BLOCKDAEMON

Institutional Self-Custody Planning Guide

What is Institutional Digital Asset Self-Custody

In simple terms, institutional digital asset self-custody is where institutional investors directly manage and secure their own digital assets without relying on custodial services.

Self-custody involves institutions taking direct responsibility for private key safety and maintaining control over associated digital assets.

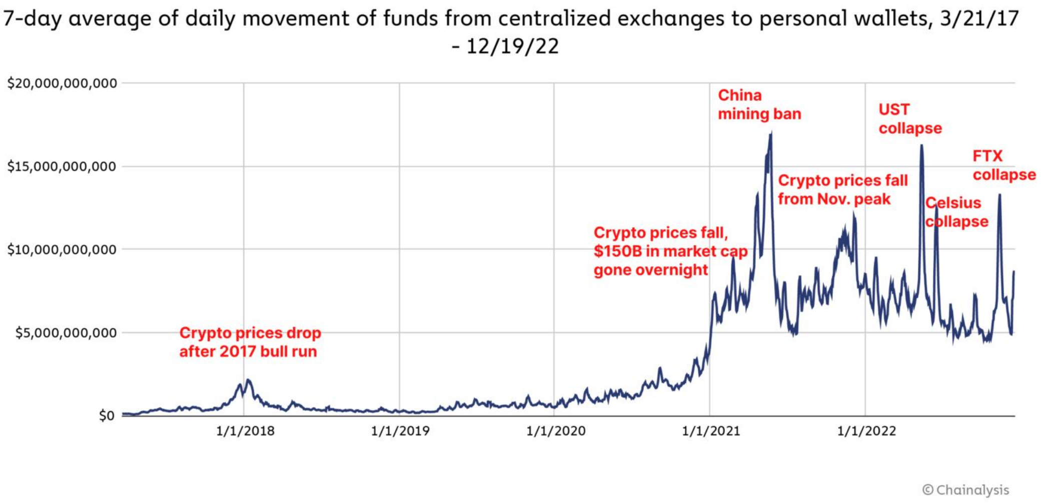
Institutional digital asset self-custody offers several advantages over third-party or shared custody, such as:

- Enhanced security
- Control over funds
- Increased liquidity
- Increased transparency
- Fewer third-party risks and dependencies.

The Case for Institutional Digital Asset Self-Custody

While many benefits are associated with institutional self-custody, the dominant benefits are security and control. In particular, the ability to access and trade digital assets without any dependency on a third party.

Events such as the failure of FTX highlight the risks that can exist with a reliance on third parties without proper transparency, oversight and auditing. The following chart from a December 2022 Chainalysis report highlights the correlation between significant market events and withdrawals from centralized exchanges (CEX) to private wallets.



7-day average of daily movement of funds from centralized exchanges to personal wallets, 3/21/17 - 12/19/22

Source: Chainalysis

Each major negative market event correlated with a substantial spike in transfers from CEX wallets to private wallets. The report notes that the FTX, Celsius, and UST events each resulted in 68% to 77% of those transfers valued at greater than $100,000, signaling that institutions were leading the flight to self-custody wallets.

Liquidity is a further benefit of self-custody. In times of turbulence, market movements (positive or negative) can be dramatic. During such times, your time to liquidity can directly translate to significant gains or losses.

The transfer of assets from cold custody storage to an online wallet routinely takes several hours to a full day, potentially longer during weekends and holidays. Self-custody of digital assets with highly secure online wallets can provide immediate liquidity 24 hours per day, 365 days per year.

Increased transparency is another benefit of self-custody. Advanced wallets now support integrated staking, giving you dashboard visibility and control over your asset positions, including staked assets and associated rewards. Audit logs provide complete visibility and accountability for all transaction requests, approvals, policy modifications, user additions and more.

The combination of total control, liquidity, and transparency is difficult to achieve by even the best custodial services.

Institutional Self-Custody Considerations

With total control comes total responsibility. Therefore, institutions must enter self-custody thoughtfully, with well defined plans and a commitment to execution. There are several critical factors that institutions should carefully consider. These considerations help ensure the effective implementation of self-custody practices and mitigate potential risks.

1 Security

Implementing robust security measures is paramount. Institutions must establish comprehensive security protocols, including secure key generation, storage, use, and backup procedures. They must select reputable wallet solutions, implement multi-party approval schemes, use cryptography techniques, and regularly update security systems to protect against potential threats.

2 Operational Expertise

Institutional self-custody requires expertise in digital asset management, cybersecurity, and compliance. Institutions must assess their internal capabilities and determine if they have the necessary knowledge, resources, and personnel to manage the complexities and risks associated with self-custody. Choosing security platforms with sufficient security and operational controls can help to keep requirements manageable.

3 Regulatory Compliance

Institutions must comply with relevant regulatory frameworks governing digital asset custody. In many regions, institutional self-custody is not subject to KYC (know-your-customer). Unfortunately, regulatory requirements for KYC and AML (anti-money-laundering) may vary by jurisdiction. To ensure compliance with applicable laws and regulations, Institutions must consult with legal experts familiar with their jurisdiction's regulatory landscape.

4 Disaster Recovery and Backup

Adequate backup and disaster recovery plans are crucial to mitigate the risk of data loss, system failures, or other unforeseen events. Institutions should have well-defined backup procedures, redundant storage systems, and recovery protocols in place to ensure the continuity of operations and the ability to restore access to digital assets in case of emergencies.

5 Governance and Accountability

To ensure proper oversight and control over the self-custody process, institutions should establish clearly defined governance policies and accountability mechanisms . These policies and mechanisms should include:

- Defined roles and responsibilities
- Audit procedures
- Regular security assessments
- Adherence to internal and external compliance requirements

6 Legal and Regulatory Considerations

Institutions should seek legal counsel to assess the legal implications and obligations associated with self-custody. This includes:

- Understanding the legal ownership and fiduciary duties related to digital assets
- Contractual obligations
- Potential liability risks
- Any legal, regulatory, or organizational compliance constraints specific to their jurisdiction and company.

7 Insurance Coverage

Evaluating insurance options is essential to mitigate potential losses due to theft, loss, or other security breaches. Institutions should assess whether they can obtain suitable insurance coverage to protect their digital assets and ensure that their self-custody systems and practices align with the requirements of the insurance policies.

Institutional Self-Custody Technologies

Institutional self-custody provides the safekeeping, governance, and control over the private keys associated with the institution's digital assets. The following functional components are required to provide this self-custody service:

Secure Lifecycle Key Management

Cryptographic tools and protocols are used to generate public-private key pairs . Private keys must be securely generated, distributed, stored, used, updated, backed up, and destroyed to protect against unauthorized use or theft before, during, and after use.

Secure Key Storage

Private keys must be stored in a manner that prevents unauthorized access, protecting against key theft or misuse. Institutions typically store private keys electronically, using hardware wallets and/or software wallets designed specifically to secure private keys with institutional control.

Wallets are typically either hot, warm or cold. Hot wallets are online wallets that typically hold just enough digital assets to support planned near-term transactions. Hot wallets are internet-connected and typically used for outbound transactions. Institutional hot wallets should have at least moderate policy controls and frequently use API approvals for automated processing.

Warm wallets are also online wallets, however, they are always controlled by strict policies and require at least some level of human approval versus API approvals. Warm wallets typically fund internal hot wallets as needed. Warm wallets may hold modest to large values in digital assets, with sufficient values to fund near- and mid-term planned transactions.

Cold wallets are not connected to the internet. Cold wallets require approved users to be physically present with the wallet to sign and conduct manual operations to transfer digital assets to another wallet. Cold wallets provide the highest level of security but are the most operationally intensive and require approvers to be physically present. As a result, transfers out of cold wallets are done as infrequently as possible, primarily holding assets for long-term storage.

Institutions holding large amounts of digital assets will typically use a combination of hot and cold, or hot, warm, and cold wallets to create layers of security and segment resources, users, and approvers.

Secure Signature Generation

Blockchains use private keys to digitally sign approved transactions, creating a unique, verifiable signature to authenticate a specific transaction and the approval signature. Institutions can use wallets that require single or multiple approval signatures .

Multi-Party Approval

Institutional governance typically mandates more than one approver for transactions.

Multi-party approval may be implemented in two ways:

1. Using multi-party computation (MPC)
2. Using multiple signatures (multi-sig)

The use of multiple signatures requires smart contracts or similar on-chain processing, which adds cost, complexity, and is not universally supported by all digital asset types.

MPC allows multiple parties to each control a share of a private key to partially sign a transaction. A complete signed transaction is generated when a predefined number of parties have partially signed confirming their approval. This form of multi-party approval appears to the blockchain as a single signature transaction, because a single private key is collectively used (in the form of key shares) to create a single signed transaction. MPC for multi-party approvals works with all protocols, and has the lowest cost and complexity.

Staking

Institutions widely use staking to receive rewards on staked digital assets. Institutional wallets should natively support staking directly from the wallet or through a staking partner integration to enable seamless staking, reporting, and unstaking of digital assets.

Cold staking or the ability to stake digital assets directly from the cold wallet is a relatively new capability that maximizes security, rewards, and operational efficiency.

Cold Storage

Cold storage using offline wallets with air-gapped keys provides further isolation and security, and may be required for governance compliance. Some wallet solutions support both air-gapped and online wallet operations using a common dashboard and policy controls. This flexibility can optimize operational efficiency and security.

Key Backup and Recovery

Copies of the private keys must be encrypted and stored for emergency recovery in case of a catastrophic system loss due to natural disasters or other failure event conditions. As an institution creates new keys, and replaces existing keys, the institution must also update backup key copies. Therefore careful consideration of your backup and recovery system and processes is essential.

Policies

Protection of private keys is essential, but not sufficient. It is equally important to establish and enforce policies determining the conditions under which the keys can be used. Otherwise a bad actor could modify policies, allowing them to transfer assets for fraudulent purposes. Institutions typically require a variety of policy types such as: quorum approvals, checklists, conditional (if, then, else), and operational policies. Self-custody systems must ensure these policies are consistently enforced, and protected from unauthorized modifications.

Additional Considerations

Following are some additional points for consideration.

Self-Hosted For Complete Independence

A primary objective of self-custody is to have total and exclusive control over your digital assets, with no dependence on third parties. Cloud-hosted Wallet as a Service (WaaS) offers the convenience of letting a third party host your wallet infrastructure. It typically includes the provider hosting one or more MPC key shares. But this convenience comes with a cost relative to control.

Using a WaaS for self-custody reduces the institution's responsibility for infrastructure hosting, and creates a co-dependence on the WaaS provider. In most cases, the institution can not execute transactions, change quorum policies, create backups, or recover lost private key materials without the WaaS provider's participation. Similar to a custodian, if the WaaS provider becomes hacked, insolvent, or is frozen by regulators, the assets may become lost or stranded at least temporarily which can result in major loss of value during periods of turbulence.

Automated Deployment in Secure Clouds

While self-hosting gives you complete control it also gives you complete responsibility. Not all institutions have the depth of personnel and expertise to host and maintain system availability on a 7×24×365 basis. Hosting your wallet infrastructure in secure cloud computing environments can give you the availability of a cloud service without being dependent on a wallet service provider.

Some institutional wallets support automated deployment in cloud infrastructure such as AWS, Azure and others to make deployment and installation fast and accurately configured. This capability can reduce the burdens on your team and elevate your overall self-hosting experience.

Proven Track Record

Historically, cryptographic algorithms, such as threshold key management and signature generation using MPC, are thoughtfully designed, developed, peer-reviewed, third-party audited for vulnerabilities, and then deployed and field tested for several years before general use in commercial applications. Some of today's MPC wallets use MPC algorithms with nearly a decade of commercial deployment, undergoing years of real-world vulnerability testing in live environments and third-party attestations. Other wallets may use new and relatively unproven MPC algorithms and implementations, with little or no real-world deployments or third-party attestations.

When selecting an MPC-based self-custody solution, institutions are encouraged to conduct due diligence on the core technology, track record of the cryptography team, timeline of deployment in live commercial applications, and the security assessments of respected third parties. After all, minimizing risk is a core objective with institutional self-custody, including your solution-sourcing risk.

How to Get Started

Conducting a thoughtful approach to institutional self-custody can be intimidating. Breaking the process into manageable tasks is a great way to get started and ensure due diligence.

Criteria List

We recommended starting with a list of criteria to achieve the optimal balance between secure self-custody and practical, frictionless operations. This planning guide provides a framework for reviewing your requirements and formulating your criteria.

Research

Any security solution is only as strong as its weakest link. Therefore, thorough review and vetting of your technology options, vendor partners, and their track record can help reduce the potential need to change technologies or partners during the evaluation process.

Evaluate

Presentations and demonstrations are great, but nothing will replace the hands-on experience of test-driving the wallet(s) you'll use for institutional self-custody. Many wallets support the option to test drive and evaluate both the wallet user interface in a sandbox environment. These wallets allow you to create policies, add users, assign roles, and conduct test quorum transaction approvals. Some wallets also provide the opportunity to simulate and evaluate the deployment experience of hosting your own wallet infrastructure. Conducting these evaluations can lead to critical insights, both positive and negative, empowering you to make thoughtful and informed decisions.

Blockdaemon Can Help

Blockdaemon has been the industry's most trusted blockchain infrastructure provider since 2018. In 2022, Blockdaemon acquired Sepior, adding world-renowned cryptographers to Blockdaemon's team and industry proven MPC wallet technology to our portfolio. Today, Blockdaemon works with many of the world's largest banks, custodians, exchanges, and institutions to support institutional self-custody, qualified custody, and other digital asset services and solutions.

Get Started with Blockdaemon

Contact us to learn how we can help you power your blockchain business.

Get Started