



# The Complete Custody Handbook

LAST UPDATED: SEPTEMBER 2026

# Table of Contents

|                                                       |  |    |
|-------------------------------------------------------|--|----|
| <b>Introduction: Not All Custody Is Created Equal</b> |  |    |
| What Is Cold Storage?                                 |  | 4  |
| What About Self-Custody?                              |  | 5  |
| Not All Custody Is Created Equal                      |  | 6  |
| Wallet Keys                                           |  | 7  |
| Why Custody Matters                                   |  | 8  |
| <b>Chapter 1: The Importance of Regulated Custody</b> |  |    |
| Regulated Custody                                     |  | 10 |
| Qualified Custody                                     |  | 11 |
| Insurance                                             |  | 12 |
| <b>Chapter 2: Wallets</b>                             |  |    |
| Wallet Types                                          |  | 14 |
| Deploying Funds                                       |  | 15 |
| Custom Controls                                       |  | 16 |
| Quantum Readiness                                     |  | 17 |
| How to Evaluate Custodians                            |  | 18 |





Introduction:

# Not All Custody Is Created Equal





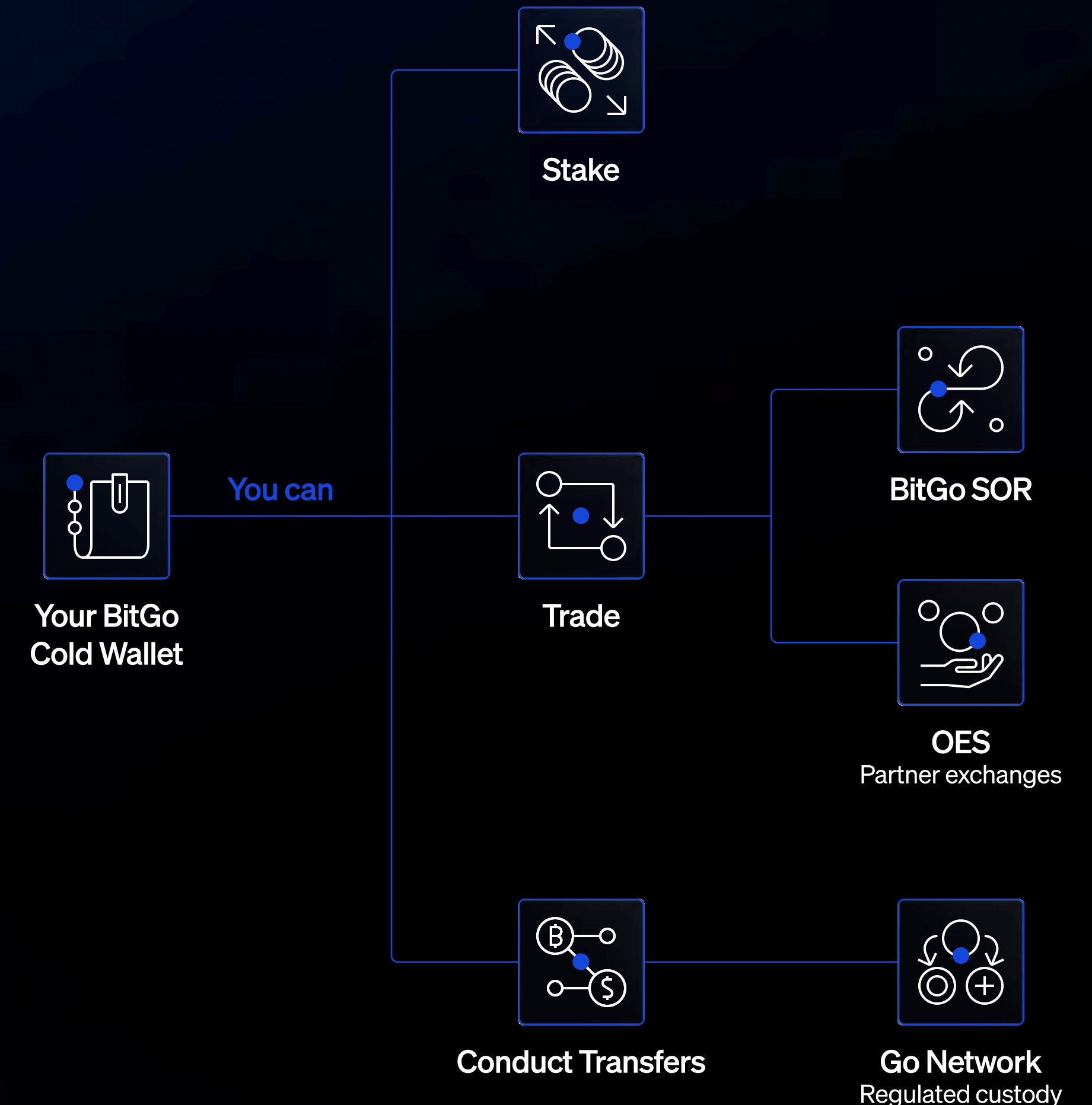


# What is Cold Storage?

Cold storage is the foundation of secure digital asset custody. It keeps the private keys used to access digital assets offline, reducing their exposure to online attacks. For those holding significant assets, it can provide a more secure foundation for long-term custody.

Cold storage doesn't have to mean keeping assets idle. BitGo enables clients to access services like trading, settlement, and staking while assets remain secured in cold storage, designed to reduce the need to move funds into a hot wallet to put them to work.

But offline does not automatically mean secure. The technology and processes used to generate, store, and protect keys remain critical.







# What About Self-Custody?

Self-custody gives you direct control over your digital assets, but it also makes you responsible for generating, storing, and protecting your keys.

That responsibility extends to planning for the unexpected. A single device, seed, or person can become a single point of failure. Loss of access, incapacity, or death can make recovery and estate planning more difficult. A qualified custodian can distribute responsibility across multiple keys, systems, controls, and people, resulting in a more resilient setup.



## **The 2026 Coldcard compromise**

**A seed-generation flaw put certain wallets at risk even though their keys were kept offline.**

**The lesson: No single device, key, or process should be a single point of failure.**





# Not All Custody Is Created Equal

Key management best practices are essential to help ensure your assets are secure. Whoever holds the keys to a wallet controls the funds inside. To safeguard your funds, conducting thorough due diligence is vital.

With self-custody, you are responsible for the devices, software, key generation, backups, and processes used to secure your assets.

|                                   | ✓ PROS                                                                                                                                                                                        | ✗ CONS                                                                                                                                  |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Manage my own keys (self-custody) | Maintain direct control over my funds.                                                                                                                                                        | Responsible for key generation, storage, devices, software, backups, and recovery. A failure in any one of these can put funds at risk. |
| Store with a trusted counterparty | 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 against security breaches.                                          |



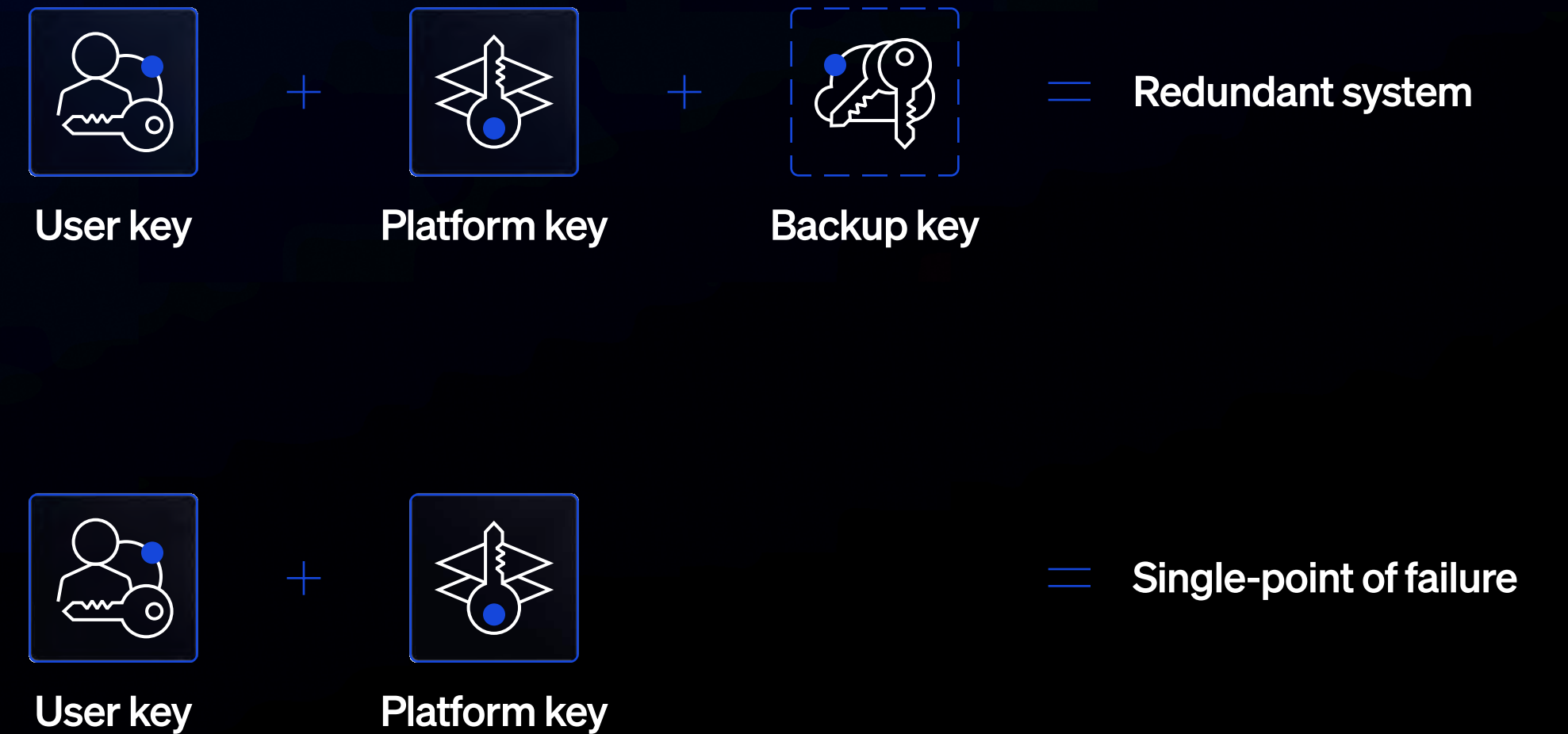


# Wallet Keys

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 (i.e., 2-of-3). This provides redundancy and, thus, resiliency.

How those keys are created and stored matters, too. Independently generated keys stored in separate environments can help prevent a flaw in one device or process from compromising the entire wallet.

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







## Why Custody Matters

Digital asset holders can't take the chance that a careless or rogue employee could compromise their wallet. Parking funds on exchanges can leave them vulnerable to hacks or other custody risks. Instead, investors 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 operate under regulatory oversight, which requires them to meet specific standards designed to protect client assets. These requirements may include audits, examinations, governance standards, and controls over how assets are held and managed.

Regulatory oversight is distinct from security certifications alone. A provider may have external accreditations, including SOC 1 and SOC 2 reports, without being a regulated custodian. When evaluating a custodian, consider both its regulatory status and the security controls protecting your assets.

Regulated  
custodian



VERIFIED

Unregulated  
custodian



“TRUST US”





# Qualified Custody

Qualified custodians are subject to regulatory requirements governing how client assets are held and safeguarded.

BitGo Bank & Trust, National Association is a federally chartered national trust bank regulated by the Office of the Comptroller of the Currency (OCC). Client assets held in BitGo's qualified custody are segregated and structured to be bankruptcy remote, keeping them separate from BitGo's corporate assets and designed to protect them from unauthorized use like rehypothecation.

-  **Audited**
-  **Segregated**
-  **Fiduciary**





# Insurance

Some custodians offer insurance for certain types of wallets and certain covered events, such as loss, theft, or misuse. 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 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.





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 (i.e., no internet access) where the custodian manages all the keys

---

**Self-managed cold wallets** → Air-gapped wallets (i.e., 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 operate in a certain jurisdiction or build 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 – i.e., 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 options are offered and their operational complexity. For options like trading or staking, ask about how they handle price execution, how they select validators, what fees they charge, and whether assets can remain in qualified custody while these activities occur.

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



Staking



DeFi integrations



Borrowing and lending



Integrations with partner exchanges





# Custom Controls

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

- ✔ Assigning user roles (such as view-only, or the permission to initiate but not approve transactions)
- ✔ Determining how many Administrators need to approve each transaction
- ✔ Ensuring outflows can only go to whitelisted wallet addresses
- ✔ Setting transaction and velocity limits, to cap the volume of assets that can leave the wallet during a specified transaction or time frame

Without these, an unauthorized actor who gains access to your keys could wipe out your holdings. With these protections in place, however, you can mitigate the potential risk.





# Quantum Readiness

Quantum computers may eventually become powerful enough to threaten the cryptography used to secure Bitcoin and other blockchains. While that threat is not immediate, you can start reducing long-term exposure now. When evaluating custodians, consider how they invest in technology to identify and mitigate emerging security risks like quantum computing.

BitGo has introduced tools to help identify and reduce this risk, including the Quantum Risk Score and wallet controls designed to limit public-key exposure.

These tools don't make Bitcoin “quantum-proof,” but they can help investors prepare while the Bitcoin network develops longer-term protections.



How exposed are your bitcoin wallets?

Check your Bitcoin Quantum Resistance Score





# Evaluation Guide

## 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<sup>1</sup>

## Wallet options

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

## Self-custody considerations

- ☐ Who is responsible for key generation, backup, and recovery
- ☐ Could one device, seed, or person compromise the wallet

## 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 complement security technology
- ☐ Custom wallet policies like user permissions, whitelisting and transaction limits
- ☐ Are keys independently generated and stored separately
- ☐ Does the wallet architecture avoid single points of failure

## Quantum readiness

- ☐ Can the provider identify and reduce public-key exposure
- ☐ Does the provider have a plan for emerging quantum risks

## 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

<sup>1</sup> [bitgo.com/resources/insurance](https://bitgo.com/resources/insurance)

©2026 BitGo, Inc. (collectively with its parent, affiliates, and subsidiaries, “BitGo”). All rights reserved. BitGo Bank & Trust, National Association (“BitGo Bank & Trust”) is a national trust bank chartered and regulated by the Office of the Comptroller of the Currency (OCC). BitGo Bank & Trust is a wholly-owned subsidiary of BitGo Holdings, Inc., a Delaware corporation headquartered in Sioux Falls, South Dakota. Other BitGo entities include BitGo, Inc. and BitGo Prime LLC, each of which is a separately operated affiliate of BitGo Bank & Trust. BitGo does not offer legal, tax, accounting, or investment advisory services. The information contained herein is for informational and marketing purposes only and should not be construed as legal, tax, or investment advice. Digital assets are subject to a high degree of risk, including the possible loss of the entire principal amount invested. Past performance and illustrative examples do not guarantee future results. BitGo Holdings, Inc., BitGo Bank & Trust, BitGo, Inc. and BitGo Prime LLC are not registered broker-dealers and are not members of the Securities Investor Protection Corporation (“SIPC”) or the Financial Industry Regulatory Authority (“FINRA”). Digital assets held in custody are not guaranteed by BitGo and are not subject to the insurance protections of the Federal Deposit Insurance Corporation (“FDIC”) or SIPC. This communication contains forward-looking statements. Forward-looking statements include all statements that are not historical facts. These statements may include words such as “aim,” “anticipate,” “assume,” “believe,” “contemplate,” “continue,” “could,” “estimate,” “expect,” “forecast,” “foreseeable,” “guidance,” “intend,” “likely,” “may,” “objectives,” “outlook,” “plan,” “potentially,” “predict,” “project,” “seek,” “should,” “target,” “will,” “would,” or variations of these terms and similar expressions. Such forward-looking statements are subject to various risks and uncertainties. Accordingly, there are or will be important factors that could cause actual outcomes or results to differ materially from those indicated in these statements. These factors include but are not limited to those described under “Risk Factors” in BitGo Holdings, Inc.’s most recent Annual Report on Form 10-K and other filings with the Securities and Exchange Commission (“SEC”), including any subsequently filed Quarterly Reports on Form 10-Q. These factors should not be construed as exhaustive and should be read in conjunction with the other cautionary statements that are included in BitGo Holdings, Inc.’s SEC filings. Although BitGo believes that the expectations reflected in its forward-looking statements are reasonable, it cannot guarantee future results. BitGo undertakes no obligation to publicly update or review any forward-looking statement, whether as a result of new information, future developments or otherwise, except as required by law. BitGo Holdings Inc.’s SEC filings are available at [www.sec.gov](https://www.sec.gov). BitGo makes no representation that the information contained herein is appropriate for use in any jurisdiction where its distribution or use would be contrary to law or regulation or would subject BitGo or any of its affiliates to any registration or licensing requirements in such jurisdiction. Persons who access this information are responsible for complying with all applicable laws and regulations.