Digital Asset Custody

A Primer for Institutions

ANCHORAGE DIGITAL

As a crypto partner for institutions, Anchorage offers an unparalleled combination of secure custody, regulatory compliance, product breadth, and client service.

Why does secure, regulated digital asset custody matter?

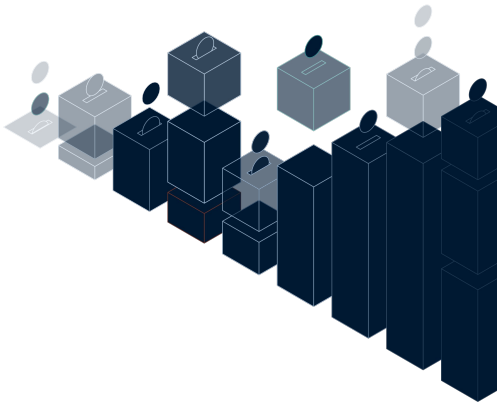
- Qualified custodians transparently meet compliance requirements
- Investments from secure custody can de-risk exposure
- The digital nature of crypto exposes a broad attack surface
- Rich valuations and untraceability attract attackers
- Exploits can be highly scalable, unlike with physical assets
- No central authority means transactions are irreversible

WHAT IS DIGITAL ASSET CUSTODY?

Core infrastructure for digital asset investing

Digital asset custody is similar to traditional custody in the following ways:

1. Qualified custody is storage of assets, meeting strict SEC guidelines for keeping institutional assets safe and secure.
2. Custodians hold valuable assets for safekeeping, such as tangible objects like gold or stock certificates, or intangible assets like crypto.
3. Custodians safeguard assets from threats like external theft, internal collusion, and human error.
4. Movement of assets into or out of custody must be accounted for. Reliable record-keeping and reporting are core functions of a custodian.



Digital Asset Custody

ANCHORAGE DIGITAL

Digital asset custody faces challenges and considerations that traditional custody does not:

1. Digital assets are intangible, with no clearing entity to serve as a centralized record-keeper. The assets' private keys can be stored on paper or on hardware devices, meaning that copies of the asset's ownership may exist. So, while it's easy to prove possession, it can be much more difficult to prove sole control.

2. Traditional custody involves keeping assets far out of reach of potential attackers. The digital asset analog is cold storage, a widespread approach to custody that keeps assets inaccessible by holding them offline. However, many digital assets are designed to incentivize active participation on their networks. Keeping assets offline in cold storage can restrict the ability to participate in a network and realize the full value of the asset.

COMMON DIGITAL ASSET CUSTODY METHODS

Types of custody and associated challenges

Exchanges

Exchanges provide online access to assets, usually keeping a subset of assets in a hot wallet, making them vulnerable to server attacks or phishing.

Software Wallets

Software wallets enable storage of private keys locally on a mobile or desktop device, but are reliant on individuals employing sophisticated security and redundancy measures. Most self-custody software wallet configurations are vulnerable to compromise by coercion, and can expose their users to greater attack risk.

Consumer Hardware Wallets

Specialized hardware devices loaded with software that stores private keys and signs transactions, but are vulnerable to theft and loss, and require a backup seed which can reduce them to a paper wallet. A compromised laptop can exploit the vulnerabilities of a hardware wallet when connected.

Paper Wallets

Pieces of paper that hold written private keys or seed phrases, which are prone to loss, configuration error, and make it hard to validate integrity of the wallet.

Multi-Signature Addresses

Ownership requiring an M-of-N approval, a minimum number of signers (M) out of the total number of signers (N), before a transaction can complete can be unreliable and cumbersome to facilitate, and processes to access assets vary by blockchain. It can also be difficult to remove or add an individual from the trusted group when necessary.

Cold Storage

Assets are stored offline in a device not connected to the internet. Downsides include vulnerability to human error or misconduct, slow processes for moving assets, limited network participation, challenges receiving staking rewards, delays in claiming forks and airdrops, and audit challenges.

The risks of self-custody

"Secure" self-custody typically leads to a process that is complex, error-prone, and vulnerable to physical compromise. Furthermore, it does not meet institutional needs for internal controls, transparent auditing, and prevention of access by single individuals.

Before implementing self-custody, an organization must answer questions such as:

- ❑ Which partners and teams have access?
- ❑ What storage method will be employed and where should assets be stored?
- ❑ Will implementation of the organization's self-custody solution include secure key ceremonies, plans for redundancy, and edits to access and permissions?
- ❑ Will assets move quickly, and how will online key exposure be avoided?
- ❑ Will teams be able to claim assets associated with forks and airdrops?
- ❑ How will audits and reports on asset movement be conducted?
- ❑ How will possession and control be securely proven to auditors?

Consider these attack vectors:

Single points of failure
Servers down, stolen devices, lost credentials, or bugs

Internal collusion
Management gone rogue and disgruntled employees

Low-tech crimes
Kidnapping, robbery, extortion, or blackmail

HOW DO CUSTODIANS AUTHENTICATE APPROVED USERS?

Eliminating vulnerabilities with thorough processes

Digital asset storage solutions vary widely in their approach to authentication. Some have extremely weak controls, with any individual able to withdraw funds using only a username and password. Some have multi-user authentication that is vulnerable to social engineering, such as requiring approval by email from one user and by phone from another, both of which can be faked.

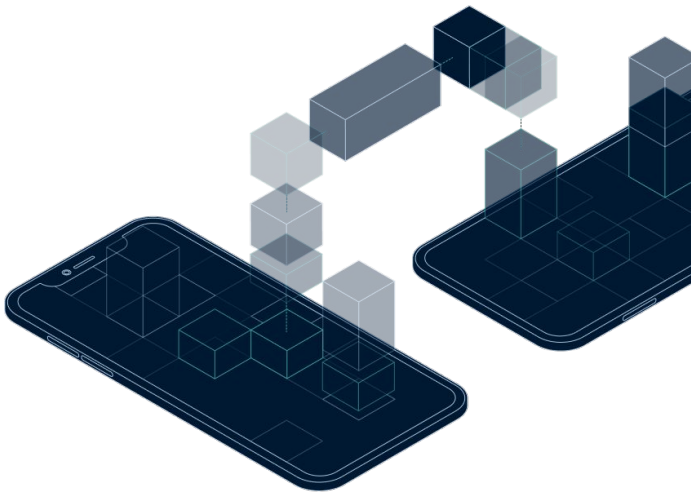
The best way to authenticate organizational intent is to require approval from multiple designated approvers, and verify the identity of each approver with multiple layers of biometrics, behavioral analytics, and unforgeable cryptographic signatures.

How to vet a digital asset custodian

When qualifying a digital asset custodian, ensure the answer to the following questions is an unambiguous “yes”:

Security

- ❑ Are the keys generated securely in hardware?
- ❑ Can transactions be signed only with your organization’s consent?
- ❑ Do transactions require strong authentication of the user, including biometrics and behavioral analytics?
- ❑ Does account access forgo the use of passwords?
- ❑ Are single points of failure eliminated?



Accessibility

- ❑ Can keys be accessed to conduct a transaction within a matter of minutes?
- ❑ Can access be customized to align with organizational permissions for administrators and users?
- ❑ Can administrators securely and easily access records?

Functionality

- ❑ Does the custodian provide crypto product integration, offering staking, trading, and financing opportunities?
- ❑ Can users participate in on-chain governance concerning assets under custody?
- ❑ Can assets under custody be accessed for forks and airdrops?

Trust

- ❑ Is the custodian subject to regulatory oversight, and do they operate in compliance with applicable laws and regulations?
- ❑ Does the custodian receive independent attestations for financial and security controls (i.e. SOC 1, SOC 2)?
- ❑ Does the security model prioritize safety of personal data?
- ❑ Does the custodian have crime insurance?

ABOUT ANCHORAGE

Anchorage Digital is a global regulated crypto platform that provides institutions with a full range of digital asset financial services and infrastructure solutions. As the first crypto-native company to receive a banking charter from the U.S. Office of the Comptroller of the Currency, Anchorage offers institutions an unparalleled combination of secure custody, regulatory clarity, product breadth, and institutional service. Founded in 2017, Anchorage is valued at more than $3 billion and is backed by leading institutions including Andreessen Horowitz, GIC, Singapore’s sovereign wealth fund, Goldman Sachs, KKR, and Visa. Learn more at anchorage.com and @Anchorage.