Chapter 64

Blockchain and Digital Assets

Lilya Tessler[*]

Partner, Sidley Austin LLP

[Chapter 64 is current as of March 1, 2019.]

[*] Ms. Tessler appreciates the contributions of Geoffrey Aronow, James Munsell, and David Teitelbaum, partners at Sidley Austin LLP. The author also gratefully acknowledges the hard work of Daniel Engoren, Verity Van Tassel Richards, and K. Braeden Anderson, associates, and Sarah Gromet, law clerk, of Sidley Austin LLP, in the preparation of this chapter.

§ 64:1 Overview

Blockchain technology and associated tokens, commonly referred to as digital assets, are recognized by the existing U.S. laws, the U.S. Securities and Exchange Commission (SEC) and the Commodities Futures Trading Commission (CFTC) to be securities, commodities, or both, depending on the facts and circumstances.[1] 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.

In 2017 and 2018, the sale of digital assets raised over $20 billion.[2] The market growth of digital assets as a new investment asset class gives rise to distinct regulatory considerations for broker-dealers and registered investment advisers offering, trading, and/or assuming custody of such assets. The use of blockchain technology in effecting digital asset transactions may be, in some instances, quite different than the technology used for transactions in other asset classes. Certain differences in market infrastructure and trade flow are being evaluated by regulators. In some instances, the existing securities laws and regulations applicable to broker-dealers and registered investment advisers may require interpretation, regulatory guidance, or SEC no-action relief in order to support a market for digital asset securities.

This chapter provides an overview of blockchain and digital assets, followed by the existing regulations applicable to broker-dealers and investment advisers engaged in digital asset activities. Various regulators

[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* SEC, FINHUB (last updated Mar. 22, 2019), https://www.sec.gov/finhub. "Blockchain," "Digital Assets" and related concepts are described in further detail in *infra* section 64:2.

[2] DANIEL DIEMERS ET AL., PWC INITIAL COIN OFFERINGS (June 2018), https://www.pwc.ch/en/publications/2018/20180628_PwC%20S&%20CVA%20ICO%20Report_EN.pdf.

may assert overlapping jurisdiction for market participants transacting in digital assets. As such, this chapter also includes a discussion of other applicable regulatory regimes, including money transmission laws and state virtual currency regulation. Regulatory considerations are driven primarily by existing regulation as applied to the nuances of blockchain technology. The discussion includes digital asset regulatory guidance being disseminated through investor warnings, public speeches, reports, and enforcement actions. The law is not yet settled as it relates to digital assets, but market participants are developing industry best practices taking into consideration the existing regulations.

§ 64:2 Blockchain Basics

§ 64:2.1 Blockchain Overview

Blockchain is a technology that contains records of transactions connected and shared among a community of users, such as shareholders of a company.[3] Blockchains enable users to record transactions in a shared ledger, such that under normal operation of the blockchain network, no record of a transaction can be changed once published.[4] This distributed database continuously grows as new sets of transactions or "blocks" are "linked" together to form a "chain."[5] Each record in the data set is individually labeled, described, and time stamped within blocks.[6]

Blockchains are distributed, meaning that instead of the database being controlled by one person or entity, numerous computers connect to a network and work together to come to an agreement on which transactions are valid.[7] The validation process is performed algorithmically

[3] *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMM., NISTIR 8202, BLOCKCHAIN TECHNOLOGY OVERVIEW (Oct. 2018) [hereinafter BLOCKCHAIN TECHNOLOGY OVERVIEW]; Telmo Subira Rodriquez, *Blockchain for Dummies: The Five Keys to Understanding What Is the Blockchain*, MEDIUM: THE STARTUP (Dec. 2, 2018), https://medium.com/swlh/blockchain-for-dummies-d3daf2170068.

[4] BLOCKCHAIN TECHNOLOGY OVERVIEW, *supra* note 3.

[5] TIANA LAURENCE, BLOCKCHAIN FOR DUMMIES (May 1, 2017).

[6] Praveen Jayachandran, *The Difference Between Public and Private Blockchain*, IBM BLOCKCHAIN BLOG (May 31, 2017), https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ [hereinafter Jayachandran].

[7] Jonathan Paul Wood, *What Is Blockchain: Explained for Beginners*, MEDIUM (Oct. 14, 2017), https://medium.com/blockchain-education-network/what-is-blockchain-explained-for-beginners-5e747cea271.

by computer programs based on a set of predetermined rules.[8] To initiate a transaction, a blockchain network user sends information to the network. The information sent may include the sender's address (or another relevant identifier), the sender's public key, a digital signature, and the transfer amount. Information contained within the blockchain is stored in encrypted format and typically requires a private key (a special passcode) to access the data or engage with the blockchain.[9] As discussed more in section 64:2.5 below, the subject of these transactions may be digital representations of assets, rights, privileges, securities, commodities, or other interests recorded on a blockchain.

§ 64:2.2 *Wallets and Private Key Storage*

A "wallet" is the software interface that allows a person to query the blockchain for information (such as the balance associated with their public key address) and to send signed transactions to the blockchain (by using their private key). Wallets are also software programs that store private keys and interact with a particular blockchain to transmit information needed to undertake transactions. The amount of digital assets associated with a particular wallet address is reflected on the blockchain.

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."[10]

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.[11]

Hot storage uses services *connected to the Internet* to store cryptographic keys. While there are a number of hot storage options available, these services generally refer to types of software that can be

[8] Joshua Oliver, *There Is No Such Thing as "the" Blockchain, Future Tense*, Slate (Jan. 5, 2018), https://slate.com/technology/2018/01/there-is-no-such-thing-as-the-blockchain.html.

[9] Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction (Princeton Univ. Press 2016).

[10] *See generally* FINRA Staff & BBB Inst., FINRA, Storing and Securing Cryptocurrencies (Nov. 29, 2018), http://www.finra.org/investors/highlights/storing-and-securing-cryptocurrencies.

[11] *See generally id.*

installed on any Internet-connected device that store cryptographic keys and may include:

- *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.[12]

Wallets are important because they store the private key that is necessary to access and control (that is, transfer) the digital assets associated with a particular public key address.

Each wallet type above has its own advantages, disadvantages, and use-cases. Hot wallets provide flexibility and fast access. These wallets can be accessed at any time or place, and from any device with an Internet connection. Cold storage wallets provide maximum safety and security to their users. By virtue of being able to physically hold and store your keys on your person or in a safe, cold storage wallets cannot be accessed by hackers on the Internet. The disadvantage is that cold storage wallets are utilized for long-term storage only, and are often inconvenient and impractical for engaging in daily transactions.[13] Common best practice would be to secure large amounts using cold storage (for safe-keeping), but maintain a hot storage wallet for daily transactions or trading (for speed and convenience).[14] Certain custodians have developed wallet technology that has the security of

[12] *Id.*

[13] MARK AUSTEN ET AL., ASIFMA BEST PRACTICES FOR DIGITAL ASSET EXCHANGES (June 2018), https://www.asifma.org/research/asifma-best-practices-for-digital-exchanges/.

[14] *Id.*

cold storage, but allows assets to be held in hot storage, which can be used for trading, voting[15] or staking[16] digital assets.[17]

§ 64:2.3 Blockchain Networks

[A] Public Blockchains

A public blockchain is defined as any cryptographic system that uses pairs of keys: public keys and private keys.[18] The encrypted data contained on the blockchain can only be decrypted with the receiver's private key.[19] These private keys (for example, a long string of letters and numbers) function as a special password and should be guarded and carefully protected. A public key can be analogized to a publicly available combination safe and the private key as the combination code.[20] People that know the safe's location can attempt to open the safe; however, the only person that can retrieve the contents of the safe is the person that has the combination code.[21] If a user loses their combination code, they lose access to the contents of the safe.[22]

[15] Certain blockchain networks allow for users to partake in the governance of the network by voting, where the number of votes cast may or may not be proportional to the amount of digital assets held. *See generally* Brian Curran, *What Is Blockchain Governance? Complete Beginner's Guide*, BLOCKONOMI (Sept. 21, 2018), https://blockonomi.com/blockchain-governance/.

[16] In a proof-of-work blockchain, "miners" compete to solve mathematically complex problems in order to verify transactions, with the winner earning a reward (a payout of the digital asset native to that blockchain). In a proof-of-stake blockchain, rather than spend computing power, validators "stake" (post as collateral) an amount of digital assets for the capability to verify transactions. Verifying transactions correctly earns transaction fees, while incorrectly verifying transactions results in a loss of digital assets. *See generally* Viktor Bunin, *Crypto Staking Is More Useful Than You Think*, TOKEN FOUNDRY (June 28, 2018), https://blog.tokenfoundry.com/crypto-staking-is-older-and-more-useful-than-you-think/.

[17] Brian Armstrong, *Busting Myths About Cryptocurrency Custody*, FORTUNE (Feb. 21, 2019), http://fortune.com/2019/02/21/cryptocurrency-custody-misconceptions-coinbase-ceo/.

[18] Toshendra Kumar Sharma, *How Does Blockchain Use Public Key Cryptography?*, BLOCKCHAIN COUNCIL (Jan. 2018), https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/ [hereinafter Sharma].

[19] J.P. MORGAN, J.P. MORGAN PERSPECTIVES, DECRYPTING CRYPTOCURRENCIES: TECHNOLOGY, APPLICATIONS AND CHALLENGES (Feb. 9, 2018), https://forum.gipsyteam.ru/index.php?act=attach&type=post&id=566108 [hereinafter DECRYPTING CRYPTOCURRENCIES].

[20] *See also generally* Sharma, *supra* note 18.

[21] *Id.*

[22] *Id.*

In the context of public blockchain networks, the private key is how the key holder effectively "signs" (or authenticates) a transaction.[23] Once a transaction is broadcasted and authenticated through the use of public and private keys, the distributed network must then validate the transaction block.[24] Bitcoin is one example of a public blockchain network. In the case of bitcoin, private keys are randomly generated 256-bit numbers and an algorithm is then used to generate a public key derived from the private key.[25] In most instances, the hashing[26] and validation process is performed by a network of computers, also known as "miners."[27] There is no one blockchain, but rather a potentially infinite number of blockchains and forms of blockchain integrations.

[B] Private or Permissioned Blockchains

A private blockchain requires a validated invitation (or permission) to interact with the network.[28] The blockchain is not publically available and only accessible by defined participants. Continuing with the analogy above, this can be analogized to a combination safe that is hidden, or located in a private residence. In order to open the safe, regardless of whether or not the user held the combination code or private key, the user would need permission. The validation process can be granted by the network's developer, or by the network's predetermined set of criteria.[29]

[23] DECRYPTING CRYPTOCURRENCIES, *supra* note 19.

[24] Sharma, *supra* note 18.

[25] *Id*.

[26] *Definition—What Does Hashing Mean?*, TECHOPEDIA, https://www.techopedia.com/definition/14316/hashing (last visited Feb. 28, 2018) ("When a user sends a secure message, a hash of the intended message is generated and encrypted, and is sent along with the message. When the message is received, the receiver decrypts the hash as well as the message. Then, the receiver creates another hash from the message. If the two hashes are identical when compared, then a secure transmission has occurred. This hashing process ensures that the message is not altered by an unauthorized end user.").

[27] *Definition—What Does Mining Mean?*, TECHOPEDIA, https://www.techopedia.com/definition/32530/mining-blockchain (last visited Feb. 28. 2018) ("Mining, in the context of blockchain technology, is the process of adding transactions to the large distributed public ledger of existing transactions, known as the blockchain. The term is best known for its association with bitcoin, though other technologies using the blockchain employ mining. Bitcoin mining rewards people who run mining operations with more bitcoins.").

[28] Jayachandran, *supra* note 6.

[29] *Id*.