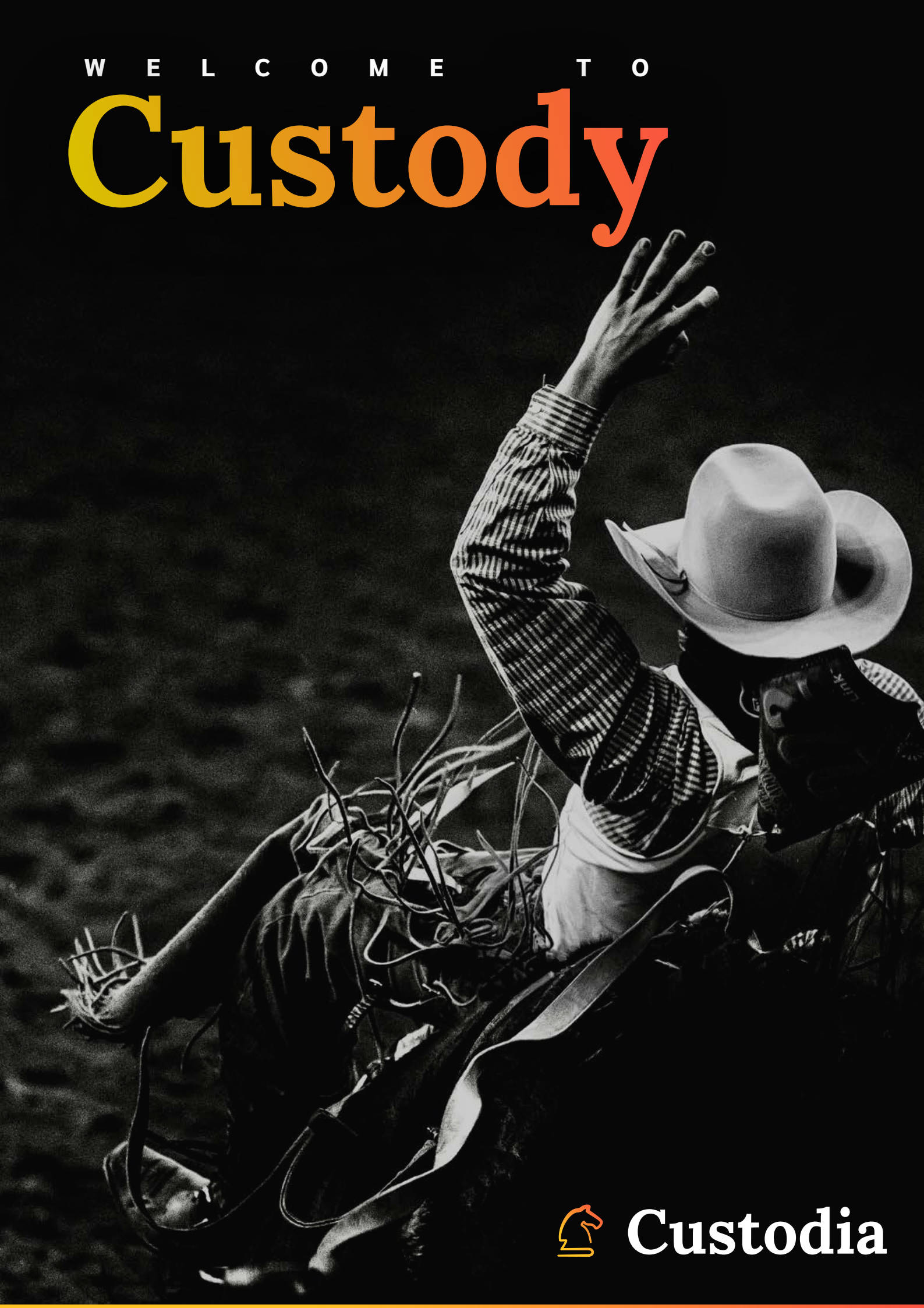
WELCOME TO

Custody



Custodia

INTRODUCTION

Our Promise

Greetings,

Thank you for your interest in learning more about Custodia and the unique approach and protections we offer as a Wyoming Special Purpose Depository Institution (SPDI), a type of bank charter designed to specialize in the custody of digital assets.

Bitcoin custody models have made headlines for infamous reasons. Starting with the Mt. Gox failure in early 2014 and continuing with more recent collapses like FTX and Prime Trust, digital asset custodians have certainly not given the industry much to crow about. As an early Bitcoin adopter and 22-year Wall Street veteran, I'm managing Custodia to provide a property-rights-respecting Bitcoin custody service to customers and aspiring to improve the digital asset industry more broadly.

In the following pages, you'll get a deep dive into what makes Custodia different. Most notably, we will contrast Custodia's segregated Bitcoin custody service to the omnibus approach of most of our competitors. Satoshi Nakamoto designed Bitcoin to provide clear property rights to Bitcoin owners, and a segregated Bitcoin custody service closely parallels Satoshi's ethos. We always recommend that you self-custody your bitcoins, but if you must use a custodian then please recognize that a segregated model provides you clearer property rights over any other form of custody.

We hope this whitepaper helps clarify some of your questions about our service and differentiators. Of course, if you have any further questions contact info@custodiabank.com and we'll get back to you.

Sincerely,

Caitlin Long, CEO

A Comprehensive Segregated Account Model for Digital Asset Custody

EXECUTIVE SUMMARY

Custodia Bank is now offering Bitcoin custody services to U.S. institutional customers in **certain US states**. We offer segregated accounts, which have superior customer protections over competing omnibus accounts that are standard offerings in the digital asset custody industry, and which commingle customer digital assets. The omnibus model brings significant risks associated with storage, transfer, and potential rehypothecation of customer digital assets, and omnibus accounts can be at risk of bail-ins in the event of a bankruptcy. In contrast, segregated accounts minimize those risks and improve transparency and auditability. As a Wyoming Special Purpose Depository Institution (SPDI), Custodia Bank's service operates within the purpose-built SPDI regulatory framework and its concept of a legal bailment, providing the strongest customer protections available in the U.S. for institutional digital asset customers.

The Segregated Account Model: Custodying Customer UTXOs

In the segregated account model for Bitcoin custody, a customer delegates digital asset storage to a custodian that stores the digital assets in-place, on-chain. This approach could alternatively be called a UTXO (Unspent Transaction Output) custody model because by leaving the assets in-place the customer's UTXOs are preserved. The custodian focuses its energy and attention exclusively on safeguarding the private keys that correspond to the customer's deposit addresses. Assets are not moved and cannot be pledged or rehypothecated to another party for any reason. Nor are the assets moved internally by the custodian, which – as discussed below – minimizes significant risks inherent to digital asset custody that have contributed to the recent loss of customer funds by other digital asset custodians.

Origin and Development of the Omnibus Model

The omnibus custody model dominates traditional financial markets, with most securities held at central securities depositories like the Depository Trust Company (DTC). This custody model rose to prominence in the late 1960s as trading volumes surged and record-keeping systems struggled to keep pace, resulting in manual errors during clearing and settlement. The omnibus arrangement uses the DTC as a central clearinghouse, with participating banks, custodians, and broker-dealers depositing customer assets at the DTC. The DTC participants own a pro rata share of the securities held at the DTC, and the participants track each customer's balance at the books & records level. With the DTC managing the custody of the actual securities, the participants are freed to focus on the recordkeeping of their customers' claims to those securities.

Applicability to Digital Assets

Traditional finance custodians, having decades of experience with omnibus structures (which were codified into US commercial law in 1994), naturally began applying this model to custodying digital assets. On the surface, this decision seems reasonable. After all, digital assets are fungible, just as shares within the same share class of traditional securities are fungible. As such, custodians could apply the pro-rata storage and ownership model to the fungible items. (Note that for this discussion we shall exclude Non-Fungible Tokens (NFTs), which by their definition would be incompatible with an omnibus model.)

Digital assets are different, however, in the sense that they are natively digital and incorporeal – unlike stock certificates or digital representations thereof (the latter of which are really just digitizations of analog stock certificates). Digital assets exist

natively on the blockchain; the assets themselves cannot be centralized. Custodians instead engage in the safekeeping of the private keys that control the assets' ability to be transferred over the blockchain network. These private keys represent the ownership and control of the assets, and custodians serve customers by protecting and safeguarding these private keys.

Alignment with Bitcoin Ethos: Comparison of Custody Models

The storage model most aligned with Bitcoin itself, and to digital assets more broadly, is self-custody. Owners of on-chain digital assets can store their private keys and create a self-custody arrangement using a vibrant and growing ecosystem of hardware and software providers, many of which have open-sourced their codebase for transparency and peer review. Assets transferred into self-custody remain in-place on-chain, with the asset owner taking responsibility for keeping them safely in-place. For institutions, the self-custody model can be difficult to implement and manage, though. Moreover, for some institutions like asset managers, SEC rules prohibit self-custody of client assets.

The storage model next closest to self-custody is collaborative custody. Using Bitcoin's multi-signature or similar multi-party approval technology, the customer holds one or more private keys and delegates one or more third parties to hold private keys (or fragments thereof), so that no single party can unilaterally move funds. A configurable quorum of approvers must agree for funds to move. The Wyoming SPDI framework specifically allows for collaborative custody, and the proposed SEC "Safeguarding Rule" 223-1 under the Investment Advisers Act, if adopted, appears to allow qualified custodians to engage in collaborative custody models. Custodia Bank is considering adding collaborative custody in the future.

The next closest approach is the segregated or UTXO model, where a customer delegates key storage to a single third-party that stores on-chain digital assets in-place. Custodia Bank's digital asset custody service currently uses this segregated UTXO model. The UTXO model is well suited for institutional customers who require high transparency of their on-chain funds but are reluctant to (or cannot) hold any private keys themselves. Many of the benefits of collaborative custody can be achieved in this model as well; multi-user withdrawal policies can create a similar setup as collaborative custody, with no single party being able to move funds.

Omnibus arrangements add another degree of separation from the purely self-custody model. Unlike in the UTXO model, the omnibus custodian moves assets after receiving them to another location on-chain, usually an address dedicated for offline cold storage or an address intended for immediate access for other purposes. The technical and legal allowance by the custodian to move digital assets from the original deposited location introduces serious risks that customers must consider, even if that movement is intended to improve the safety and transparency of those funds.

TYPE	GOOD FOR	BENEFITS	CONSIDERATIONS
Self-custody	Individuals	Inexpensive, secure	Multi-sig is complex, has a learning curve, may not be appropriate for institutions
Collaborative	Family offices, small groups	Redundant, secure	May not be compliant for some institutions
Segregated*	Institutions, large businesses	Compliant, secure, strong legal protections	Better for holding, more intensive compliance process
Omnibus	Institutions, large businesses	Compliant, secure, high fund availability	Risk of federal bankruptcy court, clouded ownership because ownership is an indirect pro rata share of omnibus pool

*Custodia uses a segregated custody model

Risks Inherent in an Omnibus Model

Recordkeeping & Storage Risk

Custodians build secure systems to create, manage, and protect the private keys associated with their controlled blockchain addresses. Superficially, an omnibus approach may seductively appear to involve fewer addresses and private keys to manage, allowing the custodian to focus on fewer items to protect. But in practice, the custodian is taking on much more work, risk, and responsibility in having to create, maintain, and protect several distinct systems: the internal ledger, the online hot wallets, the offline cold storage wallets, and perhaps other storage modes. This complexity increases the overall attack surface and opportunity-for-mistake surface.

Further, omnibus custodians are in effect asserting that their internal books & recordkeeping processes are superior to that delivered by a distributed ledger alone. After all, a main purpose of each distributed blockchain network, and the energy and computational resources spent by network participants, is to validate digital asset ownership. Omnibus custodians eschew this feature as they break on-chain traceability and centralize transactions to their internal books & records systems that must be separately maintained – and reconciled.

Further, business strategies and technical architectures change over time, and migrating digital assets to new systems introduces risk. Recent real-world examples of custodians losing private keys during or after a systems migration highlight the fact that any movements – even planned ones – involve real risk.

Transfer Risk

Digital assets are bearer instruments, meaning that only the possessor of that asset can prove ownership. Every transfer, even an internal transfer, carries the risk of loss.

Even with the help of powerful software to provide automation to set the transfer amount, destination address, and network fee amount, custodians and exchanges have committed errors that resulted in loss of customer or corporate funds. Funds may be sent to incorrect addresses or to addresses that the custodian no longer controls. Transaction activity patterns over time may provide useful information to malicious actors about custodial system design or potential attack vectors. Even if these transfer errors are committed unintentionally and in good faith, the digital asset transactions are final, and funds may be lost. When dealing with digital assets intended for long-term custodial storage, it's simply better practice to refrain from moving the funds in the first place.

Rehypothecation Risk

The next area of risk involves what the omnibus custodian does with the internally-transferred omnibus funds. While good-faith custodians may move funds from "hot" online addresses to offline cold storage, that reduction in technical risk does not mitigate the rehypothecation risk. Omnibus custodians that use contractual language permitting rehypothecation of digital assets expose customers to the risk of funds being present on the blockchain but in a compromised state of legal ownership, with the custodian potentially issuing more customer claims to digital assets than the custodian actually holds digital assets in its inventory. As witnessed in 2022 (and in each prior digital asset cycle), assets in omnibus accounts have been pledged – sometimes nefariously and sometimes with disclosure and permission – by custodians as collateral for a variety of assets whose value dropped resulting in bankruptcies and loss of customer funds. Again a symptom of the fractional reserve bank mentality of traditional finance, rehypothecation is incompatible with bearer assets like digital assets. Custodia Bank is a full-reserve bank and is unable to rehypothecate digital assets, by statute.

As witnessed in 2022 (and in each prior digital asset cycle), assets in omnibus accounts have been pledged by custodians as collateral for a variety of assets whose value dropped.

Bail-in Risk: In the Absence of Bailment Laws

As will be discussed shortly, the Wyoming bailment laws provide protections that prevent customer assets from becoming part of a custodian's bankruptcy estate in the event the custodian were to fail. But if a custodian fails while using an omnibus account (covered by UCC Article 8) absent any bailment protection, there is a risk that customers receive a pro rata share of the omnibus account – which may or may not be 100% of the customer assets transferred to the custodian. The outcome here heavily depends on whether the custodian is a bank or a non-bank, because failed banks cannot be debtors in U.S. bankruptcy court and are instead resolved through a special receivership process that generally favors customers. But if the failed custodian is a non-bank that ends up in federal bankruptcy court, such as a state-chartered trust company or a money transmitter, uncertainty increases substantially. And if the custodian was engaged in activities other than pure custody that create preferences under federal bankruptcy code, such as lending or possibly staking, the probability that custody customers face a pro rata haircut increases markedly.

A recent example is the Celsius Chapter 11, in which the bankruptcy judge held that the custody assets of Celsius belonged to the customers, but he could not release the assets until preferences were cleared – a process that could have taken years and cost a substantial percentage in legal and administrative costs. Consequently, custody customers agreed to take a 27.5% haircut, in what bankruptcy specialists call a "strong arm."

In another situation, the legal agreement of the trust company gave the trust company the rights of ownership of customer cash assets held in custody – thus muddying the segregation of those assets from the bankruptcy estate of the trust company itself. Net-net, the greater the segregation of customer assets from the custodian and other customers on the books and records of the custodian, the lower the bail-in risk – especially at banks relative to non-banks.

Put simply, segregated custody holds all branches (customer accounts) distinct, allowing for inspection or collection of each individual leaf (UTXO), keeping the remainder of the tree (other customer accounts) intact.

Omnibus custody (especially at a non-bank) requires cutting the tree down in the event of the institution's insolvency or for inspecting on-chain data. Since all UTXOs are commingled, establishing clear ownership is ambiguous and opaque.

Advantages of a Segregated Model

Transparency / Proof-of-Reserves

Blockchains are inherently pseudonymous, with assets publicly visible on-chain but the identities of the address holders unknown. Custodians, researchers, and industry participants have developed Proof of Reserves procedures that enable custodians to prove not only that the funds exist but also that a custodian controls the funds, without revealing any private information about their accounts or customer balances. Developed primarily with omnibus structures in mind, these procedures often include a two-step process of first proving control of on-chain addresses then secondly matching up total customer liabilities against the balance at those addresses. The second step evolved as a requirement because customer funds were distributed across omnibus addresses.

But in a segregated model, the second step is redundant. When custodying customer UTXOs in a single-signature arrangement, proving control of the addresses proves control of the customer funds. (Note that Custodia plans to conduct a conventional two-step Proof of Reserves procedure to match best industry practice, despite using a segregated account structure. Wyoming's digital asset custody rules require proof-of-reserves and proof-of-control of the reserves by SPDI banks.) With segregated accounts, customers must only trust that the custodian maintains control of the UTXOs; the customers can directly inspect the on-chain balance themselves. In an omnibus model, no such direct on-chain validation is possible, leaving customers to trust the custodian and any third-party attestation of a Proof of Reserves result.

Availability of Coins to Transact

Functionally, there is little difference between the omnibus and segregated custody models regarding the availability of coins to transact in large value. Here's why.

Omnibus custodians typically store the vast majority of customer funds in offline cold storage, the access to which is not immediate because the custodian must execute both technical and operational processes to access the coins from cold storage. The same is true for segregated custodians, which must execute withdrawals directly from each customer's UTXOs and these are not immediately available for transactions.

Long-term holders bear the higher security risk of the hot wallet on a pro rata basis.

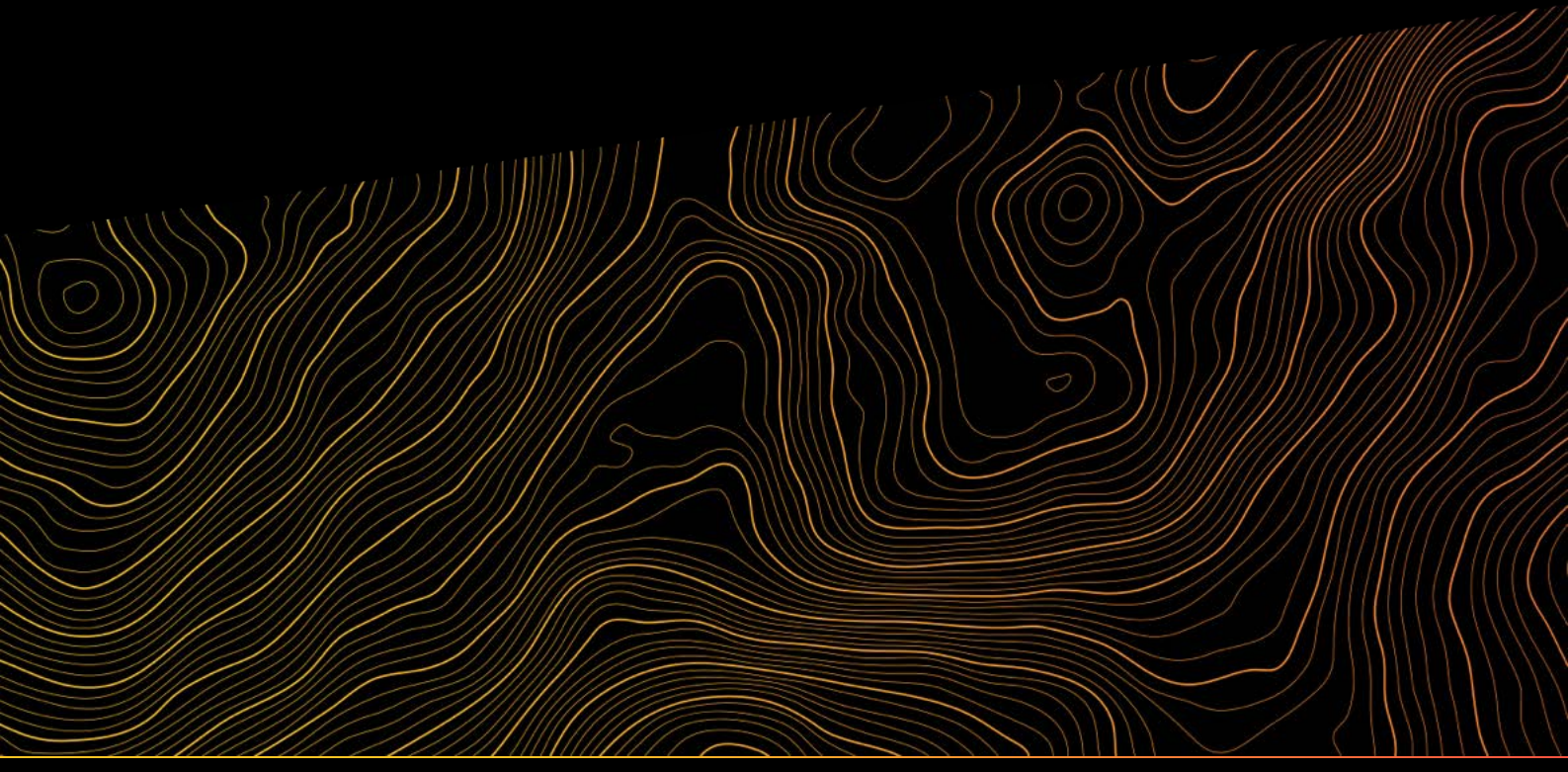
There is a difference for small withdrawals, of course, because omnibus custodians offer fast availability of coins held in a hot wallet – but, crucially, with a security trade-off because hot wallets are online and likely less secure. A recent example of higher security risk for a hot wallet is Fortress Trust, whose hot wallet was drained in an attack on a third-party integration.

So, long-term holders of coins at a custodian face an interesting counterparty credit risk issue. Why? Because all customers of an omnibus custodian share pro rata in the security risk of the hot wallet. Traders that actively trade benefit from access to the omnibus hot wallet, but long-term holders do not – yet, long-term holders nonetheless bear the heightened security risk of the hot wallet on a pro rata basis. If the custodian fails due to a hack of the hot wallet and is "bailed in" (see discussion below), both the active traders and long-term holders would share proportionately in the loss – when it was the active traders who benefited from the hot wallet. Consequently, long-term holders may prefer to use a segregated custodian.

Privacy

Public blockchains like Bitcoin make user privacy highly dependent on user activity. Less activity gives attackers less data from which to glean insights. Institutional custodians tend to have stronger privacy-protecting practices than individual users, who may engage in address reuse or risk leaking an address to an attacker. Similar to a self-custodial user, if a segregated account customer engages in poor privacy practices, that customer risks exposing the custodial balance information (which blockchain surveillance firms track using publicly available, on-chain information). No other customer at the segregated custodian would be affected by this privacy breach, as each address is uniquely identified.

Considering an omnibus model, a leak of an omnibus address does not specifically reveal customer information. However, on-chain analysis tools can typically identify omnibus custodial address clusters, as activity patterns can leave traces and linkages to these address clusters, potentially revealing customer balance information. While omnibus custodians may claim enhanced privacy over a segregated structure, the increased on-chain activity of omnibus addresses provides more opportunity for insights into customer data, so those advantages are overstated.



Technical and Risk Considerations

The omnibus model is popular because it enables custodians that demand immediate availability of coins for transacting to operate similarly to traditional financial custodians. But the omnibus model also is appealing because it neatly maps to hardened technical solutions of hot (online) and cold (offline) wallets. The omnibus custodian can use sound risk management techniques to store assets across multiple storage technologies and individual addresses therein.

It's often assumed that segregated custodians have no such capabilities and are forced to use one type of storage technology or another. This is not the case. The segregated custodian can use similar risk mitigation strategies and various technologies to those of an omnibus custodian as it constructs its systems to maximize security, availability, and transparency.

A key point though is whether the custodian relies on third-parties for its security and custody backbone, or if the custodian designs, builds, and maintains its own infrastructure. A custodian that architects its system from a technology-first mindset and invests in its own platform has more control over the system security and featureset than a custodian that is dependent on third-party vendors for timely delivery of patches and new features. Recent events resulting in loss of funds have involved custodians that relied heavily on sub-systems and third-party vendors for critical aspects of their solution.

Custodia has designed and built its custody solution in-house. While the solution uses some third-party vendors, Custodia ultimately controls the critical systems, infrastructure, and delivery of new capabilities.

Wyoming Digital Asset Framework

Most U.S. digital asset custodians are chartered as state trust companies or have state money transmitter licenses. Some traditional banks have entered the digital asset custody space, as the Federal Reserve has approved digital asset custody as an allowable line of business for certain banks (**such as BNY Mellon**). Wyoming has created a new bank charter custom-designed for the custody of digital assets, and it provides a comprehensive digital asset regulatory framework that includes significant customer protections.

Arguably the most significant innovation of the framework is applying the legal concept of a bailment to digital assets. In a bailment, one party (the custodian) holds and safeguards the digital assets on behalf of another party (the asset owner), much like a traditional financial institution holds physical assets or valuable items in a safe deposit box. Other common analogies are a valet parking or coat check service, where the asset owner relinquishes temporary control but never transfers beneficial ownership rights. As the asset ownership never changes, digital assets do not move to the Wyoming custodian's balance sheet and would not be included in the estate in the event of a bankruptcy. The Wyoming framework recognizes that the bailment model is appropriate for the custody of bearer assets like digital assets.

At a high level, the main aspects of the Wyoming framework related to custody include:

STATUTORY REQUIREMENT	BENEFIT
Digital assets are held in a legal bailment.	Ownership remains with the customer. Custodian receives temporary control of the digital asset, but not legal ownership, such as with a valet parking or coat check.
Customer digital assets must be held in separate accounts from any of the custodian's digital assets.	Segregation of customer funds from corporate funds and, as applicable, from other customer funds
The bank is unable to rehypothecate digital assets under custody.	Customer funds stay in-place; no possibility of customers having multiple claims to the same digital asset
Operational risk management program and business continuity plan	Active monitoring of risks; Plans for perpetual access in the event the bank ceases to operate
Anti-money laundering, fraud detection program	Intended to keep unlawful customers out and detect any suspicious behavior
Insurance for custodied digital assets	Baseline coverage + ability of customers to obtain more coverage
Periodic Proof of Reserves (including proof of control), verified by external auditor	Transparency of holdings, without compromising customer privacy
Specific requirements around private key generation, backups, security, and audits	Transparency of holdings, without compromising customer privacy
Multiple individuals required for transaction approval	Protection against unauthorized withdrawals
Transaction audit trail requirements	Transparency about reasoning or evidence about transaction approval or rejection
Periodic external penetration tests, internal and external vulnerability audits	Ongoing review of systems and process for security

The Wyoming SDPI charter allows for both segregated and omnibus account models, and a Wyoming SPDI that offers both models requires its custody customers to choose upfront which type of custody arrangement it will use. As such, any SPDI omnibus custodian would be required to meet the same above requirements. Net-net, the Wyoming SPDI requirements provide important customer protections.

Conclusion

While prevalent among custodians in traditional finance, for digital asset custody the omnibus model has material disadvantages compared with a segregated model. The segregated model more closely aligns with Bitcoin's ethos, enables higher transparency, and reduces storage, transfer, and rehypothecation risks. The Wyoming SPDI framework, having been natively designed for digital asset custody, augments the customer protections afforded by the segregated approach. Custodia Bank's digital asset custody service offers the structural soundness of the segregated approach with the legal and regulatory oversight of the Wyoming SDPI laws to offer a unique service for institutional custody.

To learn more, contact info@custodiabank.com.

Made in Wyoming