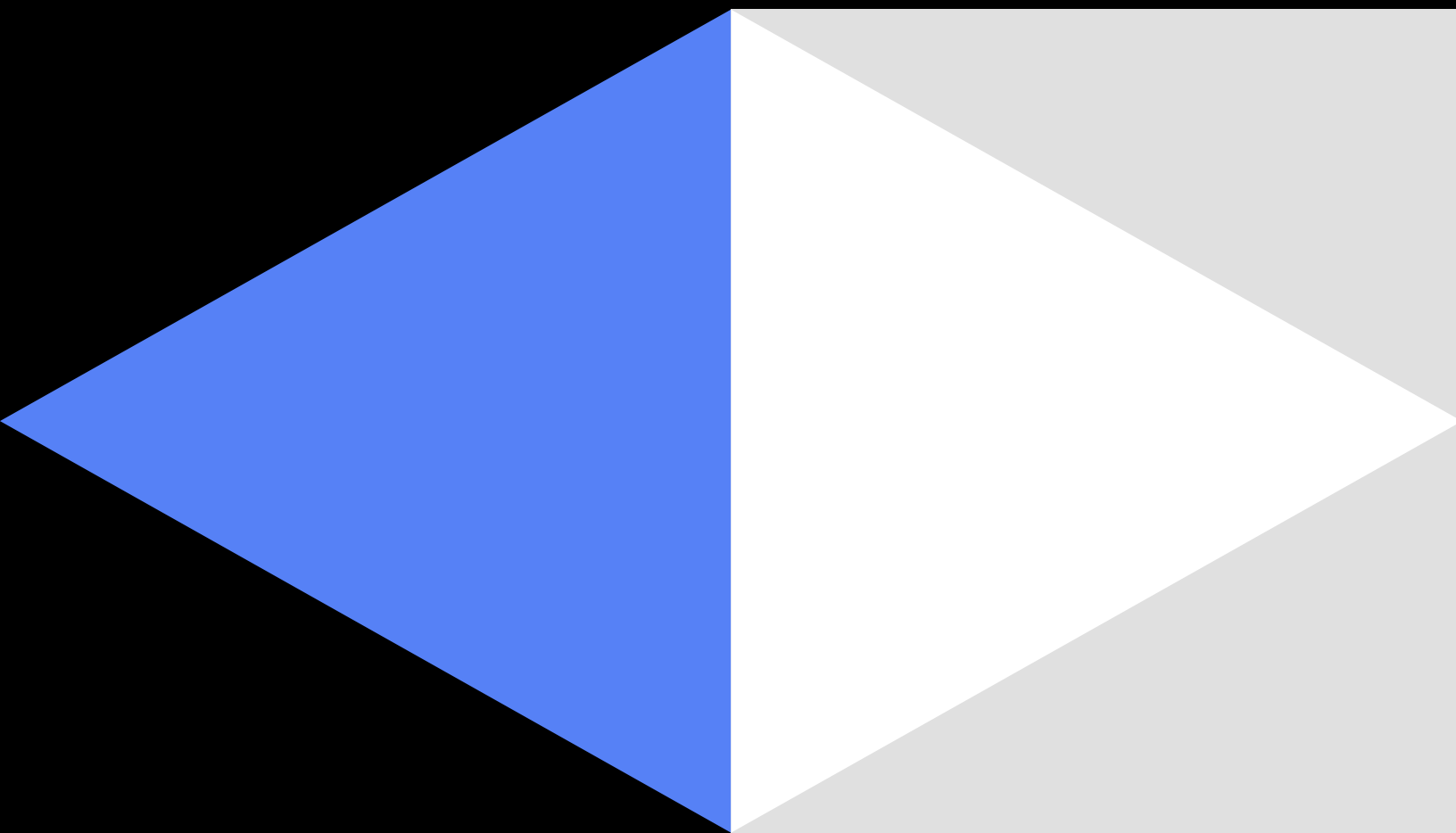
anchorage digital

GUIDE

Finding end-to-end security in crypto custody

What institutions need to consider about securing digital assets



Introduction

Anchorage Digital custody was designed to mitigate risk to the maximum extent possible. Our custody solution is the only model on the market that incorporates secure storage, strong controls, regulatory compliance, and bankruptcy protection–all with an integrated policy engine and key processing system that keeps both equally secure. Anchorage Digital custody is provided through our national bank charter, the industry's only nationally-regulated form of custody. We deliver this security in all the services we offer from trading to staking and governance, with one custody model built to scale to trillions of dollars in value.

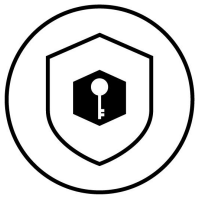
In this paper, we will discuss not just how to store digital assets, but also how to use private keys for truly safe and well-regulated institutional custody.

Custody is the most important decision an institution must make when dealing with digital assets, so any institution interested in crypto should read this.

Four components to a complete digital asset safekeeping solution

As the digital asset industry has matured, the role of responsible, regulated custody has become well-understood by market participants and institutions. While the importance of safe custody is common knowledge, what constitutes 'safe custody' remains a difficult question for institutions hoping to use crypto to answer, and the range and fragmentation of various custody providers and their solutions only adds to this complexity.

While your institution will have many operational and logistical requirements for your digital assets, the first and most important consideration is the soundness of the technical and regulatory underpinnings of safekeeping. When it comes to end-to-end security in custody, there are four critical components to consider:



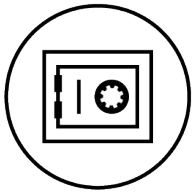
1. Generation

The first step in digital asset custody is the creation of the private key. An often overlooked stage in custody, it has the potential to be one of the most vulnerable points in the storage lifecycle of your crypto.

What to consider:

- How is the private key for the asset generated?
- Is the process manual or automated?
- Is it created in a way that cannot be influenced or eavesdropped by a malicious party?

Four components to a complete digital asset safekeeping solution (cont.)



2. Storage

The most common focus of custody due diligence is the mechanism in which your digital asset private keys are held. When evaluating private key storage, you must take into account not only the way in which your assets are protected during their expected lifecycle but also the myriad exceptional cases and vectors of compromise that can be experienced over the course of decades of data safekeeping.

What to consider:

- Where is this asset stored when it's not being used?
- Does it exist in the general memory of an inspectable computer?
- How are private keys made safe from extraction?
- Does the asset ever exist in a place where it can be connected to the internet?
- What happens in the case of disaster to make sure the private key(s) cannot be lost? Could a fire, a hardware malfunction, or a natural disaster expose your institution to loss?

Four components to a complete digital asset safekeeping solution (cont.)

3. Usage

A frequently neglected but incredibly critical component of safe custody is a rigorous, comprehensive, and deeply secure framework for access and usage to private key material. Because the extreme importance of protecting keys from even a single unauthorized usage – regardless of whether the key itself is exposed – is unique to digital assets, this is often the least mature and protected process in crypto custodians. Anchorage Digital was founded on the principle of protecting private key usage with the same level of security as the private key material itself.

What to consider:

- What protections are in place for this asset to be used?
- How are policies for private key use created and enforced?
- Can these policies be compromised such that the key can be used without proper consent?
- How closely are policies tied to the actual transactions being signed?
- Can assets be moved by the custodian without participation from my institution?

Four components to a complete digital asset safekeeping solution (cont.)

4. Responsibility

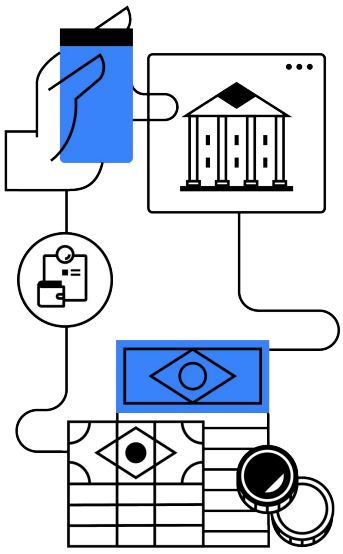
Because digital assets' safety and security lies in getting the technical setup correct end-to-end, across every link in the security chain, this technological security is extremely difficult to get right. Institutions rely on custody and safekeeping providers to be the experts in security so they can focus on their business. Having clarity on where responsibility for the safety of your assets lies is key to building trust.

What to consider:

- Whose responsibility is it to keep these keys safe?
- Does my institution have to have private key security as a core competency to confidently use this custody solution?
- Does the custodian take full accountability for the accessibility of my assets?
- Is the custodian's responsibility audited and regulated?

Four components to a complete digital asset safekeeping solution (cont.)

Digital assets are unique in that the possession of the private key gives full control of everything that can be done with an asset, not just to transfer value, but also to influence through governance the very security of a digital asset network itself. With these bearer assets, all actions are irreversible, so every step possible must be taken to avoid the misuse of the private key material. Every stage in the private key lifecycle, from generation to storage to usage for transaction signing, must be accounted for in best mitigating risk.



When you select a custodian, who bears responsibility?

Most people's initial experience with digital assets starts with a hot wallet, whether in the form of choosing to hold cryptocurrency on an exchange, or via one of the many hot wallets available. Quite often, their second interaction with custody is to use a Ledger, Trezor, or other form of cold storage. In all of these cases, as an individual, when you use a hot or cold wallet yourself, this is self-custody. If you make a mistake or break your device, you lose your assets, and it's 100% your responsibility for the loss. When you select a third-party custodian, at Anchorage Digital, we believe that responsibility should be 100% removed from your institution, however, not every custodial model takes this approach or fully mitigates your potential to lose or compromise the very assets you've turned over to be protected.

Overview of storage methods

There are four main categories of storage for crypto: hot wallets, cold wallets, multi-party computation (MPC), and hardware security modules (HSMs). The Anchorage Digital model builds on top of proven HSM technology in a distinct way that significantly de-risks custody, more than any other method alone, without compromising accessibility or security.

	Anchorage Digital	Multi-party computation	Legacy cold storage	Hot wallets
Mitigates risk of human error	◆	◆	◆	◆
Keys offline	◆	◆	◆	◆
Funds settle quickly	◆	◆	◆	◆
Staking & governance	◆	◆	◆	◆
24/7 availability	◆	◆	◆	◆
Integrated authentication methods	◆	◆	◆	◆
Policy engine powered by FIPS 140-2	◆	◆	◆	◆

1. Hot wallets - multiple vectors for attack

Hot wallets treat crypto private keys like any other piece of private customer data. Keys are **generated** in software on demand in online servers and **stored** in memory, sometimes encrypted or as part of a key management service that may use cloud HSMs. Because of this, while they are fast to transact, hot wallets are generally considered to be the weakest form of security. Hot wallets should only be used when you need instant access to be able to move funds on-chain for many millions of addresses. Exchanges usually keep a subset of assets in a hot wallet to provide online access to assets, making them vulnerable to server attacks or phishing. These hot wallets are often set up as omnibus accounts, meaning funds are commingled across customers and sometimes with the exchange's own funds.

Overview of storage methods (cont.)

When choosing to self-custody, institutions use software wallets that enable storage of private keys locally on a mobile or desktop device, or a hardware wallet, 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 as they typically do not use advanced authentication methods. When providers introduce significant high-friction security measures to increase the safety of assets by increasing the difficulty and time of access but otherwise still keep keys online, these are sometimes called "warm wallets" and should be considered through a similar lens.

2. Legacy cold storage - complex human driven processes

Cold storage, as used traditionally, derives its security primarily and almost entirely from the proposition that keys are created and held in a device that is never connected to the internet. **Generating** keys and addresses in a legacy cold storage system requires complicated human processes, in which operators must safely follow long chains of physical steps using multiple pieces of software and physical protective privacy measures. Keys are **stored** in a stable medium, often sharded into multiple geographic locations, anywhere from locked and monitored rooms in offices to high security vaults, with the goal of preventing individuals from accessing them. Executing transactions from cold storage may take anywhere from hours to days, requires many hands and steps to complete, and inherently compromises the security of the assets which means custodians usually "burn" an address after a single transaction.

Because these human driven processes are so cumbersome, legacy cold storage is highly inefficient and unscalable for any modern fintech, and scaled use cases explicitly compromise on security from both cybercrime and human error or misconduct, and typically cannot be securely scaled to allow for network participation such as staking. Lastly, they are unable to provide a full and expedient auditability of ownership.

3. MPC - a novel signing mechanism

While MPC, a mathematical model, has become a popular term, it is a solution to a specific problem for signing frameworks, rather than a custody model in itself. MPC systems allow a private key to be both generated and stored without ever having private key material assembled in one place. At its core, this solution distributes the problem of key storage (in the form of key shares) and server security across multiple machines, increasing the difficulty of compromise. Similar to a native multisig solution, this creates additive difficulty to compromising where keys are **generated** and **stored**. This also leaves room for potential human error, should one party not be able to protect their part of the sharded key, in a sense making the approach akin to self-custody when one party is your institution.

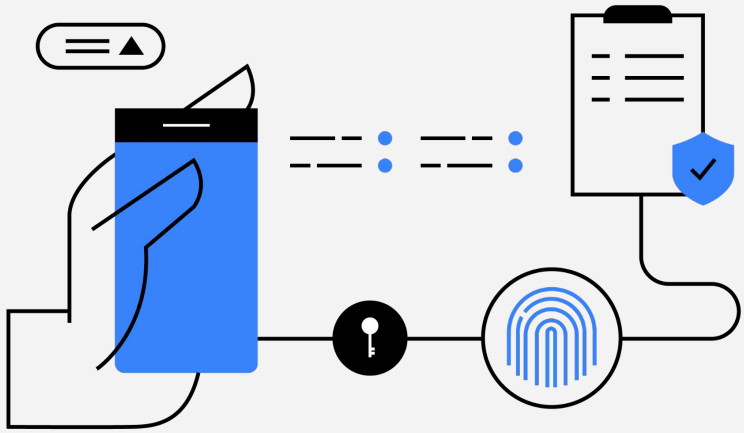
As a result, the use of MPC technology on its own does not imply sufficient security, since the sensitive machines involved in transactions may be operated like any hot wallet or cold storage method, and this should be validated independently.

4. HSMs - a proven tool

Hardware Security Modules (HSMs) are purpose-built, tamper-resistant hardware devices that are designed to manage the full lifecycle of cryptographic keys. The specialized hardware involved is well-tested and certified in independent laboratories and has been used for decades in applications across finance, military, government and modern high technology security. Key **generation** happens entirely in certified hardware through audited processes that cannot be influenced or observed. Those keys are then **stored** encrypted in a way where they can only ever be processed within the secure boundary of the HSMs, but can be backed up and maintained through modern processes. While strong in key storage and generation ability, the way signing instructions are authenticated and authorized, matched with use of HSMs, makes the difference between good and great security.

Overview of storage methods (cont.)

The Anchorage Digital HSM model keeps private key data completely offline within air gapped hardware while transacting at speeds similar to a warm or hot wallet, with the added improvement of encoding policy engines that validate signing instructions inside the hardware itself. Anchorage Digital authenticates your institution's policies, such as a quorum of user approvals, proving who initiated a transaction and verifying signer's identity through multiple biometric and cryptographic checks. All of this is done with the private key material staying within the HSM where no client, Anchorage Digital employee, or third party can view, manipulate, or lose the most important data that controls assets. The HSM hardware technology in use by Anchorage Digital has a deep history being utilized for mission-critical security and has been vetted in accordance with the FIPS 140-2 standards[1].



As your institution considers custody solutions for safekeeping, it's important to recognize that no storage method operates in isolation. So, while industry participants and institutions are used to hearing about hot versus cold storage methods and their tradeoffs, the reality is that the soundness of the technology selected is also dependent on the administration and controls around and beyond the model of custody.

[1]FIPS PUB 140-2 Level 3

Overview of storage methods (cont.)

Regardless of whether a custodian uses MPC or HSMs, or how they choose between obvious tradeoffs of traditional cold and hot storage such as security, latency, and recoverability, a consistent methodology is required that completely integrates full lifecycle safety, unimpeachable execution of your policies, and the ability to satisfy the functional needs of your institution for the services you are building.

The authority problem: using keys for digital assets

After some introductory experience with both hot and cold wallets, the majority of institutions shift their focus on the mechanisms of HSMs and MPC. This is advisable as both HSMs and MPCs aim to ensure that an attacker cannot extract private key material from your infrastructure. But focusing on these security mechanisms alone fails to consider their limitations. While these models offer better security guarantees around key generation and storage, they are both uncritical on their own on how and when to follow instructions from an authority they trust.

This means whether your institution initiates a send of $5 or $500 million in bitcoin, if instructions come from an authorized party they will be executed, and as a bearer asset, once transferred, these funds cannot be recovered. If an attacker can fool your custodian's infrastructure into accepting and signing even just one transaction by mimicking an authoritative service, that attacker can move those funds in an irreversible way. This makes their incentive to get into an institution's infrastructure very high.

Authentication methods and authorization strategies vary widely between organizations and should be heavily diligenced by your institution. Some providers may have extremely weak controls, with any individual able to withdraw funds using only a username and password. While others have multi-user authentication that is vulnerable to social engineering, such as requiring approval by email from one user and by phone from another, which are subject to cellular or SMS attacks, phishing attempts, and email provider-level compromise.

The authority problem: using keys for digital assets (cont.)

Even institutions with excellent authentication practices may have lackluster authorization strategies, relegating the authorization of policies to a central authority or indiscriminately applying the same policy authorization against high and low value transactions because their engine cannot distinguish between transactions of different risk levels.

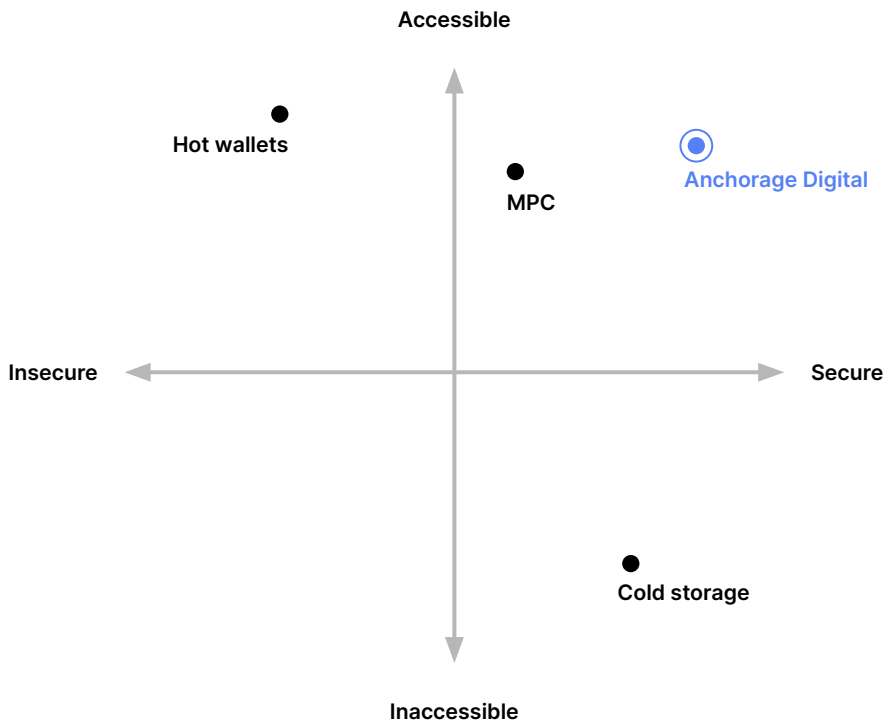
> The fundamentally irreversible model of crypto puts incredible importance on pre-transaction security. Once a transaction is initiated, a responsible custodian must verify the intent of the transaction by properly authenticating the issuer and validating that the request irrefutably meets client policies.

Most custody providers will verify policies against approvers and many will have a policy engine that controls what operations can happen once a set of policies triggers them, however, it is not possible for any traditional storage method to independently check what is being signed.

In other words, it is not possible for these other custody models to verify the contents of a transaction with the same level of trust that they verify its authorization.

> Only at Anchorage Digital is our policy engine combined and integrated with private key security within the same, secure system where we can not only validate whether you should sign, but also what you are signing.

Overview of authority for key usage



Hot vs Cold: The wrong question

While there is a wide spectrum of possibilities in authentication and authorization across all types of custody solutions, each custody model by its nature lends itself to a certain solution space for establishing authority to sign blockchain transactions. Your institution should deeply consider how your custodian avoids unauthorized access to keys from both external and internal attackers.

Online wallets and standard web security

Hot wallets and self custody software are built on top of traditional web infrastructure for the purpose of instant access and usability. Their security is akin to any other important piece of information you save or sensitive action you can take on the websites and software you use day to day. Authentication through a simple password or similar and authorization through surface level system checks is common practice. Your institution should only keep assets in hot wallets for actions that cannot be supported via safer custody practices, and according to your risk and loss tolerance.

Human processes in legacy cold storage

When you consider legacy cold storage, the approach to solving this issue is to intermediate all transactions with human beings. In theory, a person is able to exercise judgment on which transactions happen. In practice, at any meaningful scale this requires many humans to:

- Follow long, onerous, difficult to understand checklists
- Not be fooled or compromised, and
- Be incentivized to do these things very quickly while remaining 100% accurate

Ultimately, these are not things humans are known for being good at and certainly not all at once, and the speed limitations of these solutions requires that you keep much more of your funds in your hot wallet infrastructure.

MPC's policy limitations

While MPC systems, like HSMs, are designed to make private keys difficult to extract, the mathematical mechanism of MPC does not itself ensure that the right thing is being signed, it only ensures that the key material exists to sign something. Essentially, MPC requires trust that you have already validated you are meeting your policies for a given transaction when you use private key material.

Overview of authority for key usage (cont.)

In some MPC systems, all of that key material is entrusted with the custodian. The client requests that the custodian sign something and a policy engine inside the custodian's infrastructure has the right to ask all the different MPC actors to participate in signing the transaction. **This reduces the security of the custodian down to the security of the policy engine server.**

In other MPC systems, one portion of the key material is given back to the client. Very rarely does the custodian not hold enough shares of a key to have full control over the assets should they desire, so they can either initiate a transaction (usually in case of emergency) or wait for a share from the client to be used in order to have enough shares at a time to access the crypto to move it. Occasionally shares will be truly distributed such that the client must maintain security and durability of their key shares or else access to the digital assets will be permanently lost. **Either way, this puts the onus of securing private key material back onto the very customers looking to the custodian to solve this difficult problem.**

Once an attacker is in a position to send a message with enough key shares to enact a transaction, they will be able to send a transaction with nothing to stop them, as MPC has no ability to recognize who holds the keys or what it is signing, only to transact once it has the key materials. We sometimes call this a signing oracle attack. The security infrastructure is a signing oracle that blindly trusts input, and any enforcement at the policy level must happen in a separate, unintegrated system.

Responsible organizations try to mitigate this by implementing signing policy validators near their security infrastructure to verify that transactions are valid before being signed. There are many strategies for doing this well, but ultimately, these methods still rely on general purpose servers with various degrees of uncoupled hardening in an institution’s infrastructure and are subject to compromise if the infrastructure of the custodian is compromised. MPC can still be used for an additional layer of security, but in and of itself, it is not sufficient.

Overview of authority for key usage (cont.)

HSMs at Anchorage Digital

HSMs are often used the same way as MPC, making them vulnerable to the same security failings of requiring too much trust on what transactions fit a client's policies, and also lacking the auditability institutions need to meet their fiduciary obligations.

Instead of leaving things to trust, Anchorage Digital extends the security envelope of signing to include your policies. Anchorage Digital develops firmware policy engines that run inside of our hardware security modules and gate access to any sensitive material.

Whenever a transaction instruction is issued to an Anchorage Digital HSM, it independently verifies that this instruction has met your organization's policies, with cryptographic signatures from the hardware devices you hold that Anchorage Digital manages. Crucially, Anchorage Digital HSMs protect not just your cryptographic keys, but they also protect the policies of your institutions and the very contents of that transaction being signed, because **for true end-to-end security, your policies need to be as secure as the keys they are used to control.**

This hardware-to-hardware security for transactions means a movement of funds from your account can never be fabricated or tampered with, and **no amount of compromise to Anchorage Digital's infrastructure can cause an unapproved movement of funds**. Our commitment to continual investment in our hardware and internal policies is a reflection of commitment to keep our internal infrastructure strong against fraudulent behavior from risk vectors.

At Anchorage Digital, we make the secure path the easy and default path and avoid allowing you to configure your way into an insecure system. We believe that the responsibility of ensuring your assets are safe should lie primarily with us, and not be something we push back onto your institution.

Secure custody in a regulated world

Lastly, is consideration of the legal and regulatory oversight. Anchorage Digital **unequivocally meets the definition of qualified custody**, helping institutions meet their fiduciary responsibilities. With our national bank charter, we've made an ongoing commitment to regulatory oversight, accountability, and meeting the common high standards assigned to all other federally regulated banks. Our clients benefit from our ongoing commitment to meet our regulators' requirements and our strong controls around risk, capital preservation, compliance, and anti money laundering (BSA/KYC/AML). Additionally, though we have never experienced an issue, clients take comfort in knowing that we have a crime insurance policy that covers the loss of digital assets through theft, robbery, burglary, as well as third party computer and funds transfer fraud on all accounts.

A national bank charter and ongoing auditing

Alongside our security guarantees, Anchorage Digital is **the first and only crypto company to receive an operational federal bank charter**. Conversion from a state-level charter required a spotless operating history and demonstrating to regulators that our custody controls are strong enough to merit a national charter that custodies digital assets worth billions of dollars on par with other national banks. And as a security-first, compliant, and regulated company, Anchorage Digital has received multiple external audits from our clients and SOC-I and II auditing. The extensive pen testing and continuous internal risk management processes we conduct also protect your institution as the blockchain space continues to evolve.

Secure custody in a regulated world (cont.)

Proof of exclusive control and existence proofing

Anchorage Digital provides proof of exclusive control of private keys. This shows keys are held exclusively by Anchorage Digital and that no one else has or has ever had access to them. Our model provides a version of “cold” storage that doesn’t require key sharing or manual human operations that increases the risk of asset loss. A potential issue with MPC, of which a characteristic is anonymity of signing, is that the system itself cannot prove which key shares were used to execute a transaction. Like a key used to open a locked front door, the lock will open with the key inserted, but there’s no ability to audit or prove the person turning the key should be allowed to enter or who actually entered the home. Anchorage Digital’s unification of policy and signing means the same system which constructs and signs transactions can provide the audit logs approval. **We can also easily prove to external auditors and clients that we have control of keys of digital assets at any time through on-demand challenge response authentication.**

Secure custody in a regulated world (cont.)

Selecting your digital asset custodian and partner in crypto

We believe Anchorage Digital's technologically sound and regulated solution for safekeeping and using digital assets sets the industry standard. If your institution would like to discuss Anchorage Digital custody, see a demo, or learn about the various services from trading to staking we offer within our secure custody platform, please get in touch here.

anchorage digital

About Anchorage Digital

Founded in 2017, Anchorage Digital is valued at over $3 billion with funding from leading institutions including Andreessen Horowitz, GIC—Singapore's sovereign wealth fund, Goldman Sachs, KKR, and Visa. Headquartered in San Francisco, California, Anchorage Digital is remote-friendly with offices in New York; Porto, Portugal; Singapore; and Sioux Falls, South Dakota. **Learn more at anchorage.com, on Twitter @Anchorage, and on LinkedIn.**