BLOCKCHAIN 2019

A Sidley Austin LLP Educational Series

CUSTODY OF DIGITAL ASSET SECURITIES:

A Proposal to Address Open Questions for Broker-Dealers Under the SEC's Customer Protection Rule

By Lilya Tessler, David Katz, Steffen Hemmerich and Daniel Engoren

March 18, 2019

SIDLEY

SIDLEY

CUSTODY OF DIGITAL ASSET SECURITIES:

A Proposal to Address Open Questions for Broker-Dealers Under the SEC's Customer Protection Rule

The interpretations presented in this publication reflect the views of the authors. The U.S. Securities and Exchange Commission has not yet issued guidance on these topics. Further, the SEC has neither approved nor disapproved these interpretations.

By Lilya Tessler, Partner
David Katz, Partner
Steffen Hemmerich, Counsel
Daniel Engoren, Associate

INTRODUCTION

U.S. Securities and Exchange Commission ("SEC") staff has recognized that blockchains, or distributed ledger technology, could be used to issue and transfer ownership of "Digital Assets" that are securities ("Digital Asset Securities"), depending on the facts and circumstances.[1] The Financial Industry Regulatory Authority, Inc. ("FINRA") has defined "Digital Assets" generally as "cryptocurrencies and other virtual coins and tokens (including virtual coins and tokens offered in an initial coin offering ("ICO") or pre-ICO), and any other asset that consists of, or is represented by, records in a blockchain or distributed ledger (including any securities, commodities, software, contracts, accounts, rights, intangible property, personal property, real estate or other assets that are 'tokenized,' 'virtualized' or otherwise represented by records in a blockchain or distributed ledger)."[2]

Through public statements and enforcement actions, the SEC has sent clear signals that certain Digital Assets are likely to be securities.[3] SEC staff has also encouraged technological innovations that benefit investors and the U.S. capital markets and SEC staff has been consulting with market participants regarding issues presented by new technologies.[4] At least one Commissioner has stated that the Commission is likely to be faced with the choice of creating space for innovations to occur in regulated markets, or preparing for investors to seek out such innovations in less-regulated, or unregulated jurisdictions.[5]

Many market participants share the SEC's concerns regarding investor protection and have sought to develop "security token" protocols designed to enable compliance with the federal securities laws (among others). In addition, a number of entities seek to register as broker-dealers or expand their existing broker-dealer business activities in order to facilitate trading of Digital Asset Securities in a manner compliant with the federal securities laws. However, a lack of interpretative guidance on how broker-dealers, who propose to custody fully-paid Digital Asset Securities for their customers, would comply with existing laws and regulations, particularly with the SEC's customer protection rule, Rule 15c3-3 under the Securities Exchange Act of 1934 (the "Customer Protection Rule" or the "Rule"), has significantly limited industry growth, access to capital and innovation.

---

1 The terms "blockchain" and "distributed ledger technology" generally refer to databases that maintain information across a network of computers in a decentralized or distributed manner. See www.sec.gov/finhub. "Blockchain," "Digital Assets" and related concepts are described in further detail below.

2 *See* FINRA Regulatory Notice 18-20.

3 *See*, for example, Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC before the U.S. Senate Committee on Banking, Housing and Urban Affairs (Feb. 6, 2018); CarrierEQ, Inc., Rel. No. 33-10575 (Nov. 16, 2018); Paragon Coin, Inc., Rel. No. 33-10574 (Nov. 16, 2018); Zachary Coburn, Rel. No. 34-84553 (Nov. 8, 2018) (settled order); Crypto Asset Management, LP and Timothy Enneking, Rel. No. 33-10544 (Sept. 11, 2018) (settled order); and Tokenlot LLC, Lenny Kugel, and Eli L. Lewitt, Rel. No. 33-10543 (Sept. 11, 2018) (settled order).

4 Statement on Digital Asset Securities Issuance and Trading, Division of Corporation Finance, Division of Investment Management, and Division of Trading and Markets (Nov. 16, 2018).

5 Motherhood and Humble Pie: Remarks before the Cato Institute's FinTech Unbound Conference, Commissioner Hester Peirce (Sept. 12, 2018).

THE CUSTOMER PROTECTION RULE AND DIGITAL ASSET SECURITIES

The Customer Protection Rule was adopted by the SEC in 1972 to coordinate with the, then, recently enacted Securities Investor Protection Act of 1970 ("SIPA"). The primary objective of the Customer Protection Rule is "to provide safeguards regarding the acceptance of custody and use of customers' securities, and the carrying and use of customers' deposits or credit balances."[6] The Customer Protection Rule seeks to avoid, in the event of a broker-dealer failure, a delay in returning customer securities or cash or worse, a shortfall in which customers are not made whole, by requiring broker-dealers to safeguard both the cash and securities held, or carried, by a broker-dealer for its customers. The Rule's requirements work to achieve this objective by "eliminat[ing] the use by broker-dealers of customer funds and securities to finance firm overhead and such firm activities as trading and underwriting through the separation of customer related activities from other broker-dealer operations."[7] In this regard, the Rule requires a broker-dealer to promptly obtain, and thereafter, maintain possession or control over customers' fully paid securities and/or excess margin securities.

"...a broker-dealer can have 'possession'— by virtue of holding the relevant 'private key(s)' to the Digital Asset Security."

Because the Rule dates to 1972 in a non-digital era, "possession" for the purposes of the Rule generally contemplates securities held in physical form (e.g., stock or bond certificates) by a broker-dealer. But, as we will discuss in more detail below, even in the context of Digital Asset Securities, a broker-dealer can have "possession"— by virtue of holding the relevant "private key(s)" to the Digital Asset Security.[8]

Where a broker-dealer does not, itself, maintain "possession" of customers' fully-paid securities and/or excess margin securities, the Rule requires that the broker-dealer hold, or custody, such securities in a good "control location", which could be a domestic (U.S.) or foreign location, in all cases, where the customers' securities are maintained without being subject to any right, charge, security interest, lien or claim of any kind in favor of the custodian or any person claiming through such custodian and where the delivery of such securities from the custodian to the client can be effected without the payment of money or value (other than for nominal safe custody or administration fees/charges, as the case may be). We will discuss the concept of "control" with respect to Digital Asset Securities below.[9]

As discussed above, the Customer Protection Rule imposes an obligation on broker-dealers to promptly obtain, and thereafter, maintain physical possession or control of all fully paid securities and excess margin securities carried for the account of customers. As stated in the SEC's proposing release to SEC Rule 15c3-3, "[a] principal reason for this is that the law, as presently in effect, requires such securities to be held by the broker-dealer, either by recordkeeping or otherwise, in a manner which identifies a particular customer's interest in order for that customer to obtain maximum protection. Moreover, under present practice, customers expect their fully paid securities to be held in safekeeping pending their use whenever they leave them with a broker-dealer, and it can be said that to the extent this is feasible, it does in fact result in greater customer protection."[10]

The custody of Digital Asset Securities in accordance with the following Q&A is consistent with these aims.[11] The goal of this Q&A is to propose answers to the Division of Trading and Markets' frequently asked questions of interpretation with respect to how broker-dealers may comply with the possession or control requirements of the Customer Protection Rule when carrying fully-paid Digital Asset Securities for the account of customers.[12] The questions are not intended to be comprehensive, but rather consist of issues raised by FINRA and the SEC in discussions with industry participants seeking to engage in broker-dealer activities with respect to Digital Asset Securities.

---

6 Rule 15c3-3 Proposed Rulemaking, Exch. Rel. No. 9622 (May 31, 1972).

7 Rule 15c3-3 Adopting Release, Exch. Rel. No. 9775, 1972 WL 125434, at *1 (Sept. 14, 1972).

8 "Private keys", and their relevance in the blockchain/Digital Asset context, are further discussed in Section II.1 below.

9 See Section III.2 below.

10 Rule 15c3-3 Proposes Rulemaking, Exch. Rel. No. 9622 (June 10, 1972).

11 Indeed, the current securities markets and national clearance and settlement system already rely on the "dematerialization" of securities—that is, digital representations of securities reflected on databases. *See* Strengthening the U.S Financial Markets, A Proposal to Fully Dematerialize Physical Securities, Eliminating the Cost and Risks They Incur, A White Paper to the Industry, DTCC 1, 3-6 (July 2012) *and generally*, Concept Release: Transfer Agent Regulations, Release No. 34-76743.

12 For the purposes hereof, we are only discussing non-margined positions; that is, fully-paid for Digital Asset Securities.

Storage of Digital Assets, Including Digital Asset Securities

Digital Assets

Blockchain technology places no constraints on what the data that is recorded on a blockchain represents. Therefore, the characterization of a particular Digital Asset and the resulting legal and regulatory implications is not a function of the underlying blockchain technology, but is instead based on the economic realities of the proposed transaction and agreement of participants in each particular blockchain use case. As a result, Digital Assets can be used to represent anything, including securities. Digital Assets, more generally, that are not deemed to be securities by the SEC or the federal securities laws are outside the scope of this Q&A.[13]

Keys

Public and private keys are strings of data (generally expressed as an alphanumeric string) that form the basis of the cryptographic systems on which blockchain networks rely. Specifically, Digital Asset Securities utilize a public key address (derived from, and generally synonymous with, a public key) that is generally disseminated widely and therefore known to others, and a private key that is known only to the owner (or a custodian who generates and holds a private key on behalf of the owner).[14]

A public key address may be thought of as an email address—it can be shared to receive Digital Asset Securities from others (others' public key addresses), and is used to send, or deliver, Digital Asset Securities to others (others' public key addresses).

A private key may be thought of as a password to an email account—it is required to *access* Digital Asset Securities associated with a particular public key address and to *authorize the delivery of* Digital Asset Securities from that address to another/the recipient's public key address on the blockchain.[15]

Importantly, only the private key associated with a particular public key address can access, and therefore control, the Digital Asset Securities associated with that public address.[16] *Therefore, when it comes to custody, as we will discuss further below, the private key is representative of the Digital Asset Securities that are recorded on the blockchain—much like a physical stock certificate.*

Wallets

"Wallets" store and manage public and private keys, and may be hardware or software applications. Wallets are often characterized as either "cold storage" or "hot storage."

Cold storage refers to holding cryptographic keys in an environment that is not connected to the internet. Examples include storing keys on disconnected hard drives, printing them on a piece of paper or storing them on USB or similar drives. Specialized "hardware wallets" designed specifically for storing cryptographic keys are also available. Like hardware wallets, paper wallets are physical, offline cold storage options.[17]

Hot storage uses services connected to the internet to store cryptographic keys.[18] While there are a number of hot storage options available, these services generally refer to types of software that can be installed on any internet-connected device that stores cryptographic keys and may include:

---

13 The Customer Protection Rule is not applicable to Digital Assets that are neither securities under Section 3(a)(10) of the Exchange Act nor cash.

14 While it is not a technological requirement that a custodian generate the private key, doing so ensures that a regulated custodian, such as a broker-dealer, is in sole possession of the private key.

15 FINRA has described these methods in the context of storing "cryptocurrencies," but these methods can equally be used for the storage of other Digital Assets, including Digital Asset Securities. *See*, for example, The Alert Investor, Storing and Securing Cryptocurrencies, FINRA Staff, (Nov. 29, 2018).

16 A private key is mathematically related to a public key and thus integral to the cryptography. *See* Overview of Blockchain Technology, NISTIR 8282, (Oct. 2018), U.S. Department of Commerce, National Institute of Standards and Technology. By virtue of this mathematical relationship, asymmetric-key cryptography is inherently more secure than traditional database cybersecurity technologies.

17 *See* The Alert Investor, Storing and Securing Cryptocurrencies, FINRA Staff, (Nov. 29, 2018).

18 Note that an internet connection is required to broadcast transactions to the network/blockchain. *See*, The Alert Investor, Storing and Securing Cryptocurrencies, FINRA Staff, (Nov. 29, 2018).

- ***Desktop Wallets:*** Desktop wallets are software programs that can be downloaded to a PC or laptop that store cryptographic keys on that computer and can usually broadcast transactions to the blockchain network.
- ***Mobile App Wallets:*** Mobile app wallets are similar to desktop wallets, but are software that can be downloaded to a mobile device such as a smartphone, allowing for storage of cryptographic keys on that device. Mobile app wallets can similarly broadcast transactions to the blockchain network.
- ***Online Wallets:*** Also known as cloud-based wallets, online wallets are a type of software that lets users store and access their cryptographic keys from any internet-connected device. In this case, cryptographic keys are stored remotely on third-party servers owned by the provider of the online wallet/cloud operator.[19]

Wallets are important because they store the private key that is necessary to access and control (i.e., transfer) the Digital Asset Securities associated with a particular public key address.

Custody Scenarios

As with any emerging technology, businesses (including broker-dealers) continue to develop operations, processes and technologies related to Digital Asset Securities. Industry participants have developed, and may develop in the future, a variety of different solutions for custody of Digital Asset Securities. Therefore, for the purposes of this document, we discuss two general scenarios, which are not meant to be an exhaustive list of possible approaches to custody of Digital Asset Securities.[20]

"…when it comes to 'custody' of Digital Asset Securities for purposes of the Rule, possession or control of the private key equals possession or control of the Digital Asset Security."

Blockchains are designed to be tamper resistant and immutable. The blockchain data related to a particular Digital Asset Security cannot be modified on the blockchain without the use of a private key. That is, in a blockchain network, the private key is the only method to access and transfer a Digital Asset Security on the blockchain. Thus, a broker-dealer that holds, or controls, the private key on behalf of a customer has access to, and controls, the Digital Asset Security belonging to such customer. Accordingly, when it comes to the "custody" of Digital Asset Securities for purposes of the Rule, possession or control of the private key equals possession or control of the Digital Asset Security.

Scenario 1

The broker-dealer, itself, holds the private key to a fully-paid Digital Asset Security (whether the Digital Asset Security is held in "street name" or in a particular customer's name) in "cold" or "hot" storage.

Scenario 2

The broker-dealer "custodies" the private key to a fully-paid Digital Asset Security (whether the Digital Asset Security is held in "street name" or in a particular customer's name) at a third-party and such third-party holds the private key in "cold" or "hot" storage.

---

19 *See* The Alert Investor, Storing and Securing Cryptocurrencies, FINRA Staff, (Nov. 29, 2018).

20 Certain broker-dealers maintain duplicate or redundant blockchain records of an "off-chain" master security holder file that is the official list of individual security holder accounts, maintained by the issuer, a registered transfer agent or otherwise. This Q&A does not address that scenario, but rather focuses on custody of cryptographic keys used to access Digital Asset Securities reflected directly on a blockchain.

Q&A

1. How can a broker-dealer hold fully-paid Digital Asset Securities pursuant to the Rule in Scenario 1?

In Scenario 1, a broker-dealer holding a private key in "cold" storage is the equivalent of holding a securities certificate in (physical) possession. As described above, "cold" wallets—whether hardware wallets or paper wallets—are physical, offline (cold) storage options. The broker-dealer can maintain, or safekeep, these wallets like any securities certificate—on premises in a vault or other secure setting.

A broker-dealer that uses "hot" storage basically uses an electronic storage medium, i.e., a "digital storage medium or system" as defined in SEC Rule 17a-4(f)(1)(ii), to store, or maintain, the private key (an alphanumeric code) in a format that is compliant with the requirements set forth in SEC Rule 17a-4(f)(2)(ii) (e.g., the private key is maintained in WORM format).[21] In addition, the "hot" wallet application, and the private key(s) stored therein, like any other electronic data that the broker-dealer maintains, are subject to the broker-dealer's cybersecurity and other data protection policies and procedures as well as disaster recovery/business continuity plans, as required by applicable rules and regulations.

"Blockchain technology, like all other technologies (including analog and 'pen-and-paper' technology), is not immune to risk."

Blockchain technology, like all other technologies (including analog and "pen-and-paper" technology), is not immune to risk. A known risk associated with blockchain technology (which should be adequately disclosed to a broker-dealer's customer) is commonly referred to as a "double spend" or "51% attack"— basically, where a "thief" with a majority of a blockchain's processing power creates a duplicate chain, adds new blocks containing ownership information different from the original chain thereby allowing the "thief" to sell the same security twice. Eventually, however, the faster processing time of the duplicate chain would be recognized by the network as the true blockchain ledger.[22] The risk here is equivalent to a thief or rogue employee hacking into a centralized database and changing the broker-dealer's records, which results in misappropriation of funds or securities.[23]

In such an event, it is possible that a broker-dealer may issue a confirmation that a customer received a Digital Asset Security based on the original chain, but according to the new duplicate chain published later, the customer has not yet received the Digital Asset Security in his or her account. *It is important to note, however, that the risk of a 51% attack does not affect a broker-dealer's custody of private keys and the associated Digital Assets Securities.* Rather, the risk of a 51% attack is related to settlement in which a broker-dealer does not receive Digital Asset Securities it expected to receive on behalf of customers and therefore results in a failure to receive on the broker-dealer books. The risk may be mitigated or eliminated with a longer settlement cycle.[24] Lastly, the 51% attack would not have any impact on Digital Asset Securities held by the broker-dealer long-term (prior to the date the duplicate chain was created).

---

21 17 CFR 240.17a-4. *See also* Interpretative Release: Electronic Storage of Broker-Dealer Records, Release No. 34-47806.

22 A "51% attack" refers to a process when "miners" on a blockchain network using a proof-of-work consensus mechanism append new "blocks" to the blockchain. The version of a blockchain with the most blocks is typically recognized as the "correct" blockchain to append the newly mined block to. Miners with a majority of the network hashing power (the computing power necessary to mine new blocks) can take advantage of this by privately creating a forked copy of the blockchain that they are silently (not broadcasting to the network) mining, with more hashing power than the original chain. This malicious actor can later release (broadcast) these silently mined blocks, and miners will accept this as the new "correct chain" since it contains more blocks. This allows the malicious actor to send "the same" Digital Assets to different recipients—one recipient on the original chain and one recipient on the private copy. When the copy chain is accepted by miners on the network, the transaction on the original chain will effectively disappear, and the network will recognize the Digital Assets as being sent to the address from the new (copy) chain instead. Other blockchain technologies which do not use a proof-of-work consensus mechanism (such as those that utilize proof-of-stake) are also susceptible to equivalent risks, but may incorporate solutions designed to lessen the chance of these risks.

23 The cost (and difficulty) of changing historical blocks increases exponentially and therefore a 51% attack is likely to affect recent transactions, and not Digital Asset Securities that have been held in custody for a substantial amount of time. The difficulty of modifying historical blocks is an enhancement to the security of centralized databases, which once compromised, may be significantly altered and undetected.

24 Note that the availability, and likelihood of success of this type of attack is specific to individual blockchains. Furthermore, the cost (and difficulty) of changing historical blocks increases exponentially and therefore a 51% attacks are likely to affect only recent transactions. The ability to extend the settlement cycle is, of course, subject to SEC Rule 15c6-1 and margin (Regulation T) considerations.

2. How can a broker-dealer establish a third-party as a "good control location" under paragraph (c) of the Rule for fully-paid Digital Asset Securities in Scenario 2?

In Scenario 2, the broker-dealer "custodies" the private keys "away" from the broker-dealer at a third-party custodian that is a good "control location" under paragraph (c) of the Rule. The third-party custodian, in turn, will hold the private keys in "cold" or "hot" storage. When the third-party custodian maintains the private keys in "cold" storage, the private keys would be held like physical securities certificates (e.g., in a vault or any other secure setting—see also the discussion in Scenario 1 above regarding "cold" storage). When held in "hot" storage, the private key(s) would be maintained in a format and subject to the custodian's data protection/security protocols that would ensure return of, or access by the broker-dealer to, the key(s) at any time.[25]

In this regard, and regardless of whether private keys are stored in "cold" or "hot" storage, the broker-dealer would, like in any other third-party custodial arrangement, obtain from the third-party custodian appropriate "no-lien" representations, whether in the form of a "no-lien" letter or as part of the custody agreement between the broker-dealer and the third-party custodian (or both). Specifically, the third-party custodian would be required to represent to the broker-dealer that the broker-dealer will have unrestricted access to the private keys while "custodied" at the third-party custodian and that the delivery of the private keys to the broker-dealer will not require the payment of money or value (other than for nominal fees/charges for safe custody or administration)—that is, the third-party custodian would basically be required to represent, as in the "traditional" securities context, that the private keys are not subject to any right, charge, security interest, lien or claim of any kind in favor of the custodian or any person claiming through the custodian (should the custodian, in turn, use a sub-custodian to hold the private keys).

3. How are Digital Asset Securities protected in the event of a broker-dealer's insolvency?

"…Digital Asset Securities that satisfy the definition of 'investment contracts,' but are not registered with the SEC under the Securities Act of 1933) would not be covered by SIPA."

The Securities Investor Protection Corporation ("SIPC") was created under SIPA to recover customer cash and securities left in the hands of insolvent or otherwise financially troubled brokerage firms. As noted earlier, Digital Assets may or may not be securities and Digital Asset Securities may represent various types of securities. As a result, certain Digital Asset Securities may be covered by SIPA, while others (such as Digital Asset Securities that satisfy the definition of "investment contracts," but are not registered with the SEC under the Securities Act of 1933) would not be covered by SIPA.[26]

In the event Digital Asset Securities carried by a broker-dealer are not eligible for SIPC protection, the broker-dealer should clearly disclose the lack of coverage to the broker-dealer's customers. Broker-Dealers may offer customers additional protections through the creating of trusts for the benefits of customers in the event of bankruptcy and/or seeking supplemental insurance coverage for Digital Asset Securities on behalf of customers.[27]

25 The technological risks described in Scenario 1 exist regardless of the custodian. The third-party custodian would likely be subject to oversight by an appropriate regulatory agency or other authority responsible for ensuring the sufficiency of its physical-security and cyber-security safeguards.

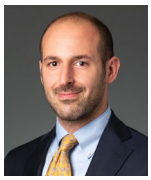
26 15 U.S.C. §78lll(14).

27 SIPC coverage is limited to $500,000. 15 U.S.C. §78lll(14).

Lilya Tessler
Partner
New York Head of Blockchain and FinTech Group,
Securities and Derivatives Enforcement and Regulatory
New York
+1 212 839 5849
ltessler@sidley.com

David M. Katz
Partner
Securities and Derivatives Enforcement and Regulatory
New York
+1 212 839 7386
dkatz@sidley.com

Steffen Hemmerich
Counsel
Securities and Derivatives Enforcement and Regulatory
New York
+1 212 839 5825
shemmerich@sidley.com



Daniel Engoren
Associate
Securities and Derivatives Enforcement and Regulatory
New York
+1 212 839 5893
dengoren@sidley.com

SIDLEY

AMERICA • ASIA PACIFIC • EUROPE

sidley.com