EUROPEAN BLOCKCHAIN ASSOCIATION

CUSTODY WORKING GROUP

CRYPTO ASSET CUSTODY AT A GLANCE

WHAT IS CRYPTO ASSET CUSTODY?

Custody within the scope of blockchain technology means safeguarding the access keys to wallets with which owners gain the ability to manage their cryptocurrencies, tokens, and digital assets (such as Bitcoin, Ether, ERC-20 tokens, NFTs, tokenized securities, etc.) by generating a public-private key pair.

The public key of a wallet is a unique identifier similar to a bank account number. The private key is used as an authentication method for signing transactions and therefore represents power of disposition over the crypto asset.

WHAT IS THE PURPOSE OF CRYPTO ASSET CUSTODY?

As the adoption of blockchain technology is progressing at an incredible pace, investors and financial institutions may seek institutional-grade custody solutions, which offer a reduction of risks in managing and storing crypto assets as well as providing a customized user experience.

On the other hand, a reduced reliance on financial intermediaries may ensure a more equitable access to the financial system.

The custody of crypto assets within a sound regulatory framework could generate prolific value advantages whilst empowering consumers.

Provided that blockchain technology is applied to an increasing number of sectors in public and private life, European legislation should aspire to be one of the driving forces of financial inclusion.

HOW DOES IT INTEGRATE INTO THE FINANCE LANDSCAPE

REGULATORS

Crypto assets have garnered so much interest that they have become impossible to ignore. This has led to several countries introducing strict regulations to limit abuse and improve security when working with crypto assets. At the European level, the Markets in Crypto Assets Regulation (MiCA) sets a legal framework for custody service providers. In addition, some countries already have their own regulations - such as Germany, where BaFin issues licenses for crypto custody.

FINANCIAL INSTITUTIONS

As mainstream interest and customer demand for accessto cryptocurrencies rises, banks and other established financial service providers have started to extend their custody services. Encouraged by the increasing regulatory clarity across the world, these institutions are using their vast resources and large client base to rapidly catch up to existing custodians.

EXCHANGES

Specialized cryptocurrency exchanges (For example: Coinbase, Kraken, and many more) were the first players in the market to not only offer trading for crypto assets as their main business, but also include custody for them alongside. Even today, some are among the largest custodians. The majority of users of this "hot" wallet custody are retail, i.e. private customers.

CUSTODY PROVIDERS

Focused solely on custody of digital assets, these companies provide their technical infrastructure and, if necessary, regulatory licenses to clients (banks, funds, projects, etc.) with end customers. They operate in the background and usually have no direct interaction with “retail”.

WHAT TYPES OF CRYPTO ASSET CUSTODY SOLUTIONS EXIST?

CUSTODY TYPE	HARDWARE WALLET	SOFTWARE WALLET	WEB WALLET	CUSTODIAL WALLET
Description	Hardware devices specifically built to store public-private key pairs.	Application installed on a device, such a smartphone or computer.	Accessed through an internet browser, enabling quick transactions and high availability.	Third party custodian provides the wallet infrastructure for securing the public-private key pair.
Examples	Ledger Nano X, Trezor	Exodus, Coinomi	Metamask, XDefi	Tangany, Hauck und Aufhäuser Digital Custody
Security	High	Medium	Low	High
Ease of use	Medium	High	High	Depends on custodian
Connectivity*	Cold	Cold or hot	Hot	Cold or hot
Regulation, Liability	Regulated, user liability	Regulated, user liability	Regulated, user liability	Regulated, provider liability

** Hot or cold wallets are defined by their connectivity. A hot wallet is continuously connected to the internet, whereas a cold wallet can store the public-private key pair offline.*

HOW DOES CRYPTO ASSET CUSTODY WORK?

	KEY CREATION	KEY STORAGE	TRANSACTION SIGNING	KEY RECOVERY
DESCRIPTION	Private Keys are generated in a local environment that hosts the wallet	How is the generated private key stored and who has access to it?	A transaction call can be made by different individuals or parties to make a transaction valid it must be signed with the private key.	E.g. 24 words as seed phrase stored on a piece of paper. Multi-Sig requires the key holder to create a new wallet with the remaining keys.
RISK FACTOR	Can you guarantee that the computer that generates the key is not corrupted? Can you guarantee that the software that generates the private key is safe?	Is the storage environment safe? Are the online (hot wallet) access options secure? Are the offline procedures(cold wallet) secure? Is 2FA in place to avoid an attack in case a password is currupted?	Critical moment as the key might leave the secure environment. E.g. a key is assembled outside of a MPC wallet. Sometimes the private key is sent through certain parts of the server system.	Key recovery is often the weakest link in most solutions. E.g. a seed phrase on a piece of paper might be easily stolen.

NYALA TANGANY IMMUTABLE · INSIGHT