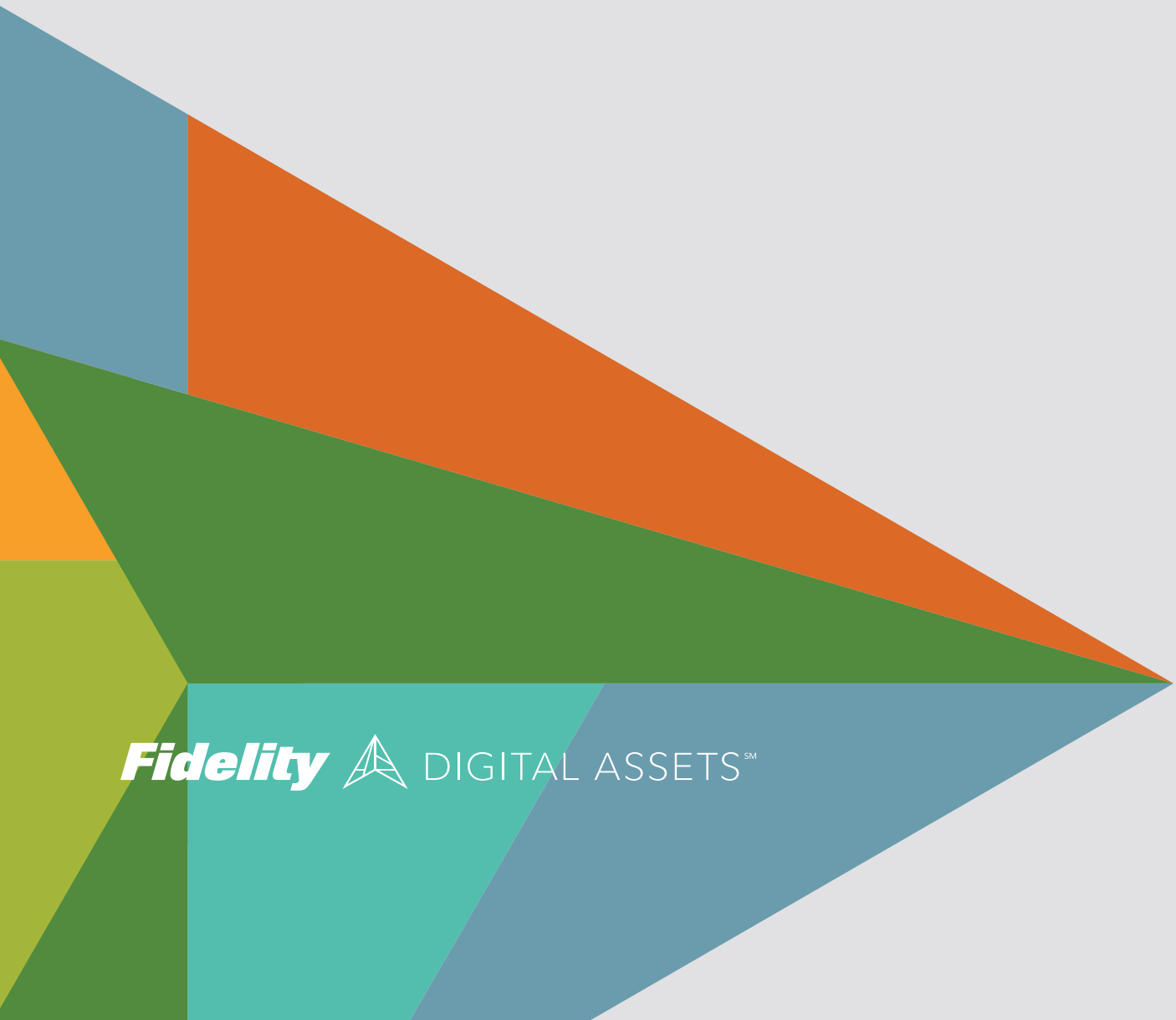
CUSTODY IN THE AGE OF DIGITAL ASSETS

OCTOBER 2018



Fidelity DIGITAL ASSETS℠

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The market for digital assets has evolved dramatically since the release of Satoshi Nakamoto's Bitcoin white paper nearly ten years ago.

From Bitcoin's origins as a peer-to-peer system of value transfer to the development of smart contracts and countless other blockchain applications, cryptography-based digital assets have become one of the most disruptive and revolutionary technologies since the advent of the internet.

Today there are at least 1,600 crypto coins and tokens, according to CoinMarketCap.com. Although it may be hard to think of another market that has developed as quickly, it is not difficult to see parallels between the development of digital assets and that of traditional asset classes such as stocks, bonds, and commodities.

Digital assets may soon become recognized as investable "stores of value," tradable on global, licensed exchanges, and accessible to a broad swath of individuals and institutions across the globe. And just as with stocks, bonds, or commodities, investors will want to keep these assets safe from theft or loss.

As the industry has evolved, solutions aimed at keeping digital assets safe have continued to develop. Enhancements to offline storage, multi-signature protocols, and other security measures are aimed at increasing investor confidence that their assets are secure. These developments are important, but for institutions holding digital assets on behalf of their clients, they may not go far enough.

For institutions, the most pressing unanswered question is how—if they choose to hold digital assets for their customers—these assets will be secured. The answer is that full-service institutional custody solutions are needed—solutions as equally robust as those provided for traditional assets. Most digital assets function as cryptographic bearer instruments, the keys to which, once lost or stolen, render the asset inaccessible and unrecoverable to its rightful owner, making secure custodianship of primary importance. Custody services for these types of assets are particularly technological, requiring new and different approaches, yet are based on sound financial principles.

In this white paper, we explain why custody services are of paramount importance to institutions and their clients, how financial custody services have evolved, and what all this means going forward for those holding digital assets. Additionally, we will cover:

- The history of financial assets custody
- An overview of the current landscape for digital asset custody
- Unique challenges associated with the custody of digital assets
- Key unanswered questions
- Our perspective

This primer is intended to be an educational tool for institutions seeking a better understanding of the custody issues surrounding this emerging asset class.

For simplicity and consistency, the term "digital assets" is applied broadly throughout this white paper to describe bitcoin and other cryptocurrencies, cryptographically issued securities, and other digital tokens.

CUSTODY THROUGH TIME

In the simplest terms, custodians safekeep financial assets. Financial institutions acting as custodians do not have legal ownership of stocks, bonds, commodities, or other assets—those rights remain with the individual or institution that own the asset—but they are tasked with holding and securing these assets, as well as performing other functions such as settlement services, recordkeeping, and foreign-exchange transactions.

US financial markets have long benefited from investors having confidence that their money is secure, but this hasn't always been the case.

Before the Stock Market Crash of 1929, investors were responsible for securing the paper certificates that claimed rights to their investments. This form of self-custody, however, started to fade away rapidly after the crash, because investors recognized the inherent risks in this system.

Custody /'kʌstədi/

The protective care or guardianship of someone or something.

OXFORD ENGLISH DICTIONARY

It was around this time that trust companies and other financial intermediaries evolved to provide custody services for the holders of stock certificates. Given the lack of technology during this period, these services involved the cumbersome physical transfer of certificates from one financial institution to another.

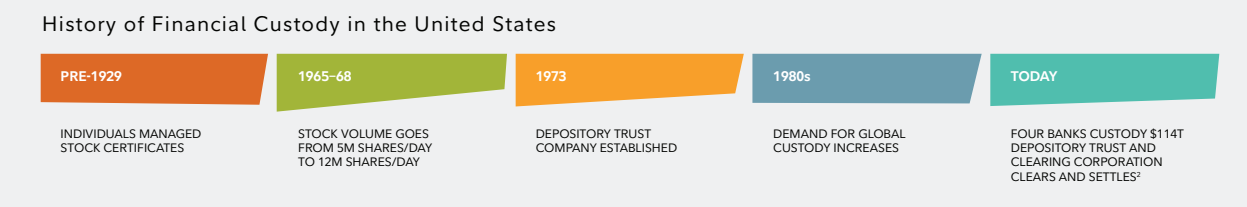
From the 1930s through the 1960s, the number of securities exchanged in the United States grew exponentially. From 1965 to 1968 alone, the trading volumes on the New York Stock Exchange jumped from five million shares a day to 12 million,[1] leading to a significant increase in the paperwork required to custody, clear, and settle these transactions. The trust companies and intermediaries were quickly becoming overwhelmed with these changing ownership records.

1. Wyatt Wells, "Certificates and Computers: The Remaking of Wall Street, 1967 to 1971." *The Business History Review.* 74, no. 2 (Summer 2000): 193–235.

This paperwork burden and its inefficiencies, along with growth in the securities markets and the need for securities-related services, led to the 1973 creation of what would become The Depository Trust & Clearing Corporation (DTCC), which established the first set of centralized ledgers and certificates of clearing. Eventually, depository functions throughout the United States would be consolidated into the DTCC.

Shortly after the creation of the DTCC, the Employee Retirement Income Security Act of 1974 (ERISA) became law, making significant changes to how US pension funds invest and manage assets. Key to these changes was the requirement that plans separate investment management and custody of plan assets.

As mutual fund investing accelerated, "global custody" became a necessity as investors required custodians to secure their investments across an ever-increasing number of securities from around the world. Today four large banks (BNY Mellon, J.P. Morgan, State Street, Citigroup) provide the bulk of global custody services with approximately $114 trillion in assets under custody.[2] Recent trends suggest this highly concentrated model will continue, as ongoing barriers to entry have prevented other firms from challenging these incumbents.[3]



2. Trefis Team. "Largest Custody Banks Overcome Industry Headwinds to See Further Growth." https://www.forbes.com/sites/greatspeculations/2018/05/18/largest-custody-banks-overcome-industry-headwinds-to-see-further-growth/#16002394363b.
3. Thorsten Ehinger, Promila Gurbuxani, Jonathan Klein, and Matthias Voelkel. "A Calm Surface Belies Transformation in Securities Services," McKinsey & Company, March 2018.

DECENTRALIZATION, REVISITED

In many ways, the creation of Bitcoin and its underlying blockchain technology has turned our understanding of custody and asset ownership on its head. Because blockchain technologies enable the confirmation of transactions without the need for centralized verification, questions of asset ownership can be answered more efficiently and with more clarity than in the past.

This ability to instantly and accurately identify who owns a particular asset without requiring a third-party intermediary will have a profound impact on financial services transactions, including the clearing and settlement of securities and other asset transactions. Blockchain architecture may also dramatically alter how securities are traded and settled, potentially altering the future role for those deeply involved in the current process.

This transformation is important for a number of reasons, including the potential for reduced systemic risk, since securities will no longer be held and cleared through the same few entities. Paradoxically, a system of clearing, settlement, and custody that started as completely decentralized and is now fully centralized may end up once again being decentralized by the technologies behind digital assets.

From Paper to a Decentralized Model

Of the lessons learned from the 2008 financial crisis, many agree a system centered around complicated, opaque investment products issued by a central few may require a dramatic update. Would things have been different had the transactions of the large investment banks and brokerages been recorded on a distributed, decentralized blockchain?

The move to the DTCC was a move away from bearer assets (which became cumbersome to manage) and toward a system of interconnected ledgers with costly reconciliation processes between those ledgers. What we're witnessing with digital assets is a move back toward bearer assets—now that users of these protocols have figured out how to trade them quickly, digitally, and without any possibility for the types of errors that lead to costly reconciliation processes.

DIGITAL ASSET CUSTODY TODAY

It's important to remember that with digital assets, such as bitcoin and ether, individuals can hold essentially an unlimited amount of currency, almost anywhere. Unlike paper and metals, for example, digital assets do not require the traditional safes and vaults typically associated with banks.

This type of accessibility to spendable assets is groundbreaking and fascinating, to say the least. But it also has created new risks. When bitcoin was first traded, there were no offline storage products or third-party services offering to keep it safe. As bitcoin became more visible and interest increased, additional digital tokens emerged and the ecosystem began to rapidly develop, providing a variety of services to keep these digital assets secure.

As part of this evolution, exchanges appeared that—unlike registered stock exchanges—were taking custody of digital assets in addition to providing a trading venue. However, it has become apparent that exchanges, by themselves, are not immune to security failures. Institutional concerns for client safety have fueled the demand for custodial services, separate from exchanges that can provide safe, secure storage for digital assets.

UNIQUE CHALLENGES

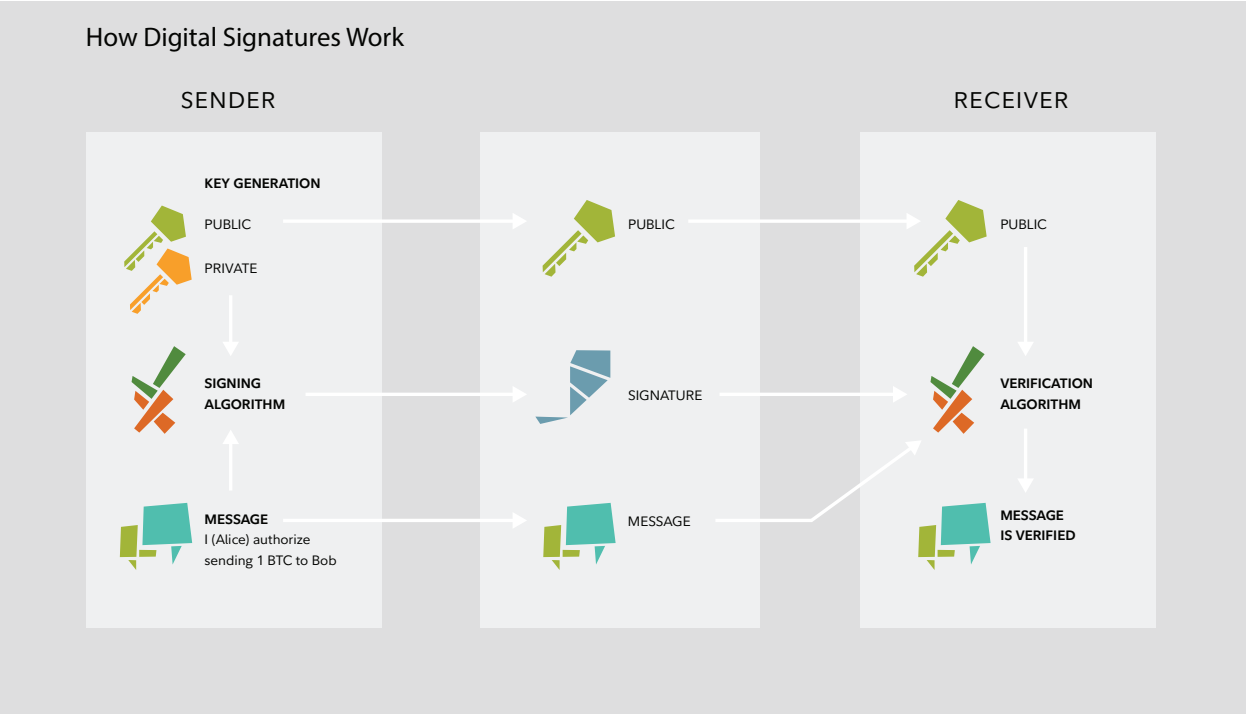
There are aspects to the custody of digital assets that contrast sharply with the security necessary for the safekeeping of stocks and other types of assets. These distinctive features present a number of challenges, the most notable being how to secure the private keys of the owners of the digital assets being stored.

Private keys are a unique, large number generated by a digital asset wallet and assigned mathematically to transactions originating from that wallet. The private key is entirely specific to the holder. Private keys are used to confirm that the owner of a digital asset is in fact who he or she claims to be via cryptographic digital signature technology.

Because these keys represent ownership of digital assets, they are never shared publicly. Instead, for digital asset transactions, a *public* key is shared with parties to the transaction, which functions as a destination address for receiving funds. For a digital asset to leave its wallet, the owner of the wallet needs to "sign" using his or her private key, which again is not shared publicly. The decentralized network of computers (nodes) then verifies the transaction details before permanently adding them to the ledger on the blockchain.

A familiar analogy for this public key cryptography is that the public key is like your email address, and the private key is like the password to your email account. You'd never share your password with a friend, but you do freely share your email address. Just as your friends can send a message to your email address, they can send digital assets to a digital asset address that is computed from your public key and can be freely shared.

This analogy isn't perfect; the private key is more akin to cash than an account password. Passwords can be reset, private keys cannot. The alphanumeric strings identify the owner of a digital asset, and—because of the immutable nature of cryptography—if these keys are lost or stolen, so too is the digital asset.



To make owning digital assets more accessible, custodial wallet providers and exchanges hold digital assets on behalf of the individual owner, giving the wallet provider (or exchange) full control over transactions. A benefit of this approach is that if the keys or passphrases to access the account are lost, the wallet provider can take steps to verify identities, making it easier to recover access.

Because custody services require that the owner of digital assets hand control to a third party, it is imperative that the custody provider demonstrate vigorous security measures and robust technological protections. Without these rigorous technology, cyber, and operational procedures, digital assets could be put at risk.

According to a 2017 study,[4] 73 percent of digital asset exchanges take custody of private keys while 23 percent let users maintain control over their keys. About three-quarters of large exchanges and just over one-half of small exchanges have a written policy in place for what happens in the event of a security breach.

4. Dr. Garrick Hileman and Michel Rauchs, "Global Cryptocurrency Benchmarking Study." Cambridge Centre of Alternative Finance. Judge Business School of the University of Cambridge, 2017.

Currently, there are several approaches to safekeeping private keys. Those online are typically called "hot" storage while offline storage is referred to as "cold."

- *Hot Storage:* Some of the most well-known exchanges provide this type of online wallet. Hot storage makes accessing and transacting with digital assets easy by keeping the private key online for accessibility by the user, which can leave the wallet and its user vulnerable to a security compromise. Generally speaking, for security reasons, most people prefer to keep as little of their digital assets in a hot wallet as possible.
- *Cold Storage:* This could mean using a USB or digital asset–specific hardware storage product to control private keys, or simply keeping paper copies of private keys stored in vaults or other secure places. Cold storage is considered by many to be a preferred solution (some firms use cold storage exclusively). Cold storage adds a manual step to accessing digital assets but provides an additional level of security. This approach is sometimes compared to how gold is stored, but, as we stated earlier, digital assets possess a number of unique attributes and make it difficult to draw perfect comparisons with the way traditional assets are safeguarded.
- *Multi-Signature:* This new type of security provision is unique to digital assets and could affect the way the financial industry designs custody for other asset types in the future. By requiring more than one key to sign a transaction to send digital assets, the "multi-sig" approach ensures that one person is not solely responsible for securing a private key, without ceding all the responsibility to a third party.

Security solutions for individual investors continue to evolve. Many of these solutions include combinations of hot, cold, and multi-sig security. Some have proposed creating digital vaults that could make it easier to recover stolen or lost digital assets.[5] Dozens of start-ups and established firms are developing ways to secure digital assets, but to date, few have focused on the unique challenges of institutional investors.

5. Malte Möser, Ittay Eyal, Emin Gün Sirer, "Bitcoin Covenants," 2016.

THE NEED FOR INSTITUTIONAL SOLUTIONS

Institutional clients represent a broad spectrum of financial firms, including mutual funds, investment managers, family offices, public and private retirement plans, registered investment advisers, insurance companies, corporations, endowments, and foundations. As many of these institutions serve as stewards for their clients' assets, these institutions must work with a custodian that can demonstrate a significant track record and experience in safeguarding client assets. Institutional investors need to know who is holding on to—and securing—the private keys.

For these institutions, self-custody is essentially a nonstarter, primarily due to regulations and the legal obligations that define their fiduciary responsibilities. Self-managed hardware wallets, regardless of how secure, are not a feasible option for a number of reasons.

Institutional investors do not want to worry about private keys or maintaining passphrases for individual digital assets. Fortunately, the ecosystem is evolving to help increase access to products that will provide the same level of custodial service expected for other assets, despite the regulatory uncertainty.

OUTSTANDING QUESTIONS

The custody requirements for digital assets have steadily evolved with this maturing asset class. The key issues for institutional investors generally fall into the following categories:

- *Regulatory:* How will existing regulations be applied to digital assets, and how will regulators respond to the growth of this asset class with new rules and guidance? Will policymakers take a dim view of pension plans investing in digital assets? Will digital asset firms pursue bank charters to offer bona fide custody services? Is every custodian in a multi-sig protocol considered an equal-part custodian?
- *Market/Network Challenges:* For custodians, trading digital assets in a volatile environment with a third party carries its own challenges. How will custodians respond to token "airdrops" or bitcoin forks, for example? Will digital asset volatility limit the number of firms offering custody services?
- *Security:* How will security processes and standards evolve? How will institutional clients and custodians implement the highest levels of protection for digital assets? Will there be industry insurance solutions that will give institutions and their clients more comfort?

Before traditional custodians go too far in their development of institutional quality services, the industry is hoping to see more institutional money in the space. However, institutional investors are finding it difficult to commit fully to digital assets until there is a reliable and respected custody solution.

OUR PERSPECTIVE

We expect continued growth in digital products and services, with many of them aimed at institutional investors. While this asset class continues to evolve, one constant is that the institutional adoption of digital assets depends on the arrival of professional custody solutions.

Creating digital asset custody solutions will demand the continued efforts of a number of market participants, ranging from wallet providers to security firms, technology developers, and regulators. We also believe that as additional reputable firms enter the space, there will be an increase in market participation, contributing to the viability of digital assets.

Over time, we believe securities will also become digitally native, and these assets will be more quickly introduced to market compared to new issuances today. We aim to be ahead of the curve.

We are focused on meeting our clients' demand for digital asset products and services, which require real innovation—leveraging some existing processes—but evolving quickly to meet the demands of this digital asset space. This includes more efficient ways to enable value transfer, the settlement of financial transactions, as well as more robust and secure protocols.

The technology is transformational, but institutions might not want to be transformed just yet—they want a solution they understand, as part of a long-term commitment to innovation.

Addressing custody issues for institutional investors is one critical step for these markets to continue to develop. The introduction of enterprise-ready tools and solutions for institutional clients is a clear sign of a future that will enable scalability and more widespread adoption. As we continue to observe progress in this space, we are encouraged by what the future holds.

Fidelity DIGITAL ASSETS℠

862518.1.0 1.9892024.100