

Securities on Blockchain

By Reade Ryan* and Mayme Donohue**

This article initially provides a high-level description of blockchain technology intended to be accessible to those without a technical background, and illustratively describes an existing blockchain system that already evidences securities issued and being traded. The article then sets forth and analyzes how Article 8 of the Uniform Commercial Code covers blockchain securities as “uncertificated securities.” Finally, the article provides guidance to corporate lawyers faced with giving a legal opinion relating to the issuance and sale of securities on a blockchain.

INTRODUCTION

Technology and innovation have a habit of reshaping the financial industry faster than the legal and regulatory framework can meaningfully adapt. For example, although personal data has been shared over the Internet for decades, federal and state laws remain in flux with respect to their treatment of the Internet and data privacy.¹ More often than not, regulators’ understanding of emerging technologies lags behind the broad use of those technologies by more sophisticated and tech-savvy private market participants. Exacerbating that trend, blockchain, the technology underlying Bitcoin, is a truly disruptive technology with the potential to fundamentally change the way our financial systems operate.² While the hype around blockchain and private investment in the technol-

* Reade Ryan is Of Counsel in the New York office of Shearman & Sterling LLP. He is a member of the firm’s Finance—Americas Group.

** Mayme Donohue is an associate on the Capital Markets and Securities team at Hunton & Williams LLP and is also a member of the firm’s Blockchain Working Group. She would like to thank Vicki Tucker for her guidance during the process of publishing this article.

1. See, e.g., Cecilia Kang, *Congress Moves to Overturn Obama-Era Online Privacy Rules*, N.Y. TIMES, (Mar. 28, 2017), <https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html>.

2. See Alex Tapscott & Don Tapscott, *How Blockchain Is Changing Finance*, HARV. BUS. REV. (Mar. 1, 2017), <http://hbr.org/2017/03/how-blockchain-is-changing-finance> [hereinafter *Changing Finance*]. Don Tapscott and his son, Alex, are leading authorities on blockchain and have written and spoken extensively on the subject. In *How Blockchain Is Changing Finance*, the Tapscotts call blockchain “a game changer” and posit that “by reducing transaction costs among all participants in the economy, blockchain supports models of peer-to-peer mass collaboration that could make many of our existing organizational forms redundant.”

ogy are growing at a fever pitch, regulators are racing to understand blockchain and its many applications that may warrant a regulatory response.³

Given the rapid proliferation of blockchain's impact on the financial markets, federal and state laws regulating the financial industry, money, currency, and securities must all be evaluated with respect to their application to blockchain. Federal regulators of all sizes and types of financial institutions are in various stages of information-gathering as the development and applications of blockchain continue to progress.⁴ Some federal agencies have offered guidance detailing the application of existing laws to blockchain-related issues, but no blockchain-specific laws have been enacted at the federal level.⁵ Notably, state governments seem to be adapting relevant state laws more quickly; for example, Delaware's General Corporation Law was recently amended to explicitly allow Delaware corporations to use blockchain technology to maintain corporate records, including stock ledgers.⁶

Despite the concern around blockchain's potential impact on our financial systems, existing commercial law accommodates reasonably well the use of blockchain to issue and trade securities. Article 8 of the Uniform Commercial Code ("UCC")⁷ covering the holding, transferring, and pledging of securities need not be amended to accommodate securities issued on a blockchain. In fact, blockchain securities bring to life various aspects of Article 8 of the UCC that have never truly been put to use.

This article provides a high-level description of blockchain intended to be accessible to someone without a technological background. After priming the

3. According to PitchBook, blockchain-related projects raised approximately \$1.95 billion during the first seven months of 2017. Kate Clark, *Can VCs Keep Pace with the ICO Market?*, PITCHBOOK (Aug. 15, 2017), <https://pitchbook.com/news/articles/can-vcs-keep-pace-with-the-ico-market>.

4. For example, the Financial Industry Regulatory Authority, Inc. ("FINRA") published a report and a request for comment from industry participants that encouraged "firms to conduct a comprehensive review of all applicable securities laws, rules, and regulations to determine potential implications" of blockchain-based operations. FIN. INDUS. REGULATORY AUTH., *DISTRIBUTED LEDGER TECHNOLOGY: IMPLICATIONS OF BLOCKCHAIN FOR THE SECURITIES INDUSTRY 1 n.1* (2017), <http://www.finra.org/industry/blockchain-report> [hereinafter FINRA REPORT]; see also THE DEPOSITORY TRUST & CLEARING CORP., *EMBRACING DISRUPTION: TAPPING THE POTENTIAL OF DISTRIBUTED LEDGERS TO IMPROVE THE POST-TRADE LANDSCAPE* (2016), <http://www.dtcc.com/en/news/2016/january/25/blockchain-white-paper> [hereinafter DTCC WHITE PAPER]; DAVID MILLS ET AL., *DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENTS, CLEARING, AND SETTLEMENT* (2016), <https://doi.org/10.17016/FEDS.2016.095> [hereinafter FED WHITE PAPER].

5. See, e.g., Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017) (providing guidance that certain initial coin offerings qualify as the offer and sale of securities and therefore must be registered with the Securities & Exchange Commission).

6. See Pete Rizzo, *Delaware Governor Signs Blockchain Bill Into Law*, COINDESK (July 24, 2017), <https://www.coindesk.com/delaware-governor-signs-blockchain-legislation-law/>. Illinois has also been progressive in terms of its proactive incorporation of blockchain technology for state government functions. For example, the state-sponsored Illinois Blockchain Initiative recently launched a program to create a digital identity blockchain for Illinois' citizens. See Michael del Castillo, *Illinois Launches Blockchain Pilot to Digitize Birth Certificates*, COINDESK (Aug. 31, 2017), <https://www.coindesk.com/illinois-launches-blockchain-pilot-digitize-birth-certificates/>.

7. References to the UCC will be to the 2017–2018 edition of the Uniform Commercial Code (issued in September 2017) unless otherwise stated.

reader with the requisite understanding of blockchain, this article analyzes how blockchain securities fit within the current language of Article 8 of the UCC as “uncertificated securities.” Finally, this article provides guidance to corporate lawyers faced with giving a legal opinion related to the issuance of securities on a blockchain. While other areas of the law will need to be amended to support blockchain securities, Article 8 of the UCC will not slow blockchain’s implementation within the financial industry.

BLOCKCHAIN 101⁸

Although the term may have only recently become familiar, the technologies underpinning blockchain are not new; it is the unique way in which the technologies are combined and implemented by blockchain that is revolutionary. Blockchain is a type of distributed ledger, comprised of digital records of transactions or assets, accessible to and trusted by all participants running the same protocol.⁹ A protocol for this purpose is a set of rules governing the format of messages that are exchanged between the participants. The fundamental innovation of blockchain is that it creates a means of establishing and maintaining consensus among the participants in a transaction without the need for either an established trust relationship or a central intermediary. Currently, the financial ecosystem relies on banks, trustees, escrow agents, and the like as central intermediaries both to verify that the counterparties in a transaction each have the assets to be exchanged and then to settle the transaction.¹⁰ As will become apparent, a blockchain can serve as the “trust” agent in a transaction, thereby cutting out the intermediaries and allowing true peer-to-peer transfer of assets, the benefits of which include reduced transaction costs, reduced transaction time, and increased privacy and security.

WHAT IS “BLOCKCHAIN”?

There are two key features that make blockchain such a revolutionary means of recording the flow of assets: (1) distributed ledgers and (2) cryptography.

Distributed Ledgers

Our current financial system operates through a network of centralized ledgers: banks, which are paid fees for verifying the assets and liabilities of the par-

8. The description of blockchain that follows does not presume to capture all of the technical nuances and intricacies that drive the operations of the technology. Rather, this description of blockchain is meant to be broadly accessible and provide enough detail to explain conceptually how a blockchain works and why its impact may be revolutionary. As an analogy, very few people fundamentally understand how the Internet works from a technical standpoint; however, the Internet is universally recognized for its impact on shaping global economies and cultures. Similarly, a reader need not master the technical underpinnings of blockchain technology to grasp its applications.

9. See generally DON TAPSCOTT & ALEX TAPSCOTT, *BLOCKCHAIN REVOLUTION* 6–8 (2016).

10. For an in-depth discussion of the role of intermediaries in financial transactions, see FED WHITE PAPER, *supra* note 4, at 4–6.

ties to a transaction, effect the actual movement of assets to settle a transaction. This system has been in place since the Medici family cornered the banking market during the Florentine Renaissance.¹¹ The Medicis created a central ledger of the community's assets and liabilities, which allowed two individuals without any reason to trust one another to engage in commerce. Because the Medicis central ledger was trusted by the community, such central ledger provided a consensus among otherwise unfamiliar parties to a transaction that each had the means to satisfy its end of the bargain. The Medicis became the necessary central intermediary in all transactions and earned fees for verifying holdings, settling transactions, and updating the central ledger. Banks, transfer agents, escrow agents, and other financial intermediaries serve this purpose today. Distributed ledgers shift the balance of power from the current system and theoretically eliminate the need for a centralized intermediary by making public each transaction such that all parties within the system may verify a transaction.¹²

Distributed ledgers are not a new phenomenon. The economy of the nineteenth century Yapese society on the island of Yap provides a helpful foundation upon which to understand the basics of how distributed ledgers work.¹³ The currency in the Yapese society was the fei, a large circular limestone wheel that could weigh up to four tons. The size of the stones made physically moving the stones between subsequent owners impractical and therefore the stones frequently remained in the physical possession of a previous owner after a transaction. In order to create a verifiable record of a transaction, the Yapese created an oral history of transactions that was communicated through generations of families. Whenever there was a transaction and a fei, or a portion of a fei, changed ownership, the parties involved would communicate the details of the trade throughout the tribe. Although there was no physical transfer, and therefore no physical proof of ownership, by spreading the knowledge of the transaction throughout the tribe each transaction was on record with each member of the tribe. In effect, the common knowledge of the history of transactions and each new transaction was verifiable by each member of the tribe. Such common knowledge created a consensus around the actual allocation of fei among the tribe.

Building off of the known accounting methods of the Yapese society, an analogy can be made to understand the fundamental operation of a blockchain.¹⁴ Within the Yapese society, the informal, word-of-mouth transfer of information to record and verify transactions depended on flawed human memories and the veracity of the person-to-person account of each trade. Hypothetically, to solve the problems caused by multiple, flawed accounts, the Yapese could have appointed one individual as the bookkeeper, responsible for maintaining a ledger

11. PAUL VIGNA & MICHAEL J. CASEY, *THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND THE BLOCKCHAIN ARE CHALLENGING THE GLOBAL ECONOMIC ORDER* 4–5 (2016) [hereinafter *AGE OF CRYPTOCURRENCY*].

12. See *Changing Finance*, *supra* note 2.

13. *AGE OF CRYPTOCURRENCY*, *supra* note 11, at 121–22 (citing Yevgeniy Brikman's 2014 article *Bitcoin by Analogy*, which is available at <http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/>).

14. *Id.* The analogy that follows is the creation of Yevgeniy Brikman.

of all transactions. This individual would have served as a centralized ledger, like the Medicis or the network of banks today. Instead, however, the Yapese economy could have operated on a distributed ledger if each family in the tribe maintained a separate written ledger of each transaction. For example, if one person wanted to pay another, the payor would announce the transaction in the center of town to all the families. Each family could check its own ledger to verify that the payor had the stones it intended to transfer and, if valid, each family could then record that new transaction on its ledger, debiting the payor's account and crediting the payee's account with the fei. If a majority of the families recognized the transaction, it would be legitimate and settle. Whenever there was disagreement between the families' ledgers, the accounting on the majority of the ledgers would prevail. Furthermore, each Yapese family's individual dependence on the trustworthiness of the system would collectively incentivize fair dealing and accurate recording.

Transactions on blockchains work in substantially the same way as the hypothetical Yapese example above. When someone requests a transaction on a blockchain (for example, sending currency from person A to person B), the requested transaction is broadcast to a network consisting of nodes.¹⁵ This network of nodes validates the transaction and the status of person A and person B using the cryptographic algorithms discussed below. Once validated, the transaction is timestamped and combined with other validated transactions in chronological order to create a new "block" of data for the ledger. This new block is then added to the existing blocks, thereby creating the blockchain, which is distributed publicly among the nodes and known to all participants in the system.

Cryptography

Until the Internet, there was no way to create a distributed ledger that could operate on the scope necessary for the international financial markets. Even with nearly instantaneous communication through the Internet, a blockchain's distributed ledger responsible for billions of dollars worth of transactions must be secure and broadly trusted before the widespread adoption of blockchain. This is where cryptography comes in: to allow individuals to rely on blockchain's distributed ledgers as the central trust agent at the speed and on the scope required by our economy.

Blockchains use cryptography to verify transactions, process payments, and provide security for individual participants that maintains trust within the system.¹⁶ Blockchains generally rely on two cryptographic schemes: *digital signatures* and *cryptographic hash functions*. Briefly, the former enables the exchange

15. "Nodes" are devices or data points on a larger network, like personal computers or smart phones, that have an IP address. Depending on the blockchain, nodes may have the ability to play a more active role in maintaining the blockchain. For example, in the Bitcoin blockchain, "miners" actively work to validate transactions on the chain in order to earn bitcoins as a reward.

16. ANTON BADEV & MATTHEW CHEN, BITCOIN: TECHNICAL BACKGROUND AND DATA ANALYSIS 7–9 (Oct. 7, 2012).

of accurate (payment or other transfer) instructions between parties to a transaction, and the latter is used to enforce discipline in writing transaction records in the public ledger. Neither of these schemes is unique to blockchain, as they are widely used to secure commercial and governmental communications. The combination of these cryptographic tools with distributed ledgers is the technological advancement that has allowed Bitcoin's blockchain to serve as the model for revolutionizing our financial systems.

The capability of sending payments on Bitcoin's blockchain is controlled via digital signatures that involve pairs of a public key and a private key. There can be only one public key associated with each private key and the unique pairs are generally stored together in digital "wallets."¹⁷ The public key serves as the publicly viewable address for an individual's account where Bitcoins are held and the private key gives the individual control over the Bitcoins held in that account, acting like a digital signature. Specifically, any payment involving a particular public key as a sending address has to be signed with the proper private key to be considered valid. Without the private key to match the public key, the Bitcoins associated with the public key cannot be traded.¹⁸ This identity verification process can be used on all types of blockchains in order to transact in any type of digital asset, including securities.¹⁹

The longer a blockchain is in use, the longer the history of transactions becomes. This is a good thing with respect to the trustworthiness of the distributed ledger, but also makes the process of achieving consensus throughout the system a procedural challenge. Blockchains use cryptographic hash functions in order to quickly verify and create consensus among all of the various ledgers within the system. A cryptographic hash function generates small digital "fingerprints," each unique to the data set entered into the function, allowing a quick comparison of large data sets and providing a secure way to verify that the underlying data has not been altered.²⁰ This is how consensus is achieved within the system without having to perform a line-by-line comparison of each participant's ledger. Without needing to understand how cryptographic hash functions work, it is enough to understand that there is only one possible output for any input data set.²¹

17. Many different companies have developed wallet software for consumers to store their public and private key pairs. See *Choose Your Bitcoin Wallet*, BITCOIN.ORG, <https://bitcoin.org/en/choose-your-wallet> (last visited Sept. 1, 2017).

18. *Id.*

19. This method of double verification digital signatures is a type of *asymmetric cryptography*—in effect, a way to send a message encrypted for specific recipients such that anyone can verify the sender's authenticity but only intended recipients can read the message contents.

20. OLIVER WYMAN, UNLOCKING ECONOMIC ADVANTAGE WITH BLOCKCHAIN: A GUIDE FOR ASSET MANAGERS 3 (2016). Each transaction submitted to a block becomes part of a "merkle tree," a technology that applies the encryption algorithm to each transaction (the "leaves" of the tree), each of which is paired with another transaction, which is again subject to the encryption algorithm, and so on, until a single hash remains. That single hash represents all of the transactions in the merkle tree.

21. Blockchain enthusiasts often say that the entire text of *War and Peace* could be entered as the input data set in a cryptographic hash function and a much shorter output of numbers and characters would be produced. If even one comma or one letter were changed in the entire text of the novel, a distinct output would be produced.

Taking the Yapese economy as an example, in order to validate a transaction, each family would need only to record the new transaction and then run that updated version of the ledger through the hash function. If each family's comprehensive ledger produced the same condensed output, the Yapese town would know that there is consensus among the ledgers and the transaction would be valid and permanently recorded on the distributed ledger.

By combining distributed ledgers and cryptography, blockchain allows for the creation of a permanent, immutable audit trail of transactions through the use of decentralized electronic nodes. Blockchain is seen as a "trustless" mechanism for the verification of all transactions or assets on the network.²² Removing the need for a central intermediary, blockchain has the potential to cut down the time and expense of transactions. It also, theoretically, shifts the balance of power away from centralized banks and financial institutions and relies on the individual participants in the system to maintain consensus regarding the ledger of transactions. However, in the case of securities transactions, as will be discussed in greater detail below, the power held by the centralized institutions maintaining the ledgers can be even more pronounced.

SECURITIES ISSUED ON BLOCKCHAIN AND THE OVERSTOCK.COM EXAMPLE

Any currency, financial contract, or financial asset can, in theory, be the subject of transfers on a system like blockchain once a digital version of the financial asset is created in place of any tangible version of the asset. Blockchain can also be used as a registry and inventory system for the recording, monitoring, identifying, and transacting of any asset. Thus, blockchain technology can be used for any form of asset registry.²³ A blockchain used for carrying a cryptocurrency like Bitcoin is relatively simple. Although a blockchain used to register and trade securities would require more advanced algorithms and coding, more complex blockchains have already been developed, tested, and used to transact digital securities.²⁴ For example, the Ethereum blockchain allows individuals to invest directly in companies in exchange for "tokens" in crowdfunding-like financing campaigns called Initial Coin Offerings.²⁵ In addition, The Depository Trust & Clearing Corporation chose to collaborate with IBM, R3, and Axoni to develop a blockchain to manage post-trade lifecycle events for standard North American single-name credit default swaps with plans to go live in the first quarter of 2018.²⁶

22. MELANIE SWAN, *BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY x* (2015).

23. SWAN, *supra* note 22, at xi. Additional cases of asset tracking on blockchain include supply chain management and authentication of unique consumer goods. See, e.g., *Blockchain for Supply Chain*, IBM, <https://www.ibm.com/blockchain/supply-chain/> (last visited Sept. 1, 2017); *Blockchain Wave Headed Toward CPG and Retail Industries*, ACCENTURE CONSULTING, <https://www.accenture.com/us-en/insight-highlights-cgs-blockchain-cpg-and-retail-industries> (last visited Sept. 1, 2017).

24. WYMAN, *supra* note 20, at 6–7.

25. *Create a Crowdsale*, ETHEREUM, <https://www.ethereum.org/crowdsale> (last visited Sept. 1, 2017).

26. Press Release, Depository Trust & Clearing Corp., DTCC Selects IBM, AXONI and R3 to Develop DTCC's Distributed Ledger Solution for Derivatives Processing (Jan. 9, 2017), <http://www>.

These complex blockchains are built specifically for creating “smart contracts” that autonomously execute different types of transactions in digital assets, the records of which are maintained on a blockchain. Essentially, smart contracts are a series of instructions that execute autonomously based on predetermined inputs.²⁷ Smart contracts have famously been described as digital vending machines: users input data or value into a smart contract and the smart contract executes and delivers its programmed output in response.²⁸ In the case of securities trading, an individual would input digital money and the smart contract would execute a transaction to purchase a corresponding amount of a security. A user’s experience would not differ greatly at the point of sale from accessing any existing online brokerage account; rather, the back-office interface between the automation of a smart contract operating on top of a blockchain’s peer-to-peer capabilities creates the revolutionary character of a blockchain transaction.

Securities trading using blockchain technology and smart contracts is a reality. In addition to the recently passed amendment to the Delaware General Corporation Law explicitly authorizing the use of blockchains to maintain stock ledgers,²⁹ the State of Delaware has partnered with a startup called Symbiont to develop a blockchain and smart contract layer technologically capable of distributing corporate shares.³⁰ The German car manufacturer Daimler AG successfully tested the use of blockchain technology to issue corporate bonds and, once allowed by regulators, intends to adopt blockchain debt issuances as a corporate practice.³¹ Goldman Sachs has been awarded a patent for its SETLcoin cryptocurrency settlement system, which contemplates the capability to exchange stocks using the SETLcoins.³² In addition, Overstock.com, Inc. (“Overstock”) had its shelf registration allowing for the sale of its digital securities via its own proprietary blockchain approved by the U.S. Securities and Exchange Commission (“SEC”) in December 2015,³³ and in December 2016 became the first publicly traded company to issue stock on a blockchain.³⁴ Both the Delaware/Symbiont blockchain

dtcc.com/news/2017/january/09/dtcc-selects-ibm-axoni-and-r3-to-develop-dtccs-distributed-ledger-resolution; see also Alex Lielacher, *DTCC to Launch Blockchain Credit Default Swaps Reporting in Early 2018*, NASDAQ (May 25, 2017), <http://www.nasdaq.com/article/dtcc-to-launch-blockchain-credit-default-swaps-reporting-in-early-2018-cm794771>.

27. See *How Do Ethereum Smart Contracts Work?*, COINDESK, <https://www.coindesk.com/information/ethereum-smart-contracts-work/> (last visited Sept. 1, 2017).

28. Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, ALAMUT (June 22, 1998), http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html.

29. S.B. 69, 149th Gen. Assemb., Reg. Sess. (Del. 2017).

30. Caitlin Long & Andrea Tinianow, *With Blockchain, the Early Lawyer Gets the Worm*, LAW360 (Oct. 4, 2017, 1:10 PM EST), <https://www.law360.com/articles/970948/with-blockchain-the-early-lawyer-gets-the-worm>.

31. Nina Trentman, *Daimler Uses Blockchain to Issue Bonds*, WALL STREET J. (July 12, 2017, 4:51 PM EST), <https://blogs.wsj.com/cfo/2017/07/12/daimler-uses-blockchain-to-issue-bonds/>.

32. Chuan Tian, *Goldman Sachs Granted “SETLcoin” Cryptocurrency Patent*, COINDESK (July 13, 2017), <https://www.coindesk.com/goldman-sachs-granted-setlcoin-cryptocurrency-patent/>.

33. Michael del Castillo, *Overstock Could Raise \$30 Million with Blockchain Stock Offering*, COINDESK (Nov. 21, 2016), <http://www.coindesk.com/overstock-raise-30-million-blockchain-stock-offering>.

34. Press Release, Overstock.com, Inc., *Overstock Closes Historic Rights Offering* (Dec. 15, 2016), <http://investors.overstock.com/mobile.view?c=131091&v=203&rd=1&rid=2230245>.

and the Overstock blockchain are designed to enable a company to issue digital securities and to allow for secondary trading of those securities.

In order to illustrate how securities would work on a blockchain, let us take the example of the blockchain securities issued by Overstock. The Overstock blockchain provides for issuing Overstock's securities on a proprietary blockchain, as outlined in an SEC-approved prospectus.³⁵ Overstock's blockchain securities trade on a closed-system trading platform regulated by the SEC as a registered alternative trading system ("ATS").³⁶ In particular, Overstock's blockchain securities trade on an ATS maintained by PRO Securities, L.L.C. ("PRO Securities") using the software technology of another subsidiary of Overstock known as t0.com, Inc. (as in, settlement occurs on a "T+0" basis, or simultaneously with the trade).³⁷ Overstock offered its blockchain securities by directly registering the securities in the applicable purchaser's name in the records maintained by Electronic Transaction Clearing, Inc. ("ETC"), which serves as the clearing broker for Keystone Capital Corporation ("Keystone"), the sole broker-dealer authorized to provide investors with access to the PRO Securities ATS.³⁸ Overstock's board of directors authorized the issuance of Overstock's blockchain securities and designated the combination of (a) the proprietary ledger, as validated by the distributed ledger, and (b) the securities holder personal identity information database, as the "book-entry" system for the Overstock blockchain securities.³⁹ Because of federal securities laws, Overstock was forced to maintain roles for the intermediaries used for traditional securities offerings in order to keep track of its security holders. Though limited in scope, the Overstock blockchain securities represent a small step toward a reimagined system of securities registry and transactions.

A person wishing to engage in transactions in Overstock's blockchain securities is required to open an online brokerage account with Keystone.⁴⁰ Customers having appropriate brokerage accounts with Keystone are able to use the broker-dealer's interface on the PRO Services ATS to directly purchase and sell Overstock's blockchain securities, which are held directly in that customer's name

35. Overstock.com, Inc., Prospectus (Dec. 9, 2015) (Registration No. 333-203607) [hereinafter Overstock Prospectus].

36. *Id.* at 34. An alternative trading system is a term for a non-exchange trading venue that matches buyers and sellers to find counterparties for transactions. Alternative trading systems are typically regulated as broker-dealers rather than exchanges (although an alternative trading system can apply to be regulated as a securities exchange). In general, for regulatory purposes an alternative trading system is an organization or system that provides or maintains a marketplace or facilities for bringing together purchasers and sellers of securities, but does not set rules for subscribers (other than rules for the conduct of subscribers trading on the system). An alternative trading system in the United States must be approved by the SEC and is an alternative to a traditional stock exchange. See Rule 301(a) of SEC Regulation ATS, 17 C.F.R. § 242.301(a) (2017). The equivalent term under European legislation is a multilateral trading facility (MTF).

37. Overstock Prospectus, *supra* note 35, at 34.

38. Overstock Prospectus Supplement S-3, S-5 (Nov. 14, 2016) (Registration No. 333-203607). [hereinafter Overstock Prospectus Supplement].

39. Letter from Dr. Patrick M. Byrne, Chief Exec. Officer, Overstock.com, Inc. to Mara L. Ransom, Assistant Dir., U.S. Sec. & Exch. Commission 1 (July 31, 2015) [hereinafter Overstock Letter].

40. Overstock Prospectus, *supra* note 35, at 34.

rather than in “street name.”⁴¹ In connection with the broker-dealer’s license to use the PRO Securities ATS, the broker-dealer is required to agree to share the identity of its customers with Overstock and Overstock’s transfer agent, trustee, or other similar agent with respect to each series of blockchain securities that Overstock issues.⁴² Because there is a sole broker-dealer that is licensed to provide access to the Pro Securities ATS, underwriters of offerings of Overstock’s blockchain securities are required to open brokerage accounts with such broker-dealer. Primary issuances of Overstock’s blockchain securities are executed as the sale of such blockchain securities to the relevant underwriter on the Pro Securities ATS, followed by a subsequent transfer transaction by such underwriter on the Pro Securities ATS to the various initial purchasers, each of which will also be a customer of such broker-dealer.⁴³

A transaction in Overstock’s blockchain securities is recorded in an electronic database, a proprietary ledger, which is maintained by the Pro Securities ATS. This proprietary ledger reflects the definitive ownership record with respect to Overstock’s blockchain securities and is electronically published (i.e., it serves as the distributed ledger for the blockchain securities). The validity of publicly available copies of the proprietary ledger can be mathematically proven using cryptographic hash functions.⁴⁴

The book-entry system with respect to each series of blockchain securities comprises the proprietary ledger maintained by the Pro Securities ATS, together with a database containing the personal identity information of holders of the applicable blockchain securities. Overstock’s transfer agent, trustee, or other similar agent with respect to the particular series of Overstock blockchain securities satisfies Overstock’s books and records obligations by combining the information received from the proprietary ledger with the personal identity information received from Keystone.⁴⁵

When an investor with access to the Pro Securities ATS executes a blockchain securities transaction, trade data for that transaction is automatically recorded electronically to the proprietary ledger. The Pro Securities ATS electronically publishes the proprietary ledger on a public basis and simultaneously records a cryptographic hash function to the distributed ledger network for Overstock’s blockchain securities for mathematical proof of the validity of the publicly available proprietary ledger.⁴⁶

Overstock’s blockchain securities are represented by proprietary ledger balances that are secured by a cryptographic pair of keys—one public key and one or more private keys. There are multiple private keys, any number of which may be required in order to authorize a transfer of ownership of the blockchain securities. A blockchain security holder’s private keys are held by

41. *Id.*

42. *Id.*

43. *Id.* at 34–35.

44. *Id.* at 35.

45. *Id.*

46. *Id.*

Overstock, by the Pro Securities ATS, and by Keystone. Depending on the security protocols used for the particular series of blockchain securities, Overstock, the Pro Securities ATS, or Keystone may be able to transfer ownership of the blockchain securities on behalf of the blockchain security holder. In addition, Overstock, the Pro Securities ATS, or Keystone may be able to block further transfers of such blockchain securities through the private keys held by such entities.⁴⁷

BLOCKCHAIN SECURITIES AND THE UCC

The existing UCC contains legal rules that define the rights and obligations of the parties in connection with many aspects of commercial transactions, including, but not limited to, instruments under UCC Article 3, funds transfers under UCC Article 4A, letters of credit under UCC Article 5, and investment securities under UCC Article 8. UCC Article 4A has already been interpreted to apply to a transfer of Bitcoins and other cryptocurrencies on blockchain.⁴⁸ What about securities on blockchain? This part of this article discusses how UCC Article 8 applies to securities on blockchain and discusses the various issues that securities on blockchain raise under UCC Article 8.

SECURITIES ISSUED AND TRADED ON A BLOCKCHAIN AND THE UCC

UCC Article 8 has already been interpreted to apply to securities on blockchains.⁴⁹

Article 8 defines a “security” as “an *obligation of an issuer or a share, participation, or other interest in an issuer or in property or an enterprise of an issuer:*

- (i) which is represented by a security certificate in bearer or registered form, or the transfer of which may be *registered upon books maintained for that purpose by or on behalf of the issuer;*
- (ii) which is one of a class or series or by its terms is divisible into a class or series of shares, participations, interests, or obligations; and
- (iii) which:
 - (A) is, or is *of a type*, dealt in or traded on securities exchanges or securities markets; or
 - (B) is a medium for investment and *by its terms* expressly provides that it is a security governed by this Article.”⁵⁰

47. *Id.*

48. Jessie Cheng & Benjamin Gera, *Understanding Block Chain and Distributed Financial Technology: New Rails for Payments and an Analysis of Article 4A of the UCC*, BUS. L. TODAY (Mar. 2016), https://www.americanbar.org/publications/blt/2016/03/05_cheng.html.

49. Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 24 U. MIAMI BUS. L. REV. 1, 66–78 (2016).

50. U.C.C. § 8-102(a)(15) (emphasis added).

Such a “security” can be, among other things, a bond (“an obligation of an issuer”) or a share of stock (“a share . . . or other interest in an issuer”).⁵¹ An “uncertificated security” is “a security that is not represented by a certificate.”⁵² Accordingly, a digital security on a blockchain would be just that, a “security that is not represented by a certificate,” and so would be an “uncertificated security” under UCC Article 8.⁵³ A bond or share of stock issued on a blockchain would be such a security with the blockchain constituting the “books” maintained for registering the transfer of the bond or share of stock.⁵⁴ In this instance, a blockchain would serve simply as a registration of the chain of ownership.⁵⁵

The term “books” in UCC section 8-102(a)(15)(i) includes electronic record-keeping as well as physical recordkeeping. A blockchain security—that is, an “uncertificated security”—which is tracked on and represented by a blockchain distributed ledger is registered upon electronic “books” maintained for that purpose.⁵⁶ UCC Article 8 does not require that the issuer itself maintain such “books,” but rather allows for such “books” to be maintained “on behalf of the issuer,” like a company using the services of an independent transfer agent to maintain the company’s securities books. Thus, the nodes on which the blockchain securities are registered could be viewed as performing the function of maintaining the securities books “on behalf of the issuer.”⁵⁷ If the issuer’s board of directors expressly provides in its authorizing resolutions that the issuer will use the blockchain as its “books” for purposes of registering the issuance and transfer of its securities, that authorization should suffice to support the function of a blockchain as the issuer’s “books” under UCC Article 8.

UCC Article 8 and the state corporate codes require an issuer to keep a transfer ledger, but do not prescribe the method for doing so. Issuers have long used independent transfer agents to maintain their ledgers. As indicated above, an is-

51. *Id.*

52. *Id.* § 8-102(a)(18). State codes also provide for “uncertificated securities.” For example, section 158 of the Delaware General Corporation Law provides: “The shares of a corporation shall be represented by certificates provided that the board of directors of the corporation may provide by resolution or resolutions that some or all of any or all classes or series of its stock shall be uncertificated shares.” DEL. CODE ANN. tit. 8, § 158 (2017). Thus, a Delaware corporation could start issuing uncertificated common stock by board resolutions without amending its charter. Section 6.26 of the Model Business Corporation Act permits the board of directors to authorize uncertificated securities “unless the articles of incorporation or bylaws provide otherwise.” MODEL BUS. CORP. ACT ANN. § 6.26 (2016). Section 508 of the New York Business Corporation Law contains a similar provision. N.Y. BUS. CORP. LAW § 508 (McKinney 2003).

Section 158 of the Delaware General Corporation Law provides that the transfer of stock of a Delaware corporation is governed by UCC Article 8. In that regard, identification of ownership is important for blockchain stock or bonds because the rights to receive notices, to vote, to receive dividends, and to exercise appraisal and other rights are limited to registered owners. UCC § 8-207(a) states: “Before due presentment . . . of an instruction requesting registration of transfer of an uncertificated security, the issuer or indenture trustee may treat the registered owner as the person exclusively entitled to vote, receive notifications, and otherwise exercise all the rights and powers of an owner.”

53. Schroeder, *supra* note 49, at 69–70.

54. *Id.*

55. FINRA REPORT, *supra* note 4, at 14.

56. Schroeder, *supra* note 49, at 69–70.

57. *Id.*

suer could, by its board resolutions, adopt a blockchain as its “books.”⁵⁸ Indeed, the blockchain’s asymmetric key (private key and public key) transfer system, properly programmed, together with blockchain nodes or other consensus verification process, might be a safer mode of determining whether an instruction is genuine and authorized than the traditional process for verifying a requested transfer of an uncertificated security.⁵⁹

Whether blockchain securities are “of the type” dealt in or traded on securities exchanges or markets within the meaning of section 8-102(a)(15)(iii)(A) is currently unclear. That being said, UCC Article 8 seems to intend a broad definition of “securities” that would include blockchain securities. While it is the case that blockchain securities are not currently being traded on a national securities exchange, there are systems already established, like that for Overstock, that provide for the trading of blockchain securities. Moreover, the definition of “security” includes securities not publicly traded, and the commentary in UCC Article 8 indicates that the definition is intended to be broad enough to cover “new forms of securities which are to be traded in the markets, even though no similar type has previously been dealt in or traded in the markets.”⁶⁰ The “of the type” requirement is not intended to limit the form of an issuer’s trading securities registry, and so it should cover securities on blockchain. In any case, out of abundance of caution, the issuer’s board of directors could make use of the “opt-in” provision of UCC section 8-102(a)(15)(iii)(B) by expressly specifying in the board’s authorizing resolutions that the issuer’s blockchain securities constitute “uncertificated securities” governed by UCC Article 8 of the issuer’s state.

IDENTIFICATION OF SECURITY HOLDERS WITHIN A BLOCKCHAIN

Under the federal securities laws, intermediaries who are holding securities for others must forward proxy statements to the persons who are beneficial owners under the securities laws.⁶¹ Fortunately, blockchains do not have to be anonymous or even pseudonymous—a permissioned blockchain such as that developed by Overstock allows for complete transparency (to at least the issuer, the transfer agent, and the broker-dealer) of the participants on the blockchain, as required for issued and traded securities. Though identifying pseudonymous owners related to the public and private keys is not currently possible as a practical matter for an issuer on a Bitcoin blockchain, a blockchain that registers securities could be programmed to enable the issuer of blockchain securities, any transfer agent, and any intermediary holding such securities for others to identify the owners of such blockchain securities.

In the case of Overstock’s blockchain securities, for which trading relies on intermediaries, each customer who wishes to trade blockchain securities is re-

58. *Id.* at 74.

59. *Id.*

60. U.C.C. § 8-102 cmt. 15.

61. SEC Rules 14b-1, 14b-2, 17 C.F.R. §§ 240.14b-1, 240.14b-2 (2017).

quired to open an online brokerage account with Keystone.⁶² Keystone (as well as each broker-dealer who otherwise gains or arranges access to the PRO Securities ATS indirectly through a direct subscriber to the ATS) is responsible for accepting customers using the same “know your customer,” suitability, and other requirements applicable when accepting customers for trading traditional securities.⁶³ The only difference from traditional securities held by a securities intermediary is that, under the ATS software technology licensing provisions, Keystone’s customer owns the blockchain securities as a record holder in his or her own name instead of in “street name” and Keystone is required to share its customer’s identity with Overstock and Overstock’s transfer agent. Such sharing happens automatically at the time each customer’s account is created by the ATS software technology.⁶⁴ Overstock will continue to have ongoing access to the proprietary ledger with respect to its blockchain securities as well as the personal identity information of the holders of its blockchain securities, and Overstock or its transfer agent will be able to query the book-entry system whenever it wants to generate a list of record holders of Overstock’s blockchain securities and the number of such securities held by each record holder as of any point in time.⁶⁵ Thus, Overstock’s blockchain system gives the issuer and its transfer agent near real-time data as to the record holders of its digital securities, enabling the issuer or its transfer agent to mail proxies, pay distributions, and take other actions with respect to its record holders as required by the applicable securities and corporate laws.⁶⁶

TRANSFER OF SECURITIES ON A BLOCKCHAIN

Pursuant to UCC section 8-104(a)(1) an uncertificated security is transferred by “delivery” to the purchaser.⁶⁷ For this purpose, delivery occurs when:

- (i) the issuer registers the purchaser as the registered owner, upon original issue or registration of transfer; or
- (ii) another person, other than a securities intermediary, either becomes the registered owner of the uncertificated security on behalf of the purchaser or, having previously become the registered owner, acknowledges that it holds for the purchaser.⁶⁸

Thus, UCC Article 8’s definition of “delivery” covers the acts necessary for the transfer of a blockchain security.⁶⁹

62. Overstock Prospectus, *supra* note 35, at 34.

63. Overstock Letter, *supra* note 39, at 4.

64. *Id.*

65. *Id.* at 2–3.

66. *Id.* at 3.

67. U.C.C. § 8-104(a)(1).

68. *Id.* § 8-301(b).

69. Schroeder, *supra* note 49, at 72–74.

The owner of an uncertificated security makes a transfer by giving an “instruction” to the issuer or to whoever maintains the issuer’s books on behalf of the issuer.⁷⁰ UCC section 8-102(a)(12) defines an “instruction” as a notification that is communicated to the issuer of an uncertificated security and that directs that the transfer of the security be registered or that the security be redeemed. UCC section 8-107(b) provides that an instruction is effective if it is made by an “appropriate person,” defined in UCC section 8-107(a)(2) to include “the registered owner of an uncertificated security,” or if it is made by a person who has “control” of the security under section 8-106(c)(2). With respect to a blockchain security, such an “instruction” could be made on the blockchain using the owner’s double-key (private key and public key) procedure.⁷¹

The issuer’s duty to register transfers of *uncertificated* securities parallels the issuer’s duty to register transfers of *certificated* securities. UCC section 8-401(a) states in relevant part:

If . . . an instruction is presented to an issuer with a request to register transfer of an uncertificated security, the issuer shall register the transfer as requested if:

1. under the terms of the security the person seeking registration of transfer is eligible to have the security registered in its name;
2. the . . . instruction is made by the appropriate person or by an agent who has actual authority to act on behalf of the appropriate person;
3. reasonable assurance is given that the . . . instruction is genuine and authorized (Section 8-402);
4. any applicable law relating to the collection of taxes has been complied with;
5. the transfer does not violate any restriction on transfer imposed by the issuer in accordance with Section 8-204;
6. a demand that the issuer not register transfer has not become effective under Section 8-403; and
7. the transfer is in fact rightful or is to a protected purchaser.

That blockchain system can be designed to be anonymous; for example the owner of a Bitcoin can be and remain anonymous. However, in order to comply with UCC section 8-401(a), as well as to comply with the legal requirements for sending or transferring proxy statements, the issuer of a blockchain security must know the identity of the owner of that blockchain security. In addition, in order to allow the transferor to be identified to the transferee so that the transferee can exercise rights in respect of the warranties under UCC section 8-108(b), the identity of the transferors of blockchain securities cannot be anonymous. Thus, a securities blockchain has to be designed differently from a Bitcoin blockchain.

In the case of Overstock, Keystone (and any other broker-dealer that is licensed to utilize the ATS software technology) is required to agree to share the identity of

70. U.C.C. §§ 8-401(a), 8-407. UCC § 8-201(c) provides that, with respect to a registration of a transfer, “issuer” means a person on whose behalf transfer books are maintained.

71. See *supra* notes 17–19 and accompanying text.

its customers with Overstock and Overstock's transfer agent, trustee, or other similar agent with respect to each series of digital securities that Overstock issues. The proprietary ledger maintained by the ATS will reflect the definitive ownership record with respect to Overstock's blockchain securities and will be electronically published.⁷²

Also, a blockchain for securities needs to be programmed so as to permit the issuer to prevent transfer. If a creditor wants to attach or otherwise bring legal process against a debtor's interest in an uncertificated security, the creditor serves such attachment or other legal process "upon the issuer at its chief executive office in the United States."⁷³ Thus, a blockchain on which an uncertificated security is registered must be programmed to enable the issuer, if, as and when an attachment or other legal process relating to such security is served on it, to identify, and then to notify, the owner of such security, and then to impose a "stay" on the transfer of such security until the attachment or other legal process is resolved. Such programming may be made by a "smart contract" embedded in the blockchain.⁷⁴

In the case of Overstock, its blockchain securities are represented by proprietary ledger balances that are secured by a digital wallet with a unique alphanumeric identifier known as a multi-signature address.⁷⁵ A trade must be initiated by the security holder on its online brokerage account at Keystone and must be signed by both a private key accessible to ETC, the clearing broker for Keystone, and a private key accessible to the transfer agent.⁷⁶ This system means that Overstock, the ATS, or Keystone may be able to *transfer* (or cause the transfer of) ownership of the blockchain securities on behalf of the blockchain security holder, and may be able to *block* (or cause the prevention of) further transfers of such blockchain securities, by means of the private keys to the multi-signature wallet.⁷⁷

BLOCKCHAIN SECURITY HOLDERS' RIGHT TO PREVENT TRANSFER

UCC section 8-403 gives the owner of a security the right to *demand* that the issuer not register transfer of the security. Pursuant to section 8-403(b) and (c), if the issuer receives an instruction to transfer an uncertificated security after receiving such a demand, the issuer must give a notice to both the person who made the demand and the person who initiated the transfer request, and then must withhold registration for a period not to exceed thirty days after the date of such notice. UCC section 8-403 gives an owner of securities time to obtain

72. See *supra* notes 35–38 and accompanying text.

73. U.C.C. § 8-112(b).

74. "Smart contracts" are computer programs that secure, enforce, and execute settlement of recorded agreements among people and organizations. TAPSCOTT & TAPSCOTT, *supra* note 2, at 101. While smart contracts enable autonomous agreement execution between parties, smart contracts rely on architects and security experts to build business rules that prevent malicious behavior, test thoroughly and end-to-end, and verify all codes. See WORLD ECON. FORUM, THE FUTURE OF FINANCIAL INFRASTRUCTURE 35 (2016).

75. Overstock Prospectus Supplement, *supra* note 38, at S-8.

76. *Id.*

77. *Id.*

legal process to protect the owner from wrongful transfer. The commentary to section 8-403 states that the section is intended to alleviate the problems faced by registered owners of certificated securities who lose or misplace their certificates.⁷⁸ In the case of blockchain securities, section 8-403 would alleviate the problems faced by registered owners who know or fear that their control of their blockchain securities is or may be adversely affected by a split blockchain⁷⁹ or a “51% attack” (though it has been theorized that this sort of attack could be done with as little as 30 percent of the total network hack).⁸⁰

The blockchain verification system that prevents spending the same Bitcoin twice (the so-called “double-spend” problem) could also be used to prevent transfers of blockchain securities.⁸¹ It would be only a matter of programming to create a smart contract in which a registered owner could, through the use of the owner’s public and private key, automatically put a thirty-day block on the trading of the owner’s blockchain securities.⁸² Moreover, a blockchain could also be programmed to send out automatically the notices required by section 8-403 when it receives an attempt to transfer during this period.⁸³

SETTLEMENT TIME FOR SECURITIES TRADED ON BLOCKCHAIN

In general, settlement of a trade of securities on a blockchain would be much faster than a trade of securities in the existing exchanges and securities markets—minutes instead of days. Ironically, this increase in speed could disadvantage an owner whose securities are registered on a blockchain.⁸⁴ With a conventional certificated security, a thief would take several days to resell the

78. U.C.C. § 8-403 cmt. 2.

79. If two different blocks are created at around the same time, it results in a 1-block fork, with either block admissible under the longest valid chain policy for the blockchain. Normally, nodes then have to decide which block to extend. However, a malicious node might send a transaction to a person, receive some goods or services in exchange for it, and then fork the blockchain to create a longer branch containing a *conflicting* transaction. The original transaction to such person will be invalid in this new consensus blockchain. See ARVIND NARAYANAN ET AL., *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES* § 515, at 158–59 (2016).

80. In this consensus attack, a group of nodes controlling a majority (51 percent) of the total network’s hashing power colludes to attack the blockchain. With the ability to mine or control the majority of the blocks, the attacking nodes can cause deliberate “forks” in the blockchain and double-spend transactions or execute denial-of-service attacks against specific transactions or addresses. A 51 percent attack allows attackers to double-spend their own transactions in the new chain, thus undoing the corresponding transaction in the old chain. Despite its name, the 51 percent attack scenario does not actually require 51 percent of the hashing power. In fact, such an attack can be attempted with a smaller percentage of the hashing power. The 51 percent threshold is simply the level at which such an attack is almost guaranteed to succeed. Such a consensus attack is essentially a tug-of-war for the next block and the “stronger” group is more likely to win. One way to look at it is that the more hashing power an attacker has, the longer fork he can deliberately create, the more blocks in the recent past he can invalidate, or the more blocks in the future he can control. Security research groups have used statistical modeling to claim that various types of consensus attacks are possible with as little as 30 percent of the hashing power. See ANDREAS M. ANTONOPOULOS, *MASTERING BITCOIN (UNLOCKING DIGITAL CRYPTOCURRENCIES)* 210–12 (2015).

81. Schroeder, *supra* note 49, at 74–76.

82. *Id.*

83. *Id.*

84. *Id.*

stolen securities, whereas a thief of a blockchain security could in theory resell such security in minutes, not giving the registered owner the time to get the protection of UCC section 8-403.⁸⁵

On the positive side, a blockchain network for securities and cash could provide near real-time settlement (assuming payments of cash could be done in a similar time-frame), a unique innovation. The recently shortened standard settlement cycle for most broker-dealer securities transactions from T+3 to T+2 (settlement occurs two business days after the date of trade) is not the result of technology limitations, but rather based on laws and market structures.⁸⁶ Blockchain could support faster clearing and settlement systems by way of securities and cash ledgers and a related smart contract, with both sides of the transaction executed simultaneously.

“PROTECTED PURCHASER” PROTECTION FOR BLOCKCHAIN SECURITIES

A good-faith purchaser of a blockchain security should get the protection of UCC section 8-303(b) for a “protected purchaser.”⁸⁷ Section 8-303(b) provides that a protected purchaser “acquires its interest in the security free of any adverse claim.” A “protected purchaser” is defined as “a purchaser of a certificated or *uncertificated* security, or of an interest therein, who:

- (1) gives *value*;
- (2) does not have *notice of any adverse claim* to the security; and
- (3) obtains *control* of the certificated or uncertificated security.⁸⁸

“Value” is defined to include “any consideration sufficient to support a simple contract,” and so any sale of a security would entail “value.”⁸⁹ Donees, in addition to thieves, would not give “value” and so could not become protected purchasers. However, donees do receive the benefit from the shelter rule of section 8-302, which provides that “a purchaser of a certificated or uncertificated security acquires all rights in the security that the transferor had or had the power to transfer.” Thus, a donee who receives a gift of a blockchain security from a donor who is a protected purchaser gets the donor’s rights as a protected purchaser.

Whether a purchaser of a security has “notice of any adverse claim to the security” is governed by UCC section 8-105, which goes beyond having actual knowledge of an adverse claim. A purchaser of a security has such notice if such purchaser “is aware of facts sufficient to indicate that there is a significant probability that the adverse claim exists and deliberately avoids information that would establish the existence of the adverse claim.”⁹⁰ However, in order for a

85. *Id.*

86. Securities Transaction Settlement Cycle, Exchange Act Release No. 34-80295 (Sept. 5, 2017).

87. U.C.C. section 8-303(a)’s definition of “protected purchaser” includes a purchaser of an uncertificated security as well as a purchaser of a certificated security.

88. U.C.C. § 8-303(a) (emphasis added).

89. *Id.* § 1-204(4).

90. *Id.* § 8-105(a)(2).

claim to be an “adverse claim,” the claim must not only assert a property interest in the security but also assert a violation of the rights of the claimant for another person to hold, transfer, or deal with the security.⁹¹ Moreover, subsection (e) of section 8-105 provides that the “filing of a financing statement under Article 9 is not notice of an adverse claim to” such security. Thus, it would seem unlikely that there would be many circumstances in which section 8-105 would apply, unless the purchaser were acting in bad faith.⁹²

A secured party having a perfected security interest in blockchain securities should be able to be a “protected purchaser” under UCC section 8-303(a). For a “purchaser” includes, under UCC section 9-102(a)(29) and (30), a person who takes by “pledge” or “security interest.” A secured party would, in order to be a secured party, normally give “value,” and a lawyer rendering a “protected purchaser” opinion covering the secured party would generally assume that the secured party does not have notice of any adverse claim. Thus, the only real issue for such lawyer is whether the secured party has “control” of the blockchain securities. In that regard, the secured party would get “control” of blockchain securities either by having the securities “delivered” to it⁹³ or by executing a control agreement with the issuer and the registered owner under which the issuer agrees that it will comply with instructions originated by the secured party without further consent by the registered owner.⁹⁴

A secured party might want to have control not only for purposes of UCC section 8-106(c) but also under and for purposes of foreclosing on the pledged blockchain securities. In this regard, the issuer is under a duty to register the transfer of blockchain securities by a secured party either (i) as a “registered owner” under UCC section 8-106(c)(1) if the secured party presents an instruction to the issuer with a request to transfer the securities⁹⁵ or (ii) if the issuer presents such an instruction to the issuer pursuant to a control agreement executed with the secured party and the registered owner pursuant to UCC section 8-106(c)(2).⁹⁶ The secured party should be able to satisfy the conditions of transfer under UCC section 8-401(a).

A secured party might, however, want the ability *by itself* to transfer the pledged blockchain securities on the blockchain to a purchaser in a foreclosure—equivalent to the secured party’s possessing a certificated security with an executed blank stock or bond power covering the security and selling that security to a purchaser in a foreclosure. For that ability, the secured party would have to be given the combination of public and private keys sufficient to transfer, without the help of the issuer or its transfer agent and without interference by the debtor, the pledged blockchain securities on the blockchain.

91. *Id.* § 8-102(a)(1).

92. Schroeder, *supra* note 49, at 76–77.

93. *See supra* notes 67–71 and accompanying text.

94. U.C.C. § 8-106(c).

95. *Id.* § 8-107(b)(1).

96. *Id.* § 8-107(b)(2).

ISSUES FOR BLOCKCHAIN SECURITIES UNDER THE UCC

There are, however, some remaining issues for the issuer of blockchain securities under UCC Article 8. Subsection (a) of UCC section 8-401 requires the issuer of a security to register a transfer of its security if the specified conditions are satisfied. Subsection (b) then provides that the issuer is liable for failing to register a transfer when it is obligated to do so. Would the issuer be so liable if a registration of transfer were not made on the securities blockchain due to a system defect, or hacking, or other cause beyond the issuer's control? The answer to that question should be no, because technically the issuer would not have "failed" to register the transfer, the transfer *not* being made due to the issuer's advertent or inadvertent act or omission.

If an "instruction" is presented to an issuer with a request to register transfer of its blockchain security, the issuer would generally try to determine that the preconditions to such registration of transfer under UCC section 8-401(a) are satisfied. That should be possible under a properly programmed blockchain for securities. Furthermore, the commentary to section 8-401 gives the issuer leeway in determining the satisfaction of such conditions:

This section [8-401] does not constitute a mandate that the issuer must establish that all preconditions are met before the issuer registers a transfer. The issuer may waive the reasonable assurances specified in paragraph (a)(3) [reasonable assurance that the instruction is genuine and authorized]. If it has confidence in the responsibility of the persons requesting transfer, it may ignore questions of compliance with tax laws [paragraph (a)(4)]. Although an issuer has no duty if the transfer is wrongful, the issuer has no duty to inquire into adverse claims, see Section 8-404.⁹⁷

Indeed, the issuer is not liable under UCC section 8-404(a) for failure to determine the satisfaction of the preconditions under section 8-401, except for registration of transfer "pursuant to an ineffective instruction."

In the case of Overstock, its transfer agent will have access to near real-time information with respect to the record holders of Overstock's blockchain securities and can query Overstock's ledger or "book-entry system" as of any point in time it wishes.⁹⁸ Because the holders of Overstock's blockchain securities are the record holders, there would be no need to run broker searches to request beneficial ownership information, as is necessary for traditional securities. Other than the differences described above in this paragraph, the transfer agent performs the same role as it would for traditional securities.⁹⁹ The transfer agent is the registrar acting on behalf of Overstock and will manage the securities registry for Overstock's blockchain securities using Overstock's ledger or "book-entry system."¹⁰⁰

97. *Id.* § 8-401 cmt. 1 (second paragraph).

98. See *supra* notes 44–45 and accompanying text.

99. Overstock Letter, *supra* note 39, at 4.

100. *Id.*

The nodes, as noted above,¹⁰¹ maintain and implement the registration of transfer of the blockchain securities on the blockchain, comparable to a transfer agent. In this regard, UCC section 8-407 imposes on a transfer agent, and therefore arguably on such nodes, the same obligations owed to the owner of an uncertificated security with regard to the particular functions performed as the issuer has in regard to those functions. However, it would seem that the nodes would not be liable in the same way as a transfer agent under section 8-407 because no one node has control of the blockchain. This is particularly true in the case of Overstock, which has an actual transfer agent that does control the blockchain and acts for the issuer in connection with Overstock's blockchain securities.

A securities blockchain must be programmed so that the sale of a security on the blockchain can be cleared—that is, so that a transfer of a blockchain security from the owner/seller to a purchaser and the transfer of the purchase price from the purchaser to the owner/seller can be effected within the time limits set forth in the SEC's rules for the clearance of a securities sale. This should not be difficult, because the programming of a transfer of Bitcoins has already been done, and so the programming for the simultaneous transfer of securities and purchase price on the blockchain should be doable. Indeed, Overstock has created a blockchain system with these capabilities.

An investor can choose to hold blockchain securities indirectly through a securities intermediary. This would forgo one of the advantages of issuing and transferring securities on the blockchain—that is, the ability to trade directly without the use of intermediaries. However, holding blockchain securities through a securities intermediary retains the advantage of faster, and probably more secure, settlement of trades than through the traditional system using clearing corporations such as The Depository Trust & Clearing Corporation.¹⁰² In the case of Overstock's blockchain securities, existing securities intermediaries became the nodes of Overstock's proprietary blockchain and thereby provide further ease of execution. Even if blockchain securities trading were to become more common so that publicly traded companies issued their securities on a blockchain, most individual investors who use investment advisers might prefer the convenience of continuing to hold their blockchain securities indirectly through a securities intermediary. But, of course, if and to the extent that blockchain securities are held indirectly by a securities intermediary in a "securities account" (as defined in UCC section 8-501(a)) in the name of the intermediary or its agent, the investor would own a "security entitlement" (as defined in UCC section 8-102(a)(17)) in respect of those blockchain securities rather than owning the blockchain securities as "uncertificated securities."¹⁰³

101. See *supra* note 15 and accompanying text.

102. Schroeder, *supra* note 49, at 78.

103. See U.C.C. § 8-501(b), (d).

LEGAL OPINIONS COVERING BLOCKCHAIN SECURITIES

When an underwriter in a public offering or a purchaser in a private placement agrees to acquire stock from a corporation directly (as distinct from acquiring securities on an exchange), such underwriter or purchaser customarily requires as a condition of closing an opinion from counsel for the issuer regarding the shares it is acquiring.¹⁰⁴ That would be true for a public offering or a private placement of uncertificated shares directly from the issuer on blockchain. The opinion would read something like this:

The [uncertificated] shares have been duly authorized and validly issued and are fully paid and nonassessable.¹⁰⁵

The opinion covering uncertificated shares on blockchain would typically address the authorization of the shares under the issuer's charter and bylaws and the applicable corporate law, the valid issuance of the shares by the issuer, the receipt by the issuer of payment for those shares, and the nonassessable nature of the shares in the hands of shareholders.¹⁰⁶

As we have seen, the corporate codes of various states generally provide for the issuance of uncertificated shares, provided that the issuer's board of directors provides by resolution for such issuance and that the issuer's charter or bylaws does not provide otherwise.¹⁰⁷ The discussion in the TriBar Opinion Committee's report on *Third-Party "Closing" Opinions*, setting forth the customary practice that a lawyer should consider in rendering the above opinion,¹⁰⁸ would apply to the issuance of uncertificated shares on blockchain. The opinion giver would not, in the case of uncertificated shares on blockchain, have to deal in the opinion with the factual mechanics of putting the shares on blockchain, just as an opinion giver in the case of certificated shares does not have to deal in the opinion with the factual mechanics of issuing share certificates. However, as a matter of prudence, the opinion giver should review evidence, or assume in the opinion, that the issuer has sent, or will send, to the registered owner of the uncertificated shares the written notice containing the information required (similar to the information set forth or stated in the case of certificated shares) for the registered owner of the uncertificated shares pursuant to the applicable state corporate statute.¹⁰⁹

Lawyers also typically render an opinion on the rights that a buyer of outstanding securities acquires in a so-called "secondary sale."¹¹⁰ For example, underwriters in registered public offerings often request a legal opinion when the offering includes outstanding securities. In addition, investors in secondary

104. TriBar Opinion Comm., *Third-Party "Closing" Opinions*, 53 BUS. LAW. 591, 648 (1998) (§ 6.2) [hereinafter 1998 TriBar Report].

105. See *id.* at 671 (paragraph 2 of the illustrative opinion letter in appendix B-1).

106. See *id.* at 648.

107. See *supra* note 39 and accompanying text.

108. See 1998 TriBar Report, *supra* note 104, at 648–52.

109. See, e.g., DEL. CODE ANN. tit. 8, § 151(f) (2017); N.Y. BUS. CORP. LAW § 508(f) (McKinney 2003); MODEL BUS. CORP. ACT ANN. § 6.26(b) (2016).

110. See *Special Report of the TriBar Opinion Committee—Opinions on the Secondary Sale of Securities*, 66 BUS. LAW. 625 (2011).

sale transactions sometimes request a legal opinion when privately acquiring outstanding securities. The same would be true of any secondary sale of uncertificated securities on blockchain. In that connection, the *Special Report of the TriBar Opinion Committee—Opinions on the Secondary Sale of Securities* (the “TriBar Secondary Sale Report”) sets forth, for uncertificated securities as well as for certificated securities, the customary opinion that a lawyer would consider in a secondary sale of securities, and that opinion reads something like:

[Name of buyer] [will be] [is] a protected purchaser of the [shares]

or

[Name of buyer] [will acquire] [has acquired] the [shares] free of any adverse claim.

or

[Name of buyer] [will be] [is] a protected purchaser of the [shares] and [will acquire] [has acquired] the [shares] free of any adverse claim.¹¹¹

The *TriBar Secondary Sale Report* sets forth not only the considerations in rendering the above opinion covering uncertificated securities in a secondary sale but also the assumptions and limitations that would accompany and support such opinion, including the scope limitation that limits the coverage of the opinion to UCC Article 8.¹¹²

CONCLUSION

UCC Article 8 was amended in 1999–2000 to cover uncertificated securities as well as certificated securities, but to date those amendments for uncertificated securities have not been much used. That would change if securities are made digital and put on a blockchain. Securities on a blockchain would be “uncertificated securities” under UCC Article 8, and they would be covered under and pursuant to the provisions of UCC Article 8 relating to uncertificated securities—but not without (as explained in this article) some interpretation and understanding.¹¹³ And

111. See *id.* at 654–55 (Appendix B—Illustrative Opinion Language).

112. See *id.* at 631–33 (§ 2.3); *id.* at 638–40 (§§ 2.5, 2.6); *id.* at 640–43 (§ 4).

113. Unlike the registry of securities on a blockchain, the registry of *instruments* on a blockchain would not be covered by the existing UCC. An instrument under UCC Article 3 is a “negotiable instrument,” which is limited under UCC Article 3 to a “promise” (U.C.C. § 3-103(a)(12)) or an “order” (UCC § 3-103(A)(8)) that is a “written undertaking” or “written instruction” to pay money “signed by the person” undertaking to pay or giving the instruction (emphasis added). U.C.C. §§ 3-104 & cmt. 1, 3-103(a)(8)(order), 3-103(a)(12)(promise); see also N.Y. U.C.C. § 3-104(1)(a) (McKinney 2013) (“Any writing to be a negotiable instrument within this Article [3] must (a) be signed by the maker or drawer” (emphasis added)). Thus, the UCC Article 3 would not cover an instrument on the blockchain, except by analogy. Although a blockchain instrument is not a negotiable “instrument” under UCC Article 3, nothing in UCC Article 3 is intended to imply that, for a blockchain instrument, a court could not arrive at a result similar to the result that would follow if the blockchain instrument were a negotiable instrument. For example, a court might find that the obligor with respect to a promise contained in a blockchain instrument is precluded from asserting a defense against a bona fide purchaser. The preclusion would be based on estoppel or ordinary principles of contract and not on the law of negotiable instruments. See, e.g., U.C.C. § 3-302 cmt. 4, case 2. As an alter-

customary opinion practice would not have to change to accommodate securities on blockchain.

native, the party or parties to the blockchain instrument could provide by agreement that specified applicable provisions of UCC Article 3 will determine their rights and obligations in respect of the blockchain instrument. Upholding such agreement and choice of applicable legal rules is not inconsistent with UCC Article 3. See U.C.C. § 3-104 cmt. 2.

Interestingly, letters of credit on a blockchain *would* clearly be covered by the UCC, namely UCC Article 5, which applies to “letters of credit and to certain rights and obligations arising out of transactions involving letters of credit.” U.C.C. § 5-103(a). UCC § 5-104 sets forth the formal requirements for a letter of credit and provides that a letter of credit (including a confirmation, advice, transfer, amendment, or cancellation of a letter of credit) “may be issued in any form that is a *record* and is *authenticated* (a) by a signature, or (b) *in accordance with the agreement of the parties or the standard practice* [of financial institutions that regularly issue letters of credit]” (emphasis added). A “record” includes information “that is stored in an electronic or *other medium* and is retrievable in perceivable form,” and so would include the blockchain. [U.C.C. § 5-0102(a)(14) (emphasis added)]. Indeed, according to Official Comment 3 of UCC § 5-104, “by declining to specify any particular medium in which the letter of credit must be established or communicated, Section 5-104 leaves room for future developments.” Blockchain is one of those developments.