 |
| 3.3 Cold Storage Wallets | 23 |
| 3.3.1 Types of Cold Storage | 24 |
| 3.3.2 Cold Wallet Basics | 25 |
| 3.4 Multi-Signature Wallets | 26 |
| 3.5 Smart Contract Wallets | 27 |
| 4. Outlook and Conclusions | 29 |
| References | 30 |

Executive Summary

According to the statistics on [Crypto.com](https://crypto.com), **the overall market capitalisation of the crypto industry has surpassed US\$2 trillion as of April 2022**. Naturally, with the growing nominal value of digital assets, the crypto industry is focussed on much-needed custody solutions that can store and protect the assets in a secure manner. Asset managers turning to custody solutions are motivated by criterias such as **security assurance, operational efficiency, and regulatory requirements**.

In terms of the role of management, crypto custody solutions can be briefly classified into two categories:

- **Self-custody (individual custody) solutions** — these allow individuals to manage their own digital assets personally, including hot wallets (e.g., desktop and mobile wallets), cold wallets (e.g., paper and hardware wallets), multi-signature wallets, and smart contract wallets.
- **Institutional custody solutions** — institutional custody solutions like centralised exchanges, digital asset managers, and custodial banks take the responsibility of securing and managing investors' digital assets.

In this report, we provide an introduction to institutional and self-custody solutions in the crypto market.

For institutional custody solutions:

- We outline the highlighted features of five representatives — BitGo, MetaMask Institutional, Fidelity, Coinbase Custody, and Fireblocks.
- A comprehensive summary is presented to indicate the funding rounds for some of the largest players in the institutional space.

For self-custody solutions:

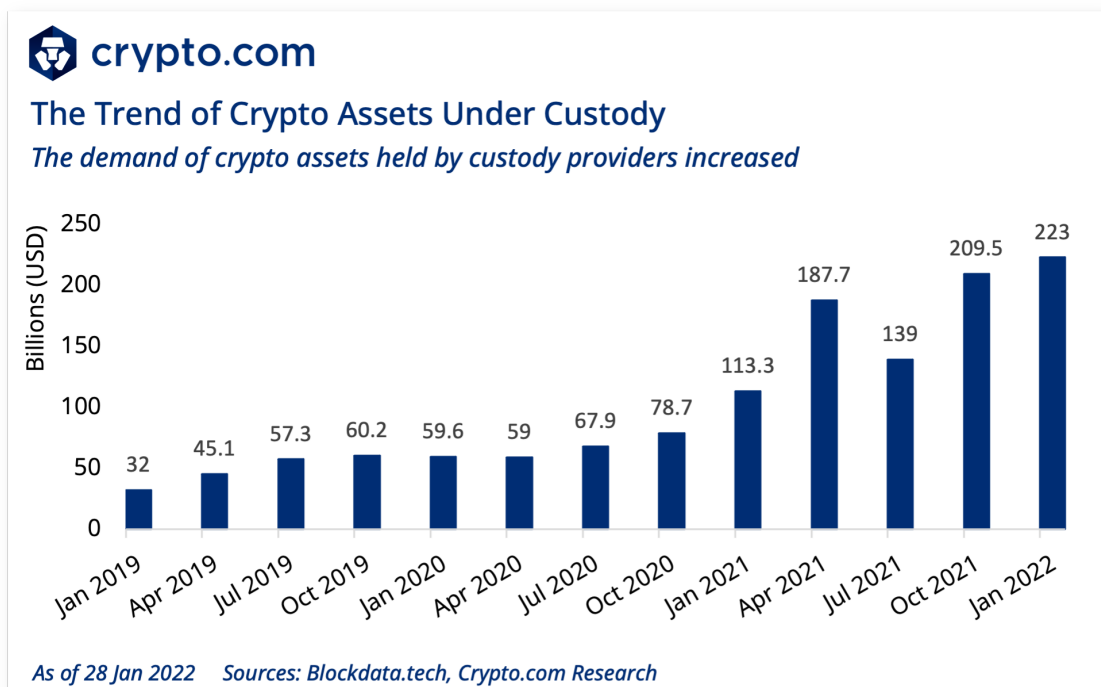
- We outline the various types of digital asset storage solutions for individuals — hot wallets, cold wallets, multi-signature (multisig) wallets, and smart contract wallets.
- A retail-point-of-view comparison is provided for hardware wallets, diving into some common details, before showing how to create a multisig wallet, and finally using a smart contract wallet.

1. Introduction

1.1 Overview

Inspired by Bitcoin and its innovative initiative, a number of blockchain-based digital assets have established a foothold in the global financial mindspace, attracting much attention and visibility in the community. According to the statistics on [Crypto.com](https://crypto.com), **the overall market cap of the crypto industry has surpassed US\$2T as of April 2022**. Intuitively, as cryptocurrency prices rise and the crypto communities seek higher security, the custody solutions able to protect digital assets securely are emerging.

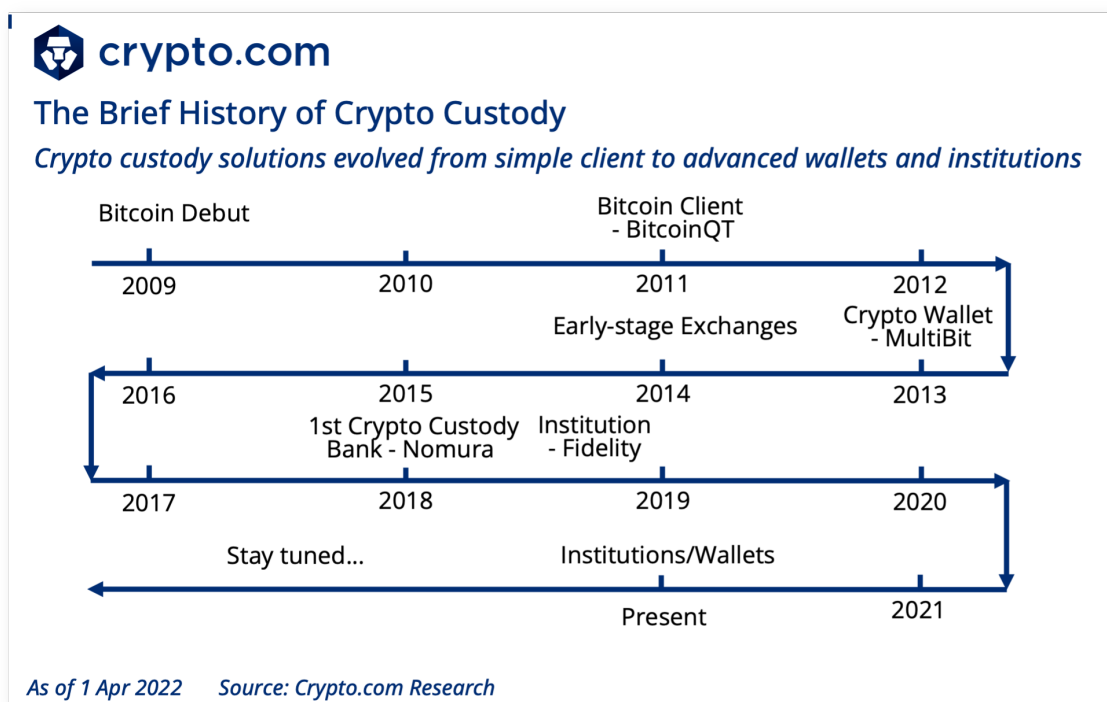
Technically speaking, cryptocurrency custody solutions are [independent storage and security systems](#) used to hold large quantities of tokens. Their essential objectives are twofold. On one hand, by leveraging and devising some advanced approaches, custody platforms may keep their customers' crypto assets in a secure place, preventing various attack vectors. On the other hand, with more assets being held, these custody providers can make profits from additions like [custody fees, setup fees, or withdrawal fees](#). As the chart below shows, **the amount of crypto assets under custody was over US\$220B in January 2022, constituting about 10% of total crypto market capitalization.**



Custody solutions have been adopted in traditional finance for quite a long time. However, these solutions don't [have a long history](#) yet in the crypto industry. Bitcoin was proposed in [January 2009](#), and this emergence led to the primary attempts to safeguard keys and coins. In November 2011, the native Bitcoin client (e.g., [Bitcoin-QT](#)) was released for regular payment. Since then, many legacy crypto wallets have been presented, such as [MultiBit](#).

At the same time, third-party custody solutions emerged, and several early-stage exchanges suffered from infamous hacks, including the [Mt. Gox hack](#) and [Bitfinex hack](#).

Institutional investors and various firms also entered into the custody market during this time, as attention on cryptocurrencies increased. [Nomura](#) became the first crypto custody bank in May 2018; and Fidelity, a leading financial institution, [made it possible](#) to handle custody for cryptocurrencies in October 2018. Nowadays, other main players include [Coinbase Custody](#), [BitGo](#), and well-known wallets, such as [MetaMask](#).



1.2 Motivations

As the crypto market continues growing, the role of custodians is becoming more important than ever. Theoretically, users can access their assets with the [private key](#) of their wallet. However, this key string is too difficult to remember in a feasible way. The main objectives of demanding custody solutions are:

1. **Security Assurance** — Safeguarding users' crypto assets is regarded as a first priority for designing a custody solution. Keeping credentials (e.g., private keys) offline seems promising, but the potential of lost keys could prove disastrous. Online situations are even more risky. In 2021, a report by Chainalysis [illustrated](#) that **approximately 20% of all existing Bitcoins**, worth US\$205.8B as of December 2021, appear to be in lost wallets. Similarly, as of 1 Apr 2022, **49 exchanges have suffered major hacks**, resulting in over [US\\$2.5B in financial loss](#). As a result, crypto communities demand crafted and security-guaranteed custody solutions to protect their cryptocurrencies.
2. **Operational Efficiency** — According to [a report](#) by Deloitte, storing assets with a custodian can be significantly easier than taking care of one's own assets. If investors hold assets privately, they would become inaccessible in the case of loss from hacking or other events. Licensed custodians provide a level of certainty of value through recourse in the event of failure at that custodian; they are also more likely to have access to trusted insurers, helping to provide investors with greater comfort. For example, [Crypto.com](#) has expanded its total insurance coverage to [US\\$750M](#), which can secure its cold storage assets on Ledger Vault.
3. **Regulatory Requirements** — The regulation requirements in certain countries are another major concern. For instance, according to SEC regulation promulgated as part of the [Dodd-Frank Act](#), institutional investors (e.g., banks, savings associations, and registered broker-dealers) with customer assets worth [more than US\\$150K](#) are required to store the holdings with a 'qualified custodian'.

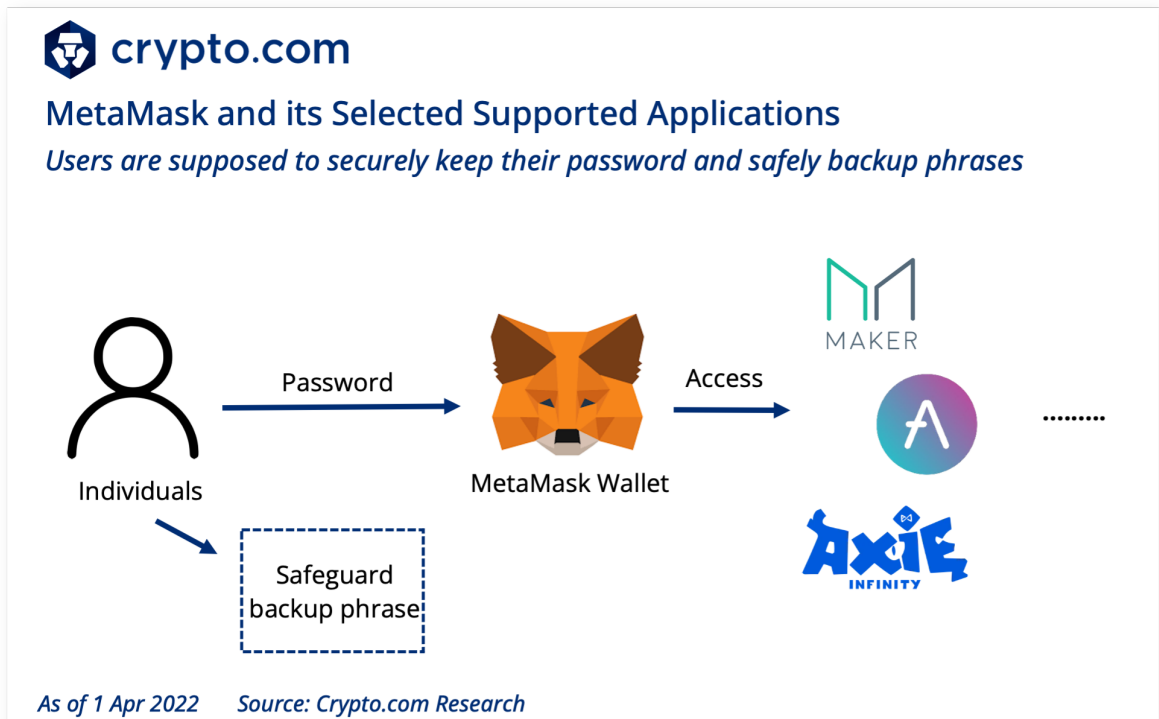
1.3 Genre

In traditional banking, [all custodians are financial institutions, as required by law](#). In contrast, crypto holders have the opportunity to manage their own digital assets. In terms of the role of management, crypto custody solutions can be categorised into two partitions: self-custody and institutional custody.

1.3.1 Self-Custody Solutions

As the name suggests, self-custody solutions allow for anyone to manage their own digital assets personally. With this type of custody, individuals are supposed to remember or securely safeguard their private key, which is proof of their ownership of digital assets. More important, the private key is what allows individuals to spend their money. Popular wallets that are effective in helping

investors to self-manage their tokens include hot wallets (e.g., web, desktop, and mobile wallets) and cold wallets (e.g., paper and hardware wallets).




As shown above, MetaMask is a popular web wallet that can support [Ethereum Virtual Machine \(EVM\)-based networks](#). Users are required to safely keep a password and backup phrases to manage their crypto assets.

1.3.2 Hosted Solutions

In contrast, practical users also outsource the responsibility of securing and managing their digital assets to a third-party custody provider, known as hosted solutions (or institutional solutions). Users can transfer their holdings to an institutional custody company, much like in the workflows of traditional banks. For instance, they can input their access credentials by logging in, similar to typing a password to access their bank account.

There are three different kinds of institutional crypto custodians, as outlined in [a report](#) by Coindesk. **Firstly**, some centralised crypto exchange platforms have made extra efforts to protect their customers' holdings, usually outsourcing their security needs to an external custody provider that safeguards the assets under management. For instance, [Crypto.com](#) partnered with [Ledger Vault](#) in 2020 as a new payment option. **Secondly**, there are a number of regulated and licensed custody providers dedicated to offering crypto custody, including [Anchorage](#), [NYDIG](#), and [Paxos](#). **Thirdly**, numerous traditional custodial banks (e.g., [Fidelity](#),

BNY Mellon, etc.) have entered the crypto custody industry. A prominent example is when [BitGo](#) acquired [Kingdom Trust](#) (a Kentucky-based custodian) in 2018, becoming a well-known custody provider for cryptocurrencies.



crypto.com

The Category of Institutional Custody Solutions
Institutional custody solutions basically include three main types.

| Exchanges | Custody Providers | Custodial Banks |
|---|---|---|
|  |  |  |
| |  |  |

As of 1 Apr 2022 Sources: Coindesk, Crypto.com Research

1.4 Potential Challenges & Risks

Although the primary goal in custody systems is to secure their clients' assets, no practical design can claim to be 100% secure. Apart from security challenges, the existing custody approaches suffer the potential for unforeseen regulatory action on cryptocurrencies in some countries.

- 1. Security Challenges** — Intuitively, storing credentials offline creates a smaller attack surface (as the wallet cannot be hacked unless the attacker can access the keys physically); but losing the private key means a user's total holdings will be inaccessible. On the other hand, hot storage options may be vulnerable to certain attack vectors. Many exploitations have occurred on both hosted wallets and exchanges. For instance, hackers managed to obtain the keys to some wallets on KuCoin, stealing [over US\\$275M](#) worth of tokens in 2020. Those who wish to learn more about previous hacks are encouraged to view a more exhaustive list of incidents [here](#).
- 2. Regulatory Challenges** — Traditional custodians are highly regulated institutions, but public crypto markets are not regulated in most countries.

The lack of clarity in terms of regulatory categorisation of crypto assets and potential for unforeseen regulatory action towards cryptocurrencies [presents a challenge for custodians](#) looking to develop an offering in this market.

In the following chapter, we introduce selected institutional custody providers, giving insight on the regulatory landscape amongst different countries.

2. Institutional Custody Solutions

It is extremely important for institutions to store their digital assets in a secure and regulated way, which is where dedicated companies who specialise in crypto custody come into play.

Generally speaking, these institutional custodians help their clients manage assets, making it easier for beginners. Moreover, due to the large amount of assets under custody, these providers usually insure assets they manage. With respect to shortcomings, they are considered to be centralised services or entities, and hence have the potential to lock crypto assets and limit withdrawals. In the worst case, a custody provider can be hacked or go bankrupt.

In this chapter, we first provide a high-level feature comparison amongst selected players; then we introduce those platforms in detail.

2.1 High-Level Comparisons

As shown in the table below, we select [BitGo](#) (which acquired Kingdom Trust with large assets under custody), [Fidelity](#) (a traditional custodian bank that entered into the crypto market), [MetaMask](#) (which recently released its institutional version), [Coinbase Custody](#), and [Fireblocks](#) in our comparisons. The metrics include the launch dates, assets under custody (AUC), insurance guarantee, regulated property, clients, and custody partnerships.

| Metric | BitGo | Fidelity | MetaMask | Coinbase | Fireblocks |
|-----------|----------|--------------|----------|-------------------|--------------------------|
| Debut | 2013 | 2019 | 2021 | 2012 | 2018 |
| AUC* | US\$64B | - | - | US\$90B | US\$38B |
| Insurance | US\$700M | Not released | - | US\$320M | US\$42.5M |
| Regulated | Yes | Yes | Yes | Yes | Yes |
| Clients | Bitstamp | Nexo | AAVE | Polychain Capital | JST Capital, Prime Trust |

Custody Partners – Fidelity Investment – BitGo, Cactus, Qredo –

* AUC denotes Assets Under Custody;

As of 10 Apr 2022 Sources: blockdata.tech, [UIAM Labs](https://uiam.labs)

2.2 Selected Big Players

In this section, we introduce five players, ranging from exchanges and wallets to traditional custody banks and dedicated custody providers.

2.2.1 BitGo

BitGo is one of the leading custody service providers in digital assets, providing institutional investors with liquidity, custody, and security solutions. Launched in 2013, BitGo has served [over 500 clients](#), among which are exchanges like [Bitstamp](#) and [Nexo](#). In 2018, it [acquired Kingdom Trust](#) and established BitGo Trust, the [first qualified custodian](#) purpose-built for storing digital assets. BitGo supports custody for over 400 coins and tokens; it spans more than 50 countries, and its customers include exchanges and institutional investors. BitGo is backed by [Goldman Sachs](#), [Craft Ventures](#), [Digital Currency Group](#), [DRW](#), [Galaxy Digital Ventures](#), [Redpoint Ventures](#), and [Valor Equity Partners](#).

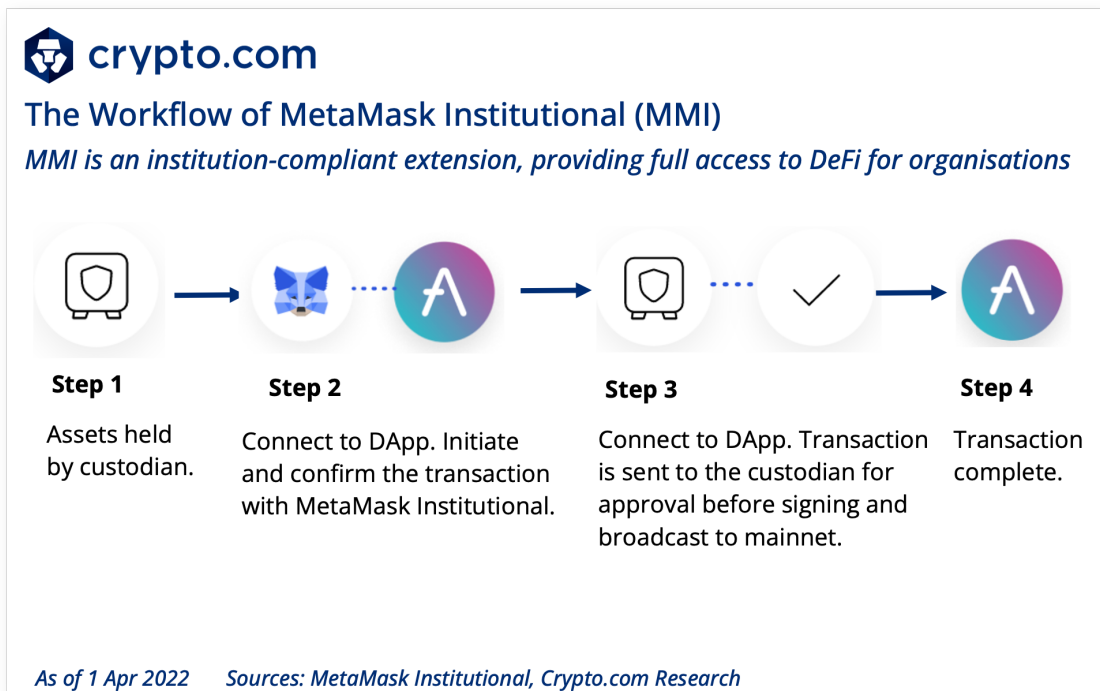
In the event of theft or loss of private keys, insider theft, or dishonest acts by BitGo employees or executives, the [US\\$100M policy](#) covers digital assets where the private keys are held by BitGo. In addition, as of May 2021, over US\$600M excess insurance has been put in place for specific BitGo clients.



2.2.2 MetaMask Institutional

Institutional investors may sometimes struggle to allocate their capital to the DeFi market due to the [heightened security, operational, and compliance requirements](#) involved in doing so. MetaMask Institutional (MMI) is an institution-compliant extension of the traditional MetaMask wallet, providing full access to DeFi without compromising on institution-required security and compliance requirements.

The workflow of MetaMask Institutional is depicted below. Custody plays a fundamental role for organisations seeking to access crypto and DeFi, and MetaMask’s services range from institution-compliant key storage and interaction with exchanges to multi-signature transaction approval and signing. These considerations are paramount to organisations safely acquiring and holding crypto assets. MetaMask Institutional [partnered with](#) multiple custodians (i.e., [BitGo](#), [Cactus Custody](#), and [Qredo](#)) in 2021 so their clients could choose from a wide variety of solutions that meet all variations of institutional-grade custody requirements.

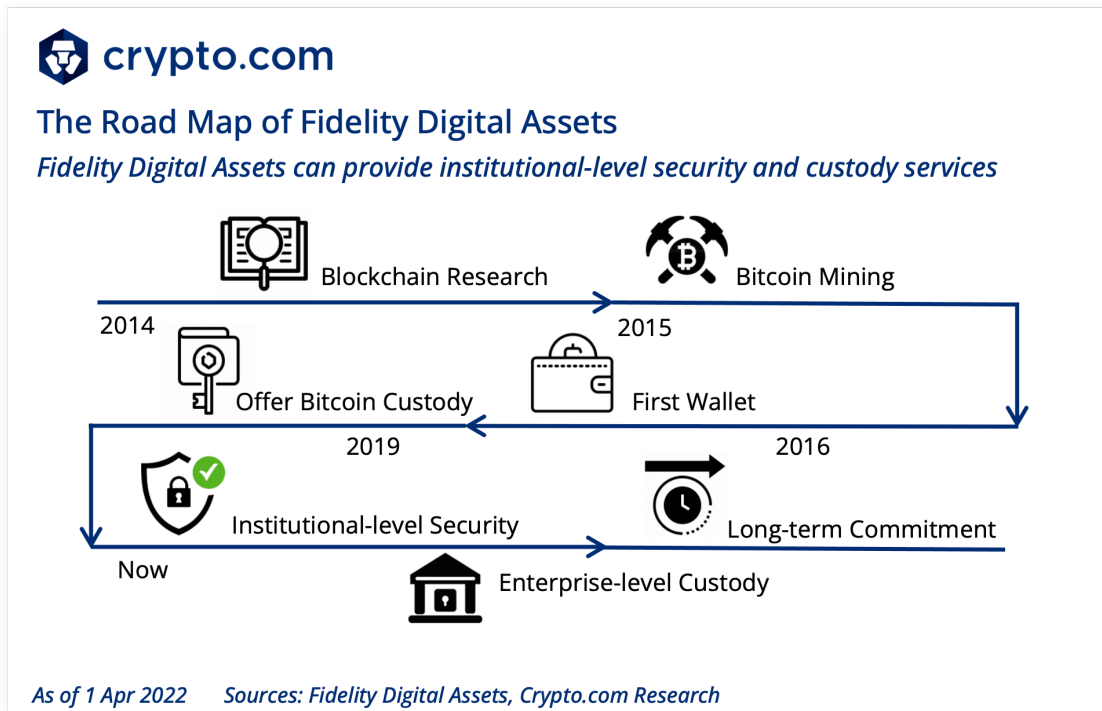


Like the traditional MetaMask wallet, **MetaMask Institutional provides access to all EVM-compatible chains.**

2.2.3 Fidelity

Established in 1946, Fidelity is a Boston-based multinational financial services corporation and one of the largest asset managers in the world, with [US\\$4.5T in assets under management](#) as of December 2021.

Fidelity's early exploration of blockchain and digital assets resulted in the establishment of [Fidelity Digital Assets](#). In 2014, the team began research and development efforts in blockchain technology. In 2015, the firm started mining Bitcoin, and tested its first wallet and storage solution with employees in 2016. Fidelity Digital Assets [began offering bitcoin custody services](#) in March 2019, and now **it can provide institutional-grade security, enterprise-level custody services, and long-term commitment to this ecosystem.**



2.2.4 Coinbase Custody

Coinbase Custody operates as [a standalone, independently capitalised business](#), separate from Coinbase. All digital assets are segregated and held in trust for the benefit of their clients. As of January 2022, it has attracted [US\\$90B](#) in digital assets to keep under its storage. Coinbase Custody has completed both the [SOC 1 type II and SOC 2 type II audits](#) and offered insurance of up to [US\\$320M \(per-incident and over all\)](#). Apart from the insurance policies in the event of a loss, Coinbase Custody also offers [a segregated cold storage ecosystem](#) with accessibility through dedicated on-chain addresses.

2.2.5 Fireblocks

Fireblocks provides enterprise-grade infrastructure for handling digital assets. [Enabling the secure transfer of crypto assets, it caters to exchanges, neo-banks, trading desks, and hedge funds](#). To date, Fireblocks has a combined total of [US\\$38B assets under custody](#), and claims to have processed [over US\\$1T in transactions](#).

In terms of performance, Fireblocks achieves an [8x faster transaction signing speed](#) by a dedicated [MPC-CMP algorithm](#), and enables up to [90% reductions in transaction fees](#). This means that customers can send and receive transactions at scale without the massive operating costs of legacy multisig solutions.

Apart from performance, security is another highlight in Fireblocks, which provides three considerations in securing clients' assets.

1. Private keys are never concentrated on a single device at any point in time. Instead, they are maintained by multi-party computation (MPC) with the proposed [MPC-CMP private key protection algorithm](#). With MPC, the private key is broken up into shares, encrypted, and divided amongst multiple parties, eliminating the risk of a single point of compromise from both external hackers and insiders.
2. With respect to storage, keys stored in SGX cannot be extracted even if malware or a hacker has control over the server's operating system. SGX is short for [Intel SGX](#), which is a secure area of a main processor that guarantees the confidentiality and integrity of code and data loaded inside to be protected. This technique is widely adopted in cryptographic applications (e.g., [Avalanche](#)) to secure the execution environment of a platform.
3. Fireblocks further devised a policy engine that enables organisations to set up specific approval policies for every transaction. The policy engine allows users to configure a list of rules that affect how transactions are handled and approved.

2.3 Fundraising Rounds

A growing demand for digital asset custody paves the way for an influx of Venture Capital money. In the table below, we take a look at the funding rounds for some of the largest players in the institutional space.

Most recent, Blockchain.com had a funding round, bringing its valuation to US\$14B, just second to the publicly listed Coinbase. Fireblocks also had a fundraiser recently, bringing its total valuation to US\$8B. As depicted in the 'Asset under Custody' column in our chart, the latest funding rounds correlate to the growing trend and demand for institutional-grade digital asset custody solutions.

| Companies | Asset Under Custody US\$ Mln | Total Funding US\$ Mln | Latest Valuation US\$ Mln | Latest Funding Amount US\$ Mln | Latest Funding Round | Latest Funding Date | Country |
|-------------------|------------------------------|------------------------|---------------------------|--------------------------------|---------------------------|---------------------|----------------|
| Coinbase | 90,000 | 538.67 | 65,325 | - | <u>Unattributed VC</u> | 1/10/2020 | United States |
| Blockchain.com | - | 490.5 | 14,000 | - | <u>Series D</u> | 31/3/2022 | United Kingdom |
| Fireblocks | 38,000 | 1,039 | 8,000 | 550 | <u>Series E</u> | 27/1/2022 | United States |
| Gemini | 30,000 | 400 | 7,100 | 400 | <u>Series A</u> | 19/11/2021 | United States |
| NYDIG | 6,000 | 1,355 | 7,000 | 1,000 | <u>Growth Equity - IV</u> | 14/12/2021 | United States |
| ConsenSys | - | 732.5 | 7,000 | 450 | <u>Series D</u> | 11/3/2022 | United States |
| BlockFi | - | 512.75 | 3,000 | 350 | <u>Series D</u> | 11/3/2021 | United States |
| Anchorage Digital | - | 487 | 3,000 | 350 | <u>Series D</u> | 15/12/2021 | United States |
| Paxos | <u>1,400*</u> | 535.25 | 2,400 | - | <u>Corporate Minority</u> | 20/1/2022 | United States |

| Companies | Asset Under Custody US\$ Mln | Total Funding US\$ Mln | Latest Valuation US\$ Mln | Latest Funding Amount US\$ Mln | Latest Funding Round | Latest Funding Date | Country |
|---------------|------------------------------|------------------------|---------------------------|--------------------------------|------------------------------|---------------------|---------------|
| Bakkt | - | 482.5 | 2,100 | 300 | Series B | 13/3/2020 | United States |
| Ledger | >10,000 | 466.38 | 1,500 | 380 | Series C | 10/6/2021 | France |
| BitGo | 64,000 | 85.72 | 1,200 | 0.22 | Unattributed | 17/7/2019 | United States |

Assets under Custody data from [Blockdata.tech 2021 Crypto Custody](#). *unless hyperlink specified.
As of 7 Apr 2022 Sources: [CB Insights](#), [Blockdata.tech](#), [Crypto.com Research](#)

In closing this chapter, we observe that value stored in institutional custody is on the rise. It comes as no surprise that venture capital continues flowing into this space as the asset management industry continues evolving and diversifying across various asset classes. Having discussed solutions for the institutions, we venture into self-custody solutions for the masses.

3. Self-Custody Solutions

The demand from institutions for secure and regulated storage for digital assets also applies equally to everyday retail investors. However, retail investors may not have the same level of understanding to require institutional-equivalent standards.

Self-custody solutions are presented to users in the form of a Web3 interface — logging in or scanning QR codes — or in a physical device like a thumb drive; although, it is possible for individuals to hold wallets, which require multiple signatories as a standard for institutional custodians. In this chapter, we provide an overview of the different types of custody solutions made available to individuals. We begin with the security features in self-custody solutions.

3.1 Security Features

When a [hot storage wallet](#) is first created or a [cold storage](#) physical wallet is purchased, they come with [secret recovery phrases, public keys, and private keys](#). Seed phrases may be in the form of 12 or 24 words.

[What are secret recovery phrases?](#) Private seed phrases are secret recovery phrases where words are selected from a list with a high level of randomness. Each of these words correspond to a series of numbers, and when placed together they form the private key to a user's account(s). MetaMask wallets, for example, use a 12-word secret recovery phrase, while other wallets use 24 -words. The recovery phrase is the key to a user's wallet. If anyone has another's recovery phrase, they also have complete access to the other's entire wallet. Note that one wallet can consist of multiple addresses spanning across multiple blockchain networks.

[What are Public Keys?](#) Public keys allow users to receive cryptocurrency transactions. To access the received cryptocurrencies, the public keys have to be paired with a private key to prove ownership. Wallet addresses are usually a shortened version of public keys.

[What are Private Keys?](#) As mentioned earlier, secret recovery phrases or private seed phrases provide users access to their wallet, which can contain multiple accounts. The difference between a private key and the secret recovery phrase is like the difference between a master key to enter a house (recovery phrase) and a private key to access only one room within a house.

Private keys exist in these formats:

- a 256-character long binary code

- a 64-digit hexadecimal code
- QR code

Here's how both public and private keys are used:

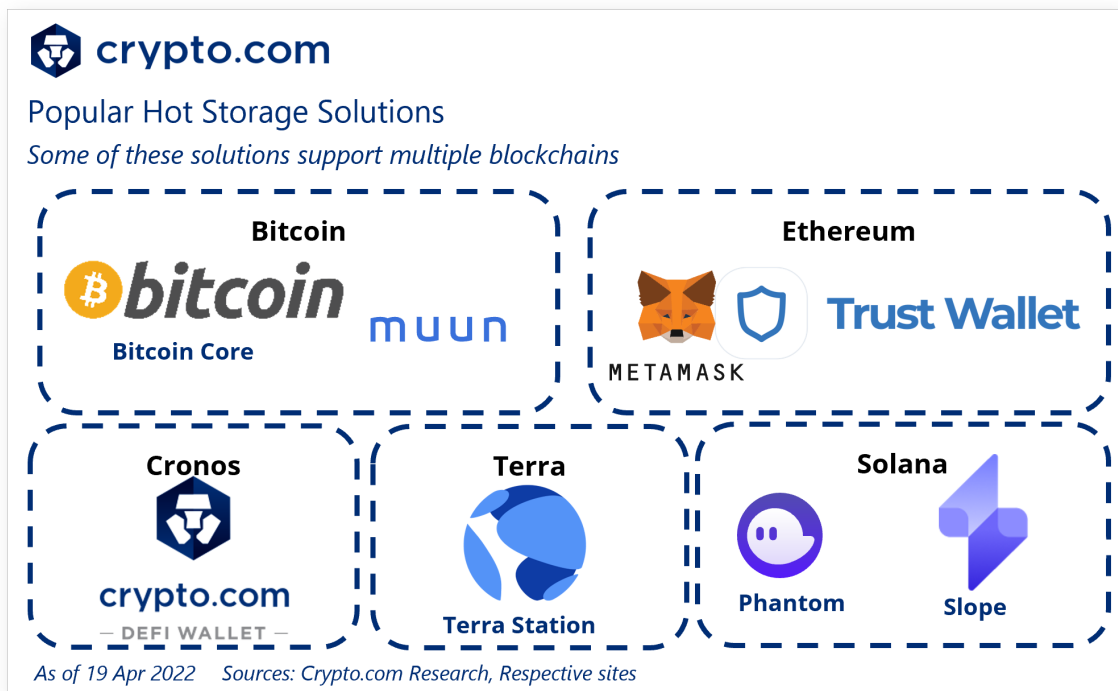
1. Alice holds a key pair (public key, private key)
2. Alice signs whatever she wants to generate a signature for the transaction
3. The signature can be verified by anybody (using Alice's publicly visible public key); in Ethereum, the signature adopts an optimised traditional [ECDSA signature scheme](#)

3.2 Hot Storage Wallets

Wallets connected to the Internet are also commonly known as 'Hot Wallets'. Hot wallets can be split into custodial and non-custodial versions. As discussed earlier, crypto wallets usually come with both a public and private key, with the exception of exchange wallets, where the private keys are held with the exchange. A custodial wallet does not provide the private keys, whereas a self-hosted (non-custodial) wallet does.

3.2.1 Types of Hot Storage

There are many different types of hot wallets, each catering to different blockchain networks, some with more functions than others. Types of functions include showcasing Non-fungible Tokens (NFTs) held in a user's wallet, instantaneously [swapping tokens](#), [staking](#), or [delegating native tokens to stake](#). Below are some popular hot wallets used by the larger blockchains:



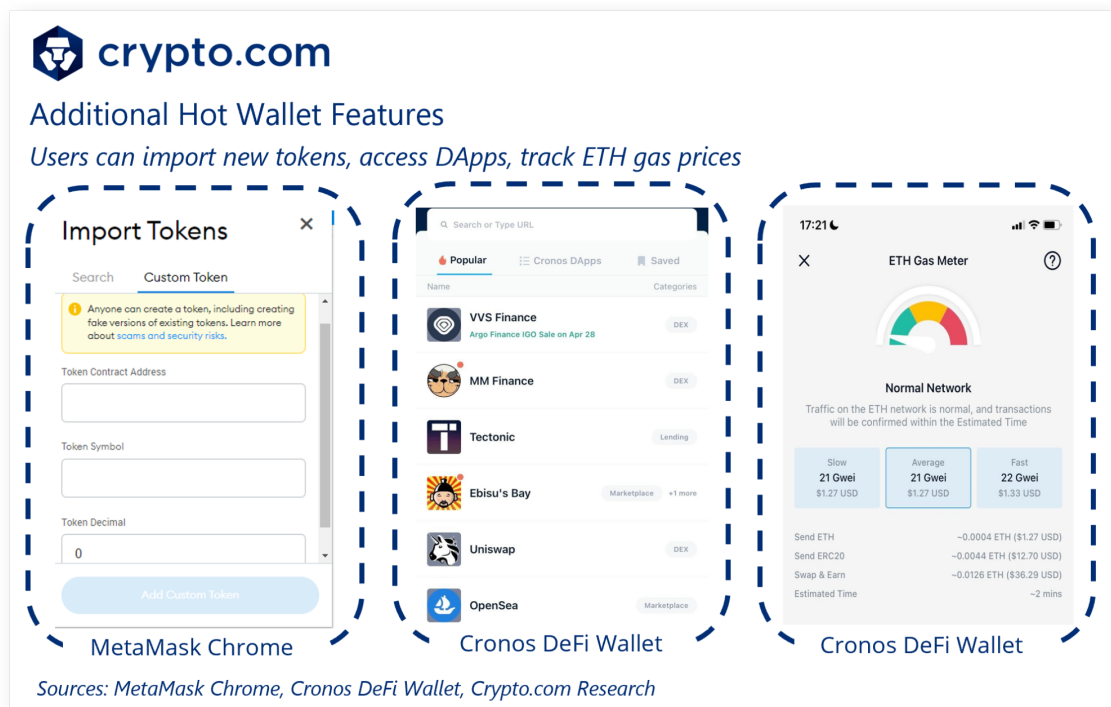
Wallets such as MetaMask for individuals and Trust Wallet support multiple blockchains. [A report in August 2021](#) by ConsenSys stated that MetaMask surpassed 10 million monthly active users (MAU). MetaMask's high active user count comes as no surprise, with the ease of its navigation and accessibility on both browser and mobile.

3.2.2 Hot Wallet Basics

Hot wallets can be installed on web browsers and personal smartphones, and in certain operating systems, some mobile versions may come with facial recognition, which serves as an additional layer of security. This makes hot wallets a popular choice for retail to access Web3 applications. In this chapter, we use MetaMask to demonstrate some of the features currently available in Web3 wallets.

Hot wallets generally come with these features:

- Buy tokens
- Send tokens
- Swap tokens
- Track historical activity/transactions
- View account on blockchain



3.3 Cold Storage Wallets

Cold storage wallets tend to be relatively less popular compared to hot wallet solutions, which provide ease of access to Web3 interfaces and decentralised applications (DApps). Unlike hot wallets, cold wallets tend mostly to be offline, with minimal to limited access to the Internet. Cold wallets vary in form — paper wallets, USB sticks, even in the shape of a [metal coin containing bitcoin stored value](#). In this chapter, we look at the various types of cold wallets and how they differ from hot wallets.

Cold wallets, like hardware wallets, tend to be hack-resistant. This is because the signing of transactions is done locally on the device, then subsequently broadcast to the network via the Internet. Being secure is not without its downsides, though, as hardware wallets usually come at a higher price compared to hot wallets, which tend to be free. For serious investors or crypto-natives, paying to secure their digital assets probably costs a fraction of their total portfolio value, and it assures users that their digital assets are kept safely.

3.3.1 Types of Cold Storage

In this segment, we look at the main players in the cold storage space — Trezor and Ledger wallets. Below is a comparison table of common specifications for the two popular hardware wallets.

| Specs | Trezor | | Ledger | |
|----------------------------|------------|--------------------|-------------------------|-------------------------|
| Product | One | Model T | Nano S | Nano X |
| Tokens Supported | 1,000+ | 1,000+ | 5,500+ | 5,500+ |
| Recovery Phrase | 24 words | 12 words | 24 words | 24 words |
| Bluetooth | N | N | N | Y |
| Display Type | Monochrome | Colour Touchscreen | Greyscale with 128 x 64 | Greyscale with 128 x 64 |
| Battery | - | - | - | 8 hrs. Standby |
| Amazon Stars | 4.5 | 4.6 | 4.5 | 4.6 |
| Amazon Rating Count | 5,472 | 1,971 | 15,765 | 4,697 |
| Price (US\$) | 85 | 170 | 59 | 149 |

As of 20 Apr 2022 Sources: [Trezor.io](https://trezor.io), [Ledger.com](https://www.ledger.com), [Amazon.com](https://www.amazon.com), Crypto.com Research

After reviewing the four different options across both brands, the Ledger Nano S seems to be the relatively popular option, with over 15,000 reviews. This may be due to the more affordable price range of the Nano S, which also meets the basic feature requirements of consumers.

3.3.2 Cold Wallet Basics

Apart from their offline and hack-resistant features, cold wallets tend to function similarly to hot wallets — like with the use of seed phrases, public and private keys, etc. The feature of signing and holding private keys locally on a device (as opposed to signing on the Chrome extension or software on the user’s computer) is the differentiator.

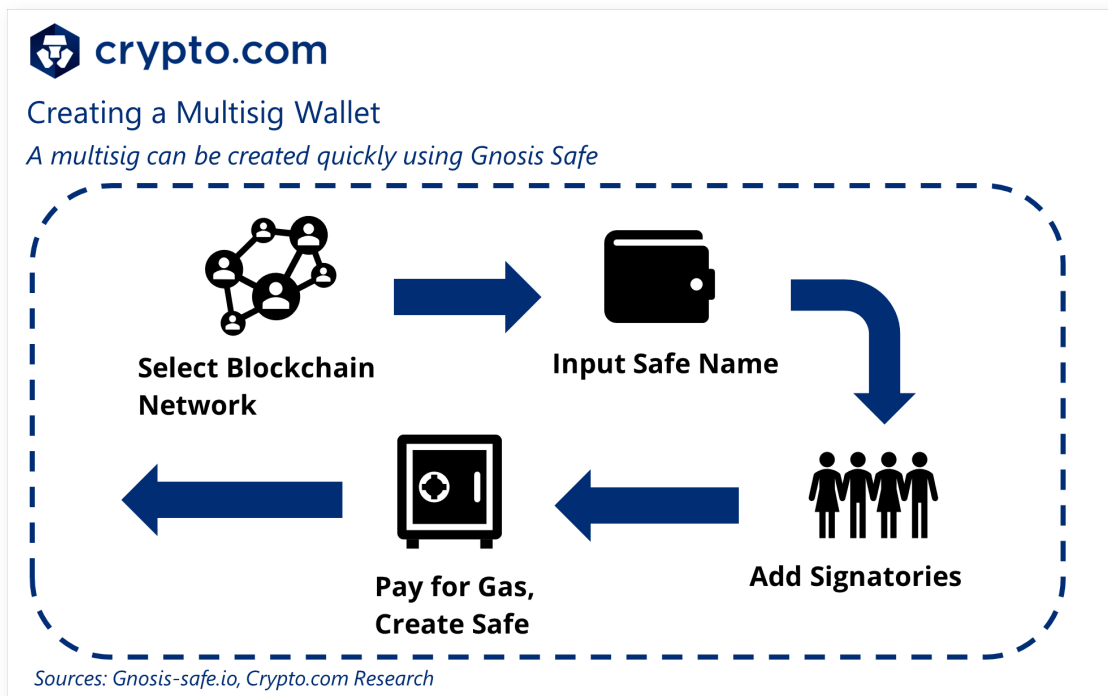
It is also important to note that hardware wallets have to connect to the Internet either by browser or mobile applications, or by desktop software. Both Trezor hardware wallets use the [Trezor suite via desktop or Android browsers](#). At the time of writing, Trezor does not provide a mobile application for its hardware wallets. In contrast, Ledger provides software for its hardware wallets, called [Ledger Live](#). While the [Trezor suite software provides basic functionality and swapping of tokens](#), Ledger Live allows users to buy, swap, exchange, and even stake tokens that run on the Proof-of-Stake mechanism. Ledger Live also allows users to [connect their hardware wallet to decentralised applications \(DApps\)](#) like [Uniswap](#) and many more. More recent, Ledger seems to have added an [NFT feature](#) for users.

3.4 Multi-Signature Wallets

[Multi-signature](#) (multisig) wallets are digital wallets that operate with multiple signatures. In a nutshell, this means the multisig wallet requires more than one private key to sign and authorise a transaction.

By requiring more than one private key, the [key person risk](#) is eliminated. For wallets with greater asset value, the multisig feature serves as an additional layer of security, reducing key person risk. Generally, the multisig wallet uses an m-of-n signatories approach, requiring a minimum number (m) of signatories (could be two signatories or more) against the total number (n) of signatories registered for the multisig wallet.

Gnosis Safe is an example of a multisig wallet. Upon accessing its website, one can [follow the workflow \(see below\)](#) to create a multisig safe in order to store digital assets. During the creation of the wallet, the creator decides the required number of private keys before the transaction is signed and accepted.



3.5 Smart Contract Wallets

A [smart contract wallet](#) works slightly different than the Web3 wallets discussed earlier. Web3 wallets can be categorised as [externally owned accounts](#), while smart contract wallets are known as [contract accounts](#). The table below sums up the key differences between externally owned accounts and contract accounts. Notably, multisig wallets fall into the contract account category, utilising code to authenticate the minimum number of signatures required.

Externally Owned Accounts (EOAs) vs. Contract Accounts
Key differences between EOAs and contract wallets

| EOA | Contract Accounts |
|--|--|
| <ul style="list-style-type: none"> >> Controlled by user(s) >> Accessed via private keys >> Makes transactions and triggers contract accounts | <ul style="list-style-type: none"> >> Transactions executed by code >> No private keys >> Can trigger contract accounts |

Sources: Ethereum.org, blog.makerdao.com, Crypto.com Research

Advanced users can take full advantage of contract accounts and smart contract wallets. [DeFi Saver](#) provides bundles of premade strategies for users, management of existing liquidity levels, and repayments. Since the minimum requirements to access these features come at a steep cost for most retail individuals, DeFi Saver provides a simulation mode so anyone can access its features with pre-loaded Testnet ETH from a fork. The chart below shows one of the premade strategies for how smart contracts help to create a new leveraged vault automatically.



Smart Contracts can Take DeFi to the Next Level

How smart contract wallets can execute strategies within MakerDAO

The screenshot shows a sequence of actions for a MakerDAO strategy:

- Create New Vault
- Wrap ETH
- Supply collateral to Vault
- Generate DAI from Vault
- Sell
- Supply collateral to Vault

The text on the right explains the strategy: "This recipe allows one to create a Maker Vault and then exchange the generated DAI for more ETH to supply even more collateral in a single transaction, allowing for greater ETH exposure." It also lists the use case: "Collateral asset (eg. ETH) is in a strong bull run or massive continuous appreciation" and notes that the protocol used is Maker.

As of 21 Apr 2022 Sources: Defisaver.com, Crypto.com Research

4. Outlook and Conclusions

Digital asset custody solutions for institutions have grown rapidly over the past several years and will likely continue to do so as clientele and assets under custody grow. More traditional asset managers are increasing their exposure to digital assets for a greater diversified portfolio, and the demand growth may lead to increased venture capital, providing funding for new entrants or existing custody providers.

Against a backdrop of a crypto-natives' growing wealth and increased demand for alternative assets, traditional financial institutions and asset managers are incorporating multisig and smart contract wallets for security and operational efficacy reasons, and to maintain relevance in the asset management industry to avoid losing both talent and customers alike.

Naturally, demand growth begets the proliferation of both hot and cold wallets, which provide ease of access to Web3 interfaces. Despite a steeper learning curve, retail wealth managers are gaining knowledge in this field and positioning themselves to capture the growing wealth of the crypto-native generation.

The rise of the digital asset economy will undoubtedly see a rise in exploits, led by the greater demand for more secure custody holdings. Hence, digital and cybersecurity are keys in this industry, given the number of smart contract exploits. Institutions are looking to seasoned smart contract developers to help build their team for the future.

References

- Avalanche. "New Avalanche Bridge Builds on Intel SGX Technology in Breakthrough for Cross-Chain...." *Medium*, 29 July 2021, <https://medium.com/avalancheavax/new-avalanche-bridge-builds-on-intel-sgx-technology-in-breakthrough-for-cross-chain-8f854e0e72e0>. Accessed 28 April 2022.
- Bitcoin Wiki. "Bitcoin Core." *Bitcoin Wiki*, 2022, https://en.bitcoin.it/wiki/Bitcoin_Core. Accessed 28 April 2022.
- Bitcoin Wiki. "Casascius physical bitcoins." *Bitcoin Wiki*, 4 June 2021, https://en.bitcoin.it/wiki/Casascius_physical_bitcoins. Accessed 28 April 2022.
- BitGo. "About." About - *BitGo*, 2020, <https://www.bitgo.com/newsroom/press-releases/bitgo-announces-16-billion-in-assets-under-custody>. Accessed 28 April 2022.
- BitGo. "BitGo Enters Into Agreement To Acquire Kingdom Trust." *Business Wire*, 25 January 2018, <https://www.businesswire.com/news/home/20180125006079/en/BitGo-Enters-Into-Agreement-To-Acquire-Kingdom-Trust>. Accessed 28 April 2022.
- Blockdata.tech. "Crypto Custody Providers Compared — 2021." *Blockdata*, 17 November 2021, <https://www.blockdata.tech/blog/general/crypto-custody-providers-compared-2021>. Accessed 28 April 2022.
- Blockdata.tech. "Crypto Custody: The gateway to institutional adoption." *Blockdata*, 28 January 2022, <https://www.blockdata.tech/blog/general/crypto-custody-the-gateway-to-institutional-adoption>. Accessed 28 April 2022.
- Buczak, Anna. "Best crypto custody providers in 2021." *Ulam Labs*, 22 January 2021, <https://www.ulam.io/blog/best-crypto-custody-providers/>. Accessed 28 April 2022.
- The Chainalysis Team. "The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds — Chainalysis." *Chainalysis blog*, 28 September 2020, <https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap/>. Accessed 28 April 2022.
- Chang, Dorothy. "Paxos in 2020 — A Year in Review." *Paxos*, 17 December 2020, <https://paxos.com/2020/12/17/paxos-in-2020-a-year-in-review/>. Accessed 28 April 2022.

- Coinbase. "Introducing the Travel Rule Universal Solution Technology ("TRUST")." *The Coinbase Blog*, 15 February 2022, <https://blog.coinbase.com/introducing-the-travel-rule-universal-solution-technology-trust-232774d76674>. Accessed 28 April 2022.
- CoinDesk. What Is Crypto Custody? 2022. *CoinDesk*, <https://www.coindesk.com/learn/what-is-crypto-custody/>. Accessed 10 April 2022.
- ConsenSys Blog. "MetaMask Surpasses 10 Million MAUs, Making It the World's Leading Non-Custodial Crypto Wallet." *ConsenSys Blog*, 2021, <https://consensys.net/blog/press-release/metamask-surpasses-10-million-maus-making-it-the-worlds-leading-non-custodial-crypto-wallet/>. Accessed 28 April 2022.
- Copeland, Tim. "QuadrigaCX: Complete story of the \$190 million scandal." *Decrypt*, 13 March 2019, <https://decrypt.co/5853/complete-story-quadrigacx-190-million>. Accessed 28 April 2022.
- Deloitte. "A Market Overview of Custody for Digital Assets Digital Custodian Whitepaper." *Deloitte*, 2020, https://www2.deloitte.com/content/dam/Deloitte/xs/Documents/finance/me_Digital-Custodian-Whitepaper.pdf. Accessed 28 April 2022.
- ethdocs.org. "Account Types, Gas, and Transactions — Ethereum Homestead 0.1 documentation." *Ethereum Homestead*, <https://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html>. Accessed 28 April 2022.
- FidelityDigitalAssets.com. "About Us." *Fidelity Digital Assets*, <https://www.fidelitydigitalassets.com/about-us#oursolutions>. Accessed 28 April 2022.
- Fireblocks.com. "Introducing MPC-CMP: Pushing MPC Wallet Signing Speeds 8X." *Fireblocks*, 13 May 2020, <https://www.fireblocks.com/blog/pushing-mpc-wallet-signing-speeds-8x-with-mpc-cmp-9/>. Accessed 28 April 2022.
- Fireblocks.com. "MPC 101 | What is MPC (Multi-Party Computation)? | Digital Asset Security." *Fireblocks*, <https://www.fireblocks.com/what-is-mpc/>. Accessed 28 April 2022.
- Fireblocks.com. "MPC Wallet Technology | Secure Digital Assets | MPC - CMP." *Fireblocks*, <https://www.fireblocks.com/platforms/mpc-wallet/>. Accessed 28 April 2022.

- Gemini.com. "Proof of Stake vs. Delegated Proof of Stake." *Gemini*,
<https://www.gemini.com/cryptopedia/proof-of-stake-delegated-pos-dpos>.
Accessed 28 April 2022.
- Gemini.com. "Public and Private Keys: What Are They?" *Gemini*,
<https://www.gemini.com/cryptopedia/public-private-keys-cryptography>.
Accessed 28 April 2022.
- Groves, Kevin. "List of Crypto Exchange Hacks: Updated 2022." *HedgewithCrypto*, 22
March 2022,
<https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/>. Accessed
28 April 2022.
- Harper, Colin, and James Rubin. "Multisignature Wallets Can Keep Your Coins Safer (If
You Use Them Right)." *CoinDesk*, 10 November 2020,
[https://www.coindesk.com/tech/2020/11/10/multisignature-wallets-can-keep-
your-coins-safer-if-you-use-them-right/](https://www.coindesk.com/tech/2020/11/10/multisignature-wallets-can-keep-your-coins-safer-if-you-use-them-right/). Accessed 28 April 2022.
- Ter Heide, Dominiek. "A Closer Look At Ethereum Signatures." *HackerNoon*, 15 February
2018,
<https://hackernoon.com/a-closer-look-at-ethereum-signatures-5784c14abecc>.
Accessed 28 April 2022.
- Intel.com. "Software Guard Extensions (Intel® SGX)." *Intel*,
[https://www.intel.sg/content/www/xa/en/architecture-and-technology/software-
guard-extensions.html](https://www.intel.sg/content/www/xa/en/architecture-and-technology/software-guard-extensions.html). Accessed 28 April 2022.
- Investopedia. "What Are Cryptocurrency Custody Solutions? 2020." *Investopedia*,
[https://www.investopedia.com/news/what-are-cryptocurrency-custody-solutions
/](https://www.investopedia.com/news/what-are-cryptocurrency-custody-solutions/). Accessed 10 April 2022.
- Jackson, Amanda. "Private Key Definition — Cryptocurrency." *Investopedia*,
<https://www.investopedia.com/terms/p/private-key.asp>. Accessed 28 April 2022.
- Jibrel.network. "The Evolution of Crypto Custody. As the cryptocurrency industry
matures... | by Jibrel | Jibrel." *Medium*, 25 February 2019,
[https://medium.com/jibrel-network/the-evolution-of-crypto-custody-dec95b0a66
e4](https://medium.com/jibrel-network/the-evolution-of-crypto-custody-dec95b0a66e4). Accessed 28 April 2022.
- Kennedy, Kara. "Crypto Custody." *BNY Mellon*, 2018,
<https://www.bnymellon.com/us/en/insights/all-insights/crypto-custody.html>.
Accessed 28 April 2022.
- King, Alicia. "What is Key Person Risk?" *PartnerMD*, 19 July 2021,
<https://www.partnermd.com/blog/what-is-key-person-risk>. Accessed 28 April
2022.

- KingdomTrust. "Kingdom Trust at the forefront of bitcoin investments." *Choice — Kingdom Trust*, 24 June 2016, <https://www.kingdomtrust.com/news/kingdom-trust-at-the-forefront-of-bitcoin-investments>. Accessed 28 April 2022.
- Ledger.com. "Connecting Ledger Live to DApps with WalletConnect." *Ledger Support*, 25 April 2022, <https://support.ledger.com/hc/en-us/articles/360018444599-Connecting-Ledger-Live-to-DApps-with-WalletConnect?docs=true>. Accessed 28 April 2022.
- Ledger.com. "Ledger Integrates Crypto.com Pay as a New Payment Option." *Ledger*, 8 April 2020, <https://www.ledger.com/ledger-integrates-cryptocom-pay>. Accessed 28 April 2022.
- Ledger.com. "Ledger Live : Most trusted & secure crypto wallet." *Ledger*, <https://www.ledger.com/ledger-live>. Accessed 28 April 2022.
- Ledger.com. "Securely store and manage your NFTs through Ledger." *Ledger*, <https://www.ledger.com/manage-your-nfts>. Accessed 28 April 2022.
- MakerDAO. "What Are Smart Contract Wallets, and How Can They Benefit DeFi Users?" *MakerDAO*, 28 May 2021, <https://blog.makerdao.com/what-are-smart-contract-wallets-and-how-can-they-benefit-defi-users/>. Accessed 28 April 2022.
- Mansa, Julius. "Cold Storage Definition — Cryptocurrency." *Investopedia*, <https://www.investopedia.com/terms/c/cold-storage.asp>. Accessed 28 April 2022.
- MetaMask.io. "User Guide: Secret Recovery Phrase, password, and private keys." *MetaMask Support*, 23 March 2022, https://metamask.zendesk.com/hc/en-us/articles/4404722782107#h_01FYVAXJQT914HCHEYFPNMEJEA. Accessed 28 April 2022.
- Multibit.org. "Multibit-Legacy/multibit: Deprecated Bitcoin Wallet." *GitHub*, 26 July 2017, <https://github.com/Multibit-Legacy/multibit>. Accessed 28 April 2022.
- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *bitcoin.org*, Satoshi Nakamoto, 2009, <https://bitcoin.org/bitcoin.pdf>. Accessed 10 April 2022.
- Parsons, Joe, and Hayley McDowell. "Nomura becomes first crypto custody bank — The TRADE." *The Trade*, 16 May 2018, <https://www.thetradenews.com/nomura-becomes-first-crypto-custody-bank/>. Accessed 28 April 2022.
- Rasure, Erika. "Hot Wallet Definition — Cryptocurrency." *Investopedia*, 8 January 2022, <https://www.investopedia.com/terms/h/hot-wallet.asp>. Accessed 28 April 2022.

- Rooney, Kate. "Fidelity launches trade execution and custody for cryptocurrencies." *CNBC*, 15 October 2018, <https://www.cnbc.com/2018/10/15/fidelity-launches-trade-execution-and-custody-for-cryptocurrencies.html>. Accessed 28 April 2022.
- Sandor, Krisztian. "Crypto Staking 101: What Is Staking?" *CoinDesk*, 1 April 2022, <https://www.coindesk.com/learn/crypto-staking-101-what-is-staking/>. Accessed 28 April 2022.
- Sandor, Krisztian. "What Is Crypto Custody?" *CoinDesk*, 18 February 2022, <https://www.coindesk.com/learn/what-is-crypto-custody/>. Accessed 28 April 2022.
- Schor, Lukas. "Create a Safe | Gnosis Help Center." *Gnosis Help Center*, <https://help.gnosis-safe.io/en/articles/3876461-create-a-safe>. Accessed 28 April 2022.
- Sergeenkov, Andrey. "The Beginner's Guide to Token Swaps | Alexandria." *CoinMarketCap*, 2021, <https://coinmarketcap.com/alexandria/article/the-beginners-guide-to-token-swaps>. Accessed 28 April 2022.
- Sharma, Rakesh, and Somer Anderson. "What Are Cryptocurrency Custody Solutions?" *Investopedia*, <https://www.investopedia.com/news/what-are-cryptocurrency-custody-solutions/>. Accessed 28 April 2022.
- Trezor.io. "User manual: Using Trezor with Android." *Trezor Wiki*, https://wiki.trezor.io/User_manual:Using_Trezor_with_Android. Accessed 28 April 2022.
- Wikipedia. "Dodd–Frank Wall Street Reform and Consumer Protection Act." *Wikipedia*, https://en.wikipedia.org/wiki/Dodd%E2%80%93Frank_Wall_Street_Reform_and_Consumer_Protection_Act. Accessed 28 April 2022.
- Wikipedia. "Fidelity Investments." *Wikipedia*, https://en.wikipedia.org/wiki/Fidelity_Investments. Accessed 28 April 2022.
- Wikipedia. "Mt. Gox." *Wikipedia*, https://en.wikipedia.org/wiki/Mt._Gox. Accessed 28 April 2022.
- Wolfson, Rachel. "Custodial Solutions Are Latest Innovation In Cryptocurrency Ecosystem As Seen By Coinbase And Others." *Forbes*, 20 September 2018, <https://www.forbes.com/sites/rachelwolfson/2018/09/20/custodial-solutions-are-latest-innovation-in-cryptocurrency-ecosystem-as-seen-by-coinbase-and-others/>. Accessed 28 April 2022.



crypto.com

e. contact@crypto.com

©2022 Crypto.com. For more information, please visit [Crypto.com](https://crypto.com).