The Investment Lawyer

Covering Legal and Regulatory Issues of Asset Management

VOL. 23, NO. 10 • OCTOBER 2016

# Blockchain 101 for Asset Managers

*By C. Todd Gibson and Tyler Kirk*

## An Introduction to Blockchain

Over the last two years, it has been difficult to attend any asset management-related event or seminar without hearing the term "FinTech," and in particular, "robo-advice" and "blockchain."[1] What is apparent, though, is that many industry participants have little understanding of what blockchain technology is and how it works. This understanding is important in order to identify creative ways of leveraging this technology to increase efficiency. The intent of this article is to give those with a limited understanding of blockchain a baseline of knowledge and to provide an update on current trends with respect to the use of blockchain by fund managers and their service providers.

## What Is Blockchain?

Blockchain was first introduced in November 2008 in a white paper titled, "*Bitcoin: A Peer-to-Peer Electronic Cash System*."[2] The white paper positioned blockchain as the recordkeeping, clearing, and settlement protocol that underpins bitcoin, the world's first and widely-accepted decentralized digital currency. Until recently, blockchain has resided in relative obscurity. However, many asset management industry participants are taking a closer look at leveraging blockchain to increase efficiency and create competitive advantages.

One approach to defining blockchain in easily-understandable terms is to weave together a collection of more established concepts. As an initial matter, blockchain is a cryptographic protocol, or detailed set of rules implemented through software, for securely tracking and transferring data utilizing the internet. In this way, blockchain is an encrypted digital ledger or database for recording and verifying transactions. Further, blockchain is a peer-to-peer (P2P) network where members of the "trusted" network exchange data directly with one another without the need for an intermediary acting as a central depository or custodian of such data. Finally, blockchain is a distributed ledger technology (DLT) allowing for transaction-by-transaction verification through distributed consensus. While the building blocks of blockchain are well established, they fit together to build a truly innovative and disruptive solution to efficiently effecting transactions.

At its most basic level, blockchain, as a P2P network, operates without intermediation. To be viable, blockchain had to solve two fundamental problems traditionally addressed by third-party intermediaries: (1) trusting the accuracy of the ledger; and (2) preventing double spending. Blockchain addresses these concerns by, among other things, (1) distributing multiple copies of the ledger to the members of the network; (2) verifying ownership ex-ante; (3) verifying transfer of ownership ex-post; and (4) cryptographically securing the ledger and each transaction. The blockchain protocol implements these solutions through a managed or immutable tokenized database.

More specifically, blockchain is a write-once, read multiple times (or "many times") (WORM) protocol for transferring ownership of digital or digitized assets. Further, a key component of transferring assets on a blockchain network is assigning each asset a unique identity. This is sometimes referred to as tokenization. The WORM protocol and tokenization are integral to preventing double spending of a tokenized asset.

Each entry in the digital ledger used by a blockchain network represents a transaction and a transfer of title from one network participant to another. When a transaction occurs, all of the copies of the ledger are updated and verified simultaneously. This establishes a "shared truth" through "distributed consensus" because all participants maintaining a copy of the ledger must mathematically authenticate the accuracy of the transaction. For immutable blockchain networks, this is known as "proof of work." In a WORM database, entries cannot be deleted. Accordingly, mistakes must be offset by a corresponding transaction. Yet, a WORM database without tokenization is not enough because it does not address fungibility.

Significantly, nearly any physical or digital asset can be tokenized. The blockchain protocol uses cryptographic hashes to generate unique identification numbers that serve as the asset's token, making an asset unique that might otherwise be fungible. Hashes are one-way deterministic functions that produce an output of a fixed length, regardless of the input. Further, the token produced by the hash can essentially never be the same unless the inputs are the same. Tokens can also be thought of as an asset's serial number. By tokenizing assets, the blockchain protocol creates a unique fingerprint or identity for an asset, that when recorded in a WORM database, prevents a network participant from double-spending that asset.

Each participant on a blockchain network, however, must establish its identity before tokenizing assets. Again, the blockchain protocol uses the tokenization concept to create a unique identifier for each participant. This token becomes the participant's address on the blockchain network, or "address token." In addition to cryptographic hashes, the blockchain protocol uses well known methods of encryption to securely sign and execute transactions. By using asymmetric ciphers, more commonly known as public key encryption, participants are able to generate unique public and private key pairs that allow counterparties to verify their respective identities after transactions have been signed with a participant's private key.

In short, blockchain is a decentralized digital ledger, and its creation established a new class of digital ledgers, DLTs. Unlike current financial settlement systems, DLTs are more efficient because all transactions are mathematically provable and do not require a multi-day verification process. DLT protocols use encryption combined with distributed copies of the ledger to replace the need for a third party to serve as the ledger's custodian. In short, DLTs create a managed or immutable record of the truth arrived at through distributed consensus. Yet, the protocol's hyper-focus on disintermediation raises the question about who develops the software that drives a blockchain network and how does the trustless model square with the need to rely on the implementation of blockchain through software?

## Blockchain as a Service

As previously noted, blockchain was initially conceived as a trustless recordkeeping protocol. However, the notion of "trustless" is not absolute in its most pure terms. The protocol itself is implemented through software, and that software must be developed in-house or sourced from a third-party vendor. Financial institutions seeking to employ blockchain in their business activities will therefore need to build their own bespoke blockchain software platform or look to third-party vendors to provide a customizable "shrink wrapped" blockchain product.

By reason of economies of specialization, most financial institutions will likely rely on trusted third-party vendors to provide the basic software to launch a blockchain network capable of being tailored to fit the needs of a specific financial institution or a consortium of institutions. Consequently, all participants in a blockchain network will be required, to a certain degree, to trust the software developed to implement the blockchain. It should be noted, however, that bitcoin mitigated this particular trust issue by making the project open source, allowing the community of users to examine the code and verify its authenticity and integrity. In short, while the blockchain protocol eliminates trust as a condition precedent to recordkeeping, participants in a blockchain network must trust the software implementing the network, an issue addressed by open source software.

Several large software vendors are already carving out market share by providing customizable blockchain products. On June 15, 2016, Microsoft released a white paper introducing Project Bletchley, Microsoft's next iteration on its blockchain as a service (BaaS) product.[3] In late 2015, Microsoft announced that it would be leveraging its cloud platform, Azure, to provide a low-risk sandbox for customers to gain experience with how blockchain may be applied in various business scenarios, such as financial transactions and supply chain management. Bletchley is positioned as incorporating the latest innovations on the blockchain protocol in the Azure cloud service.

Recently, the blockchain protocol introduced by bitcoin has become known as "blockchain 1.0." In its original form, blockchain was a decentralized digital ledger that utilized encryption combined with distributed copies of the ledger to replace the need for a third party to serve as the ledger's trusted guardian. Further, blockchain introduced unforeseen security and efficiencies by mathematically proving and settling transactions intra-day. The protocol was "append only" and distributed, thus every participant received an update to his copy of the ledger with the latest transactions. Yet, to handle the variety of possible conditions arising under transactions more complex than the transfer of bitcoin, innovation was required.

Blockchain 2.0 introduced "smart contracts" to the protocol. Smart contracts are bundles of coded logic or procedures which sit beside the entries in the ledger. The promise of smart contracts is that they will allow certain business processes to operate independently by creating self-enforcing contracts. In other words, two parties to a digital ledger can "auto-execute" a contract to the extent the pre-conditions of the smart contract are satisfied. However, it was quickly recognized that these smart contracts would have to interact with the world outside of the blockchain network.

To incorporate external signals into the blockchain network, blockchain 3.0, Project Bletchley builds on the existing concept of blockchain oracles. Oracles are dedicated software designed to inject external signals into the blockchain. These signals can be triggering events defined by a smart contract, such as date, time, price, or interest rate. Once a particular signal strikes a predetermined value, for example, the smart contract can self-execute through the blockchain and effect a transaction between counterparties.

Microsoft is not the only enterprise software giant to enter the BaaS game. IBM has contributed approximately 44,000 lines of code to the Hyper Ledger project administered by the Linux Foundation. Hyper Ledger is an open-source blockchain protocol that has partners such as ABN-AMRO, IBM, Intel, JP Morgan, Red Hat, VMware, and Wells Fargo. At bottom, blockchain technology continues to captivate the attention of the largest companies in the world, but it must be more than a solution searching for a problem.

## Why Blockchain Matters

As evidenced by its origins as the backbone for bitcoin transactions, the blockchain protocol is clearly positioned for broadest adoption by the global financial industry. According to a World Economic Forum survey released in September 2015,[4] it is estimated that approximately 10 percent of global GDP will be stored on blockchain networks. In a January 2016 survey conducted by State Street, 57 percent of institutional investors believed blockchain technology will be adopted within five years.[5] However, there are few industries whose constituents are more highly regulated than financial institutions. Therefore, before financial institutions expose themselves to regulatory, reputational, and financial risk by incorporating blockchain networks into their day-to-day business operations, the protocol must present a credible solution to a real problem.

In broadest strokes, blockchain is poised to disrupt the financial industry by disintermediating the clearing and settlement of financial transactions. In the United States, most securities transactions, for example, are required to settle in three business days, a requirement known as "T+3."[6] Historically, there has been a push to reduce the time required to settle securities transactions, their having once been subject to T+5.[7] Currently, regulators are driving to finalize a rule imposing T+2 settlement.[8] Blockchain's characteristics of digital efficiency, distributed consensus, and security allow for a shared truth to resolve all sorts of lengthy human intensive processes. Thus, by reducing human capital and hastening settlement, blockchain reduces transaction costs and liberates capital for more productive use.

In August 2016, Swiss bank UBS announced it was leading a team of the world's biggest banks in the development of a system to enable financial institutions to make payments and settle transactions quickly using the blockchain protocol. More specifically, UBS and its team of banks have developed a "Utility Settlement Coin" (USC), which the banks are defining as a digital cash equivalent of each of the major currencies backed by central banks. Because the USC is essentially a derivative of centrally managed currencies, such as the USD, Pound, and Euro, the USC is distinguishable from Bitcoin, a decentralized medium of exchange. USCs would be fully backed by cash assets at a central bank and convertible one-to-one with a bank deposit in the corresponding currency. Thus, transacting in USC would be equivalent to spending the currency with which the USC is paired. UBS and its partner banks believe the USC will revolutionize the speed with which transactions settle.

While blockchain appears capable of improving the current settlement process, it is similarly situated to mitigate the risks associated with multi-day settlement. Under many regulatory regimes, capital is escrowed until securities transactions are settled. This approach is designed to address counterparty risk, or the risk that another party to a transaction does not fulfill its obligations. This framework presents risks that can be largely mitigated by shortening the settlement cycle. As noted, capital is required to be held as collateral against unsettled securities transactions. During periods of market stress, securities prices fall and transaction volumes rise. As a result, investors are exposed to liquidity risks because their capital is tied up in escrow. In contrast, real-time, intra-day, or T+0 settlement would reduce counterparty risk and increase liquidity by freeing up capital sidelined as collateral during the traditional multi-day settlement period.

National securities exchanges and alternative trading systems are already exploring how to shorten the settlement cycle using blockchain networks. In mid-2015, Nasdaq launched a pilot program to use blockchain to trade pre-IPO shares of private companies in its new private marketplace. Similarly, the New York Stock Exchange, a unit of Intercontinental Exchange, Inc., made an investment in the bitcoin-trading platform, Coinbase, signaling its interest in exploring blockchain's propriety in effecting securities transactions. The online retailor, Overstock.com Inc., received regulatory approval in late 2015 for its S-3 shelf registration of $500 million worth of shares. More announcements are expected from Overstock in the last half of 2016 regarding its blockchain-based alternative trading platform, "t0."

Meanwhile, Digital Asset Holdings, LLC (DAH), is emerging as a clearing and settlement service provider purpose-built to utilize blockchain as its core infrastructure. In mid-2016, DAH and Depository Trust and Clearing Corporation (DTCC) partnered to develop a proof of concept blockchain network for certain asset repurchase transactions. Recently, some of Europe's largest financial institutions announced they had entered into a memorandum of understanding under which they would work together to develop a blockchain-based settlement procedure for over-the-counter transactions used by small businesses to raise capital. In short, many capital markets participants are betting that raising capital through blockchain networks can increase access to capital for private companies by eliminating the expense of informal and human capital intensive recordkeeping processes.

Additionally, blockchain has the potential to disrupt and disintermediate other practices in the financial industry besides clearing and settlement. Consider service providers to mutual funds. By incorporating the innovations of blockchain 2.0 and 3.0, funds could potentially automate anti-money-laundering and know-your-customer procedures, potentially passing along the associated cost savings of fund administration to investors. The cost of fund distribution could be reduced as well by distributing fund shares directly to investors using a blockchain network. Further, fully integrating a real-time, or nearly real-time, settlement infrastructure throughout the financial industry could allow funds to strike net asset values on demand and redeem investors more efficiently. Such an infrastructure would also be applicable in the context of securities lending. Finally, for exchange traded funds and their authorized participants, blockchain networks could introduce arbitrage efficiencies by increasing the speed of creating and redeeming in-kind units.

## Potential Uses of Blockchain by Asset Managers

The potential of blockchain technology has not been lost on asset managers and their service providers. In early 2016, a group of five of the largest asset managers in the United Kingdom formed a working group to look into several potential uses of blockchain, including how to trade illiquid securities directly among each other.[9] Fund transfer agents, administrators, custodians, and audit firms participate in a number of industry and private working groups to develop the technology for their customers and routinely issue white papers and other reports to the industry.

The most immediate application of blockchain appears to be on the portfolio transaction (that is, "buy") side. As noted above, DTCC is devoting substantial resources to potential blockchain uses, most notably for fund managers. In March 2016, DTCC announced a partnership with DAH to develop and test a distributed ledger-based solution to manage the clearing and settlement of US Treasury, Agency, and Agency Mortgage-Backed repurchase agreement (repo) transactions. According to the press release, repo agreements were selected for this proof of concept because there is an opportunity to streamline how these products are cleared, as repo transaction volumes continue to grow.[10] Blockchain technology was chosen for this application because of its real-time information sharing capabilities, enabling all parties to the repo trade to view details almost immediately after the trade is executed. This will enable buy- and sell-side firms to agree to repo trade details much more quickly, thereby lowering risks and costs. DTCC is also evaluating blockchain to replace or enhance its existing credit default swap (CDS) clearing and settlement infrastructure. Blockchain technologies can be used to increase transparency and liquidity and create more efficient markets in other asset classes such as loans and other types of illiquid securities.

Fund distribution is another area of exploration for blockchain. Fund managers could develop a distributed ledger among a trusted group of intermediaries allowing the flow of real-time fund share transactional data, which could be of tremendous utility to the fund's portfolio manager. This model could also be used to increase transparency for intermediaries' omnibus or nominee accounts. Blockchain technology could also be used among a group of intermediaries to cross-verify the status of investors or their customers as "accredited investors" through assignment of a digital identification for such investors or to create smart contracts to implement intermediary relationships in a more timely and efficient manner.

Admittedly, integrating blockchain technology into the financial system faces challenges. There is a need to establish standards and to have those standards accepted by the industry. Additionally, the scalability of a single blockchain network remains an open question. In light of recent thefts within the bitcoin ecosystem, data privacy and cybersecurity are intensely important issues to address. And finally, there is the outstanding question of regulatory approval and oversight.

## Blockchain Security

Every cyber incident "hack" in connection with bitcoin or any other blockchain related business casts doubt on the propriety of using blockchain in the financial industry. In early 2014, details came to light about how a Tokyo-based and former *Magic the Gathering*™ game card trading platform, was raided by hackers, resulting in the theft of approximately $460 million worth of bitcoin. It was further reported that an additional $27.4 million vanished from the platform's bank accounts. This was the largest bitcoin-related theft to date. In what is likely the second largest bitcoin heist, the Hong Kong-based Bitfinex was victimized around early August 2016 for 119,756 bitcoin, or about $72 million. Bitfinex, the world's biggest dollar-based bitcoin exchange and known for its deep liquidity, reported that the bitcoin was stolen directly from customer's segregated bitcoin wallets.

While most recent cyber incidents have focused on bitcoin exchanges, a similar cyber incident has struck closer to the core of blockchain technology. In mid-2016, the decentralized smart contract platform, Ethereum, was targeted in a cyber attack which resulted in over $50 million being looted. Ethereum ran "The DAO," a "decentralized autonomous organization."[11] The DAO, which resembled a venture capital style pooled investment vehicle, raised over $150 million in crowdfunding in the final weeks before the attack. The DAO appeared to have been a pool of Ethereum's own virtual currency, called "ether," whose $21 per ether value placed The DAO's worth at over $230 million. By exploiting a weakness in The DAO's code, a hacker was able to make off with about a third of The DAO's ether.

Clearly, cybersecurity will continue to be an issue for blockchain moving forward. In an environment where about one-third of bitcoin trading platforms have been hacked and most live ephemeral lives, with nearly half of all exchanges ceasing operations within the past six years, financial institutions will need to get comfortable with the security of the technology before entrusting billions of dollars to blockchain settlement. How the industry responds to answering the security question is therefore key to blockchain's adoption in the asset management industry. One approach to enhancing the reputation of blockchain as a secure environment and minimizing the cyber threats to the protocol's success is to establish recognized global security standards and protocols. On August 24, 2016, a group of blockchain enthusiasts and thought leaders met for two days and issued its report and 10-point call to action to address these issues.[12]

## US Regulatory Landscape

Given the intensive regulatory oversight of the financial industry, the blockchain revolution may stall without the blessings of regulators. On June 21, 2016, the US Financial Stability Oversight counsel (FSOC) released its 2016 annual report.[13] Notably, the 2016 report identified the use of blockchain as an emerging business practice requiring vigilant monitoring by financial regulators. This is the first time FinTech issues such as blockchain have been identified as a potential risk to US financial market stability.

In the 2016 report, FSOC noted that the use of blockchain protocols by financial institutions could positively impact the US financial system by introducing efficiencies and reducing costs. However, according to FSOC, "*[m]arket participants have limited experience working with distributed ledger systems, and it is possible that operational vulnerabilities associated with such systems may not become apparent until they are deployed at scale.*" Further, the FSOC cautioned that a "considerable degree of coordination among regulators" may be required given the distributed nature of blockchain networks. Noting that the US financial system is constantly evolving, Treasury Secretary Jacob Lew advocated for regulators to remain vigilant in order to maintain the safety, soundness, and resiliency of the US financial system. Yet, beyond vigilance, the FSOC did not recommend any specific action on blockchain by regulators, preserving the current hands-off approach.

Historically, the Securities and Exchange Commission (SEC) has had to deal with the tensions between emerging technologies (such as the internet) and federal securities laws, often by issuing guidance to the market.[14] Mutual funds registered under the Investment Company Act of 1940 (the 1940 Act) must carefully consider how to operate in a blockchain environment and meet the extensive regulatory obligations imposed by the 1940 Act. For example, the 1940 Act contains very specific requirements with respect to a fund's accounts, books, and records. More specifically, Section 31(a) of the 1940 Act[15] imposes a general obligation on mutual funds and certain of its service providers to retain a fund's records as required by the SEC, and Rules 31a-1 through 31a-3 thereunder provide details with respect to the types of accounts, books, and records that have to be maintained, who may maintain them, their preservation, as well as their accessibility and form. In 2001, the SEC amended Rule 31a-2 allowing mutual funds to maintain electronic records, subject to the requirements of the rule.[16] Rule 31a-3 permits such electronic records to be maintained by a third party (such as a transfer agent or custodian), as long as the person required to keep the books and records has obtained a written agreement from the entity maintaining such books and records.

However, as noted above, a blockchain distributed ledger is "shared" and belongs to those using the digital ledger as a whole, raising the issue of whether a distributed ledger is, for 1940 Act purposes, a fund record and, if so, whether a blockchain ledger can satisfy the legal requirements of Section 31 and the rules thereunder. For example, will a fund be required to obtain a written agreement from each of the other participants in the blockchain to meet the requirements of Rule 31a-3? At a minimum, a registered mutual fund will have to amend its policies and procedures with respect to its books and records requirements, cyber-security, and other related activities (such as portfolio trading) to reflect use of blockchain technology. Similar issues arise for investment advisers registered under the Investment Advisers Act of 1940.

The open nature of a shared, distributed ledger may also create issues for asset managers in the context of privacy and confidentiality. Participants in a blockchain are part of a trusted circle, so by its nature all participants will have access to all information on the distributed ledger, which could include details of portfolio transactions such as size and volume of trading and the terms of any trades executed through the ledger. Whether investment managers and their clients (and regulators) can get comfortable with this degree of openness remains to be seen.

## Conclusion

In the financial industry, the proposed utility of blockchain is, in part, to provide a verifiable means to keep track of ownership and transactions in a particular asset. Traditionally, a highly-regulated and therefore presumptively trusted central intermediary performs this function. The disruptive idea behind blockchain is that a trusted third-party interposed between transacting parties is no longer necessary to verify transactions if every party has a copy of the ledger and such ledger is tamper-proof. Accordingly, given the centralized model employed by most financial industry operations, blockchain has the potential to substantially disrupt current asset management service and transaction models.

**Mr. Gibson** is a partner in the Pittsburgh and Boston offices of K&L Gates, LLP, and **Mr. Kirk** is an associate in the firm's Washington, D.C. office. This publication is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied on in regard to any particular facts or circumstances without consulting a lawyer.

## NOTES

[1] Some of the legal considerations with respect to robo-advice have been discussed in a previous issue of *The Investment Lawyer*. *See* Jennifer L. Klass & Eric L. Perelman, "The Evolution of Advice: The Current Regulatory Landscape for Digital Investment Advisers," *The Investment Lawyer* (July 1, 2016).

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (Nov. 2008), *https://bitcoin.org/bitcoin.pdf.*

[3] Marley Gray, "Introducing Project 'Bletchley' " (Jun. 21, 2016), *https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md.*

[4] "Deep Shift: Technology Tipping Points and Societal Impact," *World Economic Forum* (Sept. 2015), *http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.*

[5] "Despite Positive Outlook, New Research from State Street Reveals Asset Owners, Managers Lack Readiness for Blockchain "State Street press release (May 31, 2016), *http://newsroom.statestreet.com/press-release/corporate/despite-positive-outlook-new-research-state-street-reveals-asset-owners-mana.*

[6] "About Settling Trades in Three Days: T+3," *Investor Publications* (May 21, 2004), *https://www.sec.gov/investor/pubs/tplus3.htm.*

[7] *Id.*

[8] *See* Hannah Glover, "SEC Commish Scolds Agency for Delay on Tighter Trade Settlement Times," *Ignites* (July 11, 2016); Luis A. Aguilar, "The Benefits of Shortening the Securities Settlement Cycle" (July 16, 2015).

[9] *Financial Times*, Feb. 7, 2016.

[10] "DTCC and Digital Asset to Develop Distributed Ledger Solution to Drive Improvements in Repo Clearing," (Mar. 29, 2016) *http://www.dtcc.com/news/2016/march/29/dtcc-and-digital-asset-to-develop-distributed-ledger-solution*

[11] David Siegel, "Understanding the DAO Attack" (June 26, 2016) *http://www.coindesk.com/understanding-dao-hack-journalists/*

[12] *See* Call To Action, The Muskoka Group, *http://www.muskokagroup.org/call-to-action/,* last visited Sept. 9, 2016.

[13] The purpose of the FSOC annual report is to summarize its current views on the US financial system according to its mission to: (1) identify risks; (2) promote market discipline; and (3) respond to emerging threats. *See* "FSOC 2016 Annual Report," *https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC%202016%20Annual%20Report.pdf.*

[14] *See, e.g.*, Use of Electronic Media*, Securities Act Release No. 7856, Exchange Act Release No. 42728, Investment Company Act Release No. 24426* (Apr. 28, 2000).

[15] 15 U.S.C. § 80a-30.

[16] *See Investment Company Act Release No. 24890* (Mar. 31, 2001).

Copyright © 2016 CCH Incorporated. All Rights Reserved
Reprinted from *The Investment Lawyer*, October 2016, Volume 23, Number 10, pages 7–14,
with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.wklawbusiness.com

Wolters Kluwer