10. Cryptocurrency custody

Arthur Carvalho

Introduction

Cryptocurrencies have revolutionized the financial landscape by introducing a decentralized, trustless system where individuals can hold and transfer value without the need for intermediaries such as banks or payment processors. One of the foundational principles of this new digital economy is the concept of self-custody, which empowers individuals to take full control over their assets. In particular, unlike traditional financial systems where third parties tend to have custody over clients' funds, self-custody in the cryptocurrency world allows users to be their own bank by securely storing and managing their private keys—the cryptographic keys required to access and transfer their digital assets.

The benefits of self-custody are significant. It provides users with great autonomy, eliminating the risk of losing funds due to the failure or mismanagement of intermediaries. Additionally, although advanced de-anonymization techniques might be applied, generally, self-custody can offer enhanced privacy, as individuals are not required to disclose their holdings or transactions to any centralized, intermediary entity. Self-custody also ensures that users have direct access to their assets at all times, without the potential delays or restrictions that can come with third-party control. For example, during the Canadian trucker protests against COVID-19 vaccine mandates in early 2022, the Canadian government invoked emergency powers to freeze the bank accounts of protesters and individuals who were supporting the protests financially. This included the freezing of funds from traditional crowdfunding platforms like GoFundMe. In response, supporters began to send bitcoins directly to the protesters as a means to bypass these financial restrictions (Chawaga, 2022). Because Bitcoin transactions rely on a decentralized network, donations that originated from self-custody wallets could not be blocked or censored by the government or any other third party. The protesters or organizers who held their own private keys (self-custody) had immediate access to the donated funds, and they were able to use these assets without delay or restrictions imposed by banks or other financial institutions.

However, self-custody is not without its challenges. Managing private keys securely requires a certain level of technical knowledge and responsibility. If a private key is lost or compromised, the associated assets can become irretrievable, leading to potentially significant financial losses. A well-known example of this issue was faced by James Howells, a British IT worker who accidentally discarded a hard drive containing the private keys to 8,000 bitcoins (currently valued at over US$5 billion) in 2013 (Hamilton, 2022). Despite numerous efforts to recover the hard drive from a landfill, the bitcoins are still irretrievable. Moreover, the absence of a central authority means that users have no recourse to recover their funds if they make mistakes or fall victim to fraud (Carvalho et al., 2021). For example, when Mt. Gox, the largest Bitcoin exchange at the time, was hacked in 2014, approximately 850,000 bitcoins (currently valued at over US$54 billion) were stolen (Wieczner, 2018). Because there was no central authority overseeing Bitcoin transactions, users had no legal recourse to retrieve their funds at the time, leading to substantial losses. These challenges highlight the delicate balance between the empowerment and risks associated with self-custody in the cryptocurrency ecosystem.

The emergence of cryptocurrency custody

In response to the complexities and risks associated with self-custody, the concept of cryptocurrency custody by third parties has emerged as a significant aspect of the digital asset ecosystem. Such custody services are offered by specialized firms, exchanges, and financial institutions that manage and safeguard cryptocurrencies on behalf of their clients. These custodians take on the responsibility of securely storing private keys, often utilizing advanced security measures such as multi-signature wallets, cold storage, and insurance protections to mitigate the risks of theft or loss. The primary advantages of using a third-party custodian include the added convenience, user-friendly interfaces, and peace of mind it offers, especially for individuals and institutions that may lack the technical expertise to manage their own digital assets securely. In other words, by entrusting their assets to professional custodians, users can

avoid the previously mentioned devastating consequences of losing private keys while also benefiting from additional layers of security and insurance that these services provide. This makes third-party custody particularly appealing to institutional investors, who require robust security measures and regulatory compliance.

However, third-party custody comes with its own set of trade-offs. One of the most significant drawbacks is the reintroduction of counterparty risk—the risk that the custodian could mismanage, lose, or even misuse the assets under their care. The collapse of FTX, one of the world's largest cryptocurrency exchanges, in late 2022, serves as a stark example of the counterparty risk associated with third-party custody of digital assets. FTX was a major cryptocurrency exchange that offered users a platform to trade and store their digital assets. Many users entrusted FTX with their digital assets, relying on the exchange to securely manage and safeguard their funds. However, in November 2022, FTX suddenly faced a liquidity crisis that revealed significant mismanagement of customer funds. It was discovered that FTX had been commingling customer assets with those of its sister company, Alameda Research, which engaged in high-risk trading activities. When Alameda's risky bets failed, it became apparent that billions of dollars in customer funds were missing. The exchange halted withdrawals, effectively freezing users' assets, and eventually declared bankruptcy. Users who had stored their assets on FTX lost access to their funds, with many still facing the prospect of not recovering their money (Roth, 2022).

The counterparty risk illustrated by the FTX fiasco runs contrary to the decentralized ethos of cryptocurrencies, where the goal is to eliminate the need for trust in intermediaries. Additionally, entrusting assets to a custodian can reduce a user's control and privacy, as custodians often need to comply with regulatory requirements, including Know Your Customer (KYC) and anti-money laundering (AML) policies, which involve the disclosure of personal information and transaction details to specific entities under certain circumstances. Finally, the centralization of custody services can make them attractive targets for hackers, potentially putting large amounts of digital assets at risk in the event of a security breach. This risk is amplified by the fact that in jurisdictions that lack appropriate regulatory frameworks, custodians are not subject to the same level of oversight and regulation as traditional financial institutions, leading to concerns about their long-term viability and reliability. For example, in August 2016, when regulatory oversight for digital assets was still in its early stages, Bitfinex, one of the largest cryptocurrency exchanges at the time, suffered a major security breach. In the attack, hackers exploited a vulnerability in one of the exchange's systems, resulting in unauthorized access to 119,756 bitcoins, worth approximately $72 million at the time (Tsang, 2016). The hack sent shockwaves through the cryptocurrency community as it underscored the inherent risks of centralizing large amounts of assets in a single custodian.

Key platform considerations

At the time of writing, there are several companies offering cryptocurrency custody services for individuals and institutions, such as Anchorage Digital, Coinbase, Gemini, and Fidelity. The previous discussion suggests that there are key considerations one must contemplate when selecting a cryptocurrency custody partner. We elaborate and expand on these considerations next. One of the first aspects to consider is whether the custody provider holds appropriate *regulatory licenses* and adheres to *compliance standards*. In an industry that is still evolving, regulatory oversight varies widely by jurisdiction, and a reputable custody provider must comply with relevant financial regulations, such as the previously mentioned KYC and AML policies and the newly proposed Markets in Crypto-Assets regulation (MiCA) in Europe. This not only offers a layer of protection but also ensures that the custodian is subject to regulatory oversight, which can help mitigate the risks associated with mismanagement or fraud. To further enhance trust, one should ideally narrow on custodians that undergo regular independent *third-party audits*. These audits verify that the custody provider's security practices, financial controls, and operational procedures meet industry standards and required regulations.

Another essential aspect is the existence and transparency of the custodian's *proof-of-reserves reporting*. Proof of reserves is a method by which custody providers demonstrate that they hold enough assets to cover

all customer deposits (Asmakov, 2022). A trustworthy custodian should ideally publish transparent and verifiable proof-of-reserves reports regularly, often verified by independent auditors. This practice helps prevent insolvency risks and reassures clients that their assets are fully backed and readily available, reducing the likelihood of liquidity issues in times of market stress.

The *experience* and *tenure* of a custody provider in the cryptocurrency industry are also critical reliability indicators. Companies with a longer track record are naturally more likely to have refined their security practices and developed robust systems for managing and safeguarding digital assets. This is due to experienced custodians having typically navigated various market cycles and challenges, proving their resilience and capability to handle complex situations. The *reputation* of a custody provider is another important consideration. Researching customer reviews, industry expert opinions, and case studies can provide valuable insights into a custodian's performance, reliability, and customer service. A custodian with a strong reputation and high client satisfaction is likely to offer better service, security, and responsiveness to client needs. It can also be helpful to look at the custodian's history in handling crises or security incidents, as this can reveal how well they manage unexpected challenges.

Understanding the details of how a custodian manages client assets is crucial. Reputable custody providers should practice client *asset segregation*, meaning they keep customer assets separate from their own operational funds. This segregation ensures that, in the event of the custodian's financial difficulties, client assets remain protected and can be returned to their rightful owners. Custodians who use pooled accounts without proper segregation pose a higher risk, as customers' assets could be entangled in the custodian's liabilities.

Finally, one might also consider whether a custody provider offers integration with cryptocurrency exchanges. For active traders, having a custodian that integrates seamlessly with major exchanges can significantly enhance convenience and efficiency. This integration allows for smoother, quicker transfers of assets between custody and trading platforms, reducing the time and risk associated with moving funds. Additionally, it can facilitate more strategic and timely trading decisions, which is particularly valuable in the fast-paced cryptocurrency market.

Conclusion and future outlook

The evolving landscape of cryptocurrency custody is a critical component of the broader digital asset ecosystem. As this chapter has explored, the dichotomy between self-custody and third-party custody reflects broader challenges and opportunities within the space. Self-custody offers unmatched control and autonomy, but it requires significant responsibility and technical proficiency to ensure that funds are managed securely. On the other hand, third-party custody services provide convenience and enhanced security for those less technically inclined, but they reintroduce risks associated with centralization and counterparty reliability, as seen in notable cases like the FTX collapse. The decision between these custody options depends on a careful evaluation of individual needs, technical capabilities, and risk tolerance.

Looking forward, the future of cryptocurrency custody is likely to be shaped by increasing regulatory scrutiny, technological advancements, and growing institutional interest. One can expect more stringent regulatory frameworks that will compel custody providers to adopt higher standards of security, transparency, and operational integrity, such as the MiCA regulatory body in Europe. Innovations in multi-signature wallets, hardware security modules, decentralized custody solutions, and privacy-preserving technologies, such as zero-knowledge proofs (Baldimtsi et al., 2024), may also offer new ways to balance the benefits of self-custody with the security assurances of third-party providers. As the cryptocurrency market matures, custody solutions will continue to evolve, playing a crucial role in the broader adoption and integration of digital assets into the global financial system. Users and institutions alike must remain vigilant and informed, ensuring that their choice of custody aligns with their broader financial strategies and risk management practices.

References

Asmakov, A. (2022, December 20). *What Are Proof of Reserves and Why Do They Matter?* Retrieved September 22, 2005, from Decrypt: https://decrypt.co/resources

/what-are-proof-reserves-why-do-they-matter.

Baldimtsi, F., Chalkias, K. K., Ji, Y., Lindstrøm, J., Maram, D., Riva, B., Roy, A., Sedaghat, M., & Wang, J. (2024). zkLogin: Privacy-preserving blockchain authentication with existing credentials. From arXiv: https://doi.org/10.48550/arXiv.2401.11735.

Carvalho, A., Merhout, J. W., Kadiyala, Y., & Bentley II, J. (2021). When good blocks go bad: Managing unwanted blockchain data. *International Journal of Information Management*, *57*, 102263.

Chawaga, P. (2022, June 30). *Honk, Honk, HODL: How Bitcoin Fueled The Freedom Convoy And Defied Government Crackdown*. Retrieved August 25, 2024, from Bitcoin Magazine: https://bitcoinmagazine.com/culture/how-bitcoin-fueled-canada-trucker-convoy.

Hamilton, I. A. (2022, July 24). *The Quest to Find $181 Million in Bitcoin Buried in a Dump*. Retrieved August 25, 2024, from Business Insider: https://www.businessinsider.com/james-howells-threw-away-bitcoin-dump-masterplan-get-back-2022-7.

Roth, E. (2022, November 30). *Here's Everything That Went Wrong with FTX*. Retrieved August 25, 2024, from The Verge: https://www.theverge.com/2022/11/30/23484331/ftx-explained-cryptocurrency-sbf-sam-bankman-fried.

Tsang, A. (2016, August 3). *Bitcoin Plunges After Hacking of Exchange in Hong Kong*. Retrieved August 25, 2024, from The New York Times: https://www.nytimes.com/2016/08/04/business/dealbook/bitcoin-bitfinex-hacked.html.

Wieczner, J. (2018, April 19). *Mt. Gox and the Surprising Redemption of Bitcoin's Biggest Villain*. Retrieved August 25, 2024, from Fortune: https://fortune.com/longform/bitcoin-mt-gox-hack-karpeles/.