

Institutional Custody in Crypto

May 2023



Table of Contents

Key Takeaways	2
Introduction	3
Institutional Custody 101	4
Institutional Custodian Industry Map	12
Institutional Custody Offerings	13
Key Themes to Watch	25
Conclusion	27

Key Takeaways

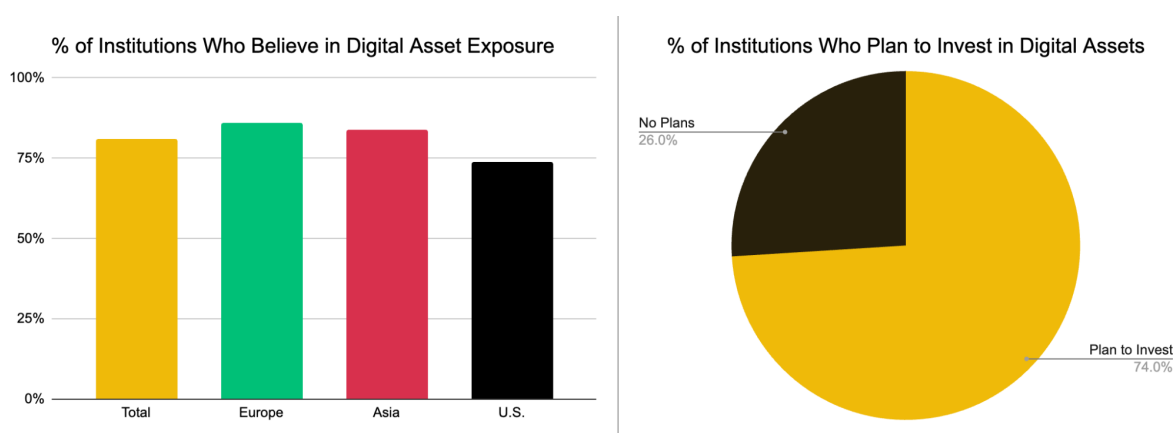
- ◆ Institutions are increasingly demanding exposure to the crypto asset class.
- ◆ By employing security, operational, and legal best practices, institutional custodians provide the peace of mind many institutions require to make an initial leap into crypto.
- ◆ There are three classifications of institutional custodians: custodians, custodial technology providers, and hybrid custodians.
- ◆ Unlike exchanges, institutional custodians are, first and foremost, focused on optimizing for asset security and protection.
- ◆ Institutional custodians are redefining what it means to be a crypto custodian by offering new, innovative custody solutions.
- ◆ Furthermore, institutional custodian offerings are not limited to custody but also include trading, staking, insurance, audit, escrow, accounting, and research offerings.
- ◆ Off-exchange settlement (“OES”) is a novel institutional custody offering that allows institutions to trade crypto assets at a convenience level similar to if their assets were on an exchange, without actually being on an exchange.
- ◆ Institutional custodians are evolving to provide similar offerings as prime brokerages.
- ◆ Crypto custody regulations are in their nascent stages but becoming clearer.
- ◆ Traditional financial custodians are beginning to enter the crypto custody space to compete with crypto-native custodians.

2 Introduction

Institutional custody is increasingly becoming a hot topic within crypto.

Over time, as crypto has grown in popularity and practicality, institutions have expressed a willingness to invest in the asset class. A global study from Fidelity that surveyed over 1,000 institutional investors across Europe, Asia, and the United States, revealed that 81% of institutions believe that crypto should be a part of an institutional portfolio. Furthermore, 74% of those institutional investors plan to invest in digital assets in the future.⁽¹⁾

Figure 1: Institutions are expressing a willingness to invest in digital assets



Source: Fidelity, Binance Research

This welcoming stance toward crypto has been driven by client demands and a desire to engage with the innovations of blockchain technology. As such, institutional-grade custodians have emerged to accommodate the anticipated flow of institutional capital into crypto.

Institutional custodians enter into a crypto ecosystem that hasn't always been accepting of custodial offerings. Many within the crypto ecosystem have regarded custodial offerings as risky and contradictory to the self-custodial and decentralized tenets of blockchain technology.

In response to these concerns, institutional custodians have been determined to differentiate themselves by redefining what it means to be a custodian within the crypto space. Now more than ever, institutional custodians are addressing public scrutiny by offering new, innovative custody solutions. Furthermore, they are evolving to cater to the diverse spectrum of institutions' risk preferences and investing styles.

In this report, we dive deeper into the institutional custody industry. More specifically, we break down what institutional custody entails, compare the current options available for institutions, and highlight future themes to watch as the industry matures.

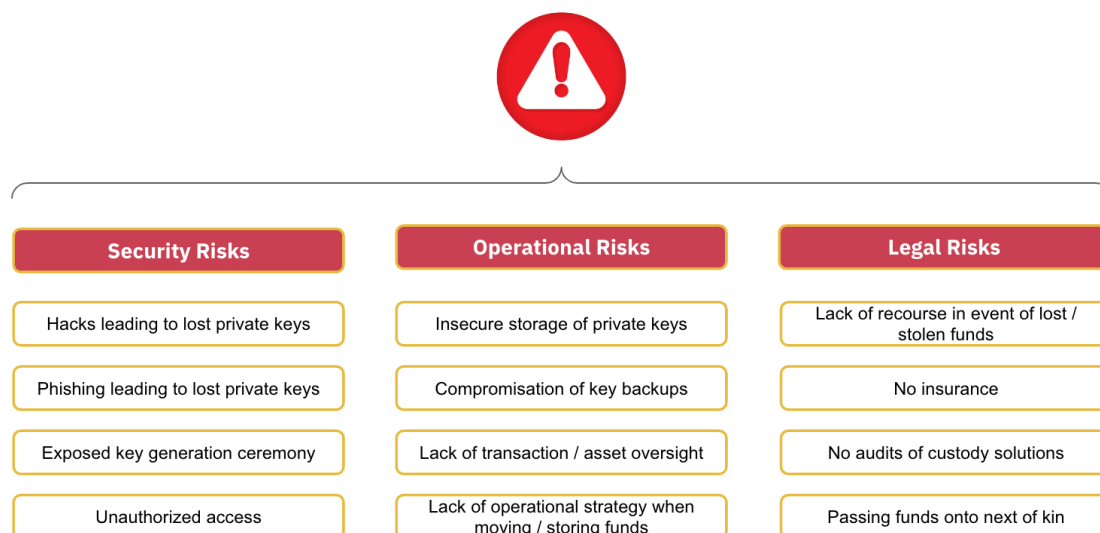
3 Institutional Custody 101

3.1 Why Is Institutional Custody Needed?

On January 3, 2009, the first block, or so-called “genesis block,” on the Bitcoin blockchain was mined by [Satoshi Nakamoto](#), Bitcoin’s pseudonymous creator. Embedded into the metadata of the genesis block was one short, text-based quote, which read “Chancellor on brink of second bailout for banks.” On the surface, the quote references the 2008 banking crisis that led many of the world’s largest custodians to lose their customers’ assets. Beneath the surface, the quote reveals one of the driving motivators behind the advent of blockchain technology; Satoshi envisioned a payment system that would not rely on centralized custodians but would allow users to self-custody their own assets.

The essence of self-custody is powerful, especially for individual investors, and can be further explored in our Binance Wallets report [here](#). However, as highlighted in **Figure 2**, **self-custody also comes with a number of security, operational, and legal risks.**

Figure 2: Risks associated with self-custody



Source: Binance Research

The risks associated with self-custody are amplified for institutions. The role of banks, government-linked companies, pension funds, sovereign wealth funds, hedge funds, private equity firms, endowments, family offices, or asset managers is to manage large

amounts of capital and serve as fiduciaries for their client's funds. In this way, institutions are accountable not only for their own assets but also for the assets of others. Furthermore, the capital that institutions are managing is often levels of magnitude greater than an individual investor. As a result, self-custody for institutions entails amplified and often intimidating security, operational, and legal risks.

Institutions can face these risks head-on and choose to self-custody in-house or distance themselves from these risks by outsourcing custody to an institutional custodian. Before deciding how to store crypto, institutions should be aware of the pros and cons associated with self-custody.

On the one hand, institutions can benefit from electing to self-custody. If institutions self-custody, they don't have to allocate money towards custodial services. Furthermore, they have complete control and privacy over their holdings. Lastly, they contribute to the self-custodial and decentralized tenets of blockchain technology. However, on the other hand, there are a number of cons associated with self-custody that institutions should consider.

Figure 3: Pros and cons for institutions considering self-custody

Pros +	Cons -
No money spent on custodial services* *if already have in-house capabilities and knowledge to self-custody	Amplified security, operational, legal risks
Direct control and access to funds	Lack of expert know-how on nuances and best practices of digital asset custody
Exclusive privacy over holdings and transactions	Miss out on exclusive custodian offerings and partnerships that can enhance custody and investing
Upholding the self-custodial and decentralized core tenets of blockchain technology	No insurance or disaster recovery. Maintain entire responsibility

Source: Binance Research

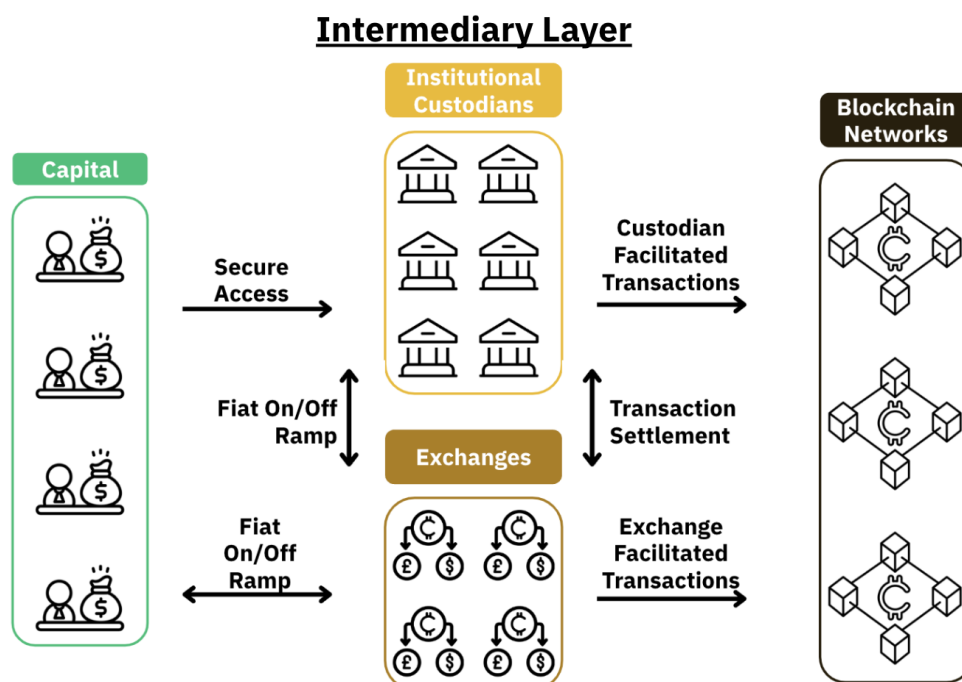
For certain institutions, the cons of self-custody will certainly outweigh the pros of self-custody. In this circumstance, institutions will often elect to utilize the services of an institutional custodian. Institutional custodians apply custodial best practices to manage institutional assets. Additionally, the institutional custodian may offer other exclusive

benefits, such as insurance, prime brokerage, and research, which the institution can use to enhance its custodial and investing practices. We elaborate on the offerings available to institutions in the **Institutional Custody Offerings** section.

3.2 The Role of Institutional Custodians in Crypto

For institutions that lack familiarity with the security, operational, and legal best practices of digital asset custody, an institutional custodian may provide the peace of mind needed to make an initial leap into investing in crypto. **In this way, institutional custodians play a vital role in attracting institutional capital to invest in the crypto asset class, which catalyzes the space's development and maturity.**

Figure 4: How institutional custodians are embedded into the crypto ecosystem



Source: Blockdata, Binance Research

Institutional custodians are embedded into the intermediary layer of the crypto ecosystem. For institutions wishing to deploy capital into crypto, their capital flows through this intermediary layer with crypto exchanges or institutional custodians.

Institutions can elect to onboard into crypto using an exchange's fiat on-ramp. In this case, the exchange maintains custody of the institutional capital. Additionally, the exchange is responsible for trading the institutional capital for crypto via a fiat on/off ramp.

Lastly, once the institution has cryptocurrency on the exchange, it can use that crypto to transact on blockchain networks. The exchange facilitates the execution of these transactions.

Conversely, institutions can elect to onboard into crypto through an institutional custodian. Onboarding through an institutional custodian will require the institution to allocate its funds to the custodian, which the custodian can then convert into the client's requested cryptocurrency via an exchange's fiat on-ramp. **Often, institutional custodians have well-defined settlement procedures, business relationships, and operational pipelines with exchanges, enabling them to fulfill most types of transactions their clients desire.** Institutional clients can then access their funds and initiate trades through a **secure access point** provided by their institutional custodian. Depending on the type of security and operational standards set forth by an institutional custodian, institutional clients will have to go through several credential verification checks, such as Know Your Business ("KYB"), Anti-Money-Laundering ("AML"), proof of incorporation, etc., before being able to access their funds.

“While exchanges and institutional custodians may have formidable relationships, it should be recognized that exchanges and institutional custodians play two very distinct roles within the crypto ecosystem.”

The primary services exchanges provide to the crypto ecosystem are their on/off-ramp and trading infrastructures. However, many **crypto exchanges additionally offer custody as an ancillary service to their users.** Custody services are almost an obligation of exchanges nowadays, mainly as remnants of the past; In the earliest days of crypto, there was a lack of custodial services. Exchanges filled this void so customers could have a place to hold and store crypto and hopefully trade on their platforms. Over time, cryptocurrency exchanges evolved into turnkey platforms offering both trading and custodial services.

While having custody and trading infrastructures in the same place may be convenient, it also makes exchanges attractive targets for hackers. In fact, a cumulative amount of nearly ~US\$3.45B has been stolen from crypto exchange custody from 48 recorded hacks since 2012.⁽²⁾ The most frequent way assets were stolen from exchanges was through hot-wallet hacks (29.4%), a type of hack that could likely be preventable by employing more secure custody techniques, such as storing customer assets in cold storage.⁽²⁾ While the top tier exchanges, such as [Binance](#) and [Coinbase](#), store their customer assets in cold storage, this is unfortunately not the case for all exchanges. Furthermore, verifying whether the exchanges truly adhere to cold storage remains challenging.

Figure 5: Over US\$3.45B in assets lost to over 48 different exchange hacks since 2012

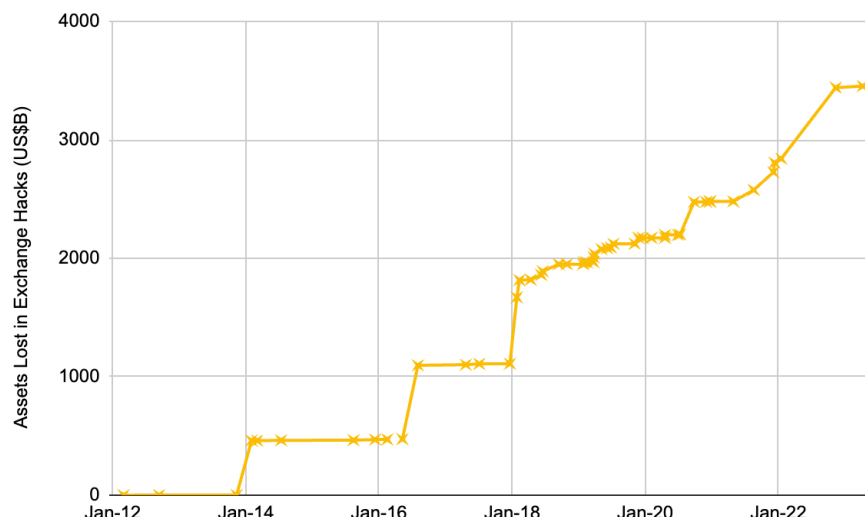
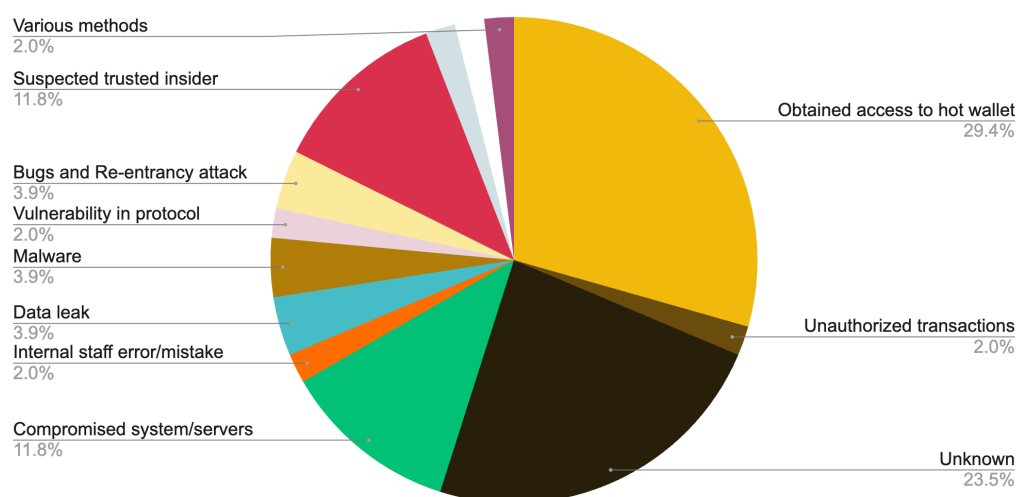


Figure 6: Over US\$3.45B in assets lost to over 48 different exchange hacks since 2012



Source: HedgeWithCrypto, Binance Research

Conversely, custody is the primary service institutional custodians provide to the crypto ecosystem. **Unlike exchanges, institutional custodians are, first and foremost, focused on optimizing for asset security and protection.** This prioritization of security often entails proven, battle-tested key-pair management, audits, operational and verification pipelines, and numerous other techniques. It also should be noted that a few institutional custodians are developing a novel custody technique called Off-Exchange Settlement (“OES”), which mimics the convenience of asset custody on an exchange while maintaining the level of security provided by an institutional custodian. We further explore offerings uniquely provided by institutional custodians in the **Custody Offerings** section.

3.3 Types of Institutional Custodians

There are three classifications of institutional custodians: custodians, custodial technology providers, and hybrid custodians. These classifications indicate the types of services the custodian can offer to institutions. In the following section, we explore each classification.



Custodians

A custodian is a third-party service provider that stores and manages an institution's private keys in a safe, accessible, protected, and often regulated manner.⁽³⁾ Crypto custodians provide custodianship via their own custody wallets, maintain control of and access to funds that lie with the custodian, and maintain a license as a trust company or crypto custody service. Custodians charge a fee for their offerings, typically based on a percentage of the assets under custody ("AUC").

Many countries have either established or are currently developing laws relating to crypto custodians. **Occasionally referred to as "qualified custodians," these are custodians that have been granted regulatory authority to hold a client's crypto.** Qualified custodians must comply with various security, accounting, and operational standards as set forth by their jurisdiction's regulations. Depending on the stringency of the regulatory environment, a qualified custodian may be considered as a safer option for institutions than a custodian who is not compliant with regulations. It should be noted that regulations relating to custodians in many jurisdictions are still nascent, a topic we discuss further in the **Key Themes to Watch** section.

Currently, custodians within the crypto space are distinguished from traditional finance ("TradFi") custodians in various ways.

Figure 7: Comparison of crypto custodians and TradFi custodians

	 Crypto Custodian	 Traditional Custodian
Asset Class	Cryptocurrencies, digital assets	Securities such as stocks, bonds, commodities such as precious metals, and currency (cash), domestic and foreign
Safeguarding Assets	Responsibility of the custodian lies with the safeguarding and control of a client's private keys and their backups	Custodians participate in central clearance and settlement systems, therefore custodians maintain records and custody ownership on behalf of clients
Settlement	Access to various blockchain networks for ultimate settlement	Access to global settlement systems and custodians.
Asset Services	Cryptocurrency trading, staking, yield farming, etc.	Collecting dividends and interest payments from securities.

Source: Blockdata, Binance Research

However, the divergence between crypto native custodians and TradFi custodians seems to be closing, as custodians within TradFi have begun to build out crypto custody offerings for interested institutions. We discuss this trend further in the **Key Themes to Watch** section.

Custodial Technology Provider

Unlike a custodian, a custodial technology provider does not manage clients' private keys. **Instead, custodial technology providers supply institutions with the underlying technology needed to build their own custody solutions.** In this way, custodial technology providers are not technically institutional custodians. However, their proprietary technology products enable the operation of institutional custody and should be mentioned here for completeness.

Custodial technology providers offer various products to institutions, including security infrastructure, asset transfer and settlement (e.g., access control systems & checks and balances for verifying transactions), and custody options (e.g., different types of wallets).⁽³⁾

Given that custodial technology providers don't maintain access to client funds, they are typically exempt from safeguards of regulatory requirements. In this way, offerings from custodial technology providers can entail more risk than those from a custodian who is compliant with a strict regulatory regime. Nevertheless, custodial technology providers still often take non-regulatory measures to safeguard the assets of institutional clients. These

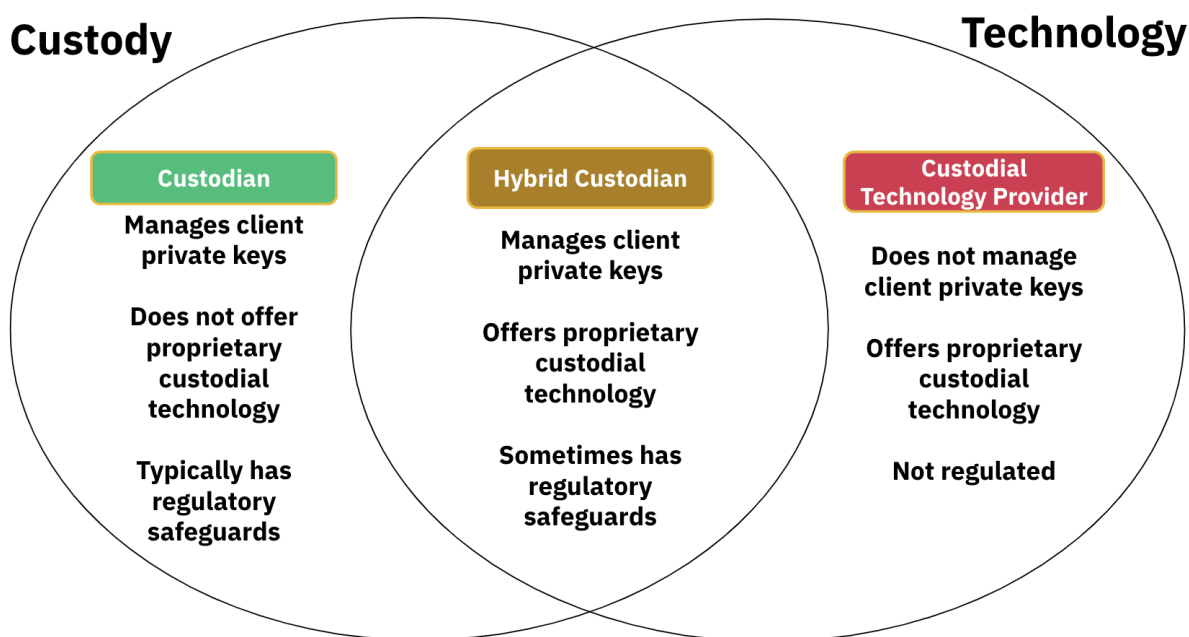
could come in the form of backup keys, disaster recovery mechanisms, and insurance policies.⁽³⁾

Hybrid Custodian

A hybrid custodian manages the private keys of institutional clients, like a custodian, but also services their clients with proprietary custodial technology, like a custodial technology provider. Hybrid custodians are perhaps the most flexible type of custodians.

Hybrid custodians offer a range of different offerings that span from completely custodial to completely self-custodial. They can customize their offerings to fit the needs of the institution they are working with. An institution that wants full custodial services can employ a hybrid custodian. Furthermore, an institution that wants to self-custody can also employ the proprietary technological offerings from a hybrid custodian. Some institutions may even fall in the middle of the spectrum and want a solution with both self-custodial and custodial aspects; hybrid custodians can customize their offerings to meet these preferences.

Figure 8: Custodian vs. hybrid custodian vs. custodial technology provider



Source: Binance Research

Institutional Custodian

Industry Map

Logo	Name	Type	Location	Date Founded
	Anchorage	Custodian	San Francisco, USA	2017
	Bitcoin Suisse	Custodian	Zug, Switzerland	2013
	BitGo	Hybrid	NYC, USA	2013
	Blockchain.com	Custodian	Luxembourg City, Luxembourg	2022
	BNY Mellon	Custodian	NYC, USA	2022
	Ceffu	Custodian	Vilnius, Lithuania	2021
	Coinbase	Custodian	NYC, USA	2012
	Copper	Hybrid	United Kingdom	2018
	Fidelity	Custodian	Boston, USA	2018
	Fireblocks	Custodial Technology Provider	NYC, USA	2018
	Gemini	Custodian	NYC, USA	2015
	Ledger	Custodial Technology Provider	Paris, France	2014
	NYDIG	Custodian	NYC, USA	2017

Source: Company Websites, Binance Research

Institutional Custody Offerings

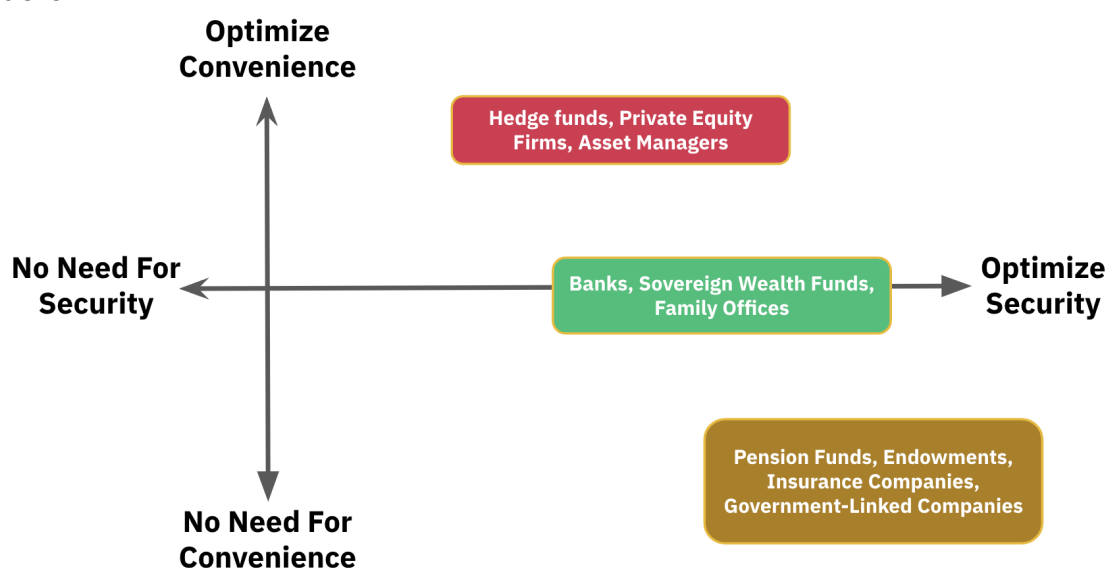
As briefly mentioned in the previous section, not all institutions will have the same custodial preferences; Different institutions have different levels of risk appetite and different investing styles. In our [Wallets: A Deep Dive into Crypto Custody](#) report, we introduced the *security vs. convenience trade-off*, which refers to the trade-off users typically face when deciding what crypto custody solution to use. Institutions face a similar trade-off when deciding how to custody their assets.

Institutional custodians tailor their custody offerings to meet the security and convenience preferences of their institutional clients. While institutional custodians will always have security as the top priority, it may be at different degrees depending on their client's preferences.

For institutions that employ buy-and-hold strategies and do not need to frequently trade their assets (e.g., pension funds, endowments, insurance companies), they will typically employ a custodial solution from an institutional custodian that optimizes for security over convenience. Some examples of custodial solutions that would apply to these cases are Ceffu's [Cold Storage](#) or BitGo's [Custodial Wallets](#).

For institutions that require the convenience of trading on-demand (e.g., high-frequency trading hedge funds, institutional investors, asset managers), they will typically employ a custodial solution from an institutional custodian that optimizes for convenience over security. Some examples of custodial solutions that would apply to these cases are [Ceffu's](#) or [Copper's](#) Off-Exchange-Settlement products.

Figure 9: Financial institutions' typical preferences on the security vs. convenience trade-off



Source: Blockdata, Binance Research

Over time, institutional custodians have developed different types of offerings to accommodate the diverse preferences of institutions. In this section, will explore the different types of offerings made available to institutions by institutional custodians.

5.1 Custody Offerings

Key Storage

A common misconception is that institutional custodians store the crypto assets of their clients. However, in reality, institutional custodians do not store their clients' assets but rather their clients' private keys. As we covered in our [Wallets](#) report, private keys provide cryptographic access to crypto assets, which are recorded and remain on a blockchain ledger.

Institutional custodians can store their institutional clients' private keys (and access to their assets) in three different ways: hot wallets, cold wallets, or warm wallets.

Figure 10: Wallets used by institutional custodians to store clients' private keys

	Hot Wallet	Cold Wallet	Warm Wallet
Internet Connection	Connected to the internet, so private keys required to access institutional funds are always online	Private keys are stored completely offline on a device that is not connected to the Internet.	The keys are held online, similar to a hot wallet.
Human Involvement	No human involvement is needed to execute transactions.	Human involvement is needed to sign each transaction, typically with some form of 2FA, pin, or biometric verification.	Human involvement is needed to sign each transaction, similar to a cold wallet.
Convenience	Since wallet is online, it can conveniently and quickly execute transactions.	Since wallet is offline, key signatures must be bridged online before executing transactions. This can be a slow process.	Similar to a hot wallet, users can conveniently and quickly execute transactions.
Security	Since wallet is online and no human involvement required to sign transactions, funds are susceptible to internet hacks.	Since wallet is not online and human involvement is required, funds are relatively more secure.	Safer than a hot wallet due to the requirement of human intervention, but keys are still online and susceptible
Use Cases	Used primarily by exchanges, rather than institutional custodians who prioritize asset protection	Corporate Treasury, Long-Term Investments, Majority of Funds	Trading, Sending Time Sensitive Transactions

Source: Binance Research

Institutional custodians tend to use cold wallets to store their clients' private keys since cold wallets are regarded as the most secure way to protect assets from being hacked. However, depending on the custodial preferences of the institution, institutional

custodians may also maintain a warm wallet, or more infrequently, a hot wallet, to allow their clients to sign transactions and make trades conveniently.

Governance Controls

Governance controls are verification measures established by institutional custodians to ensure that only authorized individuals are able to access the institution's private keys; Without governance controls, unauthorized individuals could possibly gain access to the institution's private keys and, in turn, be able to access the institution's assets.

The two primary governance controls used by institutional custodians are multi-signature ("multi-sig") and multi-party-computation ("MPC"). **Multi-sig and MPC distribute authority over private keys amongst a number of individuals. Doing so protects an institution's funds from the vulnerability of a single point of compromise.**

Figure 11 compares the two governance controls as well as a scenario in which there are no governance controls in place (i.e., single authority over private keys).

Figure 11: Wallets used by institutional custodians to store client's private keys

	Single	Multi-Sig	MPC
# of Approvals Required	Only one person is required to sign off on transactions using a singular private key	Require a quorum of users with multiple different private keys to sign off before executing a transaction (e.g. 2 of 3 signatures required)	A private key is split into shards and distributed amongst a number of users. A specific number of shards are required to execute a transaction
Single point of compromise?	Yes, if a unauthorized user gains access to the singular private key, they can access the institution's funds	No, the quorum of users serves to protect against a scenario in which one of the keys is lost to an authorized user	No, the shards of private keys serves to protect against a scenario in which one of the shards is lost to an authorized user
Protocol Agnostic	No, a private key will map only to a wallet on particular chain.	No, multi-sigs rely on smart contracts to function. Smart contract execution is not typically cross-protocol compatible.	MPC wallets are protocol agnostic
Operational Flexibility	No, one private key, one access	Once a multi-sig is deployed, the quorum threshold cannot be changed. This is operationally inflexible for institutions who may want to add signees.	Allows for continually fractioning of the private key and therefore modification of the operational threshold to sign transactions.

Source: Binance Research

Along with multi-sig and MPC, institutional custodians typically offer additional governance controls, summarized in **Figure 12**.

Figure 12: Additional governance controls offered by institutional custodians

Whitelisting	Transactions may only be sent to a list of whitelisted receiving address. Even if an unauthorized user gains control, they can only send transactions to the whitelist addresses.
2-Factor Authentication	Before a transaction is sent out, a login is required from an alternative approved device. Even if an unauthorized user gains control, they will only be able to send a transaction if a trusted device approves.
Time Locks	Assets cannot be moved until a specified point in time. Even if an unauthorized user gains control, they will only be able to send a transaction if it is within a known time as set out by the institution.
Geographic Distribution	Private keys used in a multi-sig or shards used in an MPC are geographically distributed. This removes any single geographic point of compromise.
Hardware Distribution	Zero-trust hardware architecture in which private keys / shards are stored in air-gapped Federal Information Processing Standard (FIPS) devices. This removes any hardware points of compromise.

Source: Binance Research

5.2 Trading and Asset Offerings

Most institutions will require the ability to trade and leverage their assets while those assets remain in institutional custody. If institutional custodians don't have the ability to trade or leverage their assets, they would be put at a performative disadvantage; large amounts of capital would sit in the wallets of institutional custodians without being able to capture market opportunities, earn yield, or hedge against losses. As such, **institutional custodians have developed a range of trading and asset offerings to allow their clients to maintain strong financial performance while simultaneously safeguarding against the compromise of private keys and assets.**

Off-Exchange Settlement

Off-Exchange Settlement ("OES") is perhaps one of the best examples of a safeguarded trading offering.

As previously recognized in the **Institutional Custody 101** section, exchanges are important because they allow institutions to trade their crypto assets conveniently. However, over time, exchanges have been known to lose the assets on their platform due to hacks and improper custody techniques.

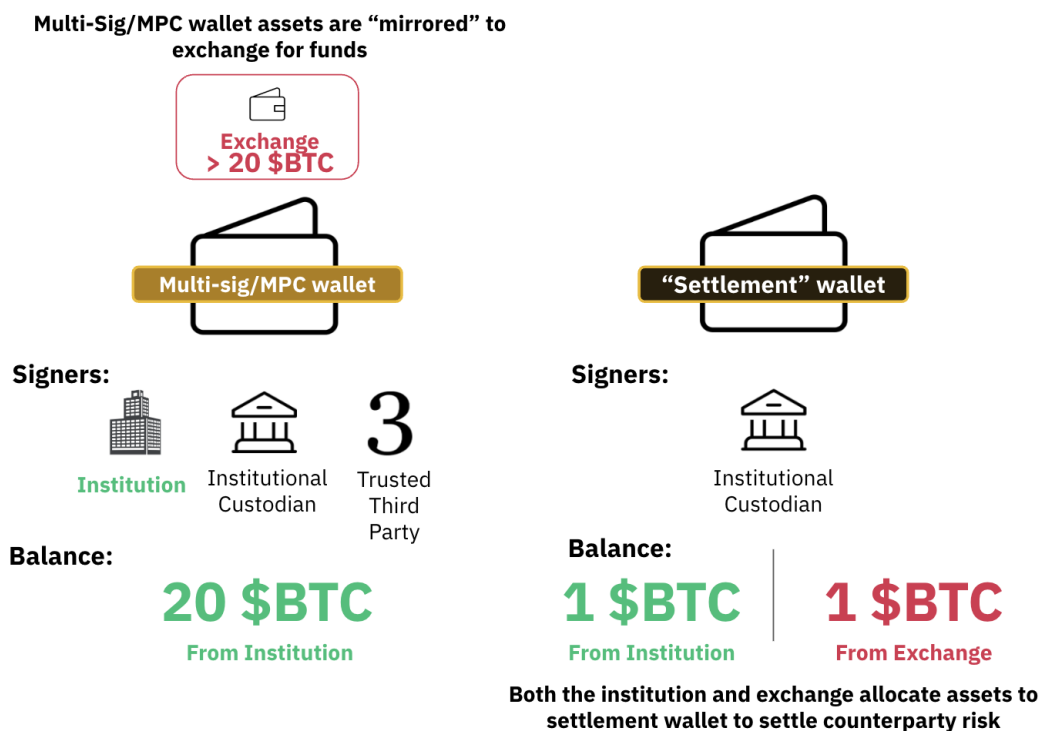
OES allows institutions to trade crypto assets at a convenience level similar to if their assets were on an exchange, without their assets ever actually being on an exchange.

So how does this work? OES follows three basic steps:

1. An institution keeps its assets with an institutional custodian.
2. The custodian locks the majority of an institution's funds in a multi-sig/MPC wallet sanctioned by a quorum of signers (2 of 3 signees are required to commit transactions. Signers include the institution, the custodian, and a trusted third party).
3. A crypto exchange provides the institution with a reflection of those funds on its platform to trade with based on the amount of assets they have locked in the multi-sig/MPC wallet. Effectively, this allows the institution to safely store its assets in an off-exchange with a custodian while also being afforded the same convenience as if their funds were actually on the exchange.

Operationally, OES entails a number of checks and balances to minimize counterparty risk between the institution, exchange, and custodian. *It should be noted that institutional custodians can implement OES in several different ways. The following description provides one example of how OES may be implemented.

Figure 13: OES reduces counterparty risk between institution, exchange, and custodian



Source: Binance Research

First, OES uses a “settlement wallet” in addition to the multi-sig/MPC wallet to continuously settle the institution’s profits and losses with the exchange. The settlement wallet, as shown in **Figure 13**, is managed by the institutional custodian and includes funds contributed from the institution as well the exchange. If the institution profits from a trade using the exchange’s margin, the institutional custodian will send a correlating amount of assets from the exchange’s contribution in the settlement wallet to the multi-sig/MPC wallet. If the institution loses on a trade using the exchange’s margin, the institution will send a correlating amount of assets from the institution’s contribution in the settlement wallet to the exchange.

If either the institution or the exchange’s contribution to the settlement wallet falls under adequate settlement levels, the institutional custodian will request the institution or the exchange to contribute more to the settlement wallet. In the normal course of business, the institution and custodian would respond to this notification by contributing more funds.

However, if the exchange fails to contribute to the settlement wallet, the institutional custodian will notify the institution to close out their positions and return the remaining exchange balance to the multi-sig/MPC wallet. In this way, even if the exchange goes bankrupt, it would not be able to lose the institution’s assets. In 2022, this exact scenario occurred; an exchange with institutional clients using OES went bankrupt, yet none of the institutions using OES suffered any losses.⁽⁴⁾






Conversely, suppose the institution fails to contribute to the settlement wallet and the exchange does not have time to liquidate the client’s positions. In this case, the custodian and trusted third party can transfer the assets from the multi-sig/MPC wallet to an exchange wallet.

Second, quorum signers on the multi-sig/MPC wallet ensure that if any of the signers lose their private key, two of the other signers can still rescue the institution’s funds.

There have been cases where both institutions and their institutional custodians have been hacked and lost their private keys. The trusted third party can provide greater assurance that the institution’s funds will be protected even in worst-case scenarios. For this reason, a trusted third party should be knowledgeable and independent, operationally capable, and regulated.⁽⁴⁾ If the trusted third party is malicious or incompetent, they could become a source of compromise.

OES is a relatively new innovation in the custody space. **Currently, only a handful of institutional custodians have operational infrastructure and relationships with exchanges in place to offer OES to institutional clients.** Two standout examples of institutional custodians who offer OES are [Ceffu](#), the institutional custody & OES partner for Binance, and [Copper](#), which also provides OES for other lower-volume exchanges.

Figure 14: Institutional custodians offering OES

Logo	OES Offering Name	Exchanges	Link
 BitGo	BitGo Network	Bitstamp, Enclave Markets, Gate.io, INX	https://www.bitgo.com/products/bitgo-network
 CEFFU	Ceffu Mirror	Binance	https://www.ceffu.com/mirror
 cobo	Cobo Superloop	Bit.com, Deribit, Pionex	https://www.cobo.com/superloop
 copper	Copper Clearloop	Bitstamp, Bitfinex, Deribit, Gate.io, OKX, Powertrade, others	https://copper.co/products/clearloop
 zodia	Zodia Interchange	Unknown	https://zodia.io/services/

Source: Company Websites, Binance Research

Although OES is still in its nascent stages, it has the potential to be transformative for the custody industry, as it can significantly reduce counterparty risk between institutions, exchanges, and custodians.

“We believe the [OES] approach allows for structural redesign of counterparty risk models in the digital assets space, taking the best lessons from traditional finance models and enhancing them with the crypto-native tools, thus paving the way for increased participation of institutional capital.”⁽⁴⁾

– Nickel Digital Asset Management

Decentralized Exchanges and dApps

Beyond centralized exchange offerings, some institutional custodians are also allowing their institutional clients to trade on [decentralized exchanges](#) and leverage their assets on a catalog of [decentralized applications](#) (“dApps”), all while segregated custodial environments safeguard their assets.

This offering is particularly unique, given that in the past, to trade on a decentralized exchange or interact with dApps, institutions have had to use self-custodial hot wallets, which are prone to numerous different risks. For example, an institution may use a self-custodial hot wallet to trade through a [smart contract](#) on a decentralized exchange. On the surface, the decentralized exchange seems non-malicious. However, embedded into the smart contract's code of the decentralized exchange may be malicious functions, which could siphon the funds within the self-custodial wallet instantaneously or sometime in the future. Unknowingly, the institution could effectively compromise its own wallet by interacting with the malicious smart contract of the decentralized exchange.

Institutional custodian decentralized exchange and dApp offerings mitigate the risks of interacting with malicious smart contracts of decentralized exchanges. For example, Fireblocks' [Institutional DeFi](#) product and Copper's [DeFi Vault](#) allow institutions to set permissions, transaction thresholds, and whitelists on the smart contracts their wallets interact with. Furthermore, DeFi Vault also allows institutions to set a timeframe in which smart contracts can be approved to interface with their institution's wallet. After that point, the connection between the institution's wallet and the smart contract is relinquished, thus limiting the risks of malicious smart contracts in the long term.

Native Staking

[Proof-of-stake](#) ("PoS") networks typically reward users with crypto-denominated yields if they "stake" or lock up their crypto assets. Staking is attractive for users, as it allows them to leverage their assets and earn a passive revenue stream (currently ranging from 5-8% on Ethereum) instead of letting their assets sit idle.⁽⁵⁾ However, to earn these yields, users have to run their own validator or contribute to a dApp [staking pool](#). Running a validator or contributing to a staking pool can be complex and comes with numerous risks, including custody risks if the user's private keys are stored on hot wallets and exposed to the internet.

Some institutional custodians are offering institutions the ability to earn PoS yields without the complexity of staking while their assets are safeguarded in institutional custodian, cold-storage wallets.

BitGo's [Staking](#) offering is a good example of such an offering. At the time of writing, BitGo offers PoS yields on 14 cryptocurrencies. Institutions simply select the assets they wish to stake. Next, BitGo handles the delegation and provision of staked assets amongst numerous validators so that the institution can maximize staking uptime, reduce [slashing](#) risk, and earn more rewards.

OTC and Escrow

Institutional custodians also offer the ability to trade off-exchange completely through over-the-counter (“OTC”) and escrow offerings.

For example, Fireblocks’s [Digital Asset Transfer Network](#) allows institutions onboarded to the Fireblocks’ network to trade OTC with each other, with instant settlement, rebalancing, and in-platform payments infrastructure.

Furthermore, Ceffu’s [escrow](#) service allows institutions to create esoteric transactions. For example, an institution can use Ceffu’s escrow services to pay parts of the total agreed amount defined in an escrow agreement to a merchant. The institution’s assets will only be transferred to the merchant when the merchant reaches specific milestones. Another example could include an institution using Ceffu’s escrow services to manage the allocation of its treasury. Treasury assets would be locked in Ceffu cold storage and would only be distributed once the release schedule in the escrow agreement establishes that it is time to do so.

5.3 Insurance, Audits, and Monitoring Offerings







Alongside **Custody Offerings**, institutional custodians also provide insurance, audits, and transaction monitoring as supplementary security offerings. These mainly serve to provide clients with peace of mind that their assets are safe within institutional custody.

Insurance

Many institutional custodians back up their custodial services with insurance. While a great deal of custody risk can be minimized by an institutional custodian’s technological and operational security measures, there could still be worst-case scenarios in which those measures fail. Insurance serves as a backstop and a final hedge against potential losses for an institution’s assets.

Over time, insurance has become an industry standard. Typically, institutional custodians will work with insurance brokers who evaluate their risk profile, create an insurance policy based on their risk profile, and find underwriters who will pay insurance to the clients in case of a claim. As cryptocurrencies are a relatively new asset class, most institutional custodians have bespoke insurance policies covering very specific claims.⁽³⁾

Figure 15: Selection of institutional custodians offering insurance

Logo	Name	Insurance Amount (M)	Claims Covered	Price of Insurance	Insured By
	Anchorage	Undisclosed	Crime insurance policy, hot and cold storage	Unknown	Aon
	BitGo	\$250	Loss, theft, misuse in situations that BitGo holds keys	Unknown	Lloyd's Syndicate
	Ceffu	Undisclosed	Cold storage	Free	Lloyd's Syndicate
	Coinbase Custody	\$320	Across platform, Crime Insurance	Unknown	Lloyd's Syndicate
	Copper	\$500	Employee collusion, theft, loss or damage of keys	Unknown	Aon
	Fireblocks	\$30	Storage, transfer, and E&O	Extra cost	Aon
	Gemini Custody	\$75	Cold storage, Crime Insurance	Unknown	Marsh and Aon

Source: Company Websites, Binance Research

It should be recognized that in some cases, not all coverage is equal, and it also depends on the custodian's architecture options (how they use hot/cold wallets). Institutions should be aware that this can cause some **potential coverage gaps**.

“A custodian may have crime insurance to cover only assets ‘in-flight,’ focusing on hot wallet holdings over cold storage. Another may have specific insurance that covers assets ‘at rest’ in cold storage, but this doesn’t cover third-party hacks or losses due to compromised key generation or transaction processes. In other words, when a custodian forces a trade-off between security and usability, the insurance reflects that risk variation.”⁽³⁾

– Anchorage Digital

Audits

In most regulatory regimes, custodians are subject to annual audits. These audits are conducted by a third-party auditor and are used to verify how effective a custodian's systems are (security, privacy, availability, etc.).⁽³⁾ **Audits serve an important purpose in verifying that an institutional custodian has the financial or technological capacity to adequately manage an institution's assets.**

The most common audit for a custodian is a System and Organization Controls ("SOC") audit. SOC is a framework provided by the American Institute of Certified Public Accountants ("AICPA"), a regulatory body in the United States responsible for accounting and finance certification. SOC audits come in various forms, with SOC 1 and SOC2 being the most common.⁽³⁾

Figure 16: SOC 1 vs. SOC 2 audits

	SOC 1	SOC 2
Main Focus	Financial Controls	Data and Security Controls
Investigates	Security of the organization's financial set-up	Security of organizational systems and data protection mechanisms
Verifies	Internal Financial Statements	Security, Availability, Processing Integrity, Confidentiality, Privacy
Application	Companies that impact their client's financial statements	Companies that store privacy and sensitive data
Goal	Prevent cascading financial inefficiencies	Prevent hacks and incorrect information

Source: Blockdata, Binance Research

Type 1 SOC audits are a one-time snapshot analysis, whereas Type 2 SOC audits look at performance over an extended period (usually 12 months).⁽³⁾

Aside from SOC 1 and SOC 2 audits, there are a few other audits that institutional custodians use to verify their operational capacity.

Figure 17: Other audits performed on institutional custodians

SOC 3	Essentially the same as a SOC 2 audit, however, SOC 3 are intended for public use
ISO 27001	International standard on how to manage information security
ISAE 3402	International assurance standard that provides assurance that a custodial has adequate internal controls
ISAE 3000	International standard for assurance over non-financial information
CCSS-QSP	CCSS is designed to augment standard information security practices and complement existing standards such as SOC2 Type II, ISO 27001, and other standards.

Source: Blockdata, Binance Research

An interesting innovation in the context of audits has been the introduction of [proof of reserves](#) (“POR”). POR blockchain-based proof reveals that a custodian is holding the correct amount of cryptocurrency assets of their clients on-chain. In turn, POR illustrates that the custodian isn’t using their client’s assets for ambiguous, potentially malicious purposes. The true innovation of POR lies in the fact that POR proofs do not need to be verified by a third-party auditor but can be verified independently and in real time by users via the blockchain.

POR is primarily applicable for custodial exchanges to ensure that assets held by the exchange in its numerous on-chain wallets are in tandem with the assets listed on its balance sheet. POR isn’t as relevant for institutional custodians, given that institutional custodians will not mix the assets of multiple clients in one wallet. Instead, institutions provide clients with on-chain addresses that represent the clients stored in institutional custodian cold storage, which are isolated from the assets of other clients.

5.4 Other Offerings

Accounting

Accounting for crypto-related holdings and transactions is still a relatively nascent field requiring specialized expertise. Some institutional custodians have built-in reporting tools to support institutions’ back-office teams in accounting.

Research

Many institutional custodians offer in-house custody and trading research to their institutional clients. This research creates a dialogue with their clients and encourages institutions to engage with different custody and trading offerings.

6 Key Themes to Watch

In the following section, we highlight some key themes to watch as the institutional custody industry matures.

6.1 Trading and Asset Offerings

Institutional custodians are starting to look like TradFi prime brokerages. Institutional custodian offerings are no longer limited to custody but include numerous trading and asset offerings such as OES, OTC trading, PoS staking, escrow, borrowing & lending, and others. Providing prime brokerage-like offerings is also supported by institutions. From a 2022 [survey](#), 72% of institutions said they would like an integrated provider for all crypto needs.⁽⁶⁾ Over time, as crypto becomes more financialized and institutions develop more ways to leverage this new asset class, institutional custodians will increasingly need to provide prime brokerage-like offerings and meet demand head-on.

6.2 Regulations

Institutional custody regulations are evolving in many geographic jurisdictions.

Most recently, on May 16, 2023, the European Union's Markets in Crypto Assets ("MiCA") regulation was unanimously approved, serving as the first major jurisdiction in the world with a crypto licensing regime. MiCA includes rules on the custody and administration of crypto-assets. On the one hand, MiCA takes a page from the rulebook of existing client asset rules, demanding that institutional custodians keep a register of positions and segregate holdings of assets. Additionally, MiCA adds new, explicit requirements for crypto institutional custodians, including crypto-custodian-specific custody agreements and policies, requirements to record any event likely to alter the client's assets (e.g., blockchain hard forks), and liability thresholds.⁽⁸⁾

Over time, other geographic jurisdictions and regulatory bodies will offer clarity on institutional custody regulations. This is a critical theme to watch as many institutional investors are demanding regulatory clarity before allocating their assets to institutional custodians. In fact, a recent May 2023 [survey](#) from Coinbase showed that 78% of

institutions said they wanted clarity from regulators about how digital assets are classified or treated. More specifically, 65% of institutions reported wanting clear regulations around custodial obligations.⁽⁷⁾

6.3 TradFi to Compete

As regulatory environments are becoming clearer and institutional clients are demanding exposure to crypto assets, traditional TradFi custodians have begun offering crypto custody.

In 2022, America's oldest traditional bank, BNY Mellon, launched its digital asset custody program. BNY Mellon cited institutional demand and a willingness to engage with innovation as drivers of their program launch.⁽⁹⁾ In the future, TradFi custodians like BNY Mellon will continue to enter the institutional custody space. Crypto-native custodians will have to compete with traditional custodians' established reputations and, typically, outcompeting assets under management.

Furthermore, from a 2022 [survey](#), it appears that institutions prefer TradFi custodians. 63% of institutions said they are only comfortable trading crypto assets with highly rated traditional custodians. This 63% also said they would accept longer settlement times to deal with a highly rated traditional custodian. Lastly, 70% of institutions said they would increase their crypto trading if they could execute with a highly-rated financial institution.⁽¹⁰⁾

6.4 Account Abstraction

Lastly, as discussed in Binance's [Wallets](#) Report, account abstraction – or [EIP-4337](#) – is radically changing how we think about custody in crypto. Account abstraction “abstracts” from the restrained architecture of traditional crypto wallet accounts and allows wallet accounts to become arbitrarily programmable. As a result, the user experience of crypto custody can become a lot more friendly and customizable. **As account abstraction becomes more widely ingrained into different custodial solutions, institutional custodians will be able to offer innovative custody offerings such as social private key recovery, multi-call transactions, quantum-resistant signature algorithms, subsidized transaction fees, and more.**

7 Conclusion

The institutional custody industry is rapidly evolving, attempting to keep pace with eager demands from institutions seeking exposure to the crypto asset class. Institutional custodians are creating innovative custodial, asset, insurance, audit, and other offerings tailored to institutions' preferences. Institutional custodians are redefining what it means to be a custodian within the crypto space.

As awareness of blockchain technology and cryptocurrencies grows, the role of institutional custodians becomes increasingly essential; Institutions will continue to look for solutions that ensure the safety of their assets. Furthermore, they will want to engage with the innovations of blockchain technology and gain exposure to the crypto asset class. Institutional custodians will be vital in offering the peace of mind many institutions require to invest in crypto. Ultimately, institutional capital and their custodial counterparts will help blockchain technology to mature, develop, and achieve real-world product market fit.

References

- 1) https://www.fidelitydigitalassets.com/sites/default/files/documents/2022_Institutional_Investor_Digital_Assets_Study.pdf
- 2) <https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/>
- 3) <https://download.blockdata.tech/BLOCKDATA-Crypto-Custody-The-Gateway-to-Institutional-Adoption-VF.pdf>
- 4) https://medium.com/@Nickel_Digital/off-exchange-settlement-215d77205e8b
- 5) <https://www.stakingrewards.com/earn/ethereum-2-0/>
- 6) https://www.bnymellon.com/content/dam/bnymellon/documents/pdf/insights/migration-digital-assets-survey.pdf?mkt_tok=MzUzLUhSQi03OTIAAAGLVmgcX3soXqYxNZbebc1V5wCBRV2xYtTMCVtqGhBtyrNeVqFA8KYh1v9QJrfH0GxP3IyUfMZ7-tka8iCzan4bWRJbWB-WFqViNeCZAWY-
- 7) <https://www.coinbase.com/blog/institutional-investors-to-regulators-we-need-clarity-on-digital-assets>
- 8) <https://www.lexology.com/library/detail.aspx?g=e39134f3-c5bd-40a0-ba56-4f71852b6138>
- 9) <https://www.bnymellon.com/us/en/about-us/newsroom/press-release/bny-mellon-launches-new-digital-asset-custody-platform-130305.html>
- 10) <https://www.bnymellon.com/content/dam/bnymellon/documents/pdf/insights/migration-digital-assets-survey.pdf>

New Binance Research Reports



BRC-20 Tokens: A Primer

A close look at the BRC-20 market, including their origins, market outlook, effects on Bitcoin's metrics, and much more



Data Insights: Lending

A data-driven analysis of the growing DeFi lending market



Monthly Market Insights: May 2023

A summary of the most important market developments, interesting charts, and upcoming events



AI x Crypto: Exploring Use Cases and Possibilities

Exploring the intersection of AI and crypto

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to, the crypto ecosystem, blockchain technologies, and the latest market themes.



Mac Naggar

Mac is currently working for Binance on their Macro Research team. Prior to joining Binance, he worked as a Web3 Product Manager for HSBC's Global Ventures, Innovation, and Partnerships team. Additionally, Mac has had experience on the trading side, spending time with Morgan Stanley's Fixed Income Division, Algorand's Capital Markets Team, and CrossTower's Digital Assets Trading Desk. Mac is a recent graduate of Cornell University and currently a Master of Science student at the University of Nicosia, where he specializes in Blockchain & Digital currencies. His sector interests primarily lie in Blockchain Design & Interoperability, DeFi, DeSo, and Institutional Adoption.

Resources



Read more [here](#)



Share your feedback [here](#)

General Disclosure: This material is prepared by Binance Research and is not intended to be relied upon as a forecast or investment advice and is not a recommendation, offer, or solicitation to buy or sell any securities, cryptocurrencies, or to adopt any investment strategy. The use of terminology and the views expressed are intended to promote understanding and the responsible development of the sector and should not be interpreted as definitive legal views or those of Binance. The opinions expressed are as of the date shown above and are the opinions of the writer; they may change as subsequent conditions vary. The information and opinions contained in this material are derived from proprietary and non-proprietary sources deemed by Binance Research to be reliable, are not necessarily all-inclusive, and are not guaranteed accurate. As such, no warranty of accuracy or reliability is given, and no responsibility arising in any other way for errors and omissions (including responsibility to any person by reason of negligence) is accepted by Binance. This material may contain 'forward-looking' information that is not purely historical in nature. Such information may include, among other things, projections and forecasts. There is no guarantee that any forecasts made will come to pass. Reliance upon information in this material is at the sole discretion of the reader. This material is intended for information purposes only and does not constitute investment advice or an offer or solicitation to purchase or sell in any securities, cryptocurrencies, or any investment strategy, nor shall any securities or cryptocurrency be offered or sold to any person in any jurisdiction in which an offer, solicitation, purchase or sale would be unlawful under the laws of such jurisdiction. Investment involves risks.