Wallet types

Research and understanding

- Type of wallets: Self custody, NCW, Custody wallets, Smart contract wallets
- Account abstraction: ERC 4337
- FireBlocks as a product

Self custody wallets

In the self-custodial model, **the customer retains full custody (possession) of their assets at all times**, using the service provider merely as an interface for conveniently managing their assets.
All self-custodial crypto wallets **enable you (and only you) to possess the private key associated with your public address.** Practically speaking, this generally takes the form of either a file you store on your device, or a 'mnemonic phrase' that consists of 12-24 randomly generated words. (The mnemonic phrase generates the private key)

Custody wallets

If your wallet doesn't have public and private key that means, it's custodial (meaning you're not in full control of your cryptoassets). Custodial crypto wallets and traditional financial institutions like banks hold your assets on your behalf, requiring you to trust they will not misuse your assets.

Wallet types

Research and understanding

- Type of wallets: Self custody, NCW, Custody wallets, Smart contract wallets
- Account abstraction: ERC 4337
- Fireblocks as a product

Self custody wallets

In the self-custodial model, **the customer retains full custody (possession) of their assets at all times**, using the service provider merely as an interface for conveniently managing their assets.

All self-custodial crypto wallets **enable you (and only you) to possess the private key associated with your public address.** Practically speaking, this generally takes the form of either a file you store on your device, or a 'mnemonic phrase' that consists of 12-24 randomly generated words. (The mnemonic phrase generates the private key)

Custody wallets

If your wallet doesn't have public and private key that means, it's custodial (meaning you're not in full control of your cryptoassets). Custodial crypto wallets and traditional financial institutions like banks hold your assets on your behalf, requiring you to trust they will not misuse your assets.

Non Custody wallets

The term "non-custodial wallet" is often used interchangeably with self-custody wallets. **There is only one master key per workspace for self custodial wallets, while each non-custodial wallet has its own master key**. Self Custodial vs Non-Custodial Wallets To be read more

Open image-20240605-033939.png

Smart Contract Accounts (SCA)

Wallets for smart contracts are based on blockchain technology, (which means they use a network of computers to record transactions). When using a smart contract wallet, users generate a unique type of contract known as a “smart contract.” This agreement contains rules and instructions governing how the funds may be utilized. Once the smart contract is created, it is stored on the blockchain, allowing anyone with permission to access and execute it. The smart contract automates and controls everything. The funds in smart wallets are accessed and managed via smart contract code, which enables nearly limitless functionality, gives users greater control over their assets

Externally Owned Accounts (EOA) and CA Difference

Self-custody wallets can be implemented on-chain in two ways, either through an externally owned account (EOA), or a contract account (CA). Externally Owned

Accounts (EOAs), which require a private key or seed phrase to access, and Contract Accounts, which are controlled by smart contract code. An EOA, or Externally Owned Account, in the context of Ethereum and other blockchain platforms, refers to **an account controlled by a private key and not by a smart contract**.

Account abstraction: ERC 4337

ERC-4337 is an account abstraction standard for the Ethereum blockchain, seeking to improve user experience and security by introducing smart contract functionality in wallets. It embeds smart contracts in users' wallets, allowing them to interact with other contracts and thus complete exchanges automatically.

Besides automating transactions, these "smart wallets" can determine the appropriate gas fees a user should incur in each exchange.

- **Paymaster**: This entity manages the gas payment system.
- **EntryPoin**t: The smart contract that performs UserOps(Imagine it as a list of all the actions you provide your Ethereum account to execute.)
- **Bundlers**: The nodes that submit UserOps to the network for verification.

Fire Blocks as a Product

MPC Wallet- MPC wallets **utilize cryptographic protocols to distribute private keys among multiple parties in a secure manner**. These wallets aim to enhance security by striving to ensure that no single party has complete control over the wallet, thus eliminating single points of failure

Useful references

- Academy
- Custodial vs Non-Custodial Wallets | Crypto.com
- What's a self-custodial wallet? | Learn all about Bitcoin, crypto, and DeFi | Get Started with Bitcoin.com
- Introduction
- Academy