

A Guide to Crypto Custody



Contents

Introduction _____ 3

Part 1: The Basics of Crypto Custody _____ 5

Three Tiers of Crypto Custody _____ 6

Online vs. Offline Custody Solutions: Defining ‘Hot’ and ‘Cold’ _____ 9

Summary _____ 11

Part 2: Understanding Institutional Grade Security _____ 12

Offline Storage Model _____ 13

Governance and Controls _____ 16

Redundancy and Business Continuity _____ 19

Transparency and Proof of Controls _____ 21

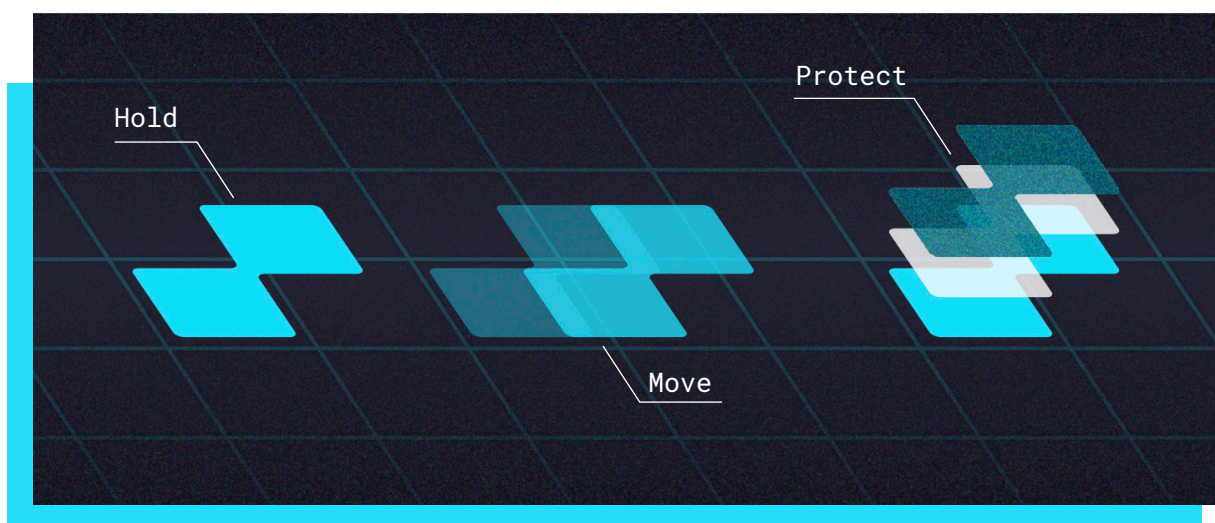
Part 3: Considerations for Customers _____ 23

Part 4: Future-Ready Custody _____ 26

Introduction

The rise of cryptocurrency as an asset class is bringing increased attention to the importance of security and trust—as well as the growing need for regulations and standards of operation—in the space. The practices of centralized and decentralized exchanges have received the most scrutiny to date, but the manner in which digital assets are stored and managed is an equally important (though less discussed) concern.

Custody is a financial services term that refers to the ability to hold, move, and protect assets.



Access to custodial infrastructure will be a growing need for hedge funds, high-net-worth individuals, and financial institutions as they expand their cryptocurrency holdings. Already, there are 150 active crypto hedge funds who collectively have US\$1bn assets under management (AuM), and 52 percent of those funds use an independent custodian.¹ A Q3 2018 survey by Greenwich Associates also found that 72 percent of institutional investors said crypto was not going away.

Custodying cryptocurrencies (such as bitcoin, litecoin, ether, and many others), as opposed to other assets like cash, securities, or objects, requires a new kind of infrastructure—one that differs from the traditional paper-and-safe approach in banking.

1. <https://www.pwc.com/gx/en/financial-services/fintech/assets/pwc-elwood-2019-annual-crypto-hedge-fund-report.pdf>

It takes a different set of processes and assumptions to design custody solutions for digital-only assets. Cryptocurrencies are created and managed using specialized technologies which come with their own unique considerations for their storage and security.

The domain expertise it takes to build such solutions, as well as design effective governance controls, is not inherent to the traditional financial services industry. Critical technical knowledge in financial services generally support the organization's existing product suite, as opposed to driving the development of new infrastructures, offerings, or solutions.

Building new architecture from the ground up—using deep domain knowledge and security-first development processes—is necessary for the secure storage and handling of cryptocurrencies. As with other areas of the technology industry, the best solutions tend to emerge from companies solving their own challenges.

Crypto-native companies, like Gemini, have been solving crypto-native challenges since their inception. In custody, the stakes for creating institutional-grade solutions are high. The maturation of crypto as an asset class depends on the long-term safety of both personal and institutional funds.

At the start, Gemini recognized the need for a world-class custody solution, for both personal and institutional use, that was compliant with applicable regulation, accessible to users in multiple geographies, and available without hefty fees. We also knew that a foundation capable of meeting our own needs (and high security standards) would be capable of serving audiences across the industry—helping elevate crypto as an asset class.

Our learnings gained from releasing multiple versions of our custody solution since 2015 are encapsulated here. Our aim is to help educate retail investors, professional crypto traders, and financial institutions on what a world-class custody infrastructure looks like. With that understanding, they can decide for themselves what kind of industry solution meets their unique needs and standards.

52% of active crypto hedge funds use an independent custodian

The Basics of Crypto Custody

Custody is a broad term that can be applied to a number of different solutions for digital asset storage. People have many choices when it comes to storing their crypto assets, and the connectivity of those solutions poses unique concerns for their customers. Solutions range from self-custody options like a hardware or software wallet, to third-party, offline storage.

Custody needs also vary. For instance, some investors might need to infrequently access or move their cryptocurrencies compared to others who trade more frequently. Some investors might prefer to self-custody, while some institutions might require a third-party solution.

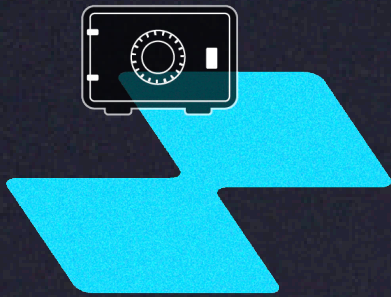
In This Section

Three Tiers of Crypto Custody 

Online vs. Offline Custody Solutions: Defining 'Hot' and 'Cold' 

Summary 

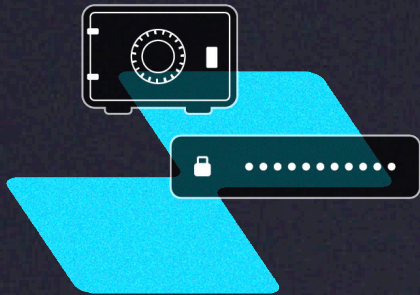
Three Tiers Of Crypto Custody



1

Self-custody:

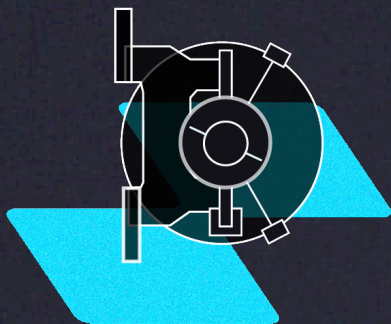
Build your own solution



2

Partial custody:

"Wallet plus" solution



3

Third-party custody:

Managed solution



1. Self-custody: Build your own solution

There are many ways to self-secure cryptocurrencies. Approaches can range from using consumer hardware wallets, to creating complex setups for the duplication, storage, and backup of printed-out private keys. —————>

Many people want complete control of their digital assets, and self-custodying provides a good solution. Consider the difficulty in managing passwords and the frequency with which you may have a password reset performed. When dealing with self-storage and private keys there are no resets, a lost key is gone forever. Self-custodying, like keeping cash in your physical wallet or locked in a drawer, poses its own risks. There is no third-party involved to manage that risk (or your funds) if you were to lose access to your keys, experience a destructive event like a fire or power outage, or pass away unexpectedly.

Holders should consider their access to software updates, as well as their personal capacity to correctly backup, restore and implement geographic redundancy. Individuals should also consider how family members or intended beneficiaries would recover funds in emergency situations.

Private Key

In public key cryptography, a **private key** is a well formed and unguessable number that is intended to be kept secret. For any valid private key, there is a unique corresponding public key. By using these keys, a holder of cryptocurrency can receive (via a public key address) and spend (via a signature from the private key).



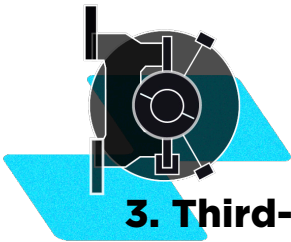
2. Partial custody: “Wallet plus” solution

An emerging option in the crypto custody market is a self-managed wallet that offers some level of third-party assistance and related institutional controls or protections. Such an option may align to the needs of certain retail or high-net-worth investors who want to control their holdings, but also desire some level of assurance and institutional protections shy of full third-party management.

“Wallet plus” solutions scale up from basic hardware wallets by applying protocols such as two-factor authentication (or other identity verifications) and/or basic multisignature protections, where the third-party possess a key for co-signing the customer’s transactions.

This amounts to a form of split or partial custody, in which the customer and the third party are generally required to cooperate as part of the signing process. However, the exact amount of control either party has to sign the transaction without the other party—such as in the event of an emergency—depends both on the legal arrangement between customer and provider and the specific key management model of the custody solution.

Customers should consider (and ask about) the potential for third-party access and/or movement of their funds without their key. They should also be mindful of how a “wallet plus” provider handles software upgrades and practical concerns such as backup, recovery, and transaction identity verification.



3. Third-party custody: Managed solution

Third-party custody solutions allow customer funds to be held and managed entirely by a solutions provider. The user entrusts their assets to the custody provider, who is then the only entity acting on the customer’s instructions (the customer is not involved as a direct signing authority). Service level agreements (SLAs) dictate the terms and timing conditions regarding the storage, access, and movement of customer funds by the third party.

Third-party solutions are best suited to investors and institutions, such as asset managers, hedge funds, and/or high-net-worth individuals. They are the only solutions capable of offering bank-level protection for crypto security and safety, as they provide the most robust level of third-party control. That said, third-party custody solutions in the market today vary drastically in terms of what they offer (as we’ll discuss in Part 2).

Customers also have the option to use multiple third parties (full-custody or wallet-plus) if they want two or more providers involved to verify instructions and move funds.

Online vs. Offline Custody Solutions

Defining 'Hot' and 'Cold'

Third-party custody solutions come in two forms, which are often referred to as online (“hot wallets”) or offline (“cold storage”) systems. The difference between the two amounts to whether the storage system is networked or in any way remotely operable.

Online	Offline
Online “hot wallets” store signing keys in internet-connected systems or in network-available hardware devices. These systems do not require a physical presence to complete transactions.	Offline “cold storage” solutions hold signing keys in hardware devices that are physically isolated (or “air-gapped”) with no connection to the internet and thus no potential for remote control through software-communicated instructions.

The two types of systems pose tradeoffs.

Online solutions are capable of greater speed and liquidity, as the use of a network connection enables automated access to the system. Being networked, however, means that they are more vulnerable to attacks delivered through the network, resulting in the creation of unauthorized transfers or the potential compromising of the signing keys. Possession of a signing key is the only requirement to move funds.

Offline solutions are generally slower to execute on customer instructions because their key-storage systems can only be accessed at their physical locations. However, this solution design significantly lowers the risk of unauthorized transfers through physical security and role-based control over key access (as we’ll discuss in Part 2).

Summary

Decisions of fit for customers, in terms of custody tier and offline vs. online networking, can depend on their size of holdings and overall risk tolerance.

The increasing sophistication of criminals involved in the space, however, means that investors with large holdings or high activity levels should pursue highly secure solutions. Institutions, who may be required to segregate client assets, also have unique needs that can only be addressed with the help of a trusted solutions provider.

For those reasons, an offline, third-party custody solution is the most robust approach for customers seeking both security and trust.

Not all offline solutions deliver institutional-grade protections, as every system has a unique infrastructure and operational framework. Customers should understand how custody solutions work in order to know which attributes and components matter most for their specific needs and concerns.

Understanding Institutional-Grade Custody

Custody solutions that can be considered institutional-grade are not just “air-gapped” computers in protected physical locations. Rather, they combine secure vaulting, cryptographic hardware, and organizational governance to provide multiple layers of security for the safeguarding of assets.

The following areas of custody system design provide a starting point for understanding how solutions vary across the market.

In This Section

Offline Storage Model 

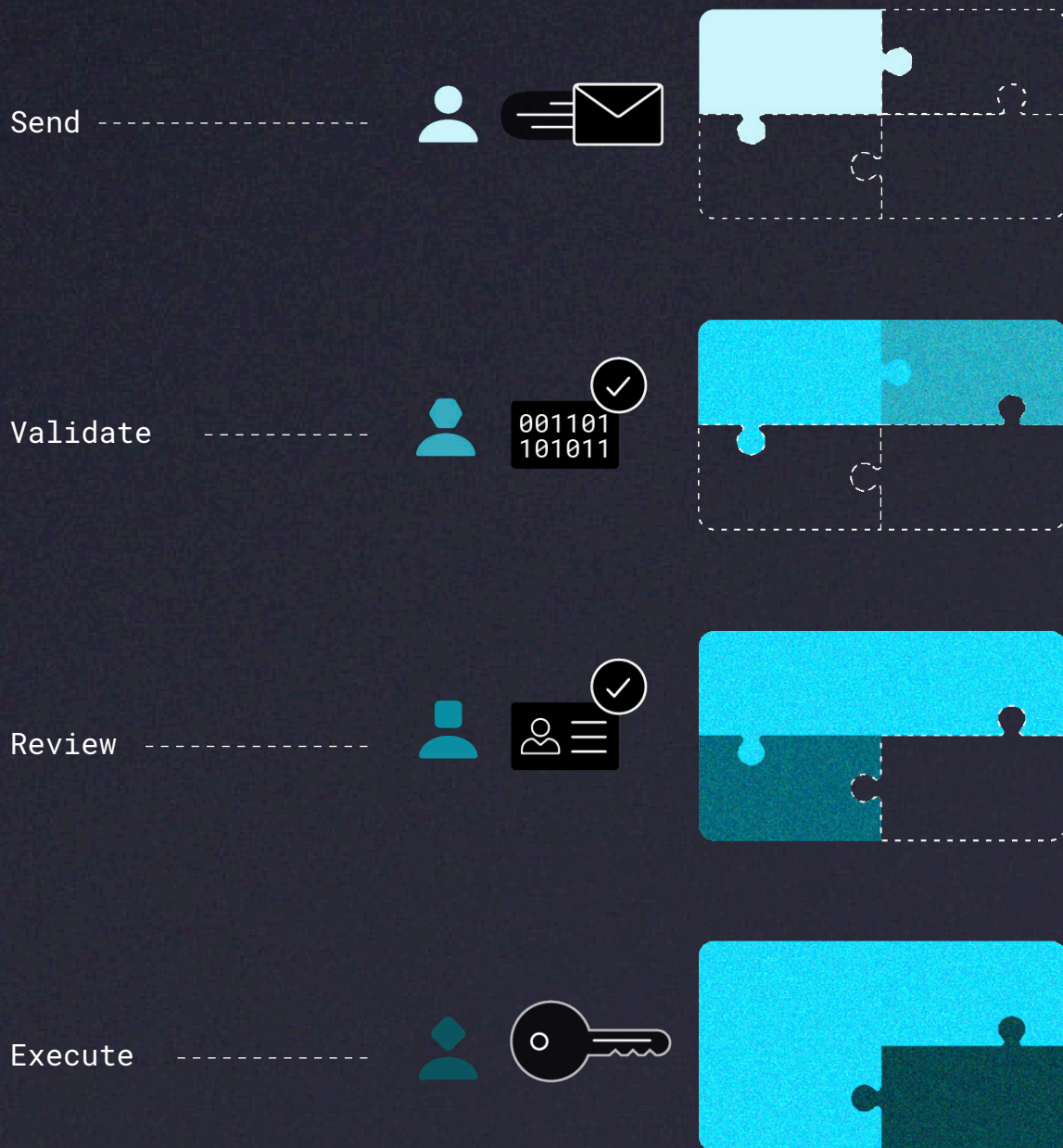
Governance and Controls 

Role-Based Permissioning 

Redundancy and Business Continuity 

Transparency and Proof of Controls 

Offline Storage Model



The minimum standard to call a custody system “offline” is currently a low one. Some may say a hardware wallet in a safe or a desk drawer is considered “offline.”

To be a truly “offline,” institutional-grade solution, there should be no networked or online component to the provider’s signing operations. All private keys should be stored in computing devices (for instance a hardware security module) from which private key information cannot be extracted or copied. Moreover, those devices should be kept inaccessible by personnel for any reason other than the execution of a customer’s transaction instructions. [See graphic: Role-based Permissioning]

To understand the security of a custody provider’s key-storing devices, which should ideally be stored in high security facilities—customers should ask how the physical storage locations operate and what access controls are in place. Customers might consider asking:

- **How does the provider ensure only authorized personnel gain entry to facilities?**
- **Are ID badge readers maintained by the provider or a third party?**
- **What type of biometrics (e.g. fingerprint), if any, are required to access physical sites and/or the devices storing keys?**

Even with answers to the above questions, the effectiveness of an offline model comes down to who does what, and what assurances are built into those processes.

Hardware security modules (HSMs)

Hardware security modules (HSMs) are physical computing devices that protect and store cryptographic secrets, including the private keys required for signing a transaction. The most secure HSMs meet U.S. Federal Information Processing Standard (FIPS) security ratings.

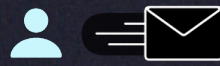
Unlike USB devices or other computing hardware, HSMs help protect against the copying of private key information. If an offline solution uses HSM devices, the cryptographic secrets on those HSMs cannot be extracted even if they’re retrieved from the system in an unauthorized way. This ensures no one can use or access the private key without the customer’s or provider’s knowledge.

If different components of a custody transaction are permissioned to separate personnel, no party has sole control of the full process. Since the raw ingredients of a transaction cannot be assembled by a single individual, there is no ability for one party to take arbitrary actions in isolation.

Role-Based Permissioning

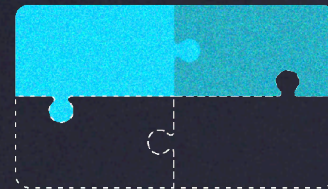
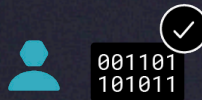
Customer

Customer sends digital instructions for a fund-moving transaction to their custody provider.



Role 1

Role 1 translates customer instructions into valid transactions on the network and verifies the *Issuance* of digital instructions. Once this is done, the instructions cannot be modified; any changes will result in the instructions being invalidated and the offline system rejecting the transaction request.



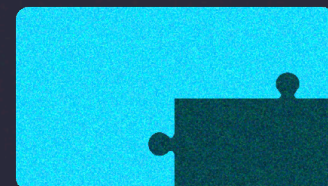
Role 2

Role 2 receives, *Reviews*, and approves the issued instructions. This second approval can apply additional checks on customer intent and identity as well as confirm network-level transaction details ahead of signing within the offline system.

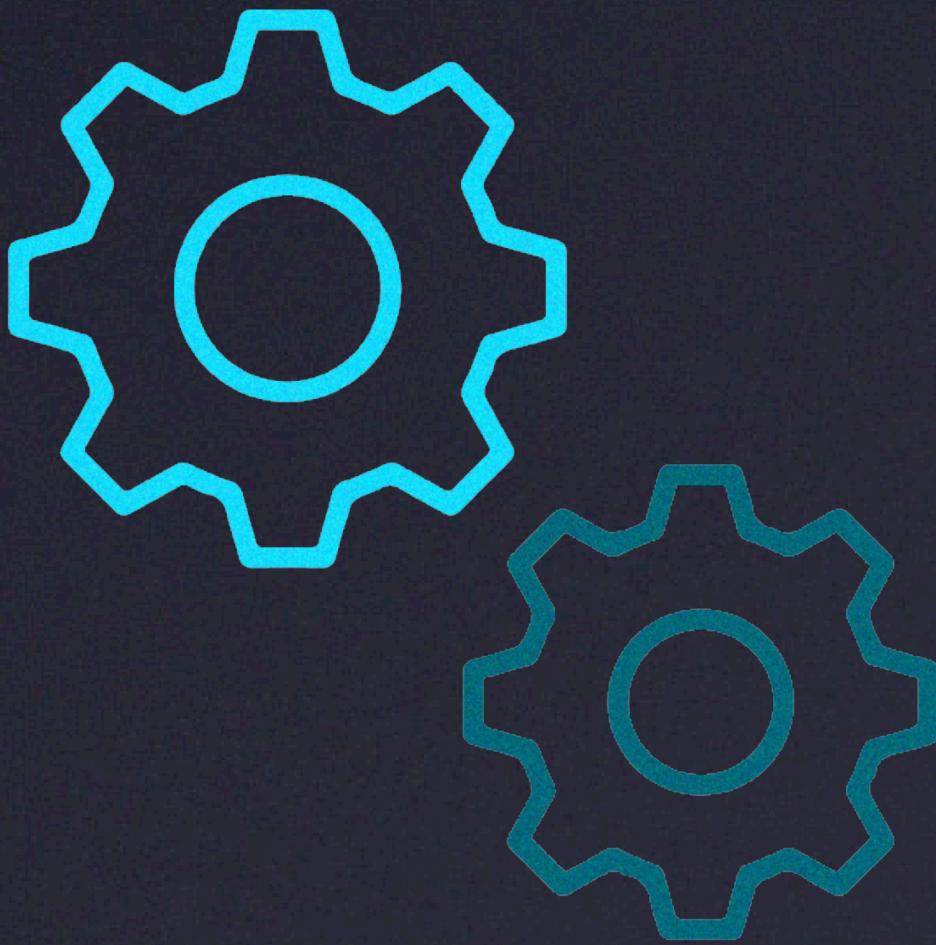


Role 3

Role 3 securely accesses the private keys to *Execute* the customer's instructions via signing (with no other knowledge of the transaction information).







Governance and Controls



It is not enough for a storage center to be offline; human governance and role separation controls must work together for effective security design. The instructions issuance process and governance controls are almost as important as how securely keys are stored.

The funds movement process for custodying digital assets needs to 1) be designed in a way that diffuses the level of control among parties and 2) ensure that no single party can take over or corrupt that process.

Third-party custody solutions providers must protect certain information about their governance architecture for security reasons, but there are minimum disclosures that customers should expect. At the very least, there should be:

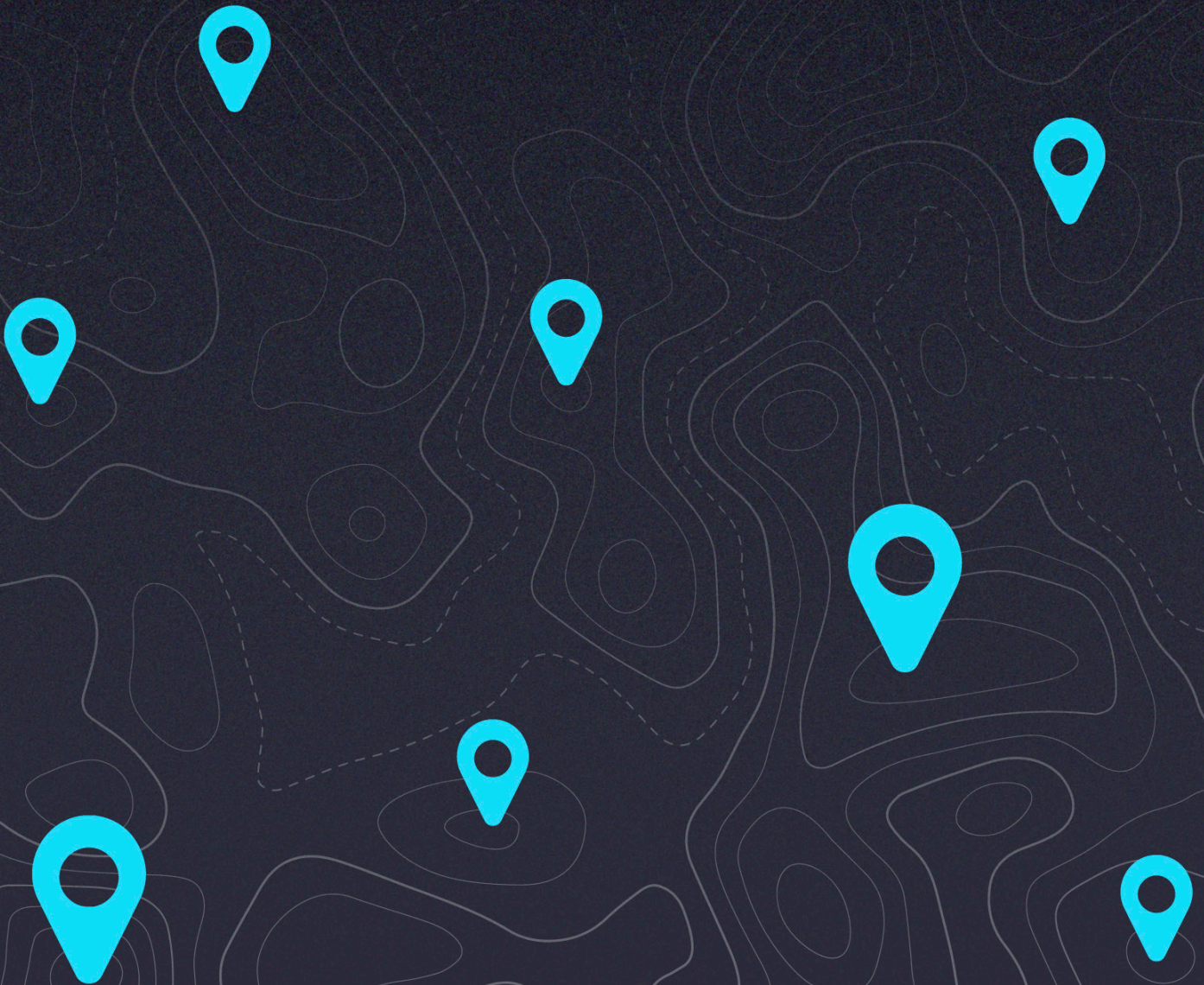
-  **No single points of failure** in their processes. Dual control should be required at as many steps in the funds movement workflow as possible, and it should take ideally three or more employees to effect fund movements. Company leadership should have no ability to move funds or make system changes in isolation.
-  **Data authentication** to verify the legitimacy of customer identity and customer instructions. Review processes that prevent the tampering of data or manipulation of instructions (and combine to provide an audit trail).
-  **Internal activity logging** that transcribes who does what and when, with broadcast mechanisms that rapidly notify personnel of critical actions in case the occurrences should be further scrutinized or challenged.
-  **Change management protocols** stating how many individuals it takes to operationalize the system and issue or execute system upgrades and other changes.

Controls also depend on the model a custody provider uses for key management, be it sharding (in which a single private key is split into different pieces that must be assembled for a transaction to execute), or multisignature, aka “multisig.”

A custody provider should be able to discuss how their signing model works and what protections they've built into the process. Since sharding poses the potential for a single private key to be assembled and thus permanently uncovered and exposed, institutional-grade systems tend to rely on a multisignature model.

In a multisig approach, there are N number of distinct, independent keys in existence, as opposed to one single key. Some quorum of M keys out of the larger set of N is required to sign a given transaction. M of N models for multisig follow best-practice security principles by requiring a minimum of two actors to move through the entire system, which reduces the potential of the system to be compromised.

Redundancy and Business Continuity



Maintaining multiple, redundant storage locations and geographically distributed backup sites is necessary for institutional custody providers.

Currently there is no best practice regarding a specific number of locations or overall site-management model, but having at least two layers of redundancy is important to maintaining operations in the event of natural disasters, power outages, or the destruction of property. Custody customers may have concerns about vulnerabilities or legal considerations in certain regions and jurisdictions; such customers can and should ask about the geographical distribution and protection of redundant sites and backup locations.

While custody providers must maintain confidentiality concerning the redundancy and durability of their locations, customers also shouldn't be afraid to ask tough questions about concentration risk and loss potential. (As a rough baseline, institutional-grade solutions providers should be able to maintain operations even if up to 50% of their system is lost.) If the backups exist in secured facilities, it adds confidence that the locations are subject to regular penetration tests and are leased based on guarantees of operational capacity. Backup sites or systems may function differently or not support all operations; additional scrutiny of secondary processes is appropriate. Customers might consider asking the following:

- **How much would have to happen in order for the system to be wiped out?**
- **What happens if there's a massive outage in a state or across an entire region?**
- **How much hardware could be lost before there was a loss of funds?**

Transparency and Proof of Controls



Visibility into custody services is more important to certain investors than others, depending on factors such as size of holdings, privacy preferences, and other variables. For some customers, it's important to have tools that allow them to easily access and view their holdings in order to confirm their provider is custodying what they claim.

For such customers, having segregated addresses is a required visibility feature proving a custody provider is managing customer funds. With segregated addresses, balances are publicly viewable and auditable "on chain," which allows customers to review transactions using block explorers at any time. Custody providers may also make monthly account statements available to help keep customers informed.

Beyond balance information, customers must decide for themselves how much transparency they expect when it comes to asset movement processes, audits, and system changes. Customers should consider how processes and activities are recorded and updated, who has access to that information, and what updates are communicated to customers.

Licensing is also a factor of consideration. We'll dive deeper in Part 3, but the licensing status of your provider may affect who audits what, and when. As the regulatory landscape for digital assets evolves, licensing and related compliance concerns may become more significant. Customers should ask providers how they expect their offerings and reporting tools will adapt as new compliance requirements take shape.

Considerations for Customers

Lawmakers and regulators may ultimately establish a broader set of legal and regulatory requirements to ensure safekeeping of digital assets by custody providers. But for the time being, it's largely cryptocurrency customers who must consider security, alongside other features and capabilities, in selecting a custody provider. Some of the chief considerations for customers today are summarized below.

In This Section

Considerations and Questions Worksheet 

Considerations	Questions
<p>Liquidity</p> <p>The speed at which customers want to access funds must be balanced with security concerns around transaction verification. Customers should ask if the same speed of liquidity is available to all account holders (regardless of holdings) or tiered only to certain asset-amount thresholds. If the SLA designates a minimum amount, for example, account holders may have a more difficult time withdrawing funds in the event price movements lower portfolio values.</p>	<ol style="list-style-type: none"> 1. If asset movement requests can be handled ultra fast, how “offline” is the system really—is the provider simply relying on on-site storage? 2. Are withdrawal requests subject to minimums?
<p>Scalability</p> <p>Institutional customers should consider how a custody solution can support users across activity levels, and rise to greater levels of volume over time.</p>	<ol style="list-style-type: none"> 1. Are there sub-accounting tools for multi-user accounts? 2. How does whitelisting work? How are new account holders verified, background-checked, and onboarded? 3. How do the risk parameters change as a customer’s usage of the system grows?
<p>Fees</p> <p>The prices charged by custody solutions providers vary widely across the market. Rather than seek out a solution based on sticker prices, customers are wise to consider how well a given solution meets their needs and how its price model aligns with the security, features, and value delivered. Many providers customize rates based on the scope of each customer’s needs, and all should be able to consult on how fee structures affect overall costs.</p>	<ol style="list-style-type: none"> 1. Are there minimum holdings required to custody assets? 2. Is there a set up fee? 3. How do the fees scale with usage?
<p>Leadership</p> <p>A company’s senior leaders should not have the ability to access or move funds. Asking about leadership’s role in system governance can help customers understand how a custody provider ensures there is no single point of failure in the security architecture.</p>	<ol style="list-style-type: none"> 1. Does the company’s leadership have any role in the movement of funds? 2. Can anyone change any of the governance processes in isolation?

Considerations	Questions
<p>Monitoring and Change Management</p> <p>A best-in-class system should be continually assessed and enhanced in a methodological way.</p>	<ol style="list-style-type: none"> 1. What mechanisms are in place for visiting sites and auditing equipment? 2. How are upgrades and staff rotations executed? 3. What controls are applied for the testing and certification of site-by-site performance?
<p>Licensing and Audits</p> <p>Many providers of crypto custody solutions operate without a license, which can leave customers with limited recourse in the event of unauthorized funds loss (while the provider continues operating). Even among licensed providers, there are key differences in terms of the type of license and granting jurisdiction. In our view, a New York State Department of Financial Services, regulated New York Trust company, is the gold standard, ensuring a more predictable, established statutory framework, and oversight by a well-informed banking regulator. Customers should ask who audits the company, and how often, and its approach to compliance generally.</p>	<ol style="list-style-type: none"> 1. Are you subject to capital reserve requirements and banking standards, and fiduciary duties to customers? 2. Are you audited by a reputable accounting firm?
<p>Insurance</p> <p>The insurance market for cryptocurrencies is highly limited today, with most insurance covering only offline (cold) storage (where less risk is posed) or online (hot) wallets but with very limited coverage. When it comes to institutional-grade custody solutions, even the most robust policies available to providers are limited in terms of amount and incidents covered. Customers should ask specific questions about insurance so as not to be oversold on the value of a provider's coverage.</p>	<ol style="list-style-type: none"> 1. Does the insurance cover offline storage or the online (hot) wallet? 2. Does the coverage address the wallets with the biggest amount of risk exposure? 3. How much of the underlying asset does your insurance cover in both offline and online storage? 4. If coverage is limited, how is it allocated in the event of a loss?

Future-Ready Custody

With cryptocurrencies fast maturing as an asset class, customers choosing a custody provider should think long-term about what the provider brings to the table.

Adapting to the future of the crypto industry will be necessary for all market participants. While no one knows exactly what the future will look like, several rising concerns are coming into focus.



Latency vs. Speed: SLAs, or the turnaround for executing customers' instructions, vary. Fast access to funds may be increasingly important for trading at low latency, but customers should not consider speedy liquidity to be their only option for needs-based use. For example, some providers can apply funds to your account for trading, while still completing the full verification and withdrawal process through offline mechanisms.



New Coins: More cryptocurrencies will continually be released and traded on exchanges, but not all funds movement procedures support the custodying of newly invented coins. Some solutions providers are more selective than others when it comes to which cryptocurrencies they support, so customers should be sure the strategies align.



Staking: Making money off the holding and storage of one's assets is already common to traditional banking. For some cryptocurrencies, "interest" takes the form of staking—an incentive structure which allows customers to earn tokens for investing in a given asset at a certain amount. Staking is still taking shape for institutional and individual crypto custody customers, but providers should be responsive to questions about this option.



Regulations: As legal and regulatory requirements for custody providers take shape, it may become even more important for custody customers to think twice before working with unlicensed or unaudited solutions providers. Custody is an evolving, iterative service, and those providers with a strong commitment to compliance and security will be best-positioned to serve customers today and in the future. For these reasons, customers should understand their custodian's viewpoint on legal and regulatory compliance.

At Gemini, our knowledge of digital asset custody has developed from the ground up. Cryptocurrency has matured significantly as an asset class since the first version of our custody product, and our offering has too. Over multiple iterations of our solution, we've continually gained and applied new learnings to our development processes and security architecture.

Gemini's unique position as a crypto-native company—and an early, ongoing innovator in blockchain and cryptocurrency infrastructure—is unmatched among our peers in traditional financial services. Our institutional-grade custody solution was designed and developed by leading technologists and security experts, and built to serve as a foundation for Gemini's entire business. Our team's deep expertise in global finance and regulatory compliance has informed every decision we've made to date, helping our solution rise to standards on par with the world's top financial institutions.

Gemini has operated from day one with a security-first mentality, and trust is our product. Providing customers confidence in the safety and protection of their assets—and meeting global compliance expectations now and in the future—is our company's top priority. As we build a bridge to the future of money, world-class custody is necessary infrastructure for all participants. We hope all custody customers select the right solutions for their needs.



To learn more about Gemini Custody, go to gemini.com/custody or email custody@gemini.com.



This content is for general informational purposes only, and should not be used as a substitute for consultation with appropriately licensed and qualified professional advisors.

© 2019 Gemini Trust Company, LLC.