The importance of custodians in bitcoin adoption and ownership

Why bitcoin's decentralized properties require reliable custodians and diligent investors

In this report we will:

Demonstrate the importance of custodial firms to bitcoin's growth and adoption

Explain the risks that custodians must mitigate in order to safeguard bitcoin holdings

Highlight the attack vectors custodians must protect against as well as the common mitigation strategies they employ

Offer strategies for evaluating custodial partners

Why is custody so important in bitcoin and what does the custody landscape look like today?

One of the core tenets of bitcoin is the ability to own and control your assets without any counterparty risk or dependencies on third parties. But what does it really mean to own bitcoin? Property rights in the bitcoin network are not enforced by companies or governments but instead are enforced through cryptography. In the earliest days of bitcoin, the only way to own bitcoin was to use your own cryptographic "private keys," a practice known as self- custody.

Self-custody means controlling your own private keys without the use of a centralized custodian. If you lose your private key(s), then you will have lost your bitcoin. If an attacker discovers your private key(s), then that attacker can use them to sign a bitcoin transaction transferring your bitcoin to the attacker's wallet. Since the bitcoin network is decentralized, all transactions are immutable, which means no individual or company has the ability to reverse a transaction.

Custodians play a critical role within the digital asset ecosystem and were created to relieve users of the responsibility and complexity of managing their own private keys. In a custodial relationship, users delegate the responsibility to protect their private keys to the custodian, who in turn use a web or mobile application to authenticate users, authorize transactions, and subsequently move the assets on their behalf.

Over the years, custodians and the processes they employ to safeguard customer assets have continued to evolve. New models for self-custody such as "collaborative custody" build on bitcoin's native multisignature (multisig) capabilities to distribute the risks and responsibilities of protecting private keys across multiple parties. Multisig is a function native to bitcoin that uses cryptographic techniques to require "m of n" signatures to send a transaction. For example, 3 of 5 people must authorize the transaction prior to it being made. This removes single points of failure and is an example of requiring multiple parties, rather than a single party, to make a transaction on bitcoin's base layer.

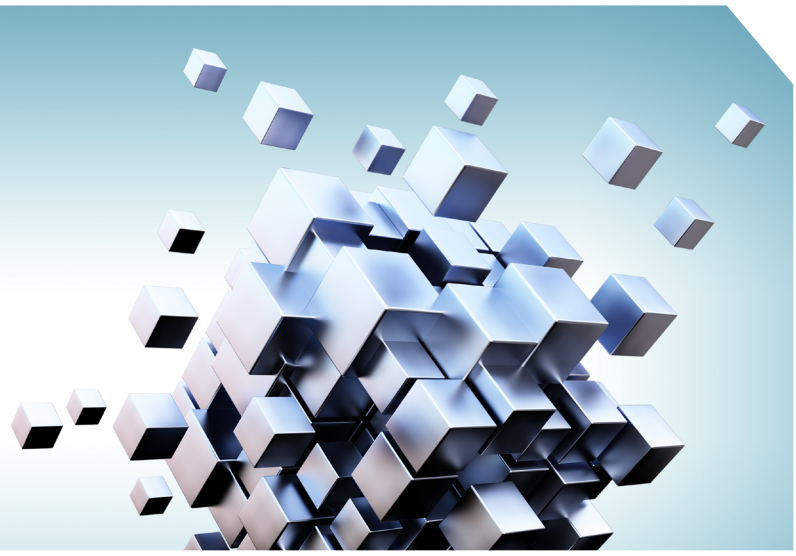
It takes time—sometimes years—for bitcoin investors to develop enough confidence and conviction to take on the added complexities of managing their own private keys. Relying on a custodian is oftentimes the easiest and most convenient option. In this way, custodians are critically important to bitcoin adoption, as they are the first port of call for any new investor. This is especially true with the recent launch of the bitcoin ETFs as each of the ETF issuers use a third-party custodian for the bitcoin held in their respective fund. According to Bloomberg's James Seyffart, "the 11 bitcoin ETFs approved this year currently have approximately $59 billion in assets under management. Prior to these ETFs, the record time for an ETF to reach $10 billion in assets was 647 trading days (nearly three years). The top two bitcoin ETFs, IBIT and FBTC, got there in just 49 days and 77 days, respectively." Given the significant amount of bitcoin being custodied for the ETFs, the issuers were required to exercise caution and due diligence before naming a custodian for their ETF holdings on behalf of their investors.

While the US is known to have a number of household names that provide custodial services, each of which are subject to oversight by various regulatory agencies such as the Securities and Exchange Commission (SEC), Financial Crimes Enforcement Network (FinCEN), New York State Department of Financial Services, etc., many custodians over the years have operated outside of a regulatory framework. This has resulted in riskier operations with fewer investor protections and has resulted in numerous incidents where customer funds were lost or stolen. As such, any custodian comes with risks that we will further explore throughout this paper.

Risks with bitcoin custody

Custodians must protect cryptographic private keys against theft, loss, and corruption, which requires having strong internal controls around the custody processes they employ to keep them secure. This means that details about the locations, processes, and controls around protecting the key(s) from external threats must remain secret and secure, but without transparency on how this is achieved, how can people obtain the assurances they need? Business operations, quality assurance, and protecting from internal threats requires some divulgence of information, which requires the best custodians to strike a careful balance between obscurity and transparency.

In addition to these security requirements, custodians must also use the private key(s) they protect to regularly sign bitcoin transactions on behalf of their users throughout the day. This requires communication between online systems that interact with customers and employees, as well as the offline systems that manage private keys (e.g., HSMs). Applications or personnel that can authorize the use of private keys become additional attack vectors that custodians must secure.



Since custodians move bitcoin on behalf of their customers/clients, they must also properly verify the identity of users requesting a withdrawal or transfer. Account takeovers within a custodian's website or mobile app leading to the withdrawal of bitcoin to an attacker's personal wallet are all-too-common experiences throughout bitcoin's history. Some of these common attacks include subscriber identity module (SIM) swaps—a practice where an attacker gains access to the SIM card of the victim's cell phone and uses it to go around SMS-based two-factor authentication—and phishing—a practice where a fake (and often realistic) email is sent requesting the victim to share their credentials with the attacker.

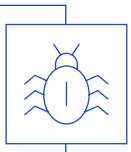
The failure of a custodian due to poor financial risk management or regulatory actions is also a common occurrence. In these cases, clients who did not withdraw their bitcoin before the custodian freezes withdrawals may have to wait years for their bitcoin to be returned. In some cases, this will never happen or, when it does, investors are not always compensated in bitcoin but in dollars, in an amount determined by the market value of the original bitcoin at the time of loss. Given bitcoin's historical rate of return, this could result in a significant loss.

Private key management is the central challenge of bitcoin custody. As the market for exchanges and custodians has grown, lessons have been learned about how to manage private keys and operate the businesses supporting that central function. Unfortunately, it has been a trial by fire. We can see the mistakes made by countless exchanges and custodians over the years, which have resulted in hacks leading to billions of dollars in digital assets being lost or stolen.

For the customer or client entrusting a bearer asset like bitcoin to a custodian, there are a number of risks that could result in the complete and permanent loss of funds. In this paper, we will take a closer look at six common attack vectors custodians must solve for.

Six attack vectors that custodians must mitigate

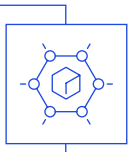
Outside attackers



One of the most common threats to custodians are outside attackers that look to compromise the custodian's key management, applications, personnel, and/or devices.

Tokyo-based exchange Mt. Gox—which at one point accounted for approximately 70 percent of all bitcoin transactions—was hacked (using stolen credentials) on multiple occasions between 2011 and 2014, resulting in a loss of over 809,000 bitcoin (over $52 billion today), which ultimately led to the exchange filing for bankruptcy.[1] Mt. Gox did not begin making distributions to their creditors until July 2024, nearly a decade after filing for bankruptcy.

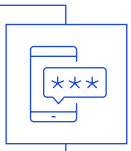
Insider threats



Outsiders aren't the only threat to consider, as often the most significant threat to a custodian's security comes from within. Custodians are responsible for properly securing client funds, but they must also be prepared to access and use those keys to sign transactions on behalf of their users. Personnel who can trigger the use of private keys—or choose not to trigger the use of private keys when authorized by a user—present additional risk that custodians must mitigate against.

One such example of an insider threat was an exchange called BitGrail, which suffered an estimated loss of $170 million worth of cryptocurrency from its platform. This event was initially reported as an outside attack, but as investigators took a closer look, it became increasingly apparent that one of the exchange's operators was likely behind the attack.[2]

Securing account credentials



Within the bitcoin network, all bitcoin are controlled by private keys; hence the common bitcoin parlance "not your keys, not your coins."

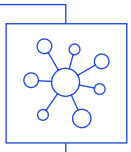
Since custodians move bitcoin on behalf of their customers, they must take responsibility for proper security not just with the private keys, but also with the customer's account, to ensure that withdrawals are going to the intended recipient. Unfortunately, compromises at the account level that irreversibly send bitcoin to an attacker's wallet are a common occurrence.

Social engineering and phishing attacks are routinely attempted on individual customers. While the ultimate responsibility may rest with the customer, custodians and exchanges must take proactive measures to secure account information and effectively mitigate the risk of customer impersonation.

[1] Mark Hunter, "Mt. Gox: What We Still Don't Know 10 Years After the Collapse," CoinDesk, February 28, 2024

[2] Tanzeel Akhtar, "BitGrail Operator May Have Hacked Own Exchange to Steal €120M, Police Allege," CoinDesk, September 14, 2021

Borrowing and rehypothecation



Several exchanges over the years have offered users a yield on the assets they deposit on the exchange's platform. They are able to offer this yield as the assets that a customer deposits are then lent out for other purposes; as such, the user is earning a yield as compensation for the risk they're taking in lending their assets. Similarly, rehypothecation involves using a customer's collateral for other purposes such as collateral for additional loans or other trading strategies. Both of these scenarios present risk to the user (e.g., liquidity, market, counterparty, etc.) as well as to the exchange or custodian.

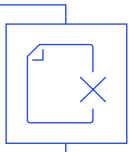
The risks associated with borrowing and rehypothecation were highlighted in 2022 when FTX, the now-defunct crypto exchange, became insolvent and users were unable to withdraw their assets. Among the numerous findings identified through the bankruptcy proceedings, including outright fraud, was that FTX represented to hold nearly $1.6 billion in bitcoin on behalf of their customers; however, they held only $1 million in bitcoin at the time of their collapse.[3]

Regulatory actions

Custodians can be shut down by governments or regulatory agencies due to failure to comply with relevant laws and regulations. In 2018, the Federal Bureau of Investigation (FBI) seized the domain of a popular exchange platform called 1Broker. In an SEC press release, it was noted that a special agent with the FBI, acting in an undercover capacity, was able to purchase a number of security-based swaps on the 1Broker platform. The agent was able to do so from the US, which led to the SEC alleging that 1Broker was operating as an unregistered dealer.[4] Additional charges were brought by the Commodities Futures Trading Commission (CFTC) for failing to implement sufficient anti-money-laundering (AML) and related supervisory procedures, requirements of the CFTC.[5]

While this situation didn't lead to the loss of funds for clients or end users, it did lead to a temporary loss of access for customers as the company had to wait for US regulator approval to resume business. However, later in 2018, 1Broker closed for good.

Operational failure



Numerous types of operational failure modes can cause custodians to become insolvent. Sometimes, a custodian's insolvency is not even known to them until they attempt to fulfill their clients' withdrawal requests.

As detailed in a cease-and-desist order from the state of Nevada, crypto custodian Prime Trust became unable to fulfill customer withdrawal requests due to, among other things, a cold storage wallet that became inaccessible.[6] Following the transition to a new custody management platform, the company began to reintroduce legacy customer wallets that were not managed on the new custody platform. As a result, they were unable to access these wallets and were unable to honor customer withdrawals. In order to satisfy these requests, Prime Trust began selling existing customer assets to fund the withdrawal requests from legacy wallets. In July 2023, Prime Trust was placed into receivership by the Nevada Financial Institutions Division.[7]

[3] Kroll Restructuring, "Preliminary Analysis of Shortfalls at FTX.com and FTX.US," March 2, 2023

[4] Yahoo!Finance, "1Broker Shut Down, Will More Bitcoin Exchanges be Targeted by US Gov't?," October 2, 2018

[5] CFTC.gov, https://www.cftc.gov/sites/default/files/2018-09/enf1poolpatrickajeltakecomplaint092718.pdf

[6] State of Nevada, Department of Business and Industry Financial Institutions Division, June 2023.

[7] Caitlin Ostroff, "Crypto Custodian Prime Trust Files for Bankruptcy Protection," The Wall Street Journal, August 14, 2023

Key considerations for choosing a custodian

Despite the risks and challenges custodians face, many have operated successfully for years without major losses or failure. What sets these organizations apart is:

- Emphasis on security, compliance, and financial health
- Ability to effectively build and maintain software, hardware, and infrastructure that can withstand extreme market conditions
- Hiring in-house for roles that support or control custodial capabilities as opposed to relying on contractors or vendors.

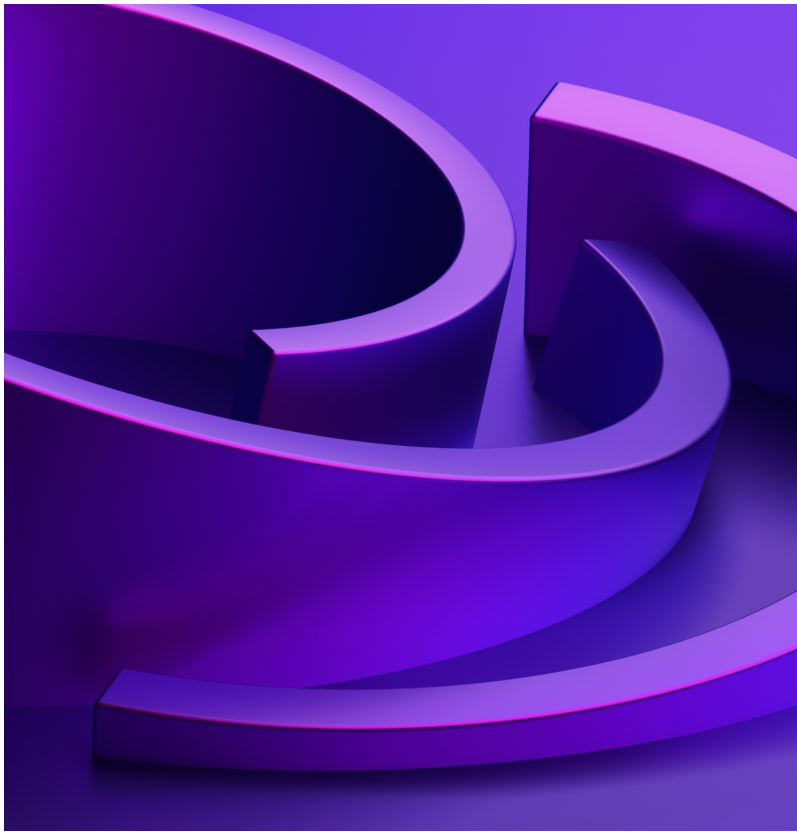
In evaluating threats that exchanges and custodians face, as well as the most common methods they use to mitigate these threats, we can identify some key criteria for choosing a custodian across four main categories: security, compliance and legal, transparency and reporting, and operational reliability.

Security

A primary indication of mature organizational security is whether an organization hires for and controls its own custodial capabilities. While details on this are rarely disclosed in full, there are some good indicators for whether a custodian invests in the necessary infrastructure to accomplish this.

Does your custodian:

- Control its own custodial capabilities?
- Have a dedicated security function?
- Have an ISO/IEC 27000 certification?
- Geographically distribute their backup keys as part of disaster recovery?
- Provide robust end-user security with 2FA/MFA?
- Conduct penetration tests?



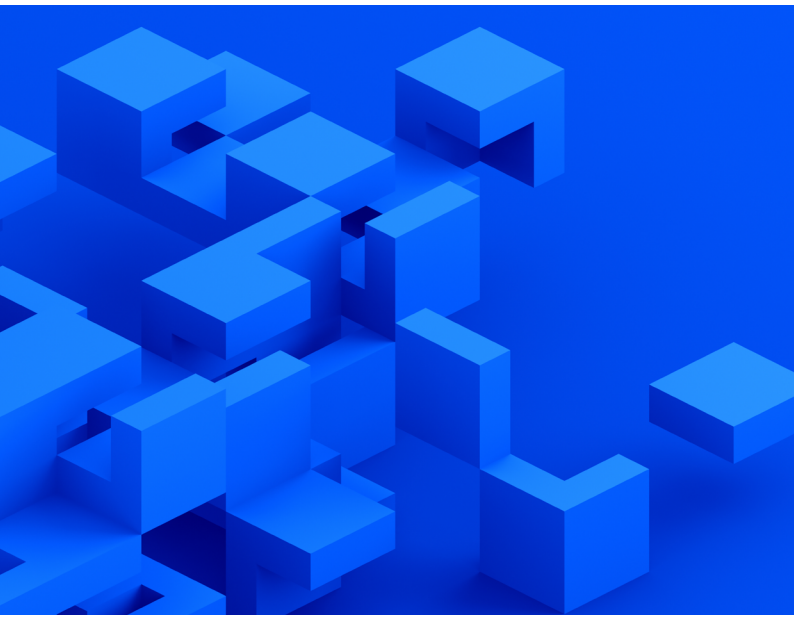
Compliance and legal

In the United States, bitcoin custodians are required to abide by money transmission laws and corresponding regulations in the states they operate given their requirement to register as a Money Services Business (MSB) with FinCEN. Additionally, they must comply with know your customer (KYC) and AML laws such as the Bank Secrecy Act and the Patriot Act. Any reputable custodian operating in the United States will be required to meet these basic regulatory requirements.

When using a custodian to custody your bitcoin, you're entrusting control over your private keys to another institution that must abide by local laws and regulations. Some jurisdictions have more robust regulatory frameworks which help provide more assurances to its customers.

Does your custodian:

- Have a Money Service Business license?
- Have established KYC/AML procedures?
- Conduct on-chain transaction analysis?
- Have a chief compliance officer?
- Reside in a country with a stable regulatory regime?



Transparency and reporting

Custodians must strike a careful balance between obscurity and transparency in their data classifications and access controls. The most secure custodian is not always the most transparent, but there are some key areas where transparency and reporting have clear benefits for choosing a custodian that maximally mitigates the threats described in the section above.

Does your custodian:

- Have current SOC 1 Type 2 and SOC 2 Type 2 reports issued by reputable audit firms?
- Provide a proof of reserves report?
- Commingle client assets with their company-owned assets?
- Have a record of prompt incident reporting and resolution?

Custodians that commingle assets create unnecessary risks and are often required to segregate customer funds due to regulatory requirements.

Operational reliability

A key indicator of a reliable custodian is one who invests heavily in its own custodial capabilities instead of relying on contractors or vendors, but operational reliability extends far beyond private key management.

Does your custodian have:

- Contingency plans for business continuity and disaster recovery?
- Insurance, which typically covers large fiat-denominated amounts of cryptocurrency held in hot or cold wallets?
- Qualified custodianship, which requires baseline safekeeping practices to be transparently disclosed and subjected to periodic audits/attestations?

Additional considerations

Client support and communication

Unfortunately, many of the details outlined above are not readily available through a custodian's website and marketing materials. Furthermore, history is full of examples where customers were not aware of the numerous shortcomings in security, compliance, financial responsibility, or operational reliability until it was far too late. To mitigate these risks, clients should choose custodians with robust communication channels and high responsiveness.

Does your custodian have:

- A customer support team that supports your local jurisdiction?
- Clearly defined support ticket tiers and escalation paths?

Cost and fee structures

Another factor to consider is cost and fee structures. Custodians vary widely in their pricing models, which may include account setup fees, transaction fees, and account maintenance fees. Not only should the explicit costs be considered, but so should potential hidden fees and the total cost of ownership. Consider the additional cost of insurance in the context of disaster risk—exchanges with more robust controls and reliability might be more expensive on paper, but that upfront cost could save a client in the long run. In bitcoin, there are no takebacks.

Does your custodian have:

- A fixed annual fee or variable pricing based on the amount of assets under management?
- Insurance that covers your bitcoin specifically?
- Additional support costs or hidden fees?

Collaborative custody

An emerging trend among modern bitcoin custodians is a concept referred to as "collaborative custody." Unlike traditional custodians, collaborative custody partners enable investors to maintain sovereignty over their bitcoin—making their funds less vulnerable to exchange hacks and collapses—without the risks of self-custody, (e.g., loss of private keys). In collaborative custody, bitcoin wallets are constructed from multiple private keys, of which a subset of them are required to move or send bitcoin. This prevents collaborative custodians from unilaterally moving or lending a user's assets. In most collaborative custody arrangements, the client holds one or more keys alongside independent third parties or custodians who control the remaining keys. In this setup, two out of three authorizations may be required, for example, ensuring that no one party can accidentally or maliciously move funds. In an enterprise context, the key holders involved are regulated US entities that meet many of the considerations defined above.

Even if a client doesn't wish to hold a key, emerging solutions take advantage of bitcoin's native multisig properties to provide custody solutions that distribute key control among multiple institutional grade key agents.[8]

[8] Unchained Capital, https://unchained.com/features/bitcoin-network-of-keys

Future outlook and recommendations

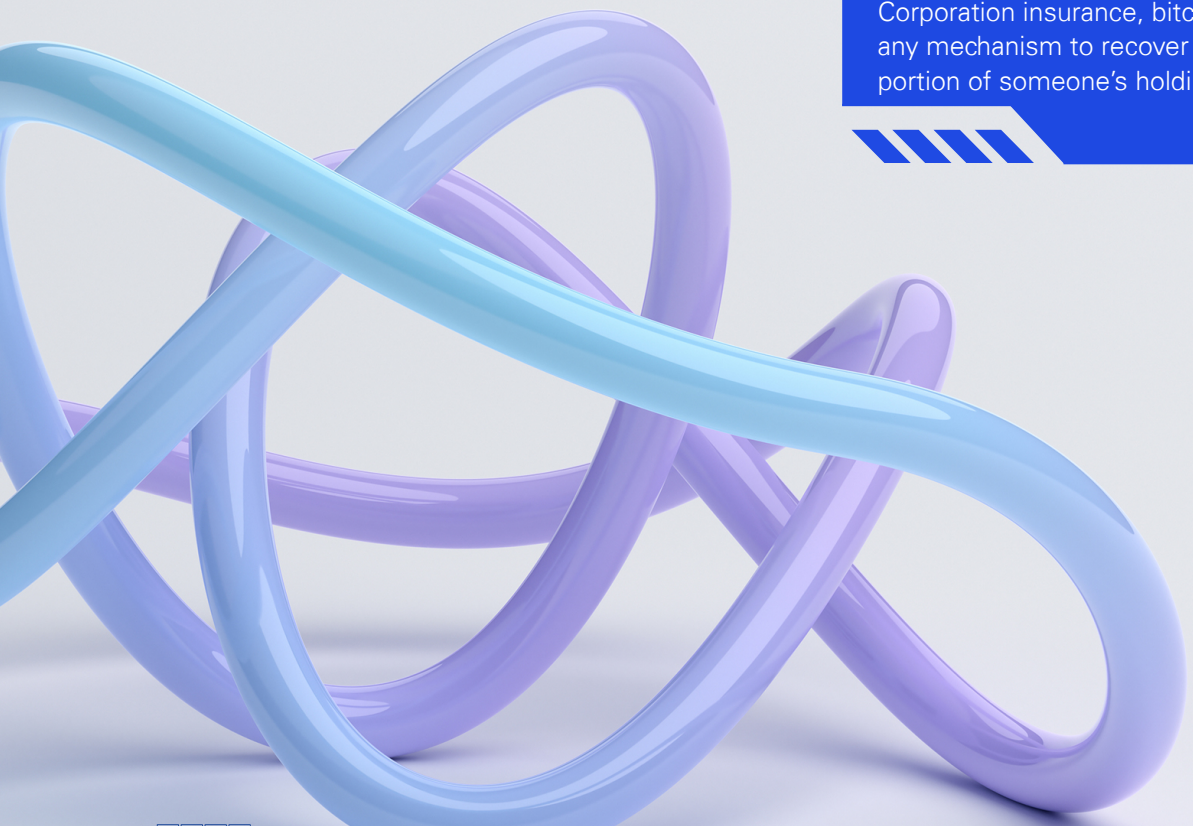
The landscape of bitcoin custody is ever evolving. With the addition of new regulated financial products such as spot ETFs, the continued growth of the bitcoin network, and the emergence and rising popularity of layer 2 scaling solutions, the challenges and threats that institutional bitcoin holders face will continue to evolve.

One example of an emerging threat is artificial intelligence (AI). While large language models and generative AI tools like ChatGPT, Dall-E, and Midjourney could be a massive boon for productivity and creativity, it may be the case that the killer app for AI is social engineering. AI-powered attackers will soon be able to trick the perfunctory liveness tests used by most banks and exchanges. This will bring withdrawal limits, increased verification through centralized identity providers, and the deployment of counter-AI to "detect" bad actors through training them on ever-more information about us all.

Considerations for future changes

While the above rubric can be a good starting point for choosing a bitcoin custodian today, the qualifications that define a sound custodian will evolve in the years ahead. As the global financial system reorients itself and more deeply understands bitcoin, custody options will expand over time based on new technologies and a willingness of companies to use multiple custodians.

All of the considerations in this report should be carefully evaluated when choosing a custodian today. Bitcoin's native capabilities—namely multisig wallets—may emerge as the backbone for institutional and enterprise-grade products of the future. Most who apply the principles in this report in choosing the ideal custodian may still have reservations about relying on one entity to manage their private keys. Custodian diversification and/or the use of a collaborative custody model allows customers to mitigate this concern by splitting their bitcoin holdings among multiple custodians: putting their eggs into multiple baskets. Unlike dollar-denominated holdings that can be split among different bank accounts covered by Federal Deposit Insurance Corporation insurance, bitcoin does not have any mechanism to recover from the loss of any portion of someone's holdings.



Conclusion

Despite the challenges associated with directly managing private keys, custodians play a critical role in the bitcoin ecosystem. There are many benefits to trusted centralized custodians as they have helped protect user assets and accelerate bitcoin adoption to this day. Understanding the complexities and risks with bitcoin custody involves choosing a custodian who prioritizes security and compliance, is financially stable, and has the appropriate infrastructure associated with managing its own custodial capabilities.

Authors:

Brian Consolvo
Principal
Technology Risk
KPMG LLP
E: bconsolvo@kpmg.com

Dhruv Bansal
Cofounder
Unchained
E: dhruv@unchained.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**