BLOCKCHAIN STUDENT ASSOCIATION for Syz

Different ways of cryptocurrency custody

Cryptocurrency custody is currently under the spotlight, a development that is both timely and deserved. Following the SEC's green light for spot bitcoin ETFs, a wide range of investors, financial advisors, and institutions are delving into the realm for their initial exploration, aiming to grasp the intricacies of how digital assets are securely stored and safeguarded.

With a variety of custody solutions available, understanding the nuances between them is crucial. This article delves into the distinctions between hot wallets, cold wallets, and third-party custody solutions, shedding light on the different techniques used in banking and how entities like Taurus in Europe and Coinbase in the United States are pioneering in the custody space.

Definition of self-custody and third-party custody:

Self-custody refers to the practice where individuals or organisations hold and manage their own keys, which are used to access and control their digital assets. This means that the asset holder has full control over their funds without relying on any third party. There are mainly two ways to achieve self-custody: using a hot wallet or a cold wallet.

Third-party custody solutions, on the other hand, involve entrusting the security of one's digital assets to an external service provider. These providers are responsible for safeguarding the keys on behalf of the asset holder. As we will see later, there are also multiple different ways to achieve this.

Hot Wallet:

A hot wallet is akin to your physical wallet but in the digital realm. It remains connected to the internet, facilitating quick and easy transactions. A popular example is MetaMask, a browser extension and mobile app that acts not only as a wallet for Ethereum and other ERC-20 tokens[1] but also as a gateway to decentralized applications (dApps[2]). However, this constant internet connectivity also makes hot wallets more susceptible to online attacks and thefts. For example, phishing attacks are susceptible to happen

1 *"The Ethereum Standard Token (ERC20) is used for smart contracts on the Ethereum network. Developed in 2015, ERC20 defines a common list of rules that the Ethereum token must implement. This standard is one of the best known in the world."*

2 *Decentralized applications (DApps) are software programs that run on a blockchain. What makes DApps really special is that they are not controlled by a single company or person. Unlike the classic applications we use every day, where data and control are centralized on a server.*

with a Metamask wallet. Other common attacks might be linked to browser extensions or malware on your computer, as your private key, that is used to sign and authenticate your transactions, is stored on your computer.

Cold Wallets:

In contrast, a cold wallet is an offline storage method for cryptocurrencies, similar to a safe in the physical world. Companies such as Ledger and Trezor represent this category, offering hardware solutions that store users' private keys offline, on the hardware. These wallets are considered significantly more secure against online attacks, as they require physical access to the device for transactions. However, the trade-off comes in the form of convenience, as accessing funds is less straightforward than with hot wallets.

Third-Party Custody Solutions:

For institutions that deal with large volumes of cryptocurrencies, third-party custody solutions have emerged as a secure and compliant way to manage digital assets. These solutions often combine the security benefits of cold storage with the operational efficiency necessary for institutional needs.

These companies provide a complete infrastructure to manage the lifecycle of all types of digital assets issued on the blockchain. There are actually three different ways for these companies to offer their custody solution: on-premises solutions (where the infrastructure is hosted by the client), cloud solutions (leveraging the security and scalability of cloud services), and hybrid models that combine both.

Storing on-premises vs. the cloud vs. hybrid solutions

The decision between storing assets on-premises, in the cloud, or opting for a hybrid solution depends on a myriad of factors including security concerns, the need for accessibility, and regulatory compliance. On-premises storage, while offering maximum control, requires in-depth knowledge of security practices. Cloud solutions offer scalability and ease of access but might raise concerns about data sovereignty and reliance on third-party providers. Hybrid solutions attempt to offer the best of both worlds, balancing control with scalability.

The on-premises approach is often fortified by employing Hardware Security Modules (HSMs), specialised physical devices designed to securely manage, process, and store keys and digital certificates. HSMs provide a robust layer of security by performing cryptographic operations within a tamper-resistant hardware environment, thereby significantly reducing the risk of key compromise. HSMs might work automatically, but in the highly secure world of banking, physical persons are needed to sign HSM transactions.

Cloud storage, conversely, relies on the infrastructure of providers like AWS or Azure, emphasising scalability and easy access. These

platforms often employ Multi-Party Computation (MPC) to secure cryptographic keys by distributing operations across multiple parties, ensuring no single point of failure.

Leaders in third-party custody solutions

Two companies stand out when it comes to custody of digital assets.

Taurus, a leader in digital asset infrastructure in Europe for institutional customers and banks, offers a glimpse into how sophisticated custody solutions work. They are known for offering the three third-party custody solutions that have been talked about above, tailoring the needs of their customers. Taurus is the partner selected by Bank Szy for its digital assets custody solution.

Coinbase, a household name in the cryptocurrency world, has extended its expertise to institutional clients, becoming the crypto custodian for a significant number of spot bitcoin ETF mandates. With its Coinbase Prime offering, Coinbase successfully attracted 8 out of the 11 bitcoin ETFs approved in January. This move underscores the trust and reliability that Coinbase has built in the digital asset custody space, combining their security practices with regulatory compliance to serve institutional needs. Notably, the leader boasts two significant achievements: its 12-year track record without a security breach and being among the first cryptocurrency firms to receive a license from the NY Department of Financial Services (NYDFS). Currently, it oversees the protection of $193 billion in digital assets, which includes $101 billion belonging to institutional clients, as reported in the fourth quarter of 2023.

Conclusion: a diverse custody ecosystem

The cryptocurrency custody ecosystem offers a spectrum of solutions tailored to different needs and preferences, from individual investors prioritising convenience to institutions requiring the utmost in security and compliance. As the digital asset space continues to mature, the evolution of these custody solutions will play a pivotal role in the broader acceptance and integration of cryptocurrencies into the global financial system. Indeed, trust is one of the main limitations to the broader acceptance of digital assets.

Sources:

LEUNG Alan, "How we keep digital assets safe", Coinbase, March 4th 2024, www.coinbase.com/blog/how-we-keep-digital-assets-safe

RAKESH SHARMA, "What Are Cryptocurrency Custody Solutions?", Investopedia, June 21st 2020, www.investopedia.com/news/what-are-cryptocurrency-custody-solutions/

Taurus, "Taurus-PROTECT", March 2024 www.taurushq.com/protect/