Digitized Securities and the Promise of Automated Compliance

DAVID J. KAPPOS, D. SCOTT BENNETT, AND MICHAEL E. MARIANI, CRAVATH, SWAINE & MOORE LLP; JEFFREY M. AMICO, FLUIDITY; VINCENT MOLINARI, CHRISTOPHER PALLOTTA, ANNEMARIE TIERNEY, AND PETER CHIARO, TEMPLUM INC.

This Article examines digitized securities (sometimes called smart securities or security tokens) and the ability of blockchain-enabled smart contracts to automate compliance with certain aspects of US federal securities laws, reducing a major barrier to secondary liquidity in private markets. It further provides a high-level overview of distributed ledger systems, including their potential benefits as compared to existing technologies, analyzes certain obstacles that must be overcome for this technology to gain widespread adoption, and considers which existing solutions are most likely to generate widespread adoption.

Currently, private companies have little infrastructure to facilitate legally compliant secondary trading on any significant scale. But blockchain could add real, near-term value to private companies, serving as the "smart" settlement system that tracks security ownership in real time and automates functions like compliance across trading venues. Despite blockchain's nascent stage, several companies have already begun experimenting with and implementing this vision. The first generation of blockchain has 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 (such as 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 blockchain 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.

This Article discusses:

- Blockchain, distributed ledgers, and digitized securities.
- US federal securities laws.
- How capital markets could benefit from blockchain-enabled automated compliance.
- Current limitations on using blockchain in capital markets.

For more information on blockchain and distributed ledger technologies generally, see Blockchain Toolkit (W-018-8660).

OVERVIEW OF DISTRIBUTED LEDGER SYSTEMS

A digitized security is a digital representation of a security that can be programmed to automate certain functions and the ownership of which is traced in real time using a distributed ledger. 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 issuers and regulators with greater assurance regarding compliance with applicable laws.
- Eliminate 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. The value of a digitized security in this context over the status quo is that these compliance checks would be enforced

automatically on any transfer without requiring any post-trade intervention or reconciliation to ensure compliance and track ownership. This technology is especially apt for asset classes that have traditionally experienced low liquidity levels, such as private real estate investment trusts and limited partnership interests.

This is possible because distributed ledgers allow the various entities necessary to effect a securities transaction (such as brokers, exchanges, and custodians) to all share a common, programmable data layer. This marks a drastic 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. 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.

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. 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 (typically transactions) are 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.

Public/Private and Permissionless/Permissioned Blockchains

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 or require permission to join, or both.

The distinction between public and private refers to which members can access the blockchain in any capacity:

- Public blockchains are open to all.
- Private blockchains are open only to pre-approved members.

The distinction between permissioned and permissionless refers to which members can add data (commonly in the form of submitting transactions and executing smart contracts) to the blockchain:

- Permissionless blockchains allow all members to add data.
- Permissioned blockchains restrict this right to approve members.

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.

A public, permissionless blockchain is a truly distributed ledger, in that:

- There is no central authority
- The decision on whether a new block should be added to the chain is vested with the consensus of the blockchain community.

In a private, permissioned blockchain, however, central intermediaries may be necessary. Therefore, in a fully 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 may 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 ten of them must sign every block 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 with transaction privileges on the blockchain according to certain rules implemented within the protocol.

Another distinction between public and private blockchains is that:

- Public blockchains are generally immutable.
- Private blockchains may have more flexibility for risk depending on the perspective for changes in the blockchain.

For a further discussion of public and private blockchains, see Practice Note, Blockchain and Supply Chain Management (W-017-3806).

Smart Contracts

Certain distributed ledgers also allow users to embed computer scripts into the ledger that execute 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).
- Enable the transfer of digitized securities between users.

Smart contracts are effectively computer programs that are 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 may include smart contracts that only allow transfers:

- Up to a spending cap.
- Within certain time periods
- To pre-approved persons, such as accredited or institutional investor accounts.

For additional information on smart contracts, see Practice Note, Understanding Smart Contract Mechanics (W-005-3262).

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. For example, there can be either:

- A central administrator of the blockchain.
- A consortium of members given administration privileges.

Though blockchains can be used to store other forms of data (such as identity-based information), their primary use case to date has been to:

- Track ownership of assets
- Facilitate the transfer of those assets between users.

Public blockchains of this variety (like Bitcoin) can be thought of as peer-to-peer asset registries. Public blockchains with more advanced scripting languages (like Ethereum), as well as certain private blockchain solutions (like Symbiont), take on a more active role, serving as both:

- The asset registry.
- The computer that actually executes the transactions.

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:

- The various entities needed to effect a securities transaction today (such as exchanges, brokers, and custodians) could all share a single set of records, instead of maintaining (and reconciling) their own respective ledgers daily.
- This shared settlement layer could then be programmed by an issuer to automate certain functions like regulatory compliance or cash flow distributions and these functions would execute automatically as programmed.

These functions 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-on record of which party owns a particular security at any moment, updated in real time, regardless of the particular venue or medium through which a transaction occurred. In that state of the world, it becomes irrelevant whether the buyer and seller connect via:

- A regulated trading venue (such as a traditional public exchange or an alternative trading system).
- An unregulated trading venue (such as a message board or even in person).

As long as the seller sends the token from the seller's 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 (such as transfer agents and 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 US public markets, the Depository Trust Company (DTC) provides this asset registry service, keeping what is effectively the master record of who owns which securities daily.

However, where blockchain systems are automated, programmable, fast, and in trades with a discrete buyer and seller, peer-to-peer, today's securities settlement 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, because (unlike the blockchain system previously described), 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 (their clients). The brokerages then need to manually reconcile their individual records with each other to ensure their respective ledgers match. For more information on the existing settlement system with DTC, see Practice Note, Clearing and Settlement of Debt Securities: Overview (1-502-0059).

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. 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. Despite that today there are certain market participants helping issuers manage their capitalization tables in a digitized framework, given that issuers must keep the list current, they usually require holders to seek their permission before 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), the transactional frictions inherent to this system are likely a contributing factor. Blockchains may offer a way to reduce certain of these frictions by:

- Providing a real-time audit trail of a security's ownership.
- Automating key functions necessary to facilitate secondary trading, including compliance 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 applications of this technology involves coding transfer restrictions directly into the smart contract to automate compliance with:

- Certain key securities laws.
- An issuer's specific transfer restrictions.

Done properly, this could ensure that any attempted secondary transfer of the digitized security that does not comply with the applicable rule set does not execute. For a discussion of the limitations of these applications, see Limitations.

There are various open-source protocols being designed today to help 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.
- 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. Before 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 may be able to ensure that 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 US. The Securities Act and the Exchange Act together serve as the foundation of US securities law. At a high level, the Securities Act requires an issuer of securities to either file a registration statement with 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 generally then becomes subject to the ongoing reporting requirements and other disclosure obligations set out 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 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 wishing 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.

For a more detailed overview of US securities laws, see Practice Note, US Securities Laws: Overview (3-383-6798). For an overview of exempt offerings, see Practice Note, Unregistered Offerings: Overview (9-382-8837).

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.
- Holding periods.

For many companies, this is done in either one of two ways:

- In a manual, error-prone fashion, often via internal spreadsheets and paper contracts.
- 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 filing public reports with the SEC under the Exchange Act. For more information, see Practice Note, Exchange Act Registration: Calculating Size Thresholds Under Section 12(g) (7-506-3135).

To avoid this fate, most issuers of private securities 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. For more information on restrictions on secondary liquidity, see Practice Note, Resales Under Rule 144 (4-382-8769).

Even where issuers take these precautions, it may 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. 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 before any secondary trading. Not all of these requirements can be readily converted into code and hardwired into a digitized security's smart contract to ensure compliance. However, there are several examples that may be particularly well-suited for automation in the near term.

Note that, in addition to requirements with which issuers must comply (which is the focus of this Article), broker-dealer intermediaries also often face their own set of requirements, (such as "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.

ACCREDITATION STATUS

Accreditation status is relevant both at the time of issuing an unregistered security and (in certain circumstances) before secondary trading. Rule 506(c) under Regulation D allows issuers to sell an unlimited amount of securities to an unlimited number of investors, if:

- The issuer has a reasonable belief that all of the purchasers are accredited investors.
- The issuer has taken reasonable steps to verify that all investors are accredited.

For more information on offerings under Rule 506(c), see Practice Note, Section 4(a)(2) and Regulation D Private Placements: General Solicitation and Advertising Allowed in Rule 506(c) Offerings (8-382-6259).

Likewise, Section 4(a)(7) of the Securities Act generally allows accredited investors who obtained unregistered securities to resell those securities before the expiration of the applicable holding period under Rule 144, if all of the following conditions are satisfied:

- The purchaser is also accredited.
- There is no general solicitation.
- Certain information is made available to the purchaser.
- The class of securities has been outstanding for at least 90 days.

For more information on resales under Section 4(a)(7), see Practice Note, Resales Under Rule 144A and Section "4(1½)": Section 4(a)(7) Resales (6-382-8768).

Current Approach

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

New Approach

Using a digitized security, an issuer can create a whitelist of accredited investors 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.
- 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 (see Practice Note, Section 4(a)(2) and Regulation D Private Placements: Non-Exclusive List of Steps to Verify Accredited Investor Status (8-382-6259)).

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 goes through. If the account is not on the whitelist, the transfer is blocked. This creates a liquidity pool in which whitelisted investors can freely trade in the secondary market, with a quicker settlement, without incurring the delays and costs currently involved in getting issuer pre-approval or hiring counsel. It also helps ensure that the security cannot be transferred directly to a non-accredited investor, which is not possible today.

For a discussion of certain complications with a whitelist approach, see Complications with Whitelist Approach.

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.
- An underwriter.
- A dealer.

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 requires them to register the offering (see Practice Note, Resales Under Rule 144: What Is a Statutory Underwriter? (4-382-8769)). To comply with

Rule 144, restricted securities of non-public companies generally cannot be resold for one year following the date of purchase. Certain additional restrictions apply if the seller is an affiliate of the issuer (see Practice Note, Resales Under Rule 144: Conditions to Use Rule 144 (4-382-8769)).

Current Approach

To enforce these resale restrictions, issuers place restrictive legends on the face of the security that prohibit the holder from transferring the security before the expiration of the holding period unless the holder registers the sale or qualifies for a further exemption. The legend typically can only be removed by a transfer agent, who in turn typically requires an opinion of counsel stating that Rule 144 has been complied with and that the legend can be removed. For more information on removing restrictive legends, see Practice Note, Securities Act Restrictive Legends and Rule 144 Sales (9-526-4406).

New Approach

The digitized security can include transfer restrictions that categorically prevent any transfers before 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 before one year following issuance, except if both:

- The potential transferee is on the accredited whitelist.
- 90 days have passed since the class of securities was first outstanding.
- Information requirements are satisfied.
- There was no general solicitation.

However, for a discussion of legal complications with this approach, see Legal Limitations.

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 embedded transfer restriction could help ensure that 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 both:

- The issuer's total assets exceed $10 million.
- The issuer has more than either:
  - 2,000 total holders of record; or
  - 500 non-accredited holders of record.

(See Practice Note, Exchange Act Registration: Calculating Size Thresholds Under Section 12(g) (7-506-3135).)

The penalty for non-compliance with Section 12(g) is severe. The issuer is forced to begin filing public reports with the SEC under the Exchange Act within two years. Likewise, for an entity to qualify as a REIT in the US (which entitles it to beneficial tax treatment), it must:

- Have a minimum of 100 shareholders.
- Ensure that five or fewer individuals do not own more than 50% of the outstanding stock.

(See Practice Note, REITs: Overview (8-504-7098).)

While 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 require their securityholders to seek the issuers' prior approval before trading, which:

- Adds a barrier to secondary liquidity.
- 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 could be able to know in real time how many investors held its security. The issuer could also easily determine the breakdown between accredited and non-accredited investors, for purposes of the 2,000 total versus 500 non-accredited investor distinction under the Exchange Act. For a discussion of the complications with a whitelist approach, and the difficulty of identifying beneficial owners, see Complications with Whitelist Approach.

LOCATION

Regulation S provides a safe harbor for unregistered offers and sales of securities outside of the US. To qualify, in general, the offer cannot be made to a person in the US and the buyer must be outside the US or the seller must reasonably believe the buyer is outside the US. Depending on the level of risk that the securities may flow back into the US post-issuance, the issuer may also need to take additional precautions, such as additional holding periods of up to one year (known as distribution compliance periods). For more information on Regulation S offerings, see Practice Note, Regulation S Transactions (5-383-1182).

Current Approach

Issuers 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 US do not flow back into the US.

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-US investors, but it could also help ensure that those securities did not flow back into the US by only allowing secondary trading among other whitelisted non-US 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 help ensure compliance with certain applicable requirements ex ante, regardless of the venue or medium through which the transaction occurs. 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. These include:

- Technical limitations (see Technical Limitations).
- Market limitations (see Market Limitations).
- Legal limitations (see Legal Limitations).

TECHNICAL LIMITATIONS

There are various technical limitations that are either inherent to blockchains fundamentally or are near-term obstacles in need of solutions. These include:

- A lack of universally accepted standards for creating digitized securities (see Lack of Universally Accepted Standards).
- Limited functionality of digitized securities beyond compliance (see Limited Functionality Beyond Compliance).
- Complications with the whitelist approach (see Complications with Whitelist Approach).
- The limited number of transactions per second that public blockchains can process (see Limited Transaction Throughput on Public Blockchains).
- A lack of intuitive user experiences for investors to engage with digitized securities (see Poor User Interfaces).

Lack of Universally Accepted Standards

Several digitized security standards on public blockchains have been proposed to date. These include:

- 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 regarding the digitized security's functionality and mechanics. Any standard that does emerge must:

- Be flexible enough to allow issuers to craft bespoke mechanics for their specific security.
- Provide issuers a "back door" to modify the smart contract after it has been deployed 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 previously 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. Examples may include:

- Distributing cash flows to holders.
- 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" 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 must grapple. As a preliminary matter, these issues are not particular to digitized securities because these problems are also endemic in public markets. Although the technology does not solve for the preexisting issues mentioned here, as discussed earlier, the whitelist vetting approach does provide an additional layer of confidence traditional markets do not.

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 investment banks. 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 because participation in the blockchain is 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) under the Exchange Act holds that securities held by "a corporation, a partnership, a trust ... or other organization shall be included as so held by one person." 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, are likely to 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 (such as 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 (see Alyssa Hertig, How Will Ethereum Scale?). 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 because 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 still a largely reliable way to process millions of trades daily. 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 likely 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).

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 are likely to persist even for issuers who digitize their securities. These include (among others):

- Lack of demand for illiquid private company securities (see Thin Order Books).
- Limited public information about private companies (see Limited Disclosure).
- Informational asymmetries between counterparties (see Informational Asymmetries between Buyers and Sellers).
- Small market capitalizations of companies in the private markets (see Small Market Caps).

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 have 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 regarding 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

There are various legal limitations that must be acknowledged when evaluating the value-add of a digitized security. Many aspects of the rules highlighted previously (and others) cannot be rendered in computer code and automated by a smart contract. For example, prohibitions on general solicitation and advertising (such as those set out 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. 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-on governance rules regarding 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.

THE FUTURE OF DIGITIZED SECURITIES

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 Article can be realized. Neither issuers nor institutional investors are likely to 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 it is therefore likely to persist until blockchains see significant improvements in transaction throughput and security. In the private capital markets, however, blockchains may be able to add real, near-term value by serving as the "smart" settlement system that tracks ownership in real time and automates functions like compliance across trading venues.

11-19