Introductory Overview: Custody of Digital Assets

Quadrangle

Within the realm of traditional assets, institutional custodians serve to safekeep client assets and may offer additional services including clearing and settlement. While the same can be said for custodians of digital assets, there are additional nuances to consider in this digital context. These nuances arise notably from the ownership characteristics of digital assets.

Digital assets exist on distributed blockchain networks, such as Ethereum. These assets do not actually reside within the wallets of their owners, but rather digital asset ownership is attributed to wallets based on the immutable transaction records of the blockchain. Wallets store private keys, which effectively serve as passwords to prove ownership of and access to assets. Wallets can take various forms, from software apps to a thumb drive-type hardware wallets, or even a piece of paper stored in a vault. As access to a wallet entails the ability to use and prove ownership of its assets, security of wallets is critical in the digital context.

Unlike traditional assets, custodians are not directly safeguarding the actual digital assets, but rather through means of safeguarding the private keys to the wallet that proves ownership of and enables access to the assets. The variety of custodial offerings for digital assets has arisen largely due to these complexities around ownership. Three key types of custody for such assets are as follows:

1. Cold Storage – private keys are stored completely isolated from the internet, also typically requiring in an institutional setting that the custodian holds all keys. If the custodian is in possession of the private keys, the client must rely wholly on the custodian to access and transact with their assets.

2. Warm Storage – each the custodian and the client hold a portion of the keys. This forms a multi-signature wallet that requires signatures from both parties to approve any transaction, typically entailing some exposure of keys to the internet. For a warm storage setup, clients will typically hold a backup of the keys (e.g., in a safe) that enables the client to move coins without involvement of the custodian if needed.

3. Hot Storage – web-based, mobile, and desktop based-wallets are connected to the internet, offering more flexibility and efficiency to transact. Yet with this connectivity also comes potential vulnerability to hacks.

Cold storage is generally agreed upon as the most secure of the above-mentioned methods, and hot storage the least. Yet with additional security coming at the expense of more robust processes, more secure options tend to offer less flexibility in the ability to quickly transact. Deciding which storage option works best for you might entail consideration of both strategy and risk tolerance, and ultimately finding the optimal balance between usability and security.

Another factor to consider when selecting custodial services for digital assets is access to exchanges. Some custodians offer access to dozens of exchanges, while others may offer access to a more limited set of exchanges. The differences in access to exchanges can equate to differences in access to liquidity. These topics will be further explored in subsequent Resources on the QDS Platform.

Quadrangle has the expertise and experience to review, analyze and negotiate Custody and other digital asset-related counterparty contracts. Please reach out to your Quadrangle Contact to leverage us for such services as needed.

Quadrangle

Disclaimer

This presentation and its contents are privileged, confidential or otherwise protected from disclosure and is intended only for the individuals or entities named above and any others who have been specifically authorized to receive it. This presentation is for informational purposes only and does not constitute legal, tax, or investment advice or recommendations. Your acceptance of this presentation from Quadrangle Consulting LP ("Quadrangle") constitutes your agreement to (i) keep confidential its contents, (ii) not disclose its contents to any other person or use any such information for any purpose other than pursuant to evaluating a business proposal/relationship with Quadrangle, (iii) not to copy or disseminate it, and (iv) promptly return or destroy the presentation upon Quadrangle's request. Thank you.