The Investment Lawyer

Covering Legal and Regulatory Issues of Asset Management

VOL. 24, NO. 3 • MARCH 2017

As Fintech Platforms Grow Up, Investment Management Firms Face the 'Problems of Tomorrow'

By Jesse P. Kanach, Andrew P. Cross, and Mary C. Moynihan

Less than two decades ago, fund groups wrestled with whether it was worthwhile to create websites. We are now looking at several similarly disruptive developments, as advances in financial technology, often called Fintech, continue apace. Even as new efficiencies and opportunities blossom, regulators have pushed financial firms to recognize the dangers of technological failures.[1] As former Securities and Exchange Commission (SEC) Chair Mary Jo White admonished in the context of mutual fund boards, however, it is not enough to address existing risks: "Boards should also think more broadly about the emerging problems of tomorrow and what issues they may be missing."[2]

With that forward-looking emphasis, the SEC held its first Fintech Forum in November 2016,[3] and it is clear that there is more to come. In that same spirit, this article looks to the future of several Fintech related areas—specifically, blockchain and distributed ledger technology, investing in Fintech companies, so-called robo-advisers and algorithms, and cybersecurity—and addresses the salient regulatory issues related to them as well as how they are likely to affect and possibly disrupt the investment management industry.

Background on Blockchain and Distributed Ledger Technology

The technology harnessed by bitcoin has evolved from curiosity to a multi-faceted platform,[4] with the use of blockchain and distributed ledger technology (DLT) now making its way into core investment management functions. This technology will likely have a meaningful impact on fund companies and advisers in the future. Broader application of the technology has the potential to affect the way funds issue their shares, trade in assets and compensate sellers, and how advisers track client account information. Before turning to these various Fintech applications, however, it is helpful to begin with a brief description of the core, underlying technologies—bitcoin, the blockchain, and DLT.[5]

Introduction

We have all seen stories in the press about bitcoin. As time goes on, there are more references to the blockchain, and some niche news reports discuss DLT. What do these terms mean, and how do they tie together?

For a quick illustration, imagine a typical spreadsheet or database file. A spreadsheet might be housed on your personal computer. You may enter data into it and control it, and you alone have access to it. If your computer fails, the file is lost. To avoid that fate, you might upload the computer file into the "cloud," where it resides on a server managed by a particular company. In the cloud, the file is accessible online from anywhere and potentially with access restricted to only those with the appropriate password; as a best practice, the file is frequently backed up—copied to another location—so that if one copy fails another identical set of the data is available. A company that maintains a spreadsheet might allow authorized personnel to access the spreadsheet with a password, enter any necessary data updates, and perhaps report the updated data to others. This process is subject to the risk of errors in the data entry process, delays in entering the data, and temporary differences between the data on that spreadsheet and the data on spreadsheets maintained by others who have not yet received reports of the updated data, as well as cybersecurity risks, such as the potential hacking of the password or other unauthorized access to the file and unauthorized modification of the data.

Imagine instead:

- a single spreadsheet—*referred to below as a ledger,*
- maintaining a record of ownership of units of value—*that is, bitcoin or other virtual currency, sometimes called tokens or coins,*
- appearing identically on all computers that are running the relevant software, rather than being housed on a single server or website—*thus, distributed, as discussed below,*
- updated on all participating computers instantaneously, upon a transfer of value being made, without the need for manual data entry—*using blockchain processes discussed below,*
- with the owner of tokens or coins having access to transfer them, not by entering a password that the person has chosen and by which the hosting party allows access, but rather by entering a code that is generated by the ledger itself—*a "private key" (which as a practical matter cannot be guessed),*
- or with the owner instead enlisting a service provider to handle the private key, allowing the owner to instead use a traditional password and more convenient website or mobile app to access the user's account and instruct the service provider to effect transfers— *such account, often referred as a "wallet,"*
- with each transaction verified, or rejected, by a sufficient percentage of the ledger participants (that is, the various computers running the software), based on the computers' confirmation that the cryptographically secure "private key" mathematically fits with the address (the public key) from which the proposed transfer originated, after which verification the ledger automatically updates itself to reflect the transfer—*an overly brief summary of the cryptographic process that serves as the foundation for the soundness of the blockchain,*
- a process which prevents the same electronic token or coin from being transferred a second time because the private key has already been used and a new one has been generated for use by the recipient of the token or coin—*thus preventing the double-spending of an asset.*

With that set of images in mind, a slightly more detailed discussion of bitcoin, the blockchain, and the meaning of DLT follows.

Bitcoin. Bitcoin is commonly referred to as a virtual currency. By virtual, it means that it is not tangible: rather, it is electronic, not backed by any asset, and is established by software code.[6] It is not issued by government fiat or by any person willing to stand behind its value or accept it as payment. By currency, it means that it can transfer value and be used as a means to purchase, compensate, or reward, similar to fiat currency like US dollars. Bitcoin, however, differs from fiat currency in a number of ways.[7] Fiat currency has inherent value, in that, at the very least, it is normally accepted as payment (such as for taxes) by the government that issued it. Bitcoin's value is what the market dictates. While market valuation is arguably applicable to all assets, bitcoin differs from most in that it has no inherent value other than its utility in transferring the agreed-upon market value, which reflects the ability of the technology that underlies the currency to verify ownership, provide cryptographic protection, and instantaneously transfer the value that the parties to the transaction involving the transfer of bitcoin ascribe to it. Unlike ordinary electronic payments of money, which depend on a bank or other intermediary to prevent the same sum from being spent twice, bitcoin (like physical cash being transferred in-person) has no threat of being "double-spent," because its verified owner changes, instantaneously, as soon as the parties effect a purchase and sale transaction. An attempt to re-spend used bitcoin will be rejected by the online system. There is no way to have the equivalent of a bounced check, check kiting, or failure to deliver.

While the use of bitcoin creates a confirmable trail of payments and transfers, it also provides for a significant degree of anonymity. Its anonymous nature attracted a fair amount of criminal activity among early adopters,[8] but despite related controversies the technology's popularity proved resilient, even if extremely volatile at times.[9] Investigators have become more adept at tracking down users, and as the technology becomes more mainstream, participants including providers of the aforementioned "wallet" services are attracting more government requests for transparency.[10]

Bitcoin is decentralized, which means that the record of ownership is effectively dispersed among all computers (sometimes called nodes) running the relevant software. Unlike a record housed on a single server, no one decentralized record can be modified, tampered with, destroyed or lost. Since all participants have their software confirm whether a transaction is valid, bitcoin is sometimes said to be "trustless." This means that no one party, such as a bank, has to be trusted as arbiter of whether a person holds the amount of bitcoin the person claims to hold. Trust is established by bitcoin's processes themselves. The relevant software engages in, and applies computing power and energy to, the mathematical operation by which ownership and transactions are verified, or "mining." An in-depth discussion of the mining process is outside the scope of this article,[11] but fund managers and others involved in bitcoin, as well as other mined currencies or mining pools (computers massed together to bring greater computing power to the competitive mining of additional virtual currency), should be aware of some of the limitations on decentralized currencies generated through currency mining processes.[12]

Investors in bitcoin should keep in mind that the price of bitcoin (that is, its market value) has always been volatile relative to the price of other currencies or of securities and other instruments backed by enterprises, assets, or rights. Further, the technology is complex and requires material technical expertise to handle, transact in, or modify virtual currencies, or to responsibly delegate such conduct to service providers or other third parties. For example, a theft of bitcoin might not be detected until, perhaps much later, the victim seeks to spend it and finds the transaction rejected as an attempt to double-spend the bitcoin. These and other risks apply to both bitcoin and other virtual currencies.

The use of bitcoin and its broader acceptance in the market is still in its infancy, with the future very difficult to predict. Bitcoin itself is unlikely to significantly impact the investment management industry in the near future, with the exception of those few funds or managers who choose to either speculate in the virtual currency or purchase assets using it. However, the underlying technology, which allows for the instantaneous transfer of value and assets pegged to the blockchain, is likely to have significant impact on the way in which securities and other assets are transferred and settle. The following topics demonstrate the broad reach of the technology that underlies bitcoin.

The Blockchain. The bitcoin transaction network consists of computers around the world running the bitcoin open-source software containing the network protocol for administering bitcoin network transactions. Each computer on the network also maintains a copy of a universal ledger that contains the history of every bitcoin transaction ever made. The computers on the bitcoin network collectively verify every bitcoin transaction, and, as mentioned above, ensure that no bitcoin user can spend value that he or she does not have, or that has already been spent. Once a transaction is verified, it is included in a new "block" of transactions that is permanently added to the ledger collectively maintained by all the computers on the network (hence the term "blockchain"). The addition of the new transaction block to the blockchain serves to confirm that the included transactions took place and, by virtue of the time-stamp included along with the block, when they took place, creating an audit trail.

To date, cryptographic protocols underlying the blockchain, and software attributes that make unwinding trades essentially impossible, have prevented fraudulent transfers, absent the wrongdoer acquiring the correct private key to a wallet in which bitcoin is held. In this context, it is key to understand that bitcoin is not the only data that can be incorporated into the blockchain and any information accepted into the blockchain essentially creates a snapshot of the data, which is then auditable and tamperproof. Thus, in addition to bitcoin, numerous other virtual currencies—sometimes called tokens, coins, or other names—have been created that provide variations on the bitcoin theme.

- Some are decentralized, some are operated by numerous approved providers, and some are operated by a single provider.
- Some are open to all who are interested, and some are "permissioned," allowing only vetted users to participate.
- Some are generated by mining, and some are generated by other means, such as in exchange for certain online conduct or even from other tokens.

More important, however, the blockchain is increasingly used as a vehicle for other purposes including:

- Tokens representing access or rights to participate in some kind of activity;
- Coins that confirm ownership of digital or even tangible assets;
- Rewards for online conduct;
- A means to track inventory, including in supply chain logistics, or otherwise to record movements or changes;
- Instruments backed by assets such as commodities; and
- Securities formally registered with the SEC.

Distributed Ledger Technology. The blockchain is the basis for some forms of distributed ledger, but distributed ledgers can use various similar technologies. A "ledger" is simply a record of transactions and current ownership of assets. At one time it was a big leather-bound book; today, most ledgers are electronic. A "distributed" ledger is one housed on multiple nodes, or computer systems. As discussed above, the technology's cryptographic signatures required to engage in transactions, together with other processes, prevent duplicative ledger entries or double-spending and unwinding transfers is essentially impossible. In the bitcoin world, these ledgers are decentralized and trustless. However, as the relevance of the technology has been better understood by financial institutions, the distributed ledgers are being repurposed such that a single party may now establish a ledger for itself, or trusted parties may come together to participate in a ledger or to act as gatekeepers to allow only other trusted parties to participate. Transactions represented on the ledger can be of any kind. Since the ledger entries are necessarily electronic, the assets represented may be either digital (such as a virtual currency or a token representing a digital asset) or tangible, provided the tangible assets are held in a manner that allows for verification of their ownership and transferability consistent with the high quality of verification of digital assets on an electronic ledger. In the pre-distributed-ledger era, that reassurance has been provided by the participation of trusted parties that intermediate transactions, or augmenters of trust, such as central clearinghouses, banks, insurance policies, and regulations aimed at ensuring the safekeeping of assets and delivery when due. The breakthrough of DLT is that it presents the possibility that the need for such intermediaries could be eliminated.

A distributed ledger can enable straight-through processing on an instantaneous basis. Straight-through processing means that no additional work, such as manual intervention and intermediation, is required to complete the transaction. The "disintermediated transactions" made possible by the distributed ledger may reduce risk due to better verification and accuracy, elimination of delays, and better reporting of current holdings and rights. Instantaneous means that assets are exchanged without any delay. Today, most instances of straight-through processing may avoid the need for multiple, redundant (and thus potentially conflicting) entries in systems, but may not always occur instantly, such as being settled a day or two later (that is, T+1 or T+2).

If an asset, such as cash, is merely digitally represented by a distributed ledger entry but must be physically or electronically moved (such as through federal funds transfers), the potential of DLT is not fully realized. That is because additional steps in clearance and settlement could be required, delaying the complete effectuation of the transaction until such steps are complete.

If assets on both sides of a transaction can be digitally represented, however, the transaction might be achievable without the need for a trusted intermediary, a key function of which is often to stand behind its customer's wherewithal to complete the transaction. The verification of an investor's means and identity embedded in DLT can make that support obsolete. Similarly, with a distributed ledger, the need for escrow can be eliminated. The purpose of escrow tends to be to have a trusted party lock up an asset owned by one party to a transaction and release it once there is definitive assurance that the other side to the transaction has fulfilled the necessary conditions. If the conditions are built into the process underlying a transaction represented on a distributed ledger, there will theoretically be no risk that one side will fulfill its obligations while the other side fails to do so. This concept is sometimes called a "smart contract," which is an automated, self-executing arrangement that is effectuated upon the fulfilment of set conditions, without needing more (such as human intervention), and memorialized using DLT. In the era of the distributed ledger and smart contracts, the function of escrow and related conditional payments (such as those represented in swap transactions and other derivatives[13]) could become obsolete or at least modified.

While the use of DLT is promising, intermediaries will remain for the present, because of the regulatory purposes they serve. These include, for example, typical broker-dealer functions such as insulating retail investors from the perils of direct market access and assessing their customers' suitability for trades. Matching engines and similar mechanisms that allow buyers and sellers to "find each other" will continue to sit between market participants, but related clearinghouse-type roles could be made unnecessary if trades are instantly verified (or rejected), completed, confirmed, reported to a transfer agent or central depository, and updated on the ledger representing a market participant's holdings and available cash. Other intermediaries may continue to serve an integral function, such as market makers, who temporarily act as buyer or seller until a trader on the other side of the transaction can be found, but their additional roles could evolve away from facilitating and standing behind trades that have buyers and sellers on both sides. Intermediaries, insurance, or other backups also may be relevant in the context of a party that trades despite bankruptcy, in violation of a court order, as part of a fraudulent conveyance, or otherwise in a transaction that a court may find necessary to prevent or unwind. Financial intermediaries also play a role under the provisions of the Uniform Commercial Code (UCC) relating to (in brief) legal recognition of transfers of negotiable instruments to third parties without risk of being reversed; some parts of the UCC fit the new concepts and some could be ripe for modification, depending on the nature of the transaction.

Although historically US dollars are frequently represented electronically, transactions involving US dollars (other than in-person physical delivery of cash) are generally still not fully instantaneous. In brief, normally a bank may accept payment from a third party on the expectation that the third party's bank will deliver the amount due, but checks bounce or payments can otherwise be interrupted, which leaves risk within the financial system. A single bank may be able to instantaneously record transactions among solely its own clients, but multiple banks face the same trust-based challenges (such as fearing that the other bank could be insolvent, assets could be frozen, or clients' assets could be inaccurately verified). The lack of full inter-operability among multiple financial institutions should be expected to remain an issue for some time. That is, even if some venues and counterparties accept digital assets, others might not accept them or may accept them in different forms or utilizing different technologies.

The Blockchain and Distributed Ledgers: Considerations for Funds, Investment Advisers, and Their Service Providers

Forthcoming developments are poised to be immense. Funds may soon be considering whether to issue shares using virtual currency protocols. Fund managers and advisers are already wrestling with whether to invest in virtual currencies and tokens that are based on blockchain technology. Fund service providers, and even the national securities markets as a whole, are studying how the verification capabilities, speed, and efficiencies of DLT might revolutionize the issuance, trading, clearance and settlement, transfer agency roles and recordkeeping for both private and public issuers alike. These various Fintech applications are discussed in turn below.

The Issuance of Virtual Shares. Historically, companies issued share certificates to each shareholder. The process of sellers physically delivering paper certificates to buyers who would then have transfer agents cancel and reissue certificates became untenable as trading volume skyrocketed during the 1960s. Since the 1970s, it is common for an issuer to deliver a certificate to the Depository Trust Company (DTC), to be held by its nominee Cede & Co. (Cede stands for certificate depository), where the certificate is held in custody, sometimes referred to as being "demobilized." (Not all certificates are held at DTC, and may be held by certain qualified brokers or even by the investor, but for regulatory and logistical reasons it is difficult to sell such certificated shares without placing them into the DTC system.) Even uncertificated shares are often evidenced on DTC's books. As the securities represented by the certificate or the uncertificated shares represented on DTC's books trade among brokers on behalf of their clients, DTC's sister company, National Securities Clearing Corporation (NSCC), provides clearance and settlement services for equities, debt, depositary receipts, exchange traded funds (ETFs) or unit investment trusts (UITs). As the securities are traded, the books and records of the introducing broker (the retail broker whose customer is trading), its clearing firm (a clearing broker acting for various introducing brokers), and DTC are all updated to reflect the new ownership of the securities.[14] Such books and records must frequently be reconciled to account for errors, certain netting calculations, failed trades, and the like.

More recently, issuers have contemplated the issuance of securities represented digitally rather than by a share certificate.[15] Market participants other than issuers have progressed as well. For example, DTC and its parent, Depository Trust & Clearing Corporation (DTCC), have committed to achieve blockchain-based enhancements to their processes. For example, last year DTCC issued a white paper called "Embracing Disruption—Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape," and has taken related measures since then.[16]

A Comparison of Certain Key Considerations for Operating Companies and Funds that May Issue Virtual Shares. Unlike most operating companies, mutual fund shares are typically "dematerialized." That means no paper share certificates are issued, and shareholdings can remain documented on the books of the mutual fund or its transfer agent rather than at DTC. Many mutual funds are familiar with NSCC's Fund/SERV product, which offers back office processing services, but not necessarily in relation to share certificates held at DTC. Private funds, similarly, commonly issue interests the ownership of which is documented on the books of the fund, rather than pursuant to share certificates held by a broker or at DTC.

Operating companies have been considering the use of dematerialized shares. Because their shares trade in a secondary market, they face different issues from those faced by mutual funds and private funds. For one, acquiring shares of a company listed on an exchange ordinarily requires the use of a broker in order to gain market access, including in accordance with Rule 15a3-5 under the Securities Exchange Act of 1934 (Exchange Act). Unlike for funds, the purchase of listed company shares without a broker tends not to be an option. Brokers are subject to certain customer protection rules, including Rule 15c3-3's requirement that a broker must keep customer securities in a good control location. Good control locations are delineated by rule and no-action letter. For exchange-traded securities, DTC often serves as the good control location, consistent with Rule 15c3-3. Existing no-action guidance should be analyzed, or a new no-action position sought, depending on the findings and broker-dealers' demands for assurance that they have control of customer assets in a good control location if DLT is used.

Mutual fund shares, on the other hand, either are not always held with a broker at all, or, if broker-held, are found to be held at a good control location when ownership is recorded on the fund's books. First, mutual fund shares and private fund interests are sometimes sold to investors without the use of a broker at all, including based on the so-called issuer exemption in Rule 3a4-1 under the Exchange Act, or often involve a distributor that is a registered broker-dealer but no broker acting on behalf of the investor. Even so, the prevalence of brokerage platforms is such that ensuring a good control location exists may be necessary from a commercial standpoint. Second, in any event, the regulations provide that uncertificated mutual fund shares carried by a fund or its custodian bank in a special custody account may be considered a good control location so long as certain conditions are met. One condition in particular may become relevant in the event a fund wishes to issue uncertificated shares that are represented by technology based on blockchain protocols. The broker-dealer "must not be aware of any substantial problems of an operational nature which the fund may be experiencing and which may endanger the securities of the customer." Beyond reassuring itself as a matter of commercial prudence, a mutual fund that wishes to issue virtual shares should be prepared to provide appropriate assurance to selling broker-dealers of the absence of such "substantial problems" as a matter of regulatory demand.

That same condition of monitoring for substantial problems (among other conditions) applies under no-action guidance for certain operating company issuers, as well as private funds, that wish to treat issuer books and records as a good control location for purposes of broker-dealers' regulatory compliance obligations.

Based on the foregoing, a mutual fund or private fund that desires to issue virtual shares should consider the following steps, among others.

- Consult with counsel on the legality of such issuance under the laws of the state in which the fund was formed.
- Draft its charter and bylaws, or amend its existing charter and bylaws, to authorize such issuance (with board approval and subject to any required shareholder approval).
- Adopt board resolutions authorizing such issuance.
- Engage a transfer agent that is comfortable handling such securities.
- Work with the transfer agent or other relevant party on policies and procedures to support, for any selling broker-dealer, that the fund should experience no substantial problems of an operational nature that may endanger the securities of the customer.
- Draft a registration statement contemplating such issuance, which will be subject to SEC Staff review, and seek no-action comfort if deemed appropriate for purposes of having the issuer's or its transfer agent's books serve as a good control location for purposes of broker-dealers' regulatory compliance.
- Issue and commence operations of the virtual shares.[17]

Exchange-Traded Funds. ETF sponsors might consider how DLT could facilitate the process of issuing and redeeming creation units in a more automated fashion. In fact, although the technology still seems to be down-the-road, smart contracts should be able to facilitate the establishment of true actively-managed ETFs. This assumes that appropriate conditions could be implemented to provide for the necessary confirmation of value and opportunity to arbitrage so that the ETF share price tracks its net asset value, despite the necessary lack of transparency into the ETF's underlying holdings.

Service Providers—Tracking Compensation, Rights, and Other Information. Certain functions conceivably may be embedded in digital securities that could greatly increase efficiencies. For example, advances might allow Rule 12b-1 payments to be tied directly to the mutual fund's digital shares to which those fees apply, even for purposes of calculating any regulatory limits on such fees over time. New "T shares" or similar classes of mutual fund shares could be linked with the selling broker for administrative purposes. Shares sold within omnibus accounts could be tracked by a fund (such as for purposes of applying redemption fees to short-term holdings), or shareholder mailings could be electronically delivered to retail shareholders, via DLT, all without necessarily divulging investors' identities or other personal information to the fund. Fund assets might be more easily tracked for custody and audit purposes. Fund administrators, distributors of mutual fund shares, and custodians alike may find it worthwhile to study how DLT could benefit their business.

Service Providers—Clearance, Settlement, and Transfer Agency. Settlement of unregulated digital asset transactions are mainly a commercial concern, although regulated entities should have appropriate policies and procedures in place before transacting in them for clients or customers. If they are securities, however, a regulatory framework applies to clearance and settlement of the transactions, as well as to the transfer agency function. If securities transactions are effected instantly, with the ownership of the security moving to the buyer and ownership of the cash or other payment moving to the seller without delay and without possibility of a failure to deliver, much of the clearance and settlement process perhaps can be eliminated, at least in theory. All relevant parties would be on notice of the updating of the distributed ledger update, could trust that the new ownership is current, and would have no fear of seeing an asset double-spent. As such, what is currently a separate post-trade clearance and settlement function, as well as reporting (such as trade confirmations or transaction data) to any interested parties, exchanges, or regulators, can conceivably be integrated into the transaction itself, resulting in instantaneous (T+0) straight-through processing, as noted above.

An issuer's transfer agent whose systems are synched with the market participants' technology can conceivably serve as the official record of shareholders, efficiently and without the need for a central depository. However, a transfer agent must take care not to act as a clearing agency. In the securities context, Section 3(a)(25) of the Exchange Act provides that the term "transfer agent" means:

> any person who engages on behalf of an issuer of securities or on behalf of itself as an issuer of securities in (A) countersigning such securities upon issuance; (B) monitoring the issuance of such securities with a view to preventing unauthorized issuance, a function commonly performed by a person called a registrar; (C) registering the transfer of such securities; (D) exchanging or converting such securities; or (E) transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates.

Section 17A of the Exchange Act provides that (1) it is generally unlawful for a transfer agent to perform any transfer agent function in respect of any security that is or should be registered under Section 12 of the Exchange Act, unless the transfer agent registered with the SEC,[18] and (2) each registered transfer agent must comply with the SEC's rules that apply to it. The SEC has begun to consider whether registered transfer agents' application of DLT should be explicitly addressed in its transfer agent rules, raising the following questions in a late-2015 concept release on a possible overhaul of the rules applicable to registered transfer agents:[19]

> A new technology, the blockchain or distributed ledger system, is being tested in a variety of settings, to determine whether it has utility in the securities industry. What utility, if any, would a distributed public ledger system have for transfer agents, and how would it be used? What regulatory actions, if any, would facilitate that utility? How would transfer agents ensure their use of or interaction with such a system would comply and be consistent with federal securities laws and regulations, including the transfer agent rules? Please explain.

As for clearing agency functions, Section 17A(b)(1) of the Exchange Act provides that a transfer agent shall not perform the functions of both a clearing agency and a transfer agent unless such transfer agent is registered under Section 17A as both a transfer agent and a clearing agency. Therefore, a transfer agent should be careful not to effect securities transactions or otherwise perform any clearing agency functions to avoid having to dually register as a transfer agent and a clearing agency. Rather, it should seek to fulfill only a traditional transfer agent role including maintaining the shareholder registry. Due to an exclusion, however, that clearing agency activities in respect of mutual funds generally will not cause a transfer agent to become subject to regulation as a clearing agency.

Should such clearing agency status be avoided, significant and potentially redundant financial intermediary activity may be eliminated. Alternatively a central depository or clearing agency could similarly integrate DLT into its own processes, making it possible for companies to issue digital shares without losing the benefits, such as financial resources, systems, and expertise, that a clearing agency may provide in addition to the services to be provided by the companies' transfer agents.

Investing in Virtual Currencies and Digital Shares: Custody. Rule 206(4)-2 (the custody rule) under the Investment Advisers Act of 1940 (Advisers

Act) has detailed provisions applicable to any SEC-registered investment adviser deemed to have custody as defined under that rule. Among other things, a qualified custodian must hold funds and securities, and the assets must be verified or audited. It will not be clear in all cases whether virtual currencies or other digital assets will be properly considered "funds or securities," and as such the custody rule may not apply.[20] This discussion assumes that digital assets would be considered funds and securities, and, in either case, investment advisers should take care to safely maintain assets even if such assets are not. Investment advisers whose clients want virtual currencies and related instruments to be placed in their accounts may need to consider whether a bank, registered broker-dealer (who may be subject to the good control locations requirements described above), or other firm that meets the definition of qualified custodian is willing to take custody of the digital asset. The functioning of the private key in respect of a wallet for virtual currency and who holds that key—the custodian, if it is willing?; the investment adviser, unless the regulatory ramifications are prohibitive?—lends additional complexity. Similarly, an adviser must confirm whether its audit firm is willing to provide the necessary asset verification or, in the case of a private fund that has adopted the so-called "audit approach" to meet its obligations, an audit in accordance with generally accepted accounting principles, if an audit of the digital assets is determined to be required.

For mutual funds, custody provisions in Section 17(f) of the Investment Company Act of 1940 (Investment Company Act) and, among others, Rule 17f-2 thereunder apply, apparently more broadly than under the Advisers Act's custody rule, to "securities and similar investments" and cash assets. Custody options are narrower for mutual funds—specifically, banks normally serve as custodian consistent with the relevant rule provisions. The ease with which digital assets may be transferred (and who holds the private key), or the foreign nature of some digital assets, could mean that self-custody provisions of the Investment Company Act's custody rule may be most appropriate.

Forming a Fund to Invest Solely in Virtual Currency. Various ideas for funds that invest solely in virtual currency have run into regulatory complexities. Such complexities have involved the Securities Act registration process,[21] the sale and repurchase of the issuer's shares at the same time,[22] and the application of securities exchange listing standards.[23] Additional requirements may apply, such as under the Investment Company Act, if a fund were to invest in digital assets that were deemed to be securities, is discussed in the following section.

Are Virtual Tokens and Coins Securities? A key question is whether the packaging of an instrument that utilizes blockchain or distributed ledger technology should result in the instrument being deemed a "security." With respect to commodities laws, the Commodities Futures Trading Commission (CFTC) has stated that bitcoin by itself is a commodity.[24] The federal securities laws are commonly analyzed for this purpose, but state law and even the laws of foreign jurisdictions—given that the internet is borderless and virtual currencies are often made available globally—are relevant, are not preempted by any federal determinations, and can be unpredictable. It is worth becoming familiar with *Howey* (investment contracts) and *Reves* (notes) cases,[25] as well as a wealth of state and federal court cases that have delved into whether certain arrangements should be regulated as securities, often in niche areas specific to the kind of asset, if any, that might "back" a particular token or coin.

A holder of tokens that are securities faces a number of considerations under the federal securities laws. Must they be registered or are they exempt from the registration requirements under the Securities Act? If unregistered in violation of the Securities Act, the securities are subject to material risk of loss. Under the Exchange Act, is a seller required to be registered as a broker-dealer? Does the security have more than 2,000 record holders, thus making it likely subject to Exchange Act reporting requirements? If so, the issuer could become subject to expensive obligations and regulatory remedies. Are buyers and sellers of the security inadvertently underwriters, subject to potential liability and other risks? Is trading required to be done on a registered exchange or ATS? Under the Investment Company Act, does the holder invest too high a proportion of its assets in the securities, or otherwise become potentially subject to registration as an investment company? Under the Advisers Act, do the relevant parties provide investment advice in a manner that results in fiduciary, registration, or other regulatory requirements? The foregoing questions pertain to a fund or account that will invest in the digital asset, but arise in similar or even more significant ways for the promoters of the digital assets (such as those who created and marketed them) as well.

Note that a similar question arises as to whether the digital asset falls within substantive CFTC regulation, such as whether it is a commodity interest. The nature of the digital asset and its underlying assets (if any), the size of the offering, the nature of investors, and the use of leverage are several of the factors that should be considered to reach an appropriate conclusion. For a mutual fund, the introduction of any digital assets that constitute commodity interests could have regulatory implications under the Commodity Exchange Act, such as whether the fund's operator would remain eligible to claim exemptions otherwise available to it from substantive regulation by the CFTC (for example, exemptions under CFTC Regulation 4.5).

Negotiability of Tokens and Coins under the Uniform Commercial Code. Participants in transactions in tokens and coins may find it prudent to determine the tokens' or coins' status under the UCC, the ramifications of such status, and appropriate measures to properly effect transactions.

Investing in Fintech Companies

The preceding section of this article finished with a discussion about investing in virtual currencies or other assets represented using blockchain technology. The following section discusses certain issues that have recently arisen in connection with investments in Fintech companies generally, with emphasis given to issues faced by mutual funds.

Valuation. Valuation of private technology companies, particularly in connection with the significant variations in valuations applied by different market participants (including different mutual funds), has come under the SEC's scrutiny.[26] Valuation can be particularly challenging because many major Fintech companies remain private. Historically, initial public offerings (IPOs) have been the goal of many private companies that sought to grow and monetize their business success and ideas. More recently, however, receiving private funding or being acquired has delayed or replaced an IPO exit strategy for some startups. This has been a function of greater access to private funding, the levels of cash on the balance sheets of major technology companies who seek opportunities to acquire synergistic companies, private offerings that are less expensive to an issuer than IPOs, the perception of regulatory burdens for publicly traded companies, "short-termism" that has the potential to make companies feel forced to chase the next quarter's results rather than the long-term goal of the enterprise, and the threat of activist shareholders or short sellers whose contributions in added efficiency and price discovery are not welcomed by issuers who (right or wrong) have their own ideas about how to manage their companies. Many Fintech companies are attractive to fund managers because of the potentially significant investment returns for clients, even some funds are constrained in their ability to hold such illiquid shares which, based on their illiquidity, result in the lack of a readily quotable market price. As a result, a fund that acquires such shares of private companies must consider how best to determine the fair value of the security for purposes of determining the fund's net asset value, which is the basis on which the fund accounts for purchases and redemptions of the fund's shares and the calculations of the fund's investment advisory fee and any other asset-based fees. Given the conflict of interest that may arise when fair valuing assets, and the threat of dilution for either departing or remaining investors in a mutual fund, the SEC has recently initiated a review of various mutual funds' valuations of Fintech firms' shares,[27] which often (inevitably, given the absence of a set price and the lack of collusion) are different across market participants holding the same security. In connection with funds' valuation of such assets, mutual fund board directors in particular should keep in mind their responsibilities under the Investment Company Act.

Registration Risks. Increasingly, companies are making use of new crowdfunding platforms. As funds consider investing in companies that have raised capital in crowdfunding programs, it is worth keeping in mind that, from a risk management standpoint, the nature of the offering must be conducted in such a way as to permit the crowdfunded company's securities to remain unregistered. If not, funds may find the value of their investments materially harmed if an unregistered offering is found to have occurred, and if remedies that could include rescission rights to investors must be applied. Relatively new Rule 506(c) under the Securities Act has been used for recent crowdfunding efforts, but some issuers shy away from it given the uncertainties and risks involved in making a fully public offering with sales made solely to accredited investors. If some non-accredited investors manage to invest, the issuer cannot fall back on an argument that the offering itself was nevertheless private in fact, which is an argument that can be made by most offerings under Rule 506(b). An adviser that places its funds' or clients' assets in securities offered pursuant to Rule 506(c) should therefore take particular care when doing so.

Unlimited Liability. A centuries-old purpose of incorporating a company is to provide its shareholders with limited liability. Absent extraordinary circumstances, an investor in a corporation can see the value of its investment fall to zero but not below—that is, shareholders do not have personal liability for the debts of the company. General partnerships and unincorporated associations, on the other hand, do not necessarily offer such a benefit to their members. Mutual funds and private funds alike tend to avoid investing in such organizations, for both regulatory (such as, for mutual funds, Section 18 of the Investment Company Act, given potential liabilities) and commercial reasons. The advent of so-called "decentralized organizations" may raise similar issues. As background, decentralized organizations, which may hold themselves out as autonomous (meaning, running on pre-set rules embedded in software code and not subject to typical manipulation by a management team), might function as fundraising mechanisms for projects or other purposes by creating and disseminating digital tokens. Tokens might represent interests in the participating community, or access to the technological platforms they offer, or other concepts; they might offer a participation in some kind of output; they might be transferable; or they might have any number of attributes. Some have qualities that could cause them to be deemed securities, and others may not. When investing in tokens issued by such decentralized organizations, investors should seek to be comfortable that they understand the potential liabilities and other risks of holding and trading in such assets.

Robo-advisers and Algorithms

The maturing of the automated advice industry, colloquially called robo-advisers by some, has led the SEC to focus its regulatory efforts on the area. For example, the SEC's Office of Compliance Inspections and Examinations (OCIE) has added automated advice to its annual list of examination priorities for 2017 for the first time, with the following description of its examination focus:

> **Electronic Investment Advice.** Investors are increasingly able to obtain investment advice through automated or digital platforms. We will examine registered

> investment advisers and broker-dealers that offer such services, including "robo-advisers" that primarily interact with clients online and firms that utilize automation as a component of their services while also offering clients access to financial professionals. Examinations will likely focus on registrants' compliance programs, marketing, formulation of investment recommendations, data protection, and disclosures relating to conflicts of interest. We will also review firms' compliance practices for overseeing algorithms that generate recommendations.[28]

The last sentence of the previous paragraph, on reviewing matters relating to algorithms that generate automated investment advice, may generate varying responses among advisory firms. A related controversy arose in the past year after the CFTC proposed Regulation Automated Trading (AT) in respect of trading activity involving exchange-traded futures contracts.[29] That proposal would call for certain firms to maintain, and turn over to the CFTC or the Department of Justice upon request (without subpoena), the source code underlying their trading algorithms. The valuable, confidential, and easy to copy nature of such code left some industry participants concerned that it could be inadvertently accessed and used or become subject to front-running by third parties, whether through hacking of CFTC systems or due to Freedom of Information Act (FOIA) requests. The rule proposal has changed,[30] but not necessarily to such participants' satisfaction.[31]

On the topic of algorithms, the SEC has brought enforcement actions in connection with algorithms that did not work as intended or as advertised. In one case, an investment adviser that implemented quantitative models, including as subadviser to a mutual fund, was found to have included an error in its coding and personnel also failed to alert the firm's compliance staff. In that case, the SEC noted: "The coding process for the model represented a serious compliance risk … because accurate coding is required for the model to function properly and in the manner represented to clients."[32] Algorithms are not just relevant to the SEC in connection with portfolio management. Trade management algorithms that do not work as intended may also lead to enforcement proceedings. For example, the SEC found that two algorithms did not function as disclosed to retail investors by a major market maker, resulting in pricing that the SEC found inconsistent with such disclosures.[33]

Avoiding Investment Company Status. Robo-advisers must avoid status as an investment company. That could occur if the investment platform were deemed akin to a single entity that manages the assets of numerous investors. Rule 3a-4 under the Investment Company Act provides a safe harbor from investment company status on which such firms generally rely. To fulfill the conditions of the safe harbor, the adviser may be well-served to make sure that:

- Each client's account in the program is managed on the basis of the client's financial situation and investment objectives and in accordance with any reasonable restrictions (such as the designation of particular securities or types of securities that should not be purchased for the account) imposed by the client on the management of the account.
- Annual outreach is made to determine if there have been changes in the client's financial situation or investment objectives, and whether the client wishes to impose any reasonable restrictions on the management of the account or reasonably modify existing restrictions, with quarterly outreach offering contact information in case the client wishes to make such changes.
- Personnel who are knowledgeable about the account and its management are reasonably available to the client for consultation.
- Detailed quarterly statements are provided to the client.
- Each client can withdraw cash, receive timely confirmations of each securities transaction,

receive copies of documents legally required to be provided to securityholders, vote securities (or designate a proxy), and bring proceedings against issuers without having to involve the program sponsor or other program participants.

Cybersecurity: A Possible Roadmap for Protective Measures

It is no surprise that the SEC has cybersecurity in its crosshairs. A firm that fails to prevent an intrusion, despite its efforts, may have to face regulatory consequences in addition to its commercial and reputational concerns. An attack may arise not only from outside hackers, but potentially as a result of the conduct of undisciplined or rogue internal personnel. Hindsight is 20/20 and there is always more that could have been done to prevent or mitigate the effects of a cybersecurity breach. Given the constant threats and possible extreme harm to investors or the markets, the SEC has no incentive not to impose a standard that approximates strict liability.

Consistent with that approach, OCIE includes cybersecurity among its latest priorities, announcing: "In 2017, we will continue our initiative to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls."[34] In this context, the SEC's Investment Management Division has identified the cybersecurity of registered investment companies and registered investment advisers as a matter of concern and has provided specific guidance on cybersecurity.[35]

Much has been written generally on the topic of best practices for cybersecurity and the breadth of the topic is beyond the scope of this article. Fiduciary duties, several states' cybersecurity laws, and general commercial prudence come into play. As for SEC rules, while many fund lawyers are familiar with the privacy policy notices required under Regulation S-P, they tend to be less familiar with implementing safeguards under that regulation that are often viewed as being within the purview of IT personnel.

With regard to safeguarding assets, Regulation S-P requires that registered funds, advisers and broker-dealers adopt policies and procedures that protect customer records and information.[36] Although Regulation S-P focuses on consumer information, related SEC and Staff guidance may offer a useful roadmap for registrants to consider when implementing an information security program.

In a 2008 proposal relating to Regulation S-P,[37] and in more recent enforcement actions,[38] the SEC communicated its expectations that SEC-registered firms should:

Adopt written procedures. Adopt and revisit written policies and procedures with the goal that they be reasonably designed to protect records and information. Designate in writing an employee or employees to coordinate the information security program.

Conduct training. Train staff to implement the information security program.

Oversee third parties. Take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the information at issue, and require service providers by contract to implement and maintain appropriate safeguards. Document such oversight in writing.

Assess risks. Periodically review and assess likely and potential risks for breaches or unauthorized access. Identify in writing reasonably foreseeable security risks that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of information or information systems.

Prevent breaches. Actually prevent hacking through security measures and employee training. Implement a firewall to protect the server containing nonpublic information. Limit employees' access to confidential financial information, and authorize access only for those having a legitimate business need. Prevent, not just prohibit, unauthorized access from employees. Prevent employees from downloading confidential information to outside computers.

Encrypt data. Encrypt confidential information in case hacking successfully accesses it, or to prevent its being useful to unauthorized personnel.

Detect attacks. Detect hacking attempts or successful hacking. Detect unauthorized internal access.

Audit and test the program. Audit and test controls, systems and procedures for effectiveness. Test for evidence of hacking, to determine whether only authorized personnel have access, and for how the company responds to a breach. Monitor and analyze employees' access to, and use of, confidential information.

Evaluate and adjust the procedures. Update information security programs to reflect the results of the testing and monitoring, relevant technology changes, material changes to operations or business arrangements, and other circumstances that may have a material impact on the program.

Respond to breaches. Maintain a response plan for cybersecurity incidents. The SEC could find a deficiency if a plan is not in place, despite a firm's actual prompt and adequate response in the event of a breach. In the event of known or suspected breach, monitor for the dissemination of confidential information.

Maintain insurance. Consider maintaining insurance that applies to cybersecurity events. Once novel, cybersecurity insurance is a key part of many firms' risk management programs—even outside of the financial services context.[39] The potential for economic loss through theft or reputational harm is immense. Such insurance can be expensive, complicated and even relatively restricted. It is of utmost importance to understand what events are covered by an insurance policy. In addition, fund boards should consider whether the limits of a particular insurance policy, combined with limitations on the liability of service providers, may have a "liability hole" or coverage gaps that may need to be filled by fund assets or, possibly, the adviser's assets.[40] Even successes in finding appropriate coverage cannot fully insulate an enterprise from reputational and other non-quantifiable harm arising from a material security breach.

Unfortunately, despite vigorously implementing all of the foregoing, risk cannot be eliminated. Regardless of steps taken, if the 2016 election season in the United States has taught us anything, it is that any computer system is at risk of being hacked.[41]

Conclusion

Fund boards, investment managers and separate account advisers should seek a deep understanding of the issues surrounding Fintech developments as they and their service providers continue their journey into this new world. "Disruption" is useful when it leads to efficiencies and novel advances, but is often accompanied by risks, known and unknown. Are systems up to speed and capable of handling the new requirements? Are inter-operability issues resolved, so that systems communicate and transact with each other in order to maintain conforming records? Are investment professionals working hand-in-hand with IT experts when necessary? How will the firm's existing risk management oversight processes dovetail with its future use of Fintech applications? Above all, is there proper human oversight with respect to the automated processes?

Whether a fund or adviser is investing in virtual currency, maintaining records on a distributed ledger, generating automated investment advice, or acquiring interests in companies that do so, an organized framework to identify, address, and monitor issues could go a long way. As boards evolve in their thinking, and as regulators allow or restrict activities, the financial services industry should expect the near future to be a dynamic period of innovation and change.

Some of these are issues to address now and others are "problems of tomorrow." Given the risks, and recognizing the rewards of taking initiative with respect to these technological opportunities, boards and advisers should value and maintain open and continuing communication among all parties and apply diligent efforts to the prompt and comprehensive resolution of issues.

Messrs. Kanach and **Cross** and **Ms. Moynihan** are partners in the Washington, DC office of Perkins Coie LLP. They would like to acknowledge the support of colleagues from Perkins Coie's broader Investment Management Group and the firm's multi-disciplinary Blockchain Technology and Digital Currency Group in considering the issues discussed in this article, although the views expressed are those of the authors.

NOTES

[1] *See, e.g.,* David Grim, director, Division of Investment Management, SEC, "Remarks to the Investment Company Institute's 2016 Mutual Funds and Investment Management Conference" (Mar. 14, 2016) (Dir. Grim Remarks), available at *https://www.sec.gov/news/speech/david-grim-remarks-to-ici-2016-mutual-funds-and-invest-mgmt-conf.html* ("Few would dispute that the investment management industry has witnessed transformational changes in the past decade, not only in terms of the products it offers, but also in terms of the investment strategies it pursues, and even the technology on which it relies. … Funds are relying increasingly on technologies and services provided by third parties to conduct their daily operations. But this convenience comes at a cost."); *Adviser Business Continuity and Transition Plans*, Investment Advisers Act Release No. 4439 (Jun. 28, 2016) (proposed rulemaking) (seeking for firms to address risks such as "technological failures with respect to systems and processes"), available at *https://www.sec.gov/rules/proposed/2016/ia-4439.pdf*. All web site citations are as accessed in February 2017.

[2] Mary Jo White, Chair, SEC, "The Fund Director in 2016: Keynote Address at the Mutual Fund Directors Forum 2016 Policy Conference" (Mar. 29, 2016), available at *https://www.sec.gov/news/speech/chair-white-mutual-fund-directors-forum-3-29-16.html*.

[3] See *https://www.sec.gov/spotlight/fintech* for information about the public SEC Fintech Forum held in the SEC's Open Meeting Room on November 14, 2016. SEC Commissioner Michael S. Piwowar, who was named Acting Chairman of the SEC in January 2017, has expressed an interest in the topic and was a proponent of the SEC Fintech Forum. *See, e.g.,* Michael S. Piwowar, "Remarks Before the Quadrilateral Meeting of the FMLC/FMLG/FLB/EFMLG" (July 20, 2016) ("I am currently pushing for the [SEC] to hold a FinTech roundtable this fall and I personally learned a lot from today's discussion of blockchain technology and virtual currencies."), available at *https://www.sec.gov/news/speech/speech-piwowar-2016-07-20.html*.

[4] The technology is not limited to financial service, of course. Across all sectors, there is a rush to be the first to implement countless different uses of the technology. *See, e.g.,* "Who owns the blockchain? A rush to patent the blockchain is a sign of the technology's promise," *The Economist* (Jan. 14, 2017), available at *http://www.economist.com/node/21714395/print*.

[5] For a bitcoin and blockchain primer, *see* Perkins Coie LLP and The Bitcoin Foundation, "Bitcoin: A Primer," available at *https://www.perkinscoie.com/images/content/1/4/v2/14394/Bitcoin-Primer.pdf*.

[6] Bitcoin was first publicly described in Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (posted online Oct. 2008), available at *https://bitcoin.org/bitcoin.pdf*. "Satoshi Nakamoto" is widely believed to be a pseudonym, and may represent the output of multiple persons.

[7] For a comparison of bitcoin to fiat currency, *see, e.g.*, Stephanie Lo and J. Christina Wang, "Bitcoin as Money?" (posted on the website of the Federal Reserve Bank of Boston (Sept. 4, 2014), available at *https://www.bostonfed.org/publications/current-policy-perspectives/2014/bitcoin-as-money.aspx*.

[8] *See, e.g.*, Laura Shin, "Federal Prosecutor Kathryn Haun On How Criminals Use Bitcoin —And How She Catches Them" (Nov. 1, 2016) (noting that "Bitcoin and blockchain technology aren't all about crime anymore than cash is"), available at *http://www.forbes.com/sites/laurashin/2016/11/01/federal-prosecutor-kathryn-haun-on-how-criminals-use-bitcoin-and-how-she-catches-them/#293329307886*.

[9] *See, e.g.*, Pete Rizzo, "Bitcoin Price Tops $1,000 in First Day of 2017 Trading," CoinDesk (Jan. 1, 2017), available at *http://www.coindesk.com/bitcoin-price-1000-january-1-2017/*. Bitcoin has had significant volatility, including surging from around $200 to over $1,000 per bitcoin during November 2013 alone, and even dropped over 30% promptly after the first of this year. *See, e.g.*, *http://www.coindesk.com/price/* (chart showing the price of a bitcoin over time, as measured by several platforms).

[10] *See, e.g.*, Robert W. Wood, "IRS Escalates Hunt For Bitcoin Users In Coinbase Summons Case," Forbes (Jan. 3, 2017), available at *http://www.forbes.com/sites/robertwood/2017/01/03/irs-escalates-hunt-for-bitcoin-users-in-coinbase-summons-case/#6be97b7c52e8*.

[11] For descriptions of bitcoin mining, *see, e.g.,* "How Bitcoin Mining Works," CoinDesk (Dec. 22, 2014), available at *http://www.coindesk.com/information/how-bitcoin-mining-works/*; "The Magic of Mining," The Economist (Jan. 10, 2015), available at *http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic.*

[12] One such limitation is the ability of an "attack" by a sufficient percentage of the existing mining capability in order to overwhelm other verifying computers and verify a different result; in short, to tamper with records or otherwise disrupt the generally preferred functioning of the decentralized virtual currency (basically, but not technically, a hack, because the processes function as designed even if not as generally preferred). A limited number of bitcoin transactions can occur during any given time period, which has led others to develop additional virtual currencies or similar instruments intended to transact with greater volume.

[13] *See, e.g.,* Antony Peyton, "DTCC selects IBM, Axoni and R3 to develop blockchain for derivatives," *Banking Technology* (Jan. 9, 2017), available at *http://www.bankingtech.com/693511/dtcc-selects-ibm-axoni-and-r3-to-develop-blockchain-for-derivatives/*.

[14] Not all DTC trades use this multi-level process. For example, certain large transactions (block trades) may be settled directly with DTC.

[15] For an example of an issuer whose registration under the Securities Act of 1933 (Securities Act) of digital securities was granted effectiveness by the SEC, *see* "SEC filings of Overstock.com, Inc.," available at *https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=0001130713&owner=exclude&count=40&hidefilings=0.*

[16] The DTCC white paper and various DTCC blockchain-related press releases, statements, and other resources are available at *http://www.dtcc.com/news/2016/january/25/blockchain*.

[17] Such steps may not be adequate for listed operating companies, because exchange-traded shares are also subject to added wrinkles not applicable to mutual fund shares or private fund interests. First, national exchanges have not yet adopted the processes or technologies necessary to transact in virtual shares. Just as investor-held share certificates must overcome barriers before being exchange-traded, virtual shares are currently constrained by technology from trading in the same manner as ordinary shares. For one thing, the national market system (NMS) generally requires that orders to buy or sell exchange-listed securities must be directed by broker-dealers to the

trading venue that offers the national best bid or offer. Virtual shares, however, cannot be directed to a venue that does not handle virtual shares, and so may have to be kept from the definition of NMS security such as by avoiding the triggering of Exchange Act registration. Such a security might trade on one or more alternative trading systems (ATSs) that adopt the virtual share technology, but would not be in the mainstream of security trading until the NMS can accept it. Issuers also face the complication that, if they have already issued non-virtual shares, they may have both ordinary and virtual shares outstanding at the same time. If such shares are part of the same class, the NMS rules may restrict them from trading differently in different venues (such as on an ordinary venue and on a digital shares venue), due to a failure to satisfy the national best bid and offer requirement.

[18] The transfer agent of a private company may not be required to be registered with the SEC.

[19] *Transfer Agent Regulations*, Exchange Act Release No. 76743 (Dec. 22, 2015) (concept release), available at *https://www.sec.gov/rules/concept/2015/34-76743.pdf*.

[20] Question II.3, *Staff Responses to Questions About the Custody Rule* (online FAQ), available at *https://www.sec.gov/divisions/investment/custody_faq_030510.htm* ("Q: If an adviser manages client assets that are not funds or securities, does the amended custody rule require the adviser to maintain these assets with a qualified custodian? A: No. Rule 206(4)-2 applies only to clients' funds and securities.").

[21] For an example of an issuer seeking Securities Act registration of a pool that will invest substantially all of its assets in bitcoin, *see* "SEC filings of Winklevoss Bitcoin Trust," available at *https://www.sec.gov/cgi-bin/browse-edgar?company=Winklevoss+Bitcoin+&owner=exclude&action=getcompany*.

[22] *See* "SecondMarket, Inc. and Bitcoin Investment Trust (BIT) Settle Charges Relating to Unlawful Redemptions of BIT Shares during a Continuous Distribution" (press release) (July 11, 2016), available at *https://www.sec.gov/litigation/admin/2016/34-78282-s.pdf* (implicating Regulation M under the Exchange Act).

[23] A national securities exchange has filed with the SEC for a rule change to allow the exchange to list shares of a trust that will invest substantially all of its assets in bitcoin. Bats BZX Exchange, Inc., filing pursuant to Rule 19b-4 under the Exchange Act (June 20, 2016), available at *http://cdn.batstrading.com/resources/regulation/rule_filings/pending/2016/SR-BatsBZX-2016-30.pdf.*

[24] *See, e.g., In the Matter of Coinflip, Inc.*, CFTC Docket 15-29 (order instituting proceedings and making findings) (Sept. 17, 2015), available at *http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf* ("Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities" under the Commodity Exchange Act).

[25] SEC v. W.J. Howey Co., 328 U.S. 293 (1946); Reves v. Ernst & Young, 494 U.S. 56 (1990). Many other federal and state cases are potentially relevant to analysis of whether a token or coin is likely to be considered a security.

[26] Mary Jo White, Chair, SEC, "Keynote Address at the SEC-Rock Center on Corporate Governance Silicon Valley Initiative*"* (Mar. 31, 2016), available at *https://www.sec.gov/news/speech/chair-white-silicon-valley-initiative-3-31-16.html*.

[27] *See, e.g.,* Sarah Krouse and Kirsten Grind, Dow Jones Newswires, "SEC Asks Money Managers To Reveal Silicon Valley Valuations" (Dec. 9, 2016), available at *http://www.morningstar.com/news/dow-jones/fund-news/TDJNDN_201612098943/sec-asks-money-managers-to-reveal-silicon-valley-valuations.print.html*.

[28] OCIE, SEC, "Examination Priorities for 2017*"* (Jan. 2017) (2017 Exam Priorities), available at *https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf*.

[29] "CFTC Unanimously Approves Proposed Rule on Automated Trading" (press release) (Nov. 24, 2015), available at *http://www.cftc.gov/PressRoom/PressReleases/pr7283-15*.

[30] "CFTC Approves Supplemental Proposal to Automated Trading Regulation," (press release) (Nov. 4,

2016), available at *http://www.cftc.gov/PressRoom/PressReleases/pr7479-16*.

[31] *See., e.g.,* Gregory Meyer and Joe Rennison, *Financial Times*, "CFTC set to tweak rules for automated trading; Regulator responds to futures industry backlash over 'source code' access" (Nov. 4, 2016), available at *https://www.ft.com/content/3cec9a30-a1dc-11e6-aa83-bcb58d1d2193*.

[32] *See, e.g.*, SEC, "SEC Charges AXA Rosenberg Entities for Concealing Error in Quantitative Investment Model" (press release) (Feb. 3, 2011), available at *https://www.sec.gov/news/press/2011/2011-37.htm*.

[33] *See, e.g.*, SEC, "Citadel Securities Paying $22 Million for Misleading Clients About Pricing Trades" (press release) (Jan. 13, 2017), available at *https://www.sec.gov/news/pressrelease/2017-11.html*.

[34] 2017 Exam Priorities.

[35] Division of Investment Management, SEC, "IM Guidance Update: Cybersecurity Guidance" (Apr. 2015), available at *https://www.sec.gov/investment/im-guidance-2015-02.pdf*.

[36] Rule 30 of Regulation S-P, 17 CFR 248.30.

[37] *Part 248—Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information*, Investment Company Act Release No. 28178 (Mar. 4, 2008) (proposed rulemaking), available at *https://www.sec.gov/rules/proposed/2008/34-57427.pdf*.

[38] *See, e.g.*, SEC, "SEC: Morgan Stanley Failed to Safeguard Customer Data" (press release) (June 8, 2016) (internal breach followed by outside hacking), available at *https://www.sec.gov/news/pressrelease/2016-112.html*; SEC, "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach" (press release) (Sept. 22, 2015) (outside hacking), available at *https://www.sec.gov/news/pressrelease/2015-202.html*; SEC, "SEC Charges Brokerage Executives With Failing to Protect Confidential Customer Information" (press release) (Apr. 7, 2011) (movement of thumbdrives from one employer to another, theft of laptops, online access by former employee), available at *https://www.sec.gov/news/press/2011/2011-86.htm*.

[39] For example, at *https://www.dhs.gov/cybersecurity-insurance*, the US Department of Homeland Security has a web page titled "Cybersecurity Insurance" that discusses the purpose of cybersecurity insurance, the need for robust risk management regardless of insurance coverage, and the fact that even insurance cannot address the risks to critical infrastructure.

[40] This concern for mutual fund boards is discussed in depth in Gwendolyn A. Williamson and Mary C. Moynihan, "The Liability Hole — Cybersecurity Risks and the Apportionment of Liability," The Investment Lawyer (Dec. 2014), available at *https://www.perkinscoie.com/images/content/1/1/v2/114956/Investment-Lawyer-December-2014.pdf*.

[41] The SEC itself has implemented a broad cybersecurity program, including maintaining the confidentiality of registrants non-public filings, data, and correspondence. *See, e.g.,* Dir. Grim Remarks (describing Chair White's acknowledgment of the critical importance of the SEC's own cybersecurity on a number of occasions, steps taken to ensure that the SEC's cybersecurity protocols are "as robust as possible," enhancing internal awareness of vulnerabilities and threats, implementing certain protocols and frameworks for cybersecurity risk mitigation, and bolstering the SEC's ability to respond rapidly and effectively to any unauthorized intrusions).

Wolters Kluwer