BitGo

The Complete Custody Handbook:

An Institutional Primer

LAST UPDATED: NOV 2024

Table of Contents

Introduction

Not all custody is created equal

Not all custody is created equal.

Key management best practices are essential to ensure your assets are secure. Whoever holds the keys to a wallet controls the funds inside. To safeguard your funds, you need to do due diligence particularly well.

There are two choices: store the keys independently, or with an entity they trust.

	✓ Pros	✗ Cons
Store myself	Not dependent on someone else to guard my funds.	Could lose the keys through accident, theft, etc. Hard to put the funds to work and do it safely.
Store with someone I trust	May provide extra security, depending on the quality of the counterparty. Often provides greater accessibility to funds. May allow policies and permissions for additional security controls.	An untrustworthy partner could mismanage my keys or fail to protect me against hackers.

Institutions can't take the chance that a careless or rogue employee could compromise their wallet. Parking funds on exchanges leaves them vulnerable to hacks or other custody risks. Instead, institutions typically rely on custodians for greater protection.

Here's the catch: Not all custody is created equal.

Keep reading to learn key distinctions in digital asset custody →

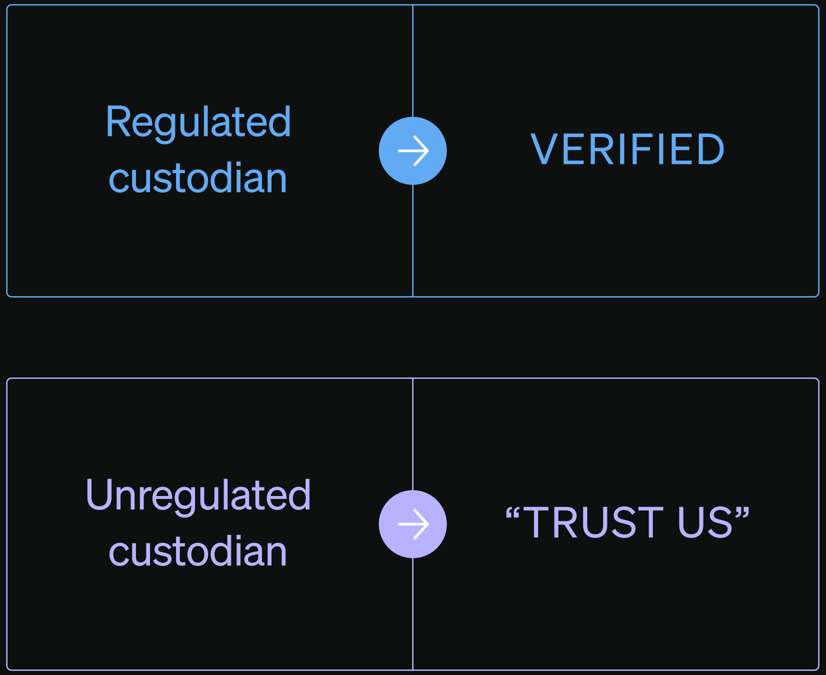
Chapter 1

The importance of regulated custody

Regulated custody

Some custodians have gained regulatory approval, which they've achieved by undergoing audits and meeting specific, rigorous standards intended to protect client funds against. Securing this approval is a lengthy process – signalling that the custodian follows well-designed procedures. By contrast, many custodians, even large ones, are not regulated, they do not hold a fiduciary duty to you as the client. While some may have achieved external accreditations – even SOC1 and SOC2 – they have not passed deep vetting by regulators. Instead, they simply ask you to trust that they will protect your funds as promised.

One of the key reasons behind this is that many digital asset custodians don't hold the funds on your behalf. Instead, they simply provide hot wallets, where you hold the keys to an internet-connected wallet. This can be a solution for easy liquidity, but it comes with risks when holding large sums.



Qualified custody

The term qualified custodian refers to a custodian regulated in the US, derived from the Investment Advisers Act of 1940. Qualified custodians must segregate clients' funds and meet rigorous regulatory standards to protect those funds from loss, theft, or misuse. It applies only to specific regulated entities, like state trusts, which operate with a fiduciary duty to their clients. Many custodians also offer additional protection by holding insurance policies, providing backup keys, and enabling customizable wallet policies.

In 2023, the SEC started considering making it mandatory for certain types of investors to store their digital assets with a qualified custodian.

- ✓ Audited
- ✓ Segregated
- ✓ Fiduciary

Chapter 2

Wallets

Wallet types

Custodians may offer multiple ways to hold your digital assets:

Hot wallets → Internet connected wallets where you hold a majority of the keys

Cold (custodial) wallets → Air-gapped wallets (ie, no internet access) where the custodian manages all the keys

Self-managed cold wallets → Air-gapped wallets (ie, no internet access) where you hold all the keys while using the custodian's vault management technology

Often, customers will keep a small percentage of their funds in hot wallets for liquidity and then the bulk of their funds in a custodial wallet for safekeeping, rebalancing periodically as needed. If they're in a certain jurisdiction or building a more advanced setup, they may also keep funds in a self-managed cold wallet. If your custodian does not offer all of these services, however – ie, they offer only hot wallets or only cold wallets – you may wind up sacrificing either security or speed.

Loosely, you can think of these three options, respectively, like a:

Debit card → Hot wallet

Great for easy access

Vault → Custodial wallet

Great for maximum security

Safe in your own home → Cold wallet

Great for taking security into your own hands

Deploying funds

Custodians may provide you with multiple ways to put your assets to work, offering products or integrations that let you access essential services.

Determine which they offer and how easy or difficult they are to use. For options like trading or staking, ask about how they handle price execution, how they select validators, what fees they charge, etc.

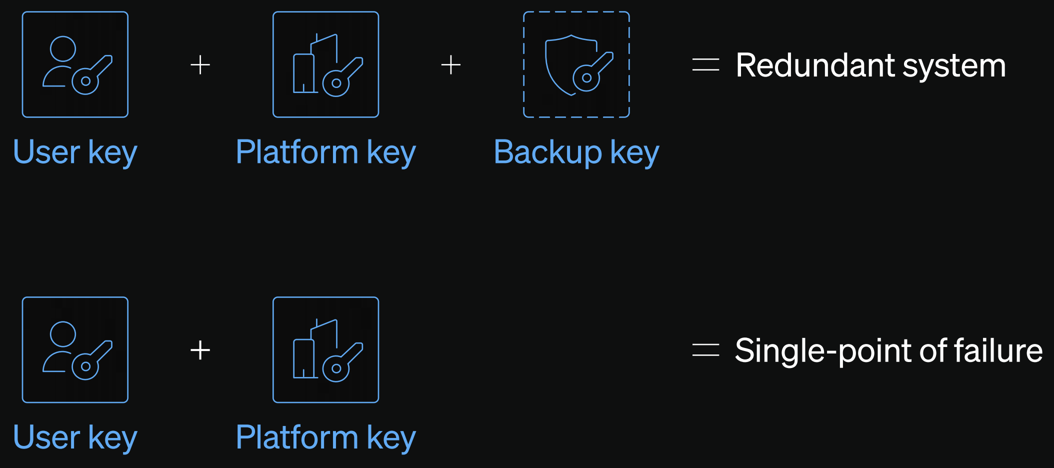
If you're a platform offering crypto services to your customers, it's often more practical to leverage your custodian's wallet infrastructure instead of recreating it yourself. Many platforms build on this foundation and then layer on their branding/marketing, AML/KYC procedures, and relevant integrations. Examine how those backing wallets work, what kind of digital assets they support, and how to connect them with the rest of your tech stack.

- Trading
- Settlement
- Borrowing and lending
- Staking
- DeFi integrations
- Integrations with partner exchanges

Wallet keys

Some wallets work on an "M of-N" model. In plain English, this means that a wallet might have, say, three keys (N) and you need any two of them (M) to approve a transaction (ie, 2-of-3). This provides redundancy and, thus, resiliency.

Something like a 1-of-1 or 2-of-2 wallet, however, creates a single point of failure; losing one key can be catastrophic.



Insurance

Custodians can offer insurance for certain types of wallets and for certain situations (eg, a key lost due to negligence). Typically, the custodian holds the policy and you may receive compensation should your wallet be affected by a covered event (though you may be able to purchase additional coverage on top of the custodian's policy). Unfortunately, not all custodians offer this protection. There have been occurrences where a custodian has lost a key – rendering the wallet unusable and permanently locking the funds – and the customer has no recourse.

Learn more about BitGo's digital asset insurance through Lloyd's of London and European Marketplace.

Custom controls and policies

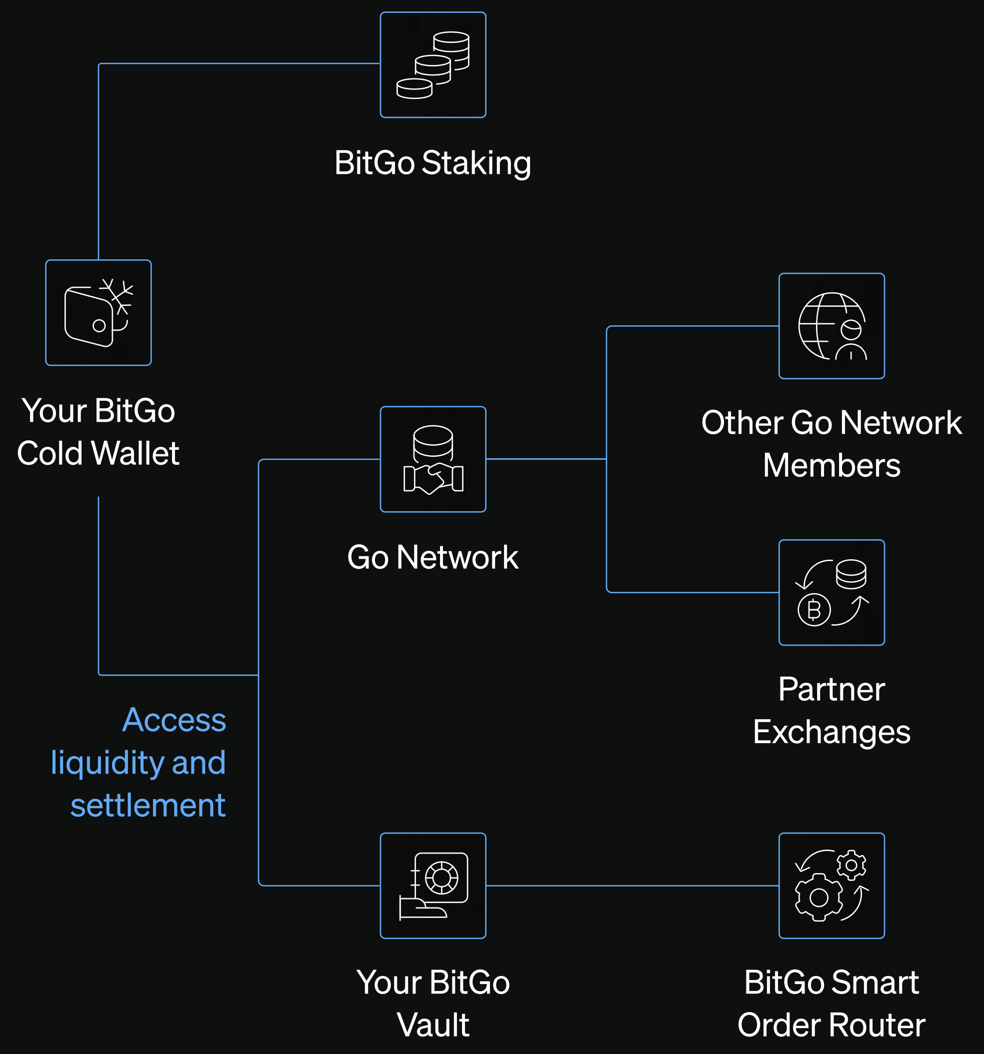
Ideally, your provider will allow you to customize policies and user permissions for each wallet. These may include:

- Assigning user roles (like view-only or the power to initiate but not approve transactions)
- Ensuring outflows can only go to whitelisted wallet addresses
- Determining how many Administrators need to approve each transaction
- Setting transaction and velocity limits, to cap the number of coins that can leave the wallet during any one transaction or time period

Without these, a bad actor who gains control over your keys could wipe out your holdings. With these protections in place, however, you can mitigate the potential damage.

Cold storage

Some custodians may offer services like settlement, staking, or integrations with trading platforms but only out of a hot wallet, which increases the chance of theft. The best-of both worlds approach would be to settle trades or stake from the safety of a cold wallet. In this setup, the funds typically stay with your custodian during trading, etc, and then get transferred only during a pre-scheduled settlement process.



How to evaluate custodians

When deciding how to securely hold digital assets, there are two choices: managing your own keys or entrusting keys with a custodian. These are the essential questions you need to answer when considering a custodian.

Regulation

- ☐ Regulated, qualified custodian
- ☐ Fiduciary duty to me or my organization
- ☐ Funds are held in a segregated manner
- ☐ Funds are never comingled with company assets
- ☐ Assets are bankruptcy remote
- ☐ Insured up to $250M[1]

Wallet options

- ☐ Hot and cold wallets
- ☐ Support most or all of the coins/tokens in my portfolio

Wallet security

- ☐ Insurance coverage against theft, loss, or misuse
- ☐ Extra insurance available to purchase
- ☐ Wallets come with backup keys
- ☐ SOC1 and SOC2 accreditations
- ☐ Secure human processes to completement security technology
- ☐ Custom wallet policies like user permissions, whitelisting and transaction limits

Deploying funds

Access to:

TRADING SERVICES

- ☐ Settlement
- ☐ Staking
- ☐ Borrowing and lending
- ☐ DeFi

OFF-CHAIN TRADE WITH PARTNER EXCHANGES

- ☐ Trading, settlement, and staking are accessible from cold storage
- ☐ Quality price execution on trades
- ☐ Reasonable fee structure

Building platforms

- ☐ Ability to build on top of their wallet infrastructure
- ☐ Ease of integration

[1] bitgo.com/resources/insurance