HODL



Self-custody in Digital Assets

In this document, we explain the functioning and importance of self-custody to empower digital assets holders.
At Hodl Funds, our self-custody implementation reflects our commitment to the safety of our investors' assets.



The importance of self-custody

Why does self-custody matter in digital assets?

Digital assets and traditional finance have many differences, with one of the most notable being self-custody. In traditional finance, self-custody is often frowned upon due to the challenges of ensuring seamless settlement and providing access to markets and services when holding assets directly. However, in the digital assets space, self-custody is a critical aspect. It has proven essential for navigating the market, as holding assets in your control is the only way to truly own them. With digital assets - without self-custody - you don't have full ownership of your assets.

Public and Private keys

To fully understand the importance of self-custody of digital assets, it is essential to briefly highlight the inner workings of blockchain technology and the role of public and private keys. Digital assets are stored on the blockchain, and accessing them requires both a public and a private key.

A public key is an alphanumeric string used to verify signatures and encrypt data. This key is meant to be shared for receiving assets. However, public keys can be incredibly long; for instance, Bitcoin public keys are 130 characters long, making them less human-readable. To address this, public keys are hashed through a cryptographic algorithm to create shorter, more manageable versions called wallet addresses. These wallet addresses act as identifiers for sending funds within the blockchain network.

You can think of your public key or wallet address as similar to an email address: they're used to receive information, or assets.

Your private key acts like a password, granting access to your wallet and authorizing transactions. Typically a 64-character hexadecimal string, it may also appear as a mnemonic phrase (12-24 random words) for user convenience. Each private key is unique, deriving its corresponding public key. Sharing your private key gives others full control of your funds, while losing it means permanent loss of access, as no central authority can recover it.

Think of your public key as an email address you share to receive digital assets, while your private key is the password you must never share. If someone gains access to your private key, they can control your wallet and send funds elsewhere with no way for you to retrieve them. This underscores the saying: "Not your keys, not your crypto" i.e. without holding your private key, you do not truly own the assets.

Self-custody in digital assets refers to safeguarding your private keys, not the assets themselves, as the private keys provide complete access to your holdings.

Different types of self custody

Due to the importance of holding your private keys, various solutions have been developed to cater to the different needs of users and an increasing number of institutions.

Hot wallet

A hot wallet is one of the most commonly used self-custody methods for digital assets because it is incredibly easy to use. A hot wallet is connected to the internet, making it always online, which is ideal for everyday transactions and short-term holdings. Well-known examples of hot wallets include web, mobile, and desktop wallets such as MetaMask and Phantom. However, because the hot wallet is always connected to the internet, the private key is also online, making it more vulnerable to hacking.

Cold wallet

At first glance, a cold wallet may seem similar to a hot wallet, but the key difference is that the private keys of a cold wallet are stored offline, making them immune to online hacking attempts. These private keys are stored on physical devices that resemble USB drives, such as a Ledger wallet. Cold wallets are ideal for storing large amounts of digital assets and long-term holdings. However, they are less convenient because you need a physical device to execute a transaction.

Multi-signature

With a traditional cold wallet, the individual holding the private key has full control over the assets. However, there are situations where multiple people, such as within a company, may require shared control over the assets. In such cases, the private key can be divided into multiple parts. For example, five parts distributed among five individuals. This ensures that no single person has complete control over the assets, requiring collaboration to execute a transaction. Organizations can also implement specific requirements, such as needing three out of the five key holders to approve a transaction or mandating all keys for transactions above a certain amount.

Shared-custody

Shared-custody is similar to a multi-signature wallet. However, instead of the private key being divided among individuals within the same organization, the key is also shared with a third party, usually a custodian. So, if an organization, such as an investment fund, wishes to execute a transaction, individuals within the organization need to approve the transaction, along with the custodian, providing an extra layer of security and reducing the chance of a single point of failure. Additionally, this solution reduces the chance of individuals withdrawing assets to unknown wallet addresses.

Hodl's implementation of self-custody



Hodl Funds have chosen to implement a self-custody solution in collaboration with the industry-leading custodian Fireblocks. Fireblocks is a blockchain security platform that provides a suite of tools for securely managing and transferring digital assets, specifically tailored for institutional use. It is widely adopted by businesses such as cryptocurrency exchanges, asset managers, banks, and fintech firms.

Through the integration with Fireblocks, Hodl Funds retain control of the private keys, while Fireblocks provides a comprehensive asset overview and facilitates secure interactions with the blockchain. Each private key is fragmented into multiple parts, which are distributed among members of the leadership team and board members of the fund manager

Governance model

To ensure transparency, security, and operational efficiency, the funds are structured into distinct vaults, each governed by a robust set of customizable rules. For instance, primary assets are safeguarded within Vault 1, which is designated for maximum security.

Within these vaults, governance mechanisms are implemented to enforce controls such as withdrawal limits and multi-signature requirements. This ensures that fund withdrawals are authorized only with the consensus of designated stakeholders.

Furthermore, specialized vaults can be created to accommodate specific operational needs, such as providing direct trading access to select traders. These traders are empowered to act swiftly in response to market opportunities while operating under strict oversight protocols.

To mitigate risks and prevent unauthorized transactions, all withdrawal addresses are subject to a whitelisting process. This process mandates prior approval from a majority of the Fund's Manager's leadership team and board members before any withdrawals can be initiated. By implementing these measures, the governance model ensures that funds are secure, compliant, and managed in alignment with organizational objectives.

Governance alignment

The Fireblocks environment is seamlessly integrated into the governance model, enabling Hodl Funds to implement precise rules and controls within its operational framework. Specific roles, such as designated members, can be assigned with tailored permissions, including limited withdrawal or trading capabilities. This structure allows Hodl Funds to execute trades efficiently on the spot market — such as converting Bitcoin to other assets or vice versa — while adhering to the governance protocols. Crucially, the governance model ensures that no individual within the organization can withdraw assets without meeting the established authorization requirements, preserving security and oversight at all times.

For the algorithmic trading bots, deployed in Hodl Funds' algorithmic strategy, Hodl Funds use different features within the Fireblocks environment. A certain amount of digital assets is placed into an escrow account within the Fireblocks environment, and these digital assets are mirrored on the exchange. At the end of each day, Fireblocks provides a P&L statement that the exchange and Hodl Funds must agree upon. In the event of a loss, the difference will be deducted from the escrow account. In the event of a profit, the exchange

settles the difference into the escrow account. If either party disagrees with the statement, a specified period is allowed for presenting evidence and reaching a resolution. For the Delta Neutral & Market Neutral strategy, we will implement the same solution as with the algorithmic trading strategy.

What happens if the Fund Manager declares bankruptcy?

In the unlikely event that the Fund Manager declares bankruptcy, client assets remain fully protected, as they are held within a separate legal entity. This structure ensures that no fees can be levied on the fund during such an event, safeguarding client interests.

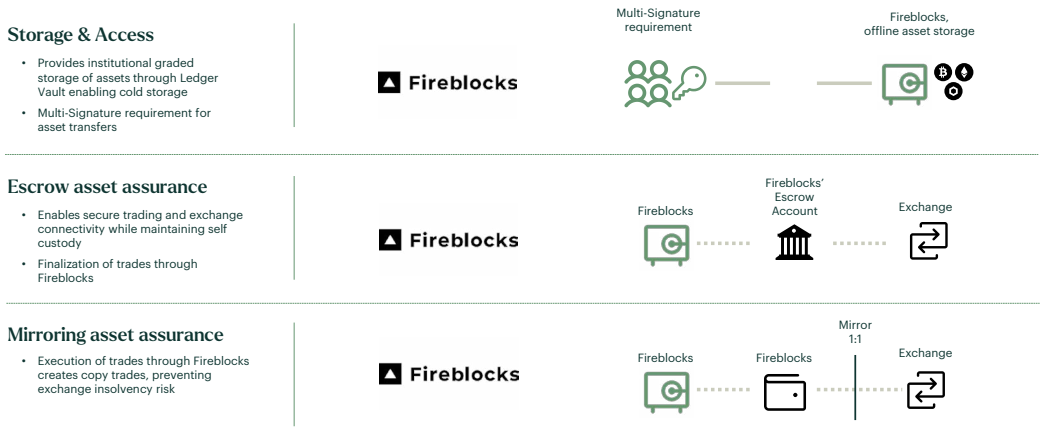
To protect private keys, a robust and secure back-up system is in place. The private key is divided into three shards, which are independently distributed among Hodl Funds, Fireblocks, and Abacus (our trusted fund administrator). This approach ensures security at the highest level.

Since its inception, Hodl Funds has prioritized the safety and security of client assets above all else. Every day, we work to implement and maintain the most advanced security solutions in the industry. Hodl Funds is proud to affirm that, to date, not a single asset has been lost due to security issues or any other concerns.

Security & Risk Management

Measures to optimize asset protection

HODL /FUNDS



About Hodl Group

Since 2020, Hodl Group has aided hundreds of high-net-worth individuals, institutions, and family offices in diversifying their portfolios with digital assets. Digital assets have evolved over the years into an asset class that has proven essential to a modern investment portfolio. However, investing in it comes with its challenges. Our investment funds tackle these challenges by providing simplified and secure exposure to digital assets via four unique strategies: Actively Managed, Algorithmic Trading, Delta & Market Neutral, and Venture Capital. These complementary strategies enable investors to choose an investment approach that aligns with their investment objectives, horizon, and risk appetite, facilitating the seamless integration of digital assets into their portfolios.

HODL

Netherlands
+31 850 607 077
info@hodl.nl
www.hodl.nl
Wilhelminakade 97
3072 AP Rotterdam

Gibraltar
+31 850 607 077
info@hodl.nl
www.hodlgroup.com
5-9 Main Street
Gibraltar

Luxembourg
+31 850 607 077
info@hodl.lu
www.hodl.lu
Route de Thionville 268
L-5885 Howald

Disclaimer

Past performance does not guarantee or indicate future results. The investments in funds are not guaranteed either by the fund administrator or by any insurance mechanism. Before deciding to invest, prospective investors must carefully read the relevant offering memorandum and subscription documents. Before investing in any fund, please carefully consider the investment objectives, risks, charges and expenses.

Investors should consider that the performance of previous years does not guarantee the future. Investing in crypto assets involves significant risks due to significant market fluctuations and high unpredictability. Therefore, it should be considered highly risky. Investors may incur significant losses and lose (part of) their investment.

Hodl has taken reasonable care to ensure that the information is up-to-date and complete but is not responsible for the accidental publication of incorrect information, nor for investment decisions taken based on this material.