SEBA BANK

March 2023

Digital Custody

The Bridge

Redefining Finance for the New Economy

Table of Contents

Authors

Yves Longchamp
Head of Research
SEBA Bank AG

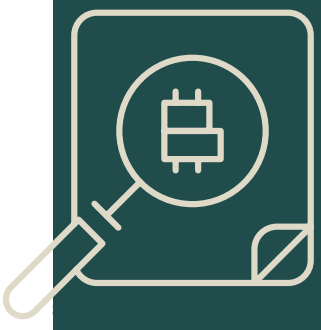
Sonali Gupta
Research Analyst
SEBA India

Anirudh Shreevatsa
Research Analyst
SEBA India

Rishabh Nagar
Research Analyst
SEBA India

Contact

research@seba.swiss



Executive summary

- The custody of digital assets is a significant hurdle for mass adoption of cryptocurrencies due to the technical know-how required for self-custodial web3 wallets
- Digital asset custodians play a vital role in increasing adoption and must provide robust security with speed, scalability, and operational flexibility
- There are two main types of wallets: Hot wallets (connected to the internet) and Cold wallets (offline). Warm and deep cold wallets are also defined depending on the level of security they provide
- With newer types of digital assets coming into the crypto ecosystem, services across custody solutions are also increasing (NFT custody is an example)

Digital asset custodians play a vital role in increasing adoption and must provide robust security with speed, scalability, and operational flexibility

Introduction

The concept of digital asset custody is not new. It has striking parallels with the way traditional financial asset custody works. The idea dates to times when people safeguarded their financial documents (paper certificates, warrants, and stock certificates) in their personal vaults.

Custody then evolved with time, and soon, custodians in the form of banks and other regulated entities came into the picture to safeguard and provide infrastructure to store and manage assets.

Future of Digital Custody

The custody of digital assets is a significant hurdle for the mass adoption of cryptocurrencies. The technical know-how required to get started with self-custodial web3 wallets makes it an issue. While it would be ideal for the industry if investors gained familiarity with self-custodial wallets like Metamask and Argent Wallet, the user experience they offered could also be improved. Digital asset custodians, therefore, play a vital role in increasing the adoption of cryptocurrencies and other digital assets. Custody providers must provide robust security with speed, scalability, and operational flexibility for smooth operations. It is also essential for banks, exchanges, and other financial institutions providing custody services to go through a phase of establishing trust before aiming to solve for adoption.

For example, in the case of the now-defunct FTX exchange, investors lost control of their cryptocurrencies since the company's balance sheet showed no segregation between its users' assets and its own. Investors became increasingly skeptical of third-party custody services in November at the heels of FTX collapse. Hence, the segregation of assets is essential. Such segregation mechanisms also protect investors when the custodian is under regulatory scrutiny, thereby limiting damage (if any) to the custodial service entity. Governments worldwide are yet to clarify if existing financial regulations concerning real-world asset custody could be imposed on digital assets. At the same time, they are also working on new frameworks.

What is digital asset custody?

Digital asset custody services entail the secure storage and management of digital assets. It also typically offers other benefits like easy accessibility and trading of assets.

However, the nature of storage is different from traditional assets' custody. In the case of digital assets, the underlying technology is the critical focus. Digital assets are created and transferred between users within a decentralized blockchain network. Digital assets are acquired via transactions executed on the underlying blockchain, and every transaction is recorded on the distributed ledger. These transaction entries are sometimes the only proof of the existence of users' assets, and to prove ownership of these, a private key is provided. And if these keys are lost or stolen, assets may not be recoverable. Custody providers, therefore, offer to store and protect these private keys on behalf of the owner of digital assets.

Private vs. Public keys

Before delving into the types of custody solutions, let us understand a basic but essential aspect of custody – cryptographic keys. It represents the claim to your digital assets. But what exactly are these keys, and how are they generated? Which key can be used publicly, and which must be kept confidential? These are questions that one faces when entering the world of crypto.

- Public keys work like traditional bank account numbers. You need them to transfer assets to someone else once you have their public key. Therefore, you would also be required to share it with a sender to receive assets. It is the address to your deposit wallet that you need if you are to make any transaction
- Private keys, on the other hand, are analogous to traditional bank accounts' personal identification numbers. (PIN) Private keys must be kept confidential, and one needs them to digitally sign a transaction, without which the transaction cannot get approved. It must always be kept private because it can be used to transfer funds from the wallet

Different types of custody solutions

The type of custody solution boils down to how your private keys are stored. Several kinds of wallets help you according to your requirements. In broad terms, there are two types of wallets: Hot, and Cold. However, you can also loosely define Warm and Deep Cold wallets as different custody service providers use naming conventions directly dependent on the level of security provided. Before going further into what these wallets are and how they work. Let us first understand what a wallet means and why you need it.

After reading how one does not own the asset, instead just the keys representing a claim to these assets, you may wonder how exactly you can transact and move your assets around using just your keys. This is where your wallet comes into the picture. Although the term "wallet" does not paint a perfect picture, it only acts as an intermediary between you and your assets on the blockchain. A public and private key is generated when a wallet is created, and as mentioned above, these keys seem similar but have distinct functions. Let us now get into the different types of wallets:

- **Hot wallet:** A hot wallet is a crypto wallet that is connected to the internet. It does not require human involvement; rather, everything happens automatically. Hot wallets offer a seamless user experience, so most of the wallets out there are of this type. It provides instant accessibility to assets. But convenience comes at the cost of security. This is because the wallet is always connected to the internet, making it vulnerable to attacks. It is recommended not to keep large amounts of crypto in your hot wallet. Examples of hot wallets include mobile wallets, exchange wallets and desktop wallets. Let's understand one example of a hot wallet: -
- **Mobile wallet:** Mobile wallets are mobile applications that manage your private keys. You have complete control of your funds via your wallet application.
- **Warm wallet:** Like hot wallets, warm wallets are always connected to the internet. However, the wallet owner must sign every transaction before sending it to the blockchain. So, everything happens automatically here as well, except for the human involvement required to sign transactions.
- **Cold wallet:** A cold wallet is the opposite of a hot wallet. Any crypto wallet offline or not connected to the internet is a cold wallet. Since one can connect to a blockchain only via the internet, this type of wallet is highly secure and is impenetrable to hackers. Being able to use a cold wallet requires technical knowledge. Mostly, people with experience or large amounts of assets use cold wallets. Hardware wallets and Paper wallets fall under the category of cold wallets. Let us consider an example of a cold wallet.
- **Hardware wallet:** Hardware wallets can be as small as a pen drive or as big as a vault inside a bank. Vaults can be customized according to the client's requirement for asset accessibility. Security features depend on the service provider. It could be based either on multiparty computation (MPC), multi-signature, or a hardware security module (HSM). Vaults are audited and licensed under required certifications.

- **Deep cold wallet:** These are nothing but cold wallets making the accessibility of your wallet more difficult. For instance, you can keep your cold wallet in a safe somewhere in the middle of a desert, making it difficult to access it compared to any other wallet.

There are different ways to make these methods of storage more secure. Custodians or custody providers use a combination of the methods mentioned above and some additional features to make it safer for the user. Multi-signature (Multisig) and multiparty computations (MPC) are two such mechanisms. Let us now get a glimpse of what these additional security features are.

- **Multi-Signature:** As the name suggests, this feature requires multiple private keys to sign a transaction. Therefore, users' assets are still protected if one or a few systems get compromised. It is typically an M-of-N arrangement where N is the number of authorized keys and M is the threshold required to sign off a transaction. No single person has complete control over the assets.
- **Multiparty Computation:** Just like Multisignature, Multiparty Computation or MPC also breaks one single point of compromise. But it does by breaking the private keys into bits and pieces, or one can call it key shards. Unlike a multi-Signature where a number of people with keys are required to complete a transaction, combining multiple keys distributed over devices to form a single private key is required. So even if one device is compromised, a hacker cannot access assets.

Challenges of digital asset custody

The balance between security, speed, scalability, and flexibility defines the best solutions. If we compare security versus speed, cold storage solutions may sometimes result in users paying some opportunity cost since it takes time for assets to go online. A hot wallet, however, is fast but compromises security. Hence, features like MPC help achieve a balance.

Growth of Digital Assets Custody

Although parallels with traditional custody can be drawn for custody of digital assets, they are different by design. Wallets don't store your assets; they act as an intermediary. At the same time, if compromised, it can lead to a loss of assets. It is, therefore, very critical to provide efficiency to the user with the best available technology.

Another way to ensure growth and trust in users is via regulations. Governments worldwide are trying to establish laws for investor protection through the stricter imposition of rules and insurance. Regulations and licensing help service providers immensely since they define a specific framework and give a clear set of instructions to support the increasing demand for digital asset custody.

With newer types of digital assets coming into the crypto ecosystem, services across custody solutions are also increasing. We first witnessed this with the industry's popularity of non-fungible tokens (NFTs). Custody solutions specially designed around NFTs came into existence with other additional features.

Digital custody plays a central role in the adoption of digital assets. Robust offerings like accessibility with safety provide confidence to investors, and features like quick trading access help grow the ecosystem. As a result, digital custody plays a vital role in expanding and adopting digital assets.

Conclusion

With the rise of digital assets, custody has become an increasingly important service for the safekeeping of cryptocurrencies and other digital assets. As the market for digital assets continues to grow, new types of custody are emerging to meet the needs of investors. Custody services are an essential aspect of the crypto ecosystem, providing a critical layer of security and protection for investors. Such services will likely continue to evolve and adapt to meet the changing needs of the industry.

Disclaimer

This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its Head Office and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial investment or to participate in any particular investment strategy. It is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction.

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been effected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifications. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have officers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affiliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. Investing in digital assets including crypto assets as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specific investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking andfinancial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in Singapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as declned in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head offce and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least GBP 5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least GBP 5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the GBP 5 million share capital / net assets requirement is reduced to GBP 500,000); (ii) a partnership or unincorporated association with net assets of at least GBP 5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least GBP 10 million at any time within the year preceding the promotion. Any financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.

SEBA BANK

SEBA Bank AG
Kolinplatz 15 • 6300 Zug • Switzerland • info@seba.swiss • seba.swiss