Blockchain and Custody of Digital Assets

DAVID J. KAPPOS, D. SCOTT BENNETT, AND MICHAEL E. MARIANI, CRAVATH, SWAINE & MOORE LLP

Search the Resource ID numbers in blue on Westlaw for more.

This Article examines the concepts and application of current law, rules, and regulations regarding the custody of digital assets.

Blockchain has introduced new questions about what it means to have "custody" of an asset. On July 8, 2019, the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) issued a joint statement in which the staffs of both institutions recognized that digital asset securities and related innovative technologies raise novel and complex regulatory and compliance questions and challenges. On the legal side, the challenge is to apply laws and regulations that were enacted in an era before Blockchain and digital asset securities. On the practical side, the challenge is to adequately prevent fraud or misappropriation without getting rid of the very same advantages that led to the development of blockchain and digital asset securities in the first place. Therefore, finding the correct balance between these sometimes competing objectives is one of the most fundamental challenges for digital asset custodians.

For more information on blockchain and distributed ledger technologies generally, see Blockchain Toolkit (W-018-8660).

This article provides an overview of:

- The laws, rules, and regulations applicable to custodians, and how these rules have been applied to the custody of digital assets.
- Typical services provided by custodians.
- Specific issues relating to digital asset custody, including the risk of loss or theft of the private keys associated with the digital assets.
- Some possible solutions to these issues, including insurance arrangements and precautionary procedures.
- Current market developments, including an overview of services currently provided by digital asset custodians.

OVERVIEW OF THE CONCEPT OF CUSTODY

In the context of securities laws, custody generally refers to independent third parties holding, safekeeping, and administering funds or securities on behalf of investors, to protect investors from fraud, theft, or misappropriation. However, maintaining custody of securities by using independent third-parties has not always been the norm. Before the stock market crash of 1929, self-custody was the rule and investors themselves secured the paper certificates that represented their rights. After the crash, the inherent risks of self-custody prompted the appearance of financial intermediaries that provided custody services.

This shift from self-custody to custody by independent third-parties did not eliminate all threats to investors, which became subject to the risks of fraud and misappropriation by the custodians of their securities. To combat these risks, legislative protection came about in legal and regulatory provisions that established certain conditions that must be satisfied by custodians to hold clients' securities, including:

- Segregating clients' assets.
- Sending notices to clients.
- Regularly conducting audits.

The custody industry has grown exponentially, spurred on by the mandatory use of custodians for certain market players and the continuous growth of trading volumes of securities exchanged in the US. For example, the four largest custodians globally (BNY Mellon, State Street, JPMorgan and Citigroup) had custody of $114.2 trillion of assets in the second quarter of 2018 and were responsible for nearly half of the total global custody of assets.

The methods for holding custody of securities have also evolved over time. Custody was historically performed by safekeeping the paper certificates that represented individual shares or principal amounts owned by the custodian's clients in the custodian's vault. With the advent of central securities depositories, custodians increasingly kept custody of clients' securities by using electronic book-entry in the clients' securities accounts.

The latest custody revolution stems from the introduction of distributed ledger technologies, which enable independent participants to reach consensus on the validity of data and record this consensus on a shared electronic ledger that is constantly updated to reflect the addition of new agreed-on data. Blockchain, in turn,

"is a particular type of distributed ledger in which data (transactions) is grouped into blocks and then chained together in chronological order using a cryptographic mechanism ... [which] creates a virtually irreversible record of all transactions that can be referenced in the future to prevent users from double-spending their digital assets" (see Article, Digitized Securities and the Promise of Automated Compliance (W-022-4261)).

LEGAL AND REGULATORY REQUIREMENTS AROUND CUSTODY

Below is a summary of the main provisions of the federal securities and commodities laws that relate to custody in general and their possible applicability in the context of digital assets. This is not a detailed discussion about the often complex requirements and intricacies of these bodies of laws, but rather gives an overview that helps understand some of the main obligations underpinning the provision of custody services and to serve as a starting point for a more detailed discussion about the main issues the custody of digital assets presents in practice.

THE EXCHANGE ACT AND THE CUSTOMER PROTECTION RULE

Together with the Securities Act of 1933 (Securities Act), the Securities Exchange Act of 1934 (Exchange Act), was "designed to restore confidence in the capital markets by providing investors and the markets with more reliable information and clear rules of honest dealing" (see SEC: What we do). The Exchange Act established the foundation for securities regulation and enhanced the federal government's role in the regulation of the business world.

Considering their importance in the securities industry, Section 15(a)(1) of the Exchange Act requires registration of broker-dealers with the SEC. Because custodians are compensated by commissions or transaction fees related to securities activity, custodians are classified as brokers for purposes of this Rule. The Exchange Act places various requirements on broker-dealers (and therefore custodians), including minimum regulatory capital requirements (for information on capital requirements for broker-dealers, see Practice Note, Capital Requirements for Broker-Dealers (W-020-6415)), restrictions on the distribution of assets to affiliates, regulation concerning the handling of customers' funds and securities, anti-money-laundering and know-your-customer requirements (for information on anti-money laundering requirements for broker-dealers, see Practice Note, Broker-Dealer Anti-Money Laundering Program: Overview (W-002-9203)).

However, Section 3(a)(4)(B)(viii) of the Exchange Act exempts certain banks that, as part of their customary banking activities, provide safekeeping or custody services from the Exchange Act's registration requirements. The custodial activities of these banks remain subject to banking law regulations, which also require asset segregation and recordkeeping.

Under its regulatory authority under the Exchange Act, the SEC adopted SEC Rule 15c3-3 (Customer Protection Rule) in 1972 as a response to the 1968 Wall Street Paperwork Crunch, which resulted in the failure of many firms and losses to their clients. The Customer Protection Rule is designed to give additional protection to customer funds and securities, "in effect forbidding brokers and dealers from using customer assets to finance any part of their businesses unrelated to servicing securities customers; e.g., a firm is virtually precluded from using customer funds to buy securities for its own account." At its core, the Customer Protection Rule mandates that broker-dealers obtain and maintain physical possession or control of fully-paid and excess margin securities free of liens or any other interests at a good control location, such as with a third-party custodian.

INVESTMENT COMPANY ACT OF 1940

Under the Investment Company Act of 1940 (ICA), an "investment company" is any issuer that:

- Is or holds itself out as being engaged primarily in the business of investing, reinvesting, or trading in securities.
- Is engaged or proposes to engage in the business of issuing face-amount certificates of the installment type or has been engaged in that business and has any certificates outstanding.
- Is engaged or proposes to engage in the business of investing, reinvesting, owning, holding, or trading in securities, and owns or proposes to acquire investment securities having a value exceeding 40% of the value of this issuer's total assets.

Section 17(f)(1) of the ICA provides that every registered management company must place and maintain its securities and similar investments in the custody of:

- A bank.
- A company that is a member of a national securities exchange.
- The investment company itself.

Rules 17f-1 and 17f-2 of the ICA require that the securities and similar investments held in custody by broker-dealers that are members of a securities exchange or by banks, respectively, must at all times be segregated. As clear evidence of a rule enacted before the era of digital assets, Rule 17f-1 states that segregation may be accomplished by putting the securities in separate containers bearing the name of the registered management investment company or by attaching tags or labels to these securities and investments.

Self-custody subjects investment companies to various requirements, including surprise physical inspections by an independent public accountant, procedures that must be followed for the deposit and withdrawal of securities, recordkeeping requirements, and the need to develop systems to enable trading.

INVESTMENT ADVISERS ACT OF 1940 AND THE CUSTODY RULE

Relevant definitions

The Investment Advisers Act of 1940 (IAA) uses specific terminology while describing the obligations placed on custodians. As used during our discussion of the IAA, the following terms have the below meanings.

Custody is holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them. Custody includes:

- Possession of client funds or securities.
- Any arrangement (including a general power of attorney) under which a person is authorized or permitted to withdraw client funds or securities maintained with a custodian on that person's instruction to the custodian.

- Any capacity (such as general partner of a limited partnership, managing member of a limited liability company or a comparable position for another type of pooled investment vehicle, or trustee of a trust) that gives legal ownership of or access to client funds or securities.

Investment advisers are those persons or entities that engage in the business of advising others, directly or indirectly, regarding the value of securities or regarding the advisability of investing in securities, for compensation.

Qualified custodians include:

- Certain banks and savings associations.
- Registered broker-dealers holding client assets in customer accounts.
- Registered futures commission merchants holding client assets in customer accounts (but only regarding client funds and security futures or other securities incidental to transactions in contracts for the purchase or sale of a commodity for future delivery and options involving that commodity).
- Foreign financial institutions that customarily hold financial assets for their customers, provided that the foreign financial institution keeps the advisory clients' assets in customer accounts segregated from its proprietary assets.

Main requirements of the Custody Rule

Subject to certain exceptions, when an investment adviser holds custody of clients' funds or securities:

- These funds or securities should be maintained by a qualified custodian, either in a separate account for each client under that client's name or in accounts that contain only the investment adviser's clients' funds and securities, under the investment adviser's name as agent or trustee for the clients.
- Notice should be sent to the client about the qualified custodian's name, address, and the manner in which the custodian maintains the funds or securities.
- Accountings must be sent to the client at least quarterly, identifying the amount of funds and of each security in the account at the end of that period, as well as all transactions during that period.
- An audit must be conducted, at least annually, by an independent public accountant at a time chosen by the accountant without prior notice or announcement.

APPLICABILITY OF THE FEDERAL SECURITIES LAWS TO DIGITAL ASSETS

One of the most often cited cases that discusses the applicability of securities legislation to digital assets arose after the Initial Coin Offering (ICO) by a decentralized autonomous organization called The DAO, which raised sums of around $150 million (see Cryptocurrency and other Digital Assets for Asset Managers, Blockchain and & Cryptocurrency Regulation, 2019). Following the exploitation of a security vulnerability and the removal of approximately $50 million from The DAO by a bad actor, the SEC's Division of Enforcement published the DAO Report. In the DAO Report, the SEC explained that digital assets can be considered investment contracts and, therefore, securities, if they satisfy the four elements of the Howey Test. This remains the applicable test to determine, on a case-by-case basis, whether a particular token or other digital asset, can be considered a digital asset security (For more information the Howey Test, see Practice Note, Security Defined: The Howey Test In Depth (0-578-9965)).

The SEC has recently sued Kik Interactive Inc. for a $100 million unregistered ICO. This case is of particular relevance, as the US District Court for the Southern District of New York is being asked to rule on the current interpretation of the Howey Test, with some expectation that a new test can be developed for digital assets (for more information, see Coindesk: Canada-based messaging app firm Kik has launched a crypto crowdfunding campaign to support a likely court battle with the U.S. Securities and Exchange Commission (SEC) over its 2017 initial coin offering (ICO)).

On the opposite side of the spectrum, the SEC has indicated that bitcoin and ether are not considered securities under federal securities laws because both of these digital assets are sufficiently decentralized such that purchasers cannot reasonably expect to derive profit due to the managerial efforts of a centralized third-party. Therefore, most provisions mentioned above are, in principle, not applicable to bitcoin or ether.

However, the SEC has not yet addressed whether virtual currencies constitute "funds" under the Custody Rule. If they do constitute "funds," then the requirements of the Investment Advisers Act applies to virtual currencies. Much clarity and guidance is still needed to determine the extent and degree of applicability of federal securities laws to digital assets and virtual currency and because of this, issues like the two described below arise.

Federal Securities Laws and the Difficulties Behind the Concept of "Control"

Federal securities laws, and in particular, the Customer Protection Rule, require custodians to have possession or control of the securities within their custody. Considering that digital asset securities do not exist in the physical world and therefore cannot be possessed, a custodian must "control" a digital asset security to have custody of it.

Digital asset securities exist merely as computer-coded entries on a distributed ledger, such as blockchain, visible to, and verifiable by, all nodes (that is, all the computers connected to the blockchain network, which keep a copy of the blockchain)(see The Custody of Digital Assets, Blockchain & Cryptocurrency Regulation, 2018). The ledger itself records every transfer effectuated on the blockchain network, but does not reflect who the record owner of the digital assets is.

Ownership of a digital asset is instead reflected in a string of numbers on the blockchain, accessible using the combination of a public key and a private key, similar to how a safe deposit box is accessible by the bank's key and the depositor's key. In this sense, "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." Public keys, on the other hand, are shared publicly and function as destination addresses. No digital asset can be transferred until the transferor enters his or her private key to authorize the transfer (see Custody in the Age of Digital Assets, Fidelity Digital Assets,

October 2018). In short, whoever knows the private key can "control" that particular digital asset.

At first glance, it seems as though custodians can satisfy the "control" requirement by holding both the public key and the private keys to a digital asset. Although this is certainly some form of control, it does not satisfy the control requirements present in the custody provisions of the federal securities laws, mainly because there is no guarantee of exclusive control. Holding a private key may not, by itself, be sufficient evidence that only the custodian has control over the digital asset, as the custodian may not be able to demonstrate that no other party has a copy of the private key. If another party holds the same private key, then that party can transfer the digital asset without the custodian's consent.

The concept of "control" also becomes confusing in the context of multi-signature arrangements, which require authorization by more than one private key before a transaction is broadcasted to the network. It may be the case that a custodian only has one of several private keys needed to complete a given transaction or to act in relation to a particular digital asset, in which case the custodian does, again, not have "control" over the virtual currency (see Custody and Transfer of Digital Assets: Key U.S. Legal Considerations, Blockchain & Cryptocurrency Regulation, 2019).

Federal Securities Laws, Audits of Custodians, and Sufficient Information Requirements

The Custody Rule provides for audits by independent accountants, but this may present difficulties in the context of digital assets as:

> "A custodian may be very reluctant to expose a private key to accountants, and accountants may not be able to confirm that a private key held by a custodian actually represents an ownership interest in the particular underlying digital asset. Unlike typical investments in securities and debt instruments, there are no registrar records, trusted securities intermediaries, trusted counterparties, administrative agents, or other traditional sources of ownership verification. Verifying ownership of digital assets may require technical expertise and knowledge that traditional accounting firms may not have at their disposal (see Custody of Digital Assets: Centralized Safekeeping of Decentralized Assets under the Investment Advisers Act, 2018)."

A similar concern has been expressed by the SEC and FINRA in their July 2019 Joint Staff Statement, in which they recognized that the nature and characteristics of digital asset securities may make it difficult for a broker-dealer to evidence the existence of these digital asset securities for the purposes of regulatory books, records, and fulfilling financial statement requirements, which may in turn create challenges for the broker-dealers' independent auditor.

CHALLENGES PRESENTED IN DEALING WITH CUSTODY OF DIGITAL ASSETS

The legal requirements outlined above have traditionally been fulfilled by using third-party custodians which hold possession or control of securities on behalf of investors. Today, custodians offer an ever-expanding spectrum of services related to the custody of digital assets. This increasing spectrum of services exposes custodians to an increasing number of risks. We briefly outline those services and risks in this section.

SERVICES DELIVERED BY CUSTODIANS

Custodians often offer a variety of services that go beyond the mere holding of securities. Although not all custodians offer all the same categories of services, the broad spectrum of possibilities can be classified in terms of:

- Core custody services, including:
  - safekeeping and record-keeping, such as recording the number of securities deposited;
  - asset processing services, such as providing services for income and tax processing, corporate action processing, securities valuation, and reporting;
  - transaction processing and settlement, such as enabling the delivery or receipt of the security and the related cash consideration; and
  - banking, such as processing payments and other transactions that result from client investment activities.
- Ancillary services, including:
  - agency securities lending services that enable clients to lend securities to other market participants; and
  - foreign exchange services, which are necessary when clients invest in securities from different countries or in a variety of currencies.
- Other administrative services, including:
  - fund accounting and administrative services, including the generation and calculation of a fund's net asset value;
  - transfer agency services, which generally consist of acting as the registrar of a fund, processing and recording subscriptions to and redemptions of fund shares by investors;
  - collateral processing services, including the verification of the amount of credit exposure, initial variation margin requirements, and executing margin calls; and
  - outsourcing services, such as transaction management, cash management, and record-keeping and accounting.

For more information on the services that custodians provide, see The Clearing House: Custody Services Provided by Banks Are Important to the Safekeeping and Management of Investments.

RISKS HISTORICALLY ASSOCIATED WITH THE CUSTODY OF SECURITIES

Some of the most significant sources for operational risks specifically relevant to custodians are:

- Corporate actions. Processing corporate actions relating to securities held under custody poses the risk that there may be errors or missed deadlines in exercising voting rights on mergers or extraordinary transactions, among others.
- Settlement. There is a risk that settlement instructions can be incorrectly entered or processed and, therefore, incorrect numbers,

amounts, or securities may be credited or debited to client accounts.

- Fiduciary risk. The custodian may fail to properly exercise discretion when acting on behalf of its clients or to follow the confidentiality and fiduciary requirements that its service implies.
- Information technology, technological, and cybersecurity risks are relevant to custodian services, as well as insufficient IT infrastructure.
- Other issues, including internal and external fraud, damage to physical assets, legal and compliance risks, and so on.

For more information on the risks associated with the custody of securities, see The Clearing House: Custody Services Provided by Banks Are Important to the Safekeeping and Management of Investments.

GENERAL CUSTODIAL ISSUES

Different digital asset custodians offer different solutions and there is no single approach to custody of digital assets. Therefore, custodians of digital assets face challenges when designing a custody arrangement that meets the extensive regulatory requirements outlined above, as well as coming up with the right technological approach that may best protect clients' assets.

Some of the associated challenges are the difficulties behind the concept of "control" and the use of a "cold" or "hot" storage system to keep the private keys safe. In their July 2019 joint statement, the SEC and FINRA also acknowledged that some challenges originate from the mechanics and risks associated with the custody of digital asset securities. For example, there is a greater risk that a broker-dealer maintaining custody of digital assets may:

- Be victimized by fraud or theft.
- Lose a private key necessary to transfer a client's digital asset securities.
- Transfer a client's digital asset securities to an unknown or unintended address without meaningful recourse to invalidate fraudulent transactions, recover or replace lost property, or correct errors.

THE RISK OF LOSS OF THEFT OF PRIVATE KEYS: STORAGE IN HOT AND COLD WALLETS

Without appropriate internal processes and security, custodians are susceptible to losing possession of their private keys due to mistakes and malicious attacks. Without their private keys, custodians have no ability to access and transfer the digital asset. It has been estimated that approximately $1.7 billion of bitcoins and other digital assets were stolen in 2018, approximately $950 million of which stemmed from cyberattacks on bitcoin trading platforms (see CipherTrace: Cryptocurrency Anti-Money Laundering Report – Q4 2018).

The risk of loss arises from the fact that private keys are generated cryptographically and are represented in hexadecimal form and, unlike an online password, cannot be recovered if lost unless it is known by another party. This problem is often solved with the use of "wallets" that store private keys, which often use a passphrase or code to later access private keys necessary for transferring any digital assets. Private keys can be stored in "hot" wallets (which are connected to the internet) or "cold" wallets (which store the private key completely offline).

Both approaches come with their risks and advantages. Maintaining private keys in an offline, hardware-based "cold" wallet protects against cyber-hacking risks, but requires continued maintenance and possession of the hardware. To avoid misappropriation, a custodian can also place a piece of paper (or hard drive) containing the private key and lock it in a physical vault. Many investors have stored digital assets directly with the exchanges on which they trade.

A hybrid approach is to maintain both "hot" and "cold" wallets simultaneously, the former for instant transactions and the latter for longer-term custody. For instance, Gemini Trust Company, a digital asset custodian, stores the majority of their cryptocurrency in their offline "cold" storage system, while a small portion is held in an online "hot" wallet hosted by Amazon Web Services.

ADVISER FRAUD RISK

Even if the custodian can set up the right degree of cybersecurity to protect its clients' digital assets against hacking and other cyber threats, the custodian still remains subject to the risk of fraud or misappropriation of the assets by an advisor or employee of the custodian. These are the risks that prompted the creation of the Custody Rule.

As a safeguard to this, some authors have suggested tracing back and blacklisting fraudulent transactions, to limit the future trading of those assets. This, however, is not a silver bullet because:

- Innocent recipients of the proceeds of a fraudulent transaction may suffer harm.
- The stolen assets may not be recoverable because the advisor who stole the assets may not provide the stolen private key.
- An adviser can quickly exchange the digital assets for cash and abscond before any action can be taken.

An alternative to minimize the risk of the type of fraud discussed above is to prevent single advisers or employees from having access to the private keys. One way in which this can be done is by using a multi-signature digital signature scheme, in which more than one party needs to authorize the transaction before it is transmitted to the network. Other alternatives have also been suggested, such as:

- The use of a new custodian technology that permits traders to effect trades on the custodian's system subject to the proceeds settling into the wallets and cash accounts held by the custodian.
- The establishment of a digital asset investor committee that signs off when instructions are provided to transfer assets out of a custodial account.

(See Custody of Digital Assets: Centralized Safekeeping of Decentralized Assets under the Investment Advisers Act, 2018.)

INSURANCE CONSIDERATIONS

Even with appropriate measures in place, theft or misappropriation of a digital asset can occur any time a bad actor obtains possession of a private key. Some industry participants have addressed this risk by obtaining insurance against loss or theft of the asset.

Two types of cryptocurrency insurance policies exist today, which may by analogy also be applicable to the insurance of digital assets held under custody:

- Crime market. Crime policies focus on "hot" wallets and cover for losses due to hacking, theft, fraudulent transfer, and so on.
- Specie market. Specie policies focus on physical damage or loss of private keys in "cold" storage, including employee misuse or theft.

The most common cause of lost private keys is the hacking of a "hot" wallet and coverage for "hot" wallet exposures are significantly more expensive than those for "cold" storage (see On Insurance and Cryptocurrency, The Coinbase Blog, April 2nd 2019).

Coinbase Custody, for example, carries an insurance commercial crime policy provided by a global syndicate that covers all storage methods, including hot, warm, and cold storage. This policy has a $255 million limit (per incident and overall). Gemini Trust, on the other hand, claims that it has commercial crime insurance coverage that covers the aggregate amount of the digital assets it keeps custody of in its online hot wallet.

While insurance may address some of the counterparty and custody risks associated with digital assets custody, it may be costly and may not completely cover all of the risks associated with misappropriation. One particular problem is that insurers are hesitant about extending policies to cover digital assets and not all custodians are able to obtain insurance or pay the high cost premiums required by insurers (see Digital Assets Insurance, Medium, October 2018).

FURTHER SOLUTIONS PROPOSED BY BLOCKCHAIN PROFESSIONALS

On September 19, 2018, a group of five blockchain professionals reached out to the SEC and offered certain solutions in relation to custody of digital assets. Some of their proposals, which are listed below, go beyond, or delve further into the issues that have been mentioned up to this point:

- No commingling of digital assets in an omnibus account by custodians is the lowest-risk practice, owing to significant cybersecurity risks of commingling, despite the transaction cost efficiencies available from commingling. Digital assets are natively segregated. Maintaining this natural segregation at all times best protects investors by conforming to the architecture of digital asset technology, which avoids the introduction of risks that then do not otherwise exist. If one client's digital assets are to be commingled with the assets of another client in limited situations as permitted under the SEC's rules, a custodian's public keys can be used for real-time monitoring of the omnibus account's coins (including potentially by the SEC itself) to ensure compliance with rules at all times. "Locktime" transactions can be provided by clearinghouses to recover assets if a loss of private keys at the clearinghouse occurs.
- No building of uncovered exposures to digital assets via securities lending-type practices, even intra-day due to the heightened risks involved with re-lending digital assets. If a fund (or any intermediary handling the fund's coins) intends to engage in coin lending, the best practice is for the funds to disclose in detail their policies and risks with regard to coin lending and rehypothecation.
- Multi-signature wallet solutions provide control tools to ensure proper authority exists before coin transfers occur. In addition to multi-signature transactions, advanced cryptographic processes allow features for the safekeeping of assets, such as:
  - funds that can be locked for a certain period of time or until a particular condition is met; and
  - obtaining proof of client holdings of digital assets, without exposing underlying digital asset balances.

(See SEC: Staff Letter: Engaging on Fund Innovation and Cryptocurrency-related Holdings.)

CURRENT DEVELOPMENTS IN THE MARKET

Several institutions organized as trust companies, state banking institutions and other entity forms have emerged to provide institutional custody services to funds in the digital asset space. Wyoming, for example, has enacted legislation authorizing a new kind of financial institution, a special purpose depository institution (SPDI), to engage in banking business and custodial services for digital assets. There are already some new institutions that deal exclusively in the digital asset ecosystem, such as Bitgo and Coinbase, while others in this space are traditional institutions, such as Fidelity. There are also state-chartered trust companies that provide custody services for digital assets. Kingdom Trust of South Dakota, a state-chartered trust company, claims to be the first trust company to allow retirement investors to hold digital currency directly on its platform. Gemini Trust Company, LLC, a New York trust company, is another example of a state chartered trust company that provides institutional custody services for digital assets.

Foreign institutions are also gaining prominence in the digital asset custody environment. Nomura, a Japanese investment bank, announced in 2018 that it intended to become the first bank to offer custodial services for cryptocurrency. Legacy Trust and Ledger, a Hong Kong-licensed and public trust company and global leader in security and infrastructure solutions for cryptocurrencies and blockchain applications, recently introduced a new institutional-grade custody solution to help accelerate the flow of institutional money into digital assets.

Below is a review of some of the services offered and certain solutions offered by three different digital asset custodians: Coinbase Custody, Gemini Trust Company and Anchorage.

COINBASE CUSTODY

Coinbase Custody launched in 2018 and is a qualified custodian for purposes of the Investment Advisers Act and a fiduciary under the New York Banking Law. The firm revealed on June 13, 2019 that it has custody of $1.3 billion in assets. Grayscale Investments, which claims to be the world's largest bitcoin and digital currency asset manager, announced on August 2, 2019 that Coinbase Custody intends to serve as the custodian of its assets and products and was expected to transfer assets of nearly $3 billion to the custodian, one of the largest single day transfers of bitcoin and crypto assets ever.

Coinbase stores the assets completely offline in cold storage. Among the innovative solutions offered by the company, it is

worth highlighting that it offers staking (which is similar to holding cryptocurrency in a wallet for a fixed period of time and earning interest on it, by using a proof-of-stake consensus mechanism)(for more information about staking, see Everything you Need to Know about Staking Coins, Medium, April 2018). It also announced that it intends to soon offer governance solutions (which allows customers to participate in governance activities like voting on protocol measures).

GEMINI TRUST COMPANY

Gemini Trust Company is also a qualified custodian for purposes of the Investment Advisers Act and a fiduciary under the New York Banking Law. Gemini Trust uses a combination of hot and cold storage. The majority of the digital assets it stores are held in the company's "cold" storage system, which uses hardware security modules (that is, hardened, tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data, and creating and verifying digital signatures), which are geographically distributed and stored in monitored, access-controlled facilities. The hot wallets, on the other hand, are hosted on Amazon Web Services.

Among the numerous security features employed by Gemini Trust, the following are worth highlighting:

- Two-factor authentication for logging into the account and making withdrawals.
- Address whitelisting, allowing customers to block or restrict cryptocurrency withdrawal activity to whitelisted addresses.
- Multi-signature measures for effecting transfer out of the company's cold storage system.

ANCHORAGE HOLD

Anchorage is one of the newest players in the field. On June 23, Anchorage became a founding member of the Libra Association, and on July 10, 2019, it announced it had raised $40 million and welcomed Visa as an investor.

From a security and technological perspective, the most remarkable feature of Anchorage is its assertion that its model is safer than "cold" storage.

There is still plenty of room for innovation in the field of digital asset custody. This room is likely to lead to new players to enter the market with new solutions until clearer parameters are introduced to describe what it means to have custody of a digital asset.

MAINTAINING REGULATIONS IN THE NEW DIGITAL ENVIRONMENT

There is a complex and developing regulatory environment around the custody of digital assets. This regulatory complexity is combined with technical challenges that can make it difficult to have and maintain exclusive control of digital assets. This challenging environment must be navigated to unlock the great potential of blockchain-based digital assets.

Digital asset custody is still in its infancy. Both the authorities and the main players in the industry have already expressed concerns about the difficulties faced in this area. The most recent official pronouncement on this topic is the Joint SEC and FINRA Statement dated July 9, 2019, which recognizes the existence of several open points that both institutions:

> "encourage and support innovation and look forward to continuing [the] dialogue as market participants work toward developing methodologies for establishing possession or control over customers' digital asset securities."

This statement implicitly recognizes that innovation in this area is likely to continue to outpace new regulation aiming to define what it means to have custody of digital assets.

The digital assets custody industry keeps growing and innovative solutions are still being developed. There is danger in crafting these solutions in the midst of legal uncertainty, where the rules of the game are not entirely clear. The system designed around the 1930s and 1940s for assuring the protection of investors through the mandatory use of third-party custodians has proved relatively sound up until this point in time. The challenge is to maintain the effectiveness of these regulations in a new digital environment because, failing that, we risk going back to an era of substantial losses suffered by investors, an era that motivated the appearance of this system in the first place. Before that happens, we expect that action is likely to be taken to bring more clarity and certainty to the legal requirements underpinning the custody of digital assets.

CUSTODY EXAMPLE

A simple explanation of the rather complex technical process for the custody of digital assets is provided below using bitcoin as an example (as the technical process and difficulties for holding custody of bitcoin are the same as those for other digital assets):

- A customer owns 100 bitcoins.
- If the customer wants its 100 bitcoins to be stored with a custodian with which it has entered into a contractual relationship, the customer sends an output transaction to an address designated by the custodian.
- Once the transaction is mined to be included in a block (which is confirmed by waiting for the customary six new blocks to be built on that original block in about 60 minutes), the custodian sends a transaction (with an input equal to the customer's output transaction to the custodian) to another address the custodian has established specifically for this customer.
- Once this second transaction is put on the blockchain and confirmed after about 60 minutes, the private key associated with this second address is put into cold storage (i.e., stored in a computer that is not connected to the internet and often maintained at a remote and secret location). The customer does not know the address or the private key associated with that address.
- If the customer later wants to transfer those 100 bitcoins, the customer requests that the custodian retrieve the private key so that the custodian can sign the instructed transaction for the customer to spend those bitcoins.

- The custodian will typically employ a procedure to verify the recipient and its control of the address to which the bitcoins are being transferred. For example, this may involve a video conference with the recipient and a transaction involving a very small amount of bitcoin (say one satoshi [one hundred millionth of a bitcoin, currently the smallest unit of the bitcoin cryptocurrency]) to be confirmed by the recipient at the time of receipt. Some custodians require all addresses of potential recipients to be pre-screened and whitelisted well before the customer desires to send bitcoin transactions to them.

See Custody of Digital Assets: Centralized Safekeeping of Decentralized Assets under the Investment Advisers Act, Debevoise, December 2018.

01-20