LEGAL EXECUTIVE INSTITUTE

DIGITIZED SECURITIES AND THE PROMISE OF AUTOMATED COMPLIANCE

By David J. Kappos, D. Scott Bennett, Michael E. Mariani, Jeffrey M. Amico, Vincent Molinari, Christopher Pallotta, Annemarie Tierney, and Peter Chiaro

the answer company™
THOMSON REUTERS®

Executive Summary

A digitized security is a digital representation of a security that can be programmed to automate certain functions and whose ownership is traced in real time using a distributed ledger.[1] The first generation of digitized securities being issued today are effectively traditional securities enveloped in a digital wrapper. That should not suggest that their potential impact is limited, however. As in the shift from "snail mail" to email, the content of the underlying information does not change. However, like email, digitization offers significant advantages over the legacy paper-based system.

Among the most promising of these advantages is the potential to use smart contracts to automate compliance with certain aspects of securities law. Using a digitized security, an issuer could write certain transfer restrictions directly into the code of the smart contract, effectively enshrining certain key securities law requirements like holding periods or shareholder caps directly into the security itself. Done properly, this could provide both issuers and regulators with assurance that applicable laws were being complied with, while also eliminating certain transactional frictions that make it difficult for investors to trade on secondary markets.

In the near term, this technology likely offers the greatest value to secondary markets for securities of private companies, as many of the applicable registration exemptions that are administratively burdensome to comply with could be rendered in code and enforced automatically.[2] The value of a digitized security in this context over the status quo is that these compliance checks would be enforced *automatically* upon any transfer, and without requiring any post-trade intervention or reconciliation to ensure compliance and track ownership. This is possible because distributed ledgers allow the various entities necessary to effect a securities transaction (e.g., brokers, exchanges, custodians) to all share a common, programmable data layer. This marks a step-function change over the status quo in the markets for private securities, where there is currently a significant lack of infrastructure to facilitate legally compliant secondary trading at scale. Over the longer term, distributed ledgers may also gain adoption in public capital markets as well, streamlining not only settlement processes but other heavily intermediated functions like distributing cash flows and managing shareholder voting as well. Ultimately, digitized securities may not be the panacea for private market liquidity issues that some advocates claim. However, they can offer real benefits to private market issuers and investors, as the status quo simply remains too inefficient and cumbersome as we move into the digital age of financial markets.

This paper proceeds as follows. First, it provides an overview of distributed ledger systems at a high level, including their potential benefits as compared to existing technologies. Second, it summarizes the basic framework that governs securities offerings in the United States, as well as the administrative burdens that smaller private companies must bear in order to comply with this regime. Third, it examines specifically how and where smart contracts could be used to automate compliance with certain of these securities law requirements, thereby reducing a major barrier to secondary liquidity in private markets. Finally, it concludes by analyzing certain obstacles that must be overcome in order for this technology to gain widespread adoption and considers which existing solutions are most likely to generate widespread adoption.

1 The lexicon of distributed ledger technology is in flux as the technology itself, and the terminology in the space, continues to evolve. We refer to "digitized securities" for consistency; "smart securities" and "security tokens" are alternative phrases used to describe the same, or similar, applications of this technology.

2 This technology is especially apt for asset classes that have traditionally experienced low liquidity levels, such as private real estate investment trusts or limited partnership interests.

An Overview of Distributed Ledger Systems

Key Concepts

A **digitized security** is a digital representation of a security that exists on a distributed ledger. A **distributed ledger** is a system that enables independent participants to reach consensus on the validity of a set of shared data in the absence of a central coordinator.[3] The product of this consensus is a shared, append-only "ledger" (resembling a computer log file) that is constantly updated to reflect the addition of new data. Distributed ledgers can either be public or private, depending on which participants are permitted to execute and validate transactions.

A **blockchain** is a particular type of distributed ledger in which data (e.g., transactions) is grouped into blocks and then chained together in chronological order using a cryptographic mechanism known as a hash function. The process of chaining one block to the next creates a virtually irreversible record of all transactions that can be referenced in the future to prevent users from double-spending their digital assets.

While the original and most common vision of blockchain is of a fully public, decentralized, permissionless network, there are a wide variety of blockchain solutions, many of which are, in fact, either fully or partly private and/or require permission to join.[4] In contrast with public, permissionless networks, **private, permissioned blockchains** employ various processes to approve new participants, including to ensure all new participants subscribe to a set of rules that govern their use of the network. One significant difference between public and private blockchains is the existence of a central intermediary. In a public blockchain – i.e., a true distributed ledger – there is no central authority and the decision on whether a new block should be added to the chain is vested with the consensus of the blockchain community, whereas in a private blockchain, central intermediaries may be necessary. Therefore, in a true private blockchain with only one central participant, the technology becomes more similar to a traditional private database. There are also hybrid solutions where the right to read the chain might be public but the transaction/data authorization process is controlled by a pre-selected set of nodes; for example, a consortium of 15 exchange institutions, each of which operates a node, where 10 of them must sign every block in order for the block to be valid.

Because anyone can join and add a new block to a public, permissionless blockchain, it is impossible to ensure participants agree to a set of rules, except to the extent the rules are built into the code of the blockchain. However, in a private, permissioned blockchain or a hybrid solution, it is possible to limit the parties who can transact on the blockchain according to certain rules implemented within the protocol. Another distinction between public and private blockchains is that a public blockchain is immutable, whereas private blockchains may have more flexibility or risk, depending on the perspective, for changes in the blockchain.

Certain distributed ledgers also allow users to embed computer scripts into the ledger that will be executed automatically by the nodes running the ledger if the conditions specified in the script are satisfied. These scripts are known as **smart contracts**.

Smart contracts can be designed to create **digitized securities** (which are digital representations of value) and enable their transfer between users. As noted, smart contracts are effectively computer programs that will be run by the network if and when the embedded conditional logic is satisfied. After the contract has been deployed by the creator, other users may interact with it to achieve a desired outcome. For example, a basic "multi-signature" smart contract would allow a transfer from one individual to another only if a requisite number of participants sign and approve the transaction. Other basic examples could include smart contracts that only allow transfers up to a spending cap, or only within certain time periods, or only to pre-approved persons, such as accredited or institutional investor accounts.

3 Michel Rauchs, et al., *Distributed Ledger Technology Systems: A Conceptual Framework* (2018), https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-08-20-conceptualising-dlt-systems.pdf.

4 The public-private distinction refers to who can access the blockchain in any capacity, as public blockchains are open to all, while private blockchains are open only to pre-approved members. The permissioned/permissionless distinction refers to who can add data (commonly in the form of submitting transactions and executing smart contracts) to the blockchain, as permissioned blockchains restrict this right to approved members, while permissionless blockchains allow all members to add data.

The Capital Markets Use Case

At its core, a public blockchain is a record-keeping system with no central administrator. In a private, permissioned blockchain, however, the degree of decentralization is based on how the members running the private blockchain choose to structure their business relationships; there can be a central administrator, or a consortium of members who administer the blockchain. Though blockchains can be used to store other forms of data (e.g., identity-based information), their primary use case to date has been to track ownership of assets and facilitate their transfer between users. Public blockchains of this variety (e.g., Bitcoin) can be thought of as peer-to-peer asset registries. Public blockchains with more advanced scripting languages (e.g., Ethereum) as well as certain private blockchain solutions (e.g., Symbiont) take on a more active role, serving as both the asset registry *and* the computer that actually executes the transactions.

As noted, the unique innovation of public blockchains over existing database technologies is that a blockchain is designed to serve these functions without a central administrator. If we think of blockchains as open-source record-keeping systems that can be programmed like computers, it becomes possible to envision an entire ecosystem of applications being built on and sharing a common data layer. For example, imagine that the various entities necessary to effect a securities transaction today (e.g., exchanges, brokers, custodians) could all share a single set of records, instead of maintaining (and reconciling) their own respective ledgers on a daily basis. Imagine further that this shared settlement layer could be programmed by an issuer to automate certain functions like regulatory compliance or cash flow distributions, and that these functions would execute automatically as programmed. The same example can also be implemented on a private, permissioned or hybrid blockchain protocol, where the governance rules implemented by exchanges or custodians serving as nodes can ensure more structured and efficient transfer of information and recording of transactions.

This notion of a shared data layer is significant in the capital markets context because it produces an agreed-upon record of who owns a particular security at any moment, updated in real time, *regardless* of the particular venue or medium through which a transaction occurred. In other words, in theory, it becomes irrelevant if the buyer and seller connect via a regulated (e.g., a traditional public exchange or an alternative trading system) or unregulated (e.g., a message board or even in person) trading venue. As long as the seller sends the token from her blockchain address to the buyer's blockchain address, that transfer will ping the digitized security's smart contract (ensuring the trade complies with any transfer restrictions) and will be logged into the ledger, updating the ownership records instantly. This technology could potentially eliminate the need for certain existing intermediaries (e.g., transfer agents, custodians) whose job it is to store securities on others' behalf and enable their transfer between holders. Indeed, blockchains could enable a more direct, straight-through relationship between the issuer and its security holders throughout the life cycle of the security. However, the implementation of this functionality for public blockchain-based digitized securities, as well as the related regulatory environment, is still developing.

To understand why this vision is important, it is helpful to draw a contrast with the settlement infrastructure in today's capital markets. In the United States public markets, the Depository Trust Company ("DTC") provides this "asset registry" service, keeping what is effectively the master record of who owns which securities on a daily basis. However, where the system described above is automated, programmable, instantaneous and – in trades with a discrete buyer and seller – peer-to-peer, today's process is manual and heavily intermediated. Most trades today are not settled near-instantaneously, but rather take two or more business days before ownership is officially transferred. This is, in part, due to the fact that (unlike the system described above), brokerages must affirmatively report all of their clients' trades to DTC, which in turn must manually update its ledger. Even further complicating the process is the fact that DTC does not track the *actual* beneficial owners of the securities it processes. Instead, it tracks ownership as between its "participants" (which include brokerages and other financial intermediaries), who in turn keep track of the beneficial owners (e.g., their clients). The brokerages then need to manually reconcile their individual records with each other to ensure their respective ledgers match.

As complex and inefficient as this system is, it is still superior to the status quo in the private markets, where no such recordation infrastructure exists at all. While some private placement trading platforms do exist, secondary trading in securities of private issuers generally relies on an ad hoc system in which issuers maintain spreadsheets tracking their security holders. Notwithstanding that today there are certain market participants

who help issuers manage their capitalization tables in a digitized framework, given that issuers must keep the list current, they will usually require holders to seek their permission prior to any secondary trading. Suffice it to say, this system is not built to handle legally compliant secondary trading on any significant scale. It is slow, error-prone, and lacks any programmable functionality. While there are many reasons why most private securities are illiquid *(See "**Limitations**" on page 8)*, the transactional frictions inherent to this system are likely a contributing factor. Blockchains may offer a way to reduce certain of these frictions. Not only can they provide a real-time audit trail of a security's ownership, they can be programmed to automate key functions necessary to facilitate secondary trading, including complying with securities laws.

Automated Compliance

Virtually any asset in the world can be represented as a digitized security and traded on a distributed ledger, including a traditional security. As mentioned, the process of digitizing a security makes it "programmable," meaning it can interact with smart contracts to automatically execute certain key functions. One of the most promising near-term applications of this technology involves coding transfer restrictions directly into the smart contract to automate compliance with certain key securities laws and an issuer's specific transfer restrictions. Done properly, this would ensure that any attempted secondary transfer of the digitized security that does not comply with the applicable rule set will not execute.

There are various open-source protocols being designed today to allow issuers to implement this vision. One option is a private, permissioned blockchain for unregistered securities transactions. Like open-source protocols, private blockchains can establish a standardized digitized security framework to allow more sophisticated transfer restrictions to be built directly into a smart contract. However, unlike public, open-source protocols, private blockchains provide issuers and investors, as well as regulators, with more certainty that transactions will occur securely, and that all participants are authorized to conduct the transaction due to their ability to decide on the rules of the blockchain protocol. Another option is public decentralized protocols (ERC including ERC-1400 and ERC-1404 for tokens issued on the Ethereum blockchain) that have a wider adoption rate due to their public nature and straightforward coding language.

Although public and private blockchains have their differences, both of these solutions aim to provide uniform standards to allow more complex regulatory restrictions in smart contracts. Prior to launch, an issuer would follow one of these protocols to write the security's smart contract in a way that imported the applicable regulatory requirements. Once the digitized security was issued, any subsequent transfer attempts would ping the digitized security's smart contract. If the necessary conditions were satisfied, the digitized security would be automatically transferred. If not, the transfer would be blocked and a message would be delivered explaining which condition was not satisfied. Using this technology, issuers can ensure they remain in compliance with certain key rules while also removing certain costly barriers that impede investors' ability to trade.

Overview of Key U.S. Securities Laws

Basic Framework Governing Primary Offerings of Securities

To understand specifically how and where this technology may add value, it is necessary to first provide a basic understanding of the laws governing securities offerings in the United States. The Securities Act of 1933 (the "Securities Act") and the Securities Exchange Act of 1934 (the "Exchange Act") together serve as the foundation of U.S. securities law. At a high level, the Securities Act requires an issuer of securities to either file a registration statement with the Securities and Exchange Commission (the "SEC") (including a prospectus that describes the issuer's business and the securities being offered) or conduct the offering in a way that qualifies for a specific exemption from registration. If the offering is registered, the issuer will generally then become subject to the ongoing reporting requirements and other disclosure obligations set forth in the Exchange Act. These obligations include filing annual, quarterly, and current reports with the SEC and delivering annual proxy statements to investors that disclose, among other things, audited and unaudited financial statements and executive compensation. While recent amendments under the JOBS Act have scaled down certain of the reporting obligations for "emerging growth companies," the compliance burden can still be onerous. Companies who want to avoid these obligations but still want access to the financing options offered by capital markets can conduct their offering in a way that qualifies for a registration exemption.

Costs of Compliance (and Non-Compliance) in Secondary Markets

While qualifying for a registration exemption can be fairly straightforward at the time of issuance, remaining in compliance while also facilitating secondary trading imposes a significant administrative burden on issuers (and particularly smaller issuers). It requires them to track certain information regarding their security holders at all times, including quantity, location, accreditation status, and holding periods. For many companies, this is done in one of two ways: (a) in a manual, error-prone fashion, often via internal spreadsheets and paper contracts; or (b) not at all. However, the cost of violating these rules can be severe for non-reporting issuers. For example, if (in the course of secondary trading) the number of security holders of a class of an issuer's equity securities rises above 500 non-accredited or 2,000 total investors (and the issuer has more than $10 million in assets), the issuer will be forced to begin reporting as a public company.

To avoid this fate, most issuers of private securities will actively take precautions that impede secondary liquidity, such as requiring a transfer agent to remove restrictive legends, or legal counsel to provide opinions affirming compliance, or even contractually forbidding secondary sales altogether. And even where issuers take these precautions, it is still possible for the securities to be traded (in contravention of the restrictive legend) without the issuer's knowledge. These barriers combine with other market forces to collectively render most private securities illiquid, which is impounded into their price via an "illiquidity discount."[5] Many issuers view this discount as a necessary cost to ensure regulatory compliance.

Key Requirements for Issuers of Unregistered Securities

As discussed, there are several key requirements that issuers of unregistered securities must comply with, both at the time of issuance and prior to any secondary trading.[6] To be sure, not all of these can be readily converted into code and hardwired into a digitized security's smart contract to ensure compliance. However, the following are examples that may be particularly well-suited for automation in the near term.

Accreditation Status

Accreditation status is relevant both at the time of issuing an unregistered security and (in certain circumstances) prior to secondary trading. **Accredited investors** are those with either: (a) a net worth in excess of $1 million; or (b) an income in excess of $200,000 in each of the two most recent years, with a reasonable expectation of reaching the same income level in the current year.[7] Rule 506(c) under **Regulation D** allows issuers to sell an unlimited amount of securities to an unlimited number of investors, so long as: (a) the issuer has a reasonable belief that all of the investors are accredited; and (b) the issuer has taken reasonable steps to verify that all investors are accredited.[8] Likewise, **Section 4(a)(7)** of the Securities Act generally allows accredited investors who obtained unregistered securities to resell those securities prior to the expiration of the applicable holding period under Rule 144, as long as the purchaser is also accredited, there is no general solicitation, certain information is made available to the purchaser, and the class of securities has been outstanding for at least 90 days.[9]

Current Approach: Most private issuers today will require initial purchasers to undergo accreditation verification to ensure compliance with Rule 506(c) prior to issuance. However, especially in the case of smaller private issuers, the only way to ensure secondary purchasers are *also* accredited (e.g., to facilitate secondary liquidity under Section 4(a)(7)) is to require all initial purchasers to seek prior approval from the issuer prior to trading, and then to run accreditation checks on all downstream purchasers. And even then, it is still possible for the security to wind up in the hands of a non-accredited investor.

5 Aswath Damodoran, *The Cost of Illiquidity*, http://people.stern.nyu.edu/adamodar/pdfiles/country/ illiquidity.pdf.

6 In addition to requirements with which issuers must comply, broker-dealer intermediaries also often face their own set of requirements (e.g., "know-your-customer" or anti-money laundering regulations imposed on certain financial institutions and other regulated entities). Automating these processes, which are often time-consuming and complex, could optimize compliance procedures for broker-dealers. However, a discussion of these and similar possible efficiencies is beyond the scope of our coverage of issuer-specific requirements in the unregistered securities context.

7 17 C.F.R. 230.501(a).

8 17 C.F.R. 230.506.

9 15 U.S.C. 77d(a)(7).

New Approach: Using a digitized security, an issuer can create a whitelist of accredited investors who qualified at the time of issuance. They can also outsource the production and ongoing maintenance of the whitelist to a third party such as a regulated broker-dealer that issues and trades the digitized security on an approved alternative trading system and which keeps a master list of all accredited investors on its platform. The issuer could pull from this master list to increase its total liquidity pool, or it could maintain its own list and add only those investors who request to be added and pass the accreditation check. From a regulatory standpoint, the SEC permits an issuer to rely on a third-party service to verify accreditation status.[10]

The accounts associated with the whitelisted investors could then be embedded into the smart contract. If a would-be purchaser's account is on the whitelist, the purchase will go through; if not, the transfer will be blocked. This creates a liquidity pool in which whitelisted investors can freely trade in the secondary market, with near instant settlement, without incurring the delays and costs currently involved in getting issuer pre-approval or hiring counsel. It also *guarantees* that the security cannot be transferred directly to a non-accredited investor, which is not possible today.

Resale Restriction Periods

Section 4(a)(1) of the Securities Act provides the primary statutory exemption for secondary trading, allowing unregistered sales by any person other than an "issuer," "underwriter," or "dealer."[11] This exemption is supplemented by Rule 144, which provides a safe harbor that persons can use to sell restricted securities in secondary markets without being deemed an "underwriter," which would require them to register the offering.[12] Restricted securities are securities acquired in unregistered sales from the issuer or from an affiliate of the issuer.[13] Generally speaking, in order to comply with Rule 144, restricted securities of non-public companies cannot be resold for one year following the date of purchase. Certain additional restrictions apply if the seller is an affiliate of the issuer.

Current Approach: To enforce for this, issuers will place restrictive legends on the face of the security that prohibit the holder from transferring the security prior to the expiration of the holding period unless the holder registers the sale or qualifies for a further exemption. Typically the legend can only be removed by a transfer agent, who in turn will typically require an opinion of counsel stating that Rule 144 has been complied with and that the legend can be removed.[14]

New Approach: The digitized security can include transfer restrictions that categorically prevent any transfers prior to the expiration of the applicable holding period. Or, to facilitate transfers under Section 4(a)(7) while still complying with Rule 144, the smart contract could prevent any transfers prior to one year following issuance, *except* if: (a) the potential transferee is on the accredited whitelist and (b) 90 days have passed since the class of securities was first outstanding. Using conditional logic, the smart contract could be coded to allow the interaction of different rule sets in this way. Doing so could reduce or even eliminate the need for issuers to require legal opinions in many cases, as the transfer restriction guarantees the resale restriction period requirement is satisfied.

Number of Required Holders

Section 12(g) of the Exchange Act requires an issuer to register a class of equity securities if: (a) its total assets exceed $10 million and (b) it has more than either 2,000 total holders of record or 500 non-accredited holders of record.[15] As noted, the penalty for non-compliance with Section 12(g) is severe – namely, the issuer will be forced to begin reporting as a public company within two years. Likewise, for an entity to qualify as an REIT in the United States (which entitles it to beneficial tax treatment), it must: (a) have a minimum of 100 shareholders[16] and (b) ensure that five or fewer individuals do not own more than 50% of the outstanding stock.[17] While

10 17 C.F.R. 230, 239 and 242.

11 15 U.S.C. 77d(a)(1).

12 17 C.F.R. 230.144.

13 Securities and Exchange Commission, *Rule 144: Selling Restricted and Control Securities* (2013), https://www.sec.gov/reportspubs/investor-publications/investorpubsrule144htm.html.

14 *Id.*

15 U.S.C. 78l(g).

16 26 U.S.C. § 856(a)(5).

17 26 U.S.C. § 856(h)(1)(A).

the shareholder number can of course be controlled at the time of issuance, it can be difficult for issuers to enforce compliance in the secondary market, as ordinary trading can (and does) result in frequent increases or decreases in the total holder count.

Current Approach: To enforce compliance today, most private issuers will require their security holders to seek their prior approval before trading, which adds a barrier to secondary liquidity and is an administrative burden for issuers to manage.

New Approach: Using a digitized security and a whitelist that connects investors' real-world identities to their user accounts, an issuer would know in real time exactly how many investors held its security. The issuer would also know the exact breakdown between accredited and non-accredited investors, for purposes of the 2,000 total versus 500 non-accredited investor distinction.

Location

Regulation S provides a safe harbor for unregistered offers and sales of securities outside of the United States.[18] To qualify, the offer cannot be made to a person in the United States and the buyer must be outside the United States or the seller must reasonably believe the buyer is outside the United States. Additionally, depending on the level of risk that the securities may flow back into the United States post-issuance, the issuer may need to take additional precautions such as additional holding periods of up to one year (known as "distribution compliance periods").

Current Approach: Issuers will place restrictive legends on securities informing holders of jurisdictional restrictions on secondary transfers. Beyond this, it is difficult (or even impossible) to guarantee that securities sold outside the United States will not flow back into the United States.

New Approach: Using a whitelist that pairs investors' real-world identities with their user accounts, an issuer could not only ensure that the securities were *issued* only to non-U.S. investors, but it could also guarantee that those securities did not *flow back* into the United States by only allowing secondary trading among other whitelisted non-U.S. investors.

Automated compliance could not only ease the burden on issuers and their security holders, it could also provide value to regulators and exchanges. Today, regulators usually only become aware of a securities law violation *ex post*, often following an investor complaint. Smart contracts provide a mechanism to guarantee compliance to certain applicable requirements *ex ante*, regardless of the venue or medium through which the transaction occurs. And to the extent a violation still does occur, a blockchain would provide a clear audit trail of the security's ownership (including any attempted transfers) at every moment following issuance. Indeed, regulators may not only permit the use of this technology by issuers, they may come to embrace it themselves.

Limitations

Despite the tangible benefits that digitized securities may offer, there are various limitations and roadblocks that must be acknowledged when evaluating their potential impact.

Technical Limitations

There are various technical limitations that are either inherent to blockchains fundamentally, or are near-term obstacles in need of solutions. The following are a few examples.

Lack of universally accepted standards: Several digitized security standards on public blockchains have been proposed to date (e.g., ERC-1400, ERC-1404, ERC-884 for shares in Delaware companies, Harbor's R-Token standard); similarly, various private blockchain-based protocols have been proposed. However, none have gained industry-wide adoption, nor have any been expressly blessed by regulators.

Whether in the form of a public or private solution, a uniform standard is important because it provides market participants with certainty as to the digitized security's functionality and mechanics. Any standard that does emerge must also be flexible enough to allow issuers to craft bespoke mechanics for their specific security. It must also provide issuers a "back door" to modify the smart contract after it has been deployed in order

18 17 C.F.R. 230.901.

to reflect changes to applicable law. Until consensus emerges around a particular standard meeting these criteria, adoption may be limited.

Limited functionality beyond compliance: While transfer restrictions of the sort outlined in the previous section are already possible using today's digitized security standards, many issuers may wait to launch digitized securities until additional functionality beyond automated compliance is possible. These include things like distributing cash flows to holders or managing voting rights. Certain obstacles exist today that inhibit the end-to-end automation of these functions, such as the difficulty in reliably encrypting shareholder votes. In these cases, issuers would still need to manually perform many steps "off-chain" in order to properly fulfill these functions in the near term. Until blockchains can fully automate these functions, issuers may not see digitized securities as adding significant value over the status quo. There are already certain providers that have identified this issue and are tapping into the space to provide a workaround to the problem in the private blockchain protocol context.

Complications with whitelist approach: There are a handful of potential issues with the whitelist approach with which the industry will need to grapple.[19] Issuers could individually vet each interested buyer for compliance with applicable rules; however, that would constrain the size of their secondary liquidity pool, and would be burdensome to administer. Ideally, industry-wide vetting standards would emerge that exchanges and other platforms would abide by when vetting potential investors. This would allow individual issuers to permit secondary trading among the broadest possible pool of investors, while still ensuring that they remained in compliance with applicable law. Indeed, issuers of large unregistered securities offerings conducted under Rule 144A today often rely on whitelists of "qualified institutional buyers" that are maintained by underwriters. Digitized securities issuers would benefit from a similar industry-wide approach. The lack of this infrastructure means that most issuers would not be comfortable allowing trading among investors that they did not personally vet.

Second, while using whitelists to trace real-world identities is straightforward for individual investors (because each whitelisted individual would be linked to a specific user account), it could become more complex for digitized securities held by crypto asset trading platforms that use a single wallet to hold the digital assets on behalf of multiple investors in a public blockchain. Private, permissioned blockchain protocols can ensure a level of transparency in tracing real-world entities since participation in the blockchain will be based on a set of rules. However, these rules are in the end contractual obligations and, as such, tracing capabilities remain lacking.

Rule 12(g)(5) holds that securities held by "a corporation, a partnership, a trust … or other organization shall be included as so held by one person."[20] Assuming the SEC applied this framework to digitized securities in the same way it does to traditional securities held by investment funds today, the outcome should be the same. However, there is no guidance on the matter to date.

Finally, it is likely that the more fervent privacy advocates in the crypto community, in particular those who believe public blockchain protocols would lose their essence if tracing is enabled, would oppose the use of and reliance on whitelists tied to real-world identities to ensure compliance with applicable law. For many of the applicable rules (e.g., accreditation status, location-based rules, anti-money laundering) there is simply no way to avoid verifying investors' real-world identities while remaining in compliance with the law.

Limited transaction throughput on public blockchains: Traditional public blockchains trade efficiency and high transaction throughput for decentralization and interoperability. At present, Ethereum can only process roughly 15 transactions per second.[21] During peak times, transaction fees can also become significant. While various initiatives are underway to increase transaction throughput, public blockchains are inherently less efficient from a throughput perspective than centralized blockchains or existing centralized databases, since the ledger must be maintained concurrently by all validator nodes. This phenomenon is one reason why public blockchains are not currently equipped to replace the public capital markets settlement system, which, though inefficient, is

19 As a preliminary matter, the issues discussed in this subsection are not particular to digitized securities; these problems are endemic in public markets as well. Although the technology does not *solve* for the preexisting issues mentioned here, as discussed earlier we note that the whitelist vetting approach does provide an additional layer of confidence traditional markets do not.

20 17 C.F.R. 240.12g5-1.

21 Alyssa Hertig, *How Will Ethereum Scale?*, https://www.coindesk.com/information/will-ethereum-scale.

still a largely reliable way to process millions of trades daily. As noted, today's public blockchains are currently better suited for the smaller, private markets where trading volume is significantly lower.

Poor user interfaces: Generally, the user-facing applications in the digital asset space are confusing and non-intuitive for most individuals who lack a technical background. Beyond hobbyists, most investors will not purchase a digitized security simply because it leverages a blockchain as the settlement layer. The application layer of most of the solutions needs to improve to the point that investors are as comfortable using new technology (whether in the form of an alternative trading system, wallet, or token exchange) as they are using their brokerage accounts currently. Given the relative simplicity of updating deficient interfaces and the payoff it promises in terms of attracting investors to a product, many companies are already expending resources to avoid this problem (for example, by shaping their solutions to look and feel like familiar platforms). There are some new platforms with significantly improved interfaces (e.g., Templum/Symbiont) and further improvements in this area are likely.

Market Limitations

Contrary to the view of many proponents, digitization is not a panacea for the illiquidity issues that plague private securities markets. There are many factors that drive illiquidity in private markets that will persist even for issuers who digitize their securities. These include the following, among others.

Thin order books: It is often difficult for buyers and sellers of private securities to find one another, as there is simply not as much demand for these assets as compared to securities of public, exchange-listed companies. Markets for private assets such as real estate – other than, for example, certain marquee names – or other similarly bespoke products are also usually fragmented by geography, meaning the number of potential buyers and sellers is capped. Although digitization of certain securities may help buyers and sellers identify potential counterparties – for example, by creating and assigning a CUSIP to a security – the technology itself cannot solve the underlying problem that inherent market interest in certain assets may not always exist.

Limited disclosure: Since non-reporting issuers are not required to make periodic disclosures concerning financial and operational performance, would-be buyers have less information, which may reduce their willingness to invest. However, there are some traits digitized securities possess that may limit the impact of this phenomenon. For example, digitized securities have the benefit of information continuity, as all documents and data related to the instrument are hashed to the security for its lifetime (even if that data is limited compared to its traditional security counterparts). Additionally, private, permissioned blockchains implement certain disclosure or reporting requirements over their participants, which may give investors additional comfort as to their investment.

Informational asymmetries between buyers and sellers: Relatedly, sellers of private market securities usually have better information regarding the true value of the asset than buyers, particularly for non-fungible assets like real estate or complex assets like Limited Partner interests in private equity funds. It can be expensive and time-consuming to conduct due diligence on these assets, adding another barrier to investment.

Small market caps: Securities with relatively smaller public floats tend to generate less trading volume than do securities with large ones.

Legal Limitations

Finally, there are various legal limitations that must be acknowledged when evaluating the value-add of a digitized security. There are many aspects of the rules highlighted previously (and others) that cannot be rendered in computer code and automated by a smart contract. For example, prohibitions on general solicitation and advertising (such as those set forth in Rule 506(b) of Regulation D) could not be enforced by a smart contract, and would instead still depend on some off-chain compliance mechanism. Likewise, certain obligations imposed on sales of restricted securities by affiliates, such as current public information requirements, would likely need to be enforced externally. And even if the digitized security could be coded to automate full compliance on-chain, there is still the possibility that holders may enter into transactions with third parties off-chain in violation of agreed-upon governance rules with respect to the security without the embedded restrictions being triggered. Therefore, even assuming advancements in the programming languages of smart contracts, certain legal concepts simply cannot be automated.

Conclusion

The digitized security space is undoubtedly in its infancy. There are significant layers of infrastructure that still need to be built out before the vision articulated in this paper can be realized. Neither issuers nor institutional investors will embrace digitized securities unless the technology adds tangible value over the status quo. In the public capital markets, the settlement infrastructure that facilitates secondary trading is convoluted and slow by the standards of today's technology age. However, it is still a mostly reliable system, and is therefore likely to persist until blockchains see significant improvements in transaction throughput and security. The status quo in the private capital markets, on the other hand, is one with virtually no infrastructure to facilitate legally compliant secondary trading on any significant scale. Blockchains can therefore add real, near-term value on the private market side, serving as the "smart" settlement system that tracks ownership in real time and automates functions like compliance across trading venues.

Indeed, despite the industry's nascent stage, several companies have already begun experimenting with and implementing this vision.[22, 23, 24, 25] This first generation of digitized securities have been launched by private issuers (primarily in the real estate space) looking for an efficient way to raise low-cost capital from a potentially global base of investors. On the investor side, these offerings provide access to assets (e.g., commercial real estate projects) that many smaller investors have traditionally been priced out of, while also enabling secondary liquidity on the back end. As the industry continues to mature, more established market participants may begin to notice this emerging technology and the potential it has to transform today's capital markets.

22 *Templum Markets Launches Digital Security Offering of St. Regis Aspen Resort*, BUSINESS WIRE (Aug. 8, 2018, 12:00 PM), https://www.businesswire.com/news/home/20180808005549/en/Templum-Markets-Launches-Digital-Security-Offering-St.

23 JD Alois, *tZero Distributes Security Token to Investors, Plans Secondary Trading*, CROWDFUND INSIDER (Oct. 16, 2018, 10:20 AM), https://www.crowdfundinsider.com/2018/10/140167-tzero-distributes-security-token-to-investors-plans-secondary-trading/.

24 Tim Fries, *Real Estate Security Token "Factor-805" Released, Brings DAI To Digital Securities*, THE TOKENIST (Feb. 25, 2019), https://thetokenist.io/real-estate-security-token-factor-805-released-brings-dai-to-digital-securities/.

25 Anna Baydakova, *French Lender Societe Generale Issues $112 Million Bond on Ethereum*, COINDESK (Apr. 23, 2019, 8:53 PM), https://www.coindesk.com/french-lender-societe-generale-issues-112-million-bond-on-ethereum.

About the Authors

David J. Kappos, one of the foremost leaders in the field of intellectual property, is a corporate partner at Cravath. He supports the Firm's clients with a wide range of their most complex intellectual property issues, including those pertaining to blockchain and financial technology.

D. Scott Bennett, a corporate partner at Cravath, focuses on representing issuers and investment banking firms in connection with securities offerings, as well as representing corporate clients in mergers and acquisitions, across a broad range of industries including blockchain and financial technology.

Michael E. Mariani is a corporate partner at Cravath whose practice focuses on representing companies and investment banks in a variety of financing transactions. He also advises clients on public disclosure and corporate governance matters, and mergers and acquisitions.

Jeffrey M. Amico is Legal Counsel at Fluidity Factora, and was formerly a corporate associate at Cravath.

Christopher Pallotta is the Co-founder and CEO of Templum. Chris is also the Managing Director at Raptor Group overseeing a portfolio of investments in technology, financial services, media, and sports sectors. Before joining Raptor Group, Chris focused on the commercialization of technologies developed at the MIT Media Lab and acted as Chief of Staff for the director of the Media Lab, Joi Ito.

Vincent Molinari is the Co-founder of Templum, Inc., and the CEO of its subsidiary, Templum Markets. Vince has nearly 30 years of experience in the financial services industry. Throughout his career, he has been a true entrepreneur founding and leading multiple companies committed to advancing market infrastructure, capital formation, impact investing, and digital assets.

Annemarie Tierney is the Head of Strategy and General Counsel of Templum Inc. Annemarie is a frequent speaker on the regulatory and legal framework for digital assets. Previously, she was the Head of Strategy at Nasdaq Private Market and General Counsel of SecondMarket (now Digital Securities Group), and held senior positions at the NYSE and the SEC.

Peter Chiaro is a Senior Associate with Templum. Peter is focused on developing and executing business initiatives as well as creating awareness in the legal community about the legal framework associated with digital assets. He has served as in-house legal counsel to numerous venture-backed media and technology companies.

LEGAL EXECUTIVE INSTITUTE

The Thomson Reuters Legal Executive Institute brings together people from across the legal industry to ignite conversation and debate, make sense of the latest events and trends, and provide guidance as you confront the opportunities and challenges that these changes present.

Through live events, blog commentary, legal news analysis, and interviews with industry leaders, the Legal Executive Institute offers keen insight into the profession of law and the legal marketplace from members of law firms, corporate legal departments, government, and academia.

For more information, visit legalexecutiveinstitute.com