What Can the History of Securities Markets Teach about Crypto Custody?

Contributed by Lisa LeFever

As digital assets become more popular, many questions surrounding their custody and safekeeping remain unanswered. The lack of standard custody protocols for digital assets has left many susceptible to loss through fraud, hackings, or improper handling of private keys. The application of traditional custody regulation to these innovative products has created consequential legal uncertainties that hinder institutional adoption. In order for this new asset class to flourish, the industry needs agreed-upon custody practices, regulatory clarity, and a greater understanding of the prevalent custody risks.

This article will offers potential solutions to these issues. First, we will provide a brief overview of custody in the traditional securities markets and how it compares to the world of digital assets. Then, we will describe current custody practices in the space and the related legal issues. Finally, we will discuss how legal and regulatory clarity will provide a foundation for these improved industry standards to develop. This will involve defining what custody, possession, and control mean in the context of digital assets. We will consider what best practices for the custody of digital assets might look like and proposing solutions which would bring security and stability to the marketplace.

Introduction

Modern products like blockchain-based assets challenge the traditional notions of custody. Investors have been trading on cryptocurrency exchanges, many of which function without the safeguards of traditional stock exchanges. In 2018, hacks reportedly reached upwards of $1.7 billion, representing a 400% increase over the previous year. Crypto exchanges also faced liquidation for mismanagement or private keys, fraud, and embezzlement.

Many established custodians find themselves unprepared to handle complex digital assets, which oppose the business model of centralized custody by representing a return to a system of decentralized ownership. Some of the largest custodians and Central Securities Depositories (CSDs) have announced that they are exploring custodial solutions for digital assets. The London Stock Exchange recently invested $20 million in Nivaura, a company looking to use blockchain technology to eliminate the “complex and paid chain of custody” we have today.

When reviewing the framework in securities markets, the following typically applies: (1) Regulation is in place to protect investors in the traditional marketplaces. (2) As technological solutions have been introduced in the securities industry, regulators like the SEC and FINRA have placed greater emphasis on reviewing a firm's technological infrastructure.

What is Custody and How Does It Work Today?

Custody generally refers to the safekeeping of assets. A custodian's role is to provide an efficient means of accounting and transfer, as well as protecting assets from theft, loss, and misuse.

Custody became an important aspect of securities markets after the “paper crunch” or “back office crisis” of the 1960s. During that time, our financial markets experienced exponential growth. This created back office overload as firms tried to process investors’ paper stock certificates.

The backlog resulted in markets shutting down, billions of dollars of failures to deliver or receive securities, and hundreds of brokerages declaring bankruptcy. Firms experienced what the Securities and Exchange Commission (SEC) called a “new phenomenon”–”the loss of control over the securities which were supposed to be in their possession for delivery, custody or safekeeping.”

When it became no longer feasible for individual investors to hold physical shares, two solutions were presented:

- ♦ dematerialization (meaning the conversion of all paper securities into electronic form), or
- ♦ immobilisation (meaning the shares would be collected and held by intermediaries or CSDs that account for and transfer them on their books).

Market participants favored the first option, proposing a direct, decentralized ownership registry using dematerialized shares, where investors’ names stayed on the issuers’ shareholder list. Regulators noted the difficulty in implementing dematerialization as each state would have to amend their blue sky laws to permit the change.

Today, after decades of immobilisation, most investors would never see or hold paper stock certificates. Ownership is recorded as a book entry by a third-party who hold the securities in “street name” for the benefit of the true owner or “beneficial owner.” The intermediary (i.e. a broker-dealer, bank, or trust company) acts as a fiduciary passing on the rights associated with ownership, like voting or receiving dividends, to the beneficial owner.

How are Custody Arrangements Historically Regulated?

Through the Securities Act Amendments of 1975, regulators set new standards for broker-dealers’ books and records, custody practices, and use of customer funds and securities. It required that the SEC use its authority “to end the physical movement of securities certificates in connection with the settlement among brokers and dealers,” effectively mandating share immobilisation.

For entities registered under the Investment Advisers Act of 1940 (the Act), Rule 206(4)-2 (known as the “Custody Rule”) requires, with few exceptions, that client assets be held by a “qualified custodian.” Advisers must also comply with the Rule's annual audit requirement and submit notice to clients detailing how their assets are being secured.

What is the Problem with this Setup?

The custody framework developed over the last half century has encountered various issues. For example, the case of Dole Foods. This was a going-private transaction which led to litigation where shareholders submitted claims for more shares than actually existed. This demonstrated a weakness in the book entry system. The judge who oversaw the matter cited in his opinion that blockchain technology could prevent similar missteps and provide “a single and comprehensive stock ownership ledger.”

How does Custody Differ for Digital Assets?

Crypto assets offer the direct, decentralized ownership that was desired at the time of the 1975 Amendments: they are digitally native bearer instruments with no physical form. As opposed to book entry, they are secured on a blockchain through cryptography using strings of digits making up the public and

private keys–one acting as a shareable address and the other like the password necessary for access. Just as holding stock certificates historically denoted ownership, possession of the private keys conveys ownership in the world of digital assets.

Broadly speaking, private keys are held through hot or cold storage. Hot storage refers to keys being stored through an online medium such as an exchange or wallet service connected to the internet. Cold storage (which is typically viewed as the safer of the two) refers to storage disconnected from the internet or "air gapped." This would usually take the form of a hardware device (Ledger, Trezor, etc.) or even a paper wallet.

Multi-signature arrangements allow multiple parties to hold the private keys and any "x of y" combination can be set to establish prerequisites for transfer. For example, 2-of-3 multi-signature is commonly used, where two of the three "key holders" must sign off on transactions.

What are the Current Approaches to Custody in the Crypto Space Generally?

Most cryptocurrency exchanges are centralized, meaning they maintain users' digital assets (i.e. private keys) which are often commingled in an omnibus exchange wallet. Decentralized exchanges, on the other hand, are "non-custodial," allowing users to keep full control over their private keys.

Other platforms provide a hybrid approach that combines features of centralized and decentralized exchanges. In such a setup, multi-signature can be used to mimic the risk-sharing infrastructure of stock exchanges by giving one key to the owner, exchange, and an intermediary like a clearing firm. Thus, users maintain their private keys while being protected in case any one key holder loses the key.

Conclusion

The distinctive features of digital assets introduced above require re-evaluating custodial services. In our next installment, we will take a deeper look at the custody practices in the crypto space and their potential legal implications to lay the groundwork for proposed improvements at both the industry and regulatory level.