Bloomberg LAW

Georgetown Law CLE

Printed By: CEOANNOU on Monday, April 23, 2018 - 12:50 PM

Georgetown Law CLE

Private and Secure Records: Distributed Ledger Technology as a Record Keeping Mechanism by the SEC

2017 Georgetown Law Advanced eDiscovery Institute

Miles Vaughn, J.D. 2017, The American University Washington College of Law.

Jason R. Baron, Of Counsel, Drinker Biddle & Reath LLP, Washington, D.C.

Introduction

The growing awareness of distributed ledger technologies in both the legal community and by the public at large initially has been due to the widespread publicity (and controversy) over the use of Bitcoin. Bitcoin remains the technology's most notable application in the form of what has come to be known as “blockchains.” However, the application of distributed ledger technology is far from limited to the use of Bitcoin or other cryptocurrencies. Distributed ledger technology has the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services.” Indeed, a growing chorus of voices are recognizing that distributed ledger technology is potentially transformative, in being a “powerful innovation that could have a profound impact on both the law and the provision of legal services.”

One important application of distributed ledger technology is its use by companies interested in creating a secure accounting system or financial-tracking platform. The Security Exchange Commission (SEC) has strict rules and regulations governing the methods by which financial information may be tracked and stored. While the SEC is spending considerable resources in determining if Bitcoin should be considered tradeable as an electronic currency,a larger discussion is occurring as to whether distributed ledger technology itself satisfies the stringent privacy and security regulations enforced by the SEC. Here we will first look “under the hood” at distributed ledger technology, to explain how it works. We will then discuss specific applications of distributed ledger technology of interest to the financial sector.

I. How Does Distributed Ledger Technology Work?

A. Defining the Blockchain

Distributed ledger technology provides for a series of recorded transactions that are shared, verified, and stored in multiple locations. The technology compiles selected transactions which are electronically recorded into ledgers called “blocks.” These ledgers are in turn compiled in succession to form an indelible ledger commonly referred to as a “blockchain.” For the purpose of this paper, the term “blockchain” will be used interchangeably with the term “distributed ledger technology,” although as a technical matter blockchains are best considered a subset of all existing types of distributed ledger technology. Once a blockchain on one computer is updated with a new transaction block, the recorded blockchains on other systems within the network will be updated. These two processes working in tandem make altering the ledger very difficult. If someone attempts to change the records on one system, the change would be recognized by the rest of the network, alerting the owner of the blockchain to the alteration almost immediately. This makes the use of distributed ledger technology very trustworthy, since to change a transaction the malefactor must simultaneously change the transaction on

every single computer in the system. Since transactions are uniformly verifiable, the blockchain has become a popular application for the financial sector. The decentralization of blockchains also means that information is not kept only by a small number of vulnerable parties. In order to understand how information is shared and verified it is important to first understand how blockchain transactions are recorded.

A blockchain begins with the origin block, the earliest transaction or series of transactions recorded in the ledger. The second set of transactions, or block, relies on the validity and the unique features of the first block. Each block has at least two unique features: a “nonce,” and a “hash.” A nonce is a number that is assigned to the block based on the block's hash. The nonce also has the benefit of giving the block an easier numerical identifier for the user. A hash is a series of characters that represents the data within the block. This code is a one-way function, easy to make but difficult to invert, and is created by what is known as a “hash algorithm.” Bitcoin, for example, uses an SHA-256 function to encrypt the hash. The SHA-256 algorithm is very secure and is considered an industry standard under the Federal Information Processing Standards (FIPS).When a transaction is completed, a hash of the block's data is produced. That hash may also rely on other factors unique to that block, including time signatures, the block immediately previous in the chain, and a shared hash of all previous transactions in the block.

For example, imagine the message, “Tell Bob Hello,” represents a series of transactions where each word represents multiple transactions within one block. The original block would contain the word “Tell,” as well has have a nonce and a hash. The second block, “Bob,” would take the previous block's hash and use it in the creation of its own hash, also containing the word “Bob” and the block's nonce. Finally, the third block would create its own hash based on the previous block and the word “Hello.” In this scenario, a malicious third party wants to alter the second block to read “Alice” instead of “Bob.” Despite the difficulty in doing so, the malefactor manages to change the ledger on a system recording the transactions. That ledger's error would immediately be apparent, since the new data (“Alice”) would change the second block's hash, ultimately invalidating the hash of the subsequent block (“Hello”). To rectify this, the malefactor then redoes the third block, creating a new hash which incorporates the second block's changed hash. Within this one system the transaction would appear valid. Importantly, however, other recordings of the transaction which are stored on other systems will have a different hash since they have the original data. The changed hash will be identified as unique and therefore altered.

B. Providing for Network Access and Security

Besides the creation of the ledger itself, it is important to know which users are recording the transactions in the distributed ledger and how secure the ledger is against future changes. There are two general pools of network access for distributed ledgers, public and private. Public network access works well for large, decentralized networks such as Bitcoin. Private ledgers work well for smaller networks with trusted (or mostly-trusted) parties.

Public ledgers are open to everyone and all users may view all transactions in the ledger. This constitutes a decentralized and open system with no central authority. All users participate in determining what new blocks are added to the blockchain, in what is called the consensus process. Consensus is made by solving complex cryptographic problems. This arguably can make validating blocks faster — since there are many users contributing to the process even if the individual computational power of each user may be small. Also, any bad actors will be exposed to the public at large. Consensus mechanisms used in blockchains help solve the classic “Byzantine Generals” problem (see infra), which in this case would account for transactional fraud. There are three popular methods to

determining consensus: the proof-of-work algorithm (PoW), the proof-of-stake algorithm (PoS), and the delegated proof-of-stake algorithm (DPoS).

The most common method to determine consensus is the proof-of-work mechanism. Like in the previous example with “Tell Bob Hello,” the ledger was verified using hash functions that must match the original transaction. This is the process by which Bitcoin verifies its payments and will reward the verifying parties with Bitcoins. The first block, “Tell,” is created by combining the hash values of the transaction. Then, so-called “miners” take the combined hash, along with a timestamp and a difficulty setting (the number of zeros that the final verified hash must begin with), and find a nonce that satisfies the protocol.

Bitcoin, for example, uses a “hashcash” PoW function to verify its transactions. Verifying the ledger is a time-consuming action which can require an immense amount of computing power. This is because hashes are a one-way or “trapdoor” function. For example, it is easy to compute y from x when y=Hash(x), but is very difficult to find x while only given y. Given a rule where the output hash must begin with ten zeros (the difficulty setting), finding a nonce would take ten to the power of twelve computations. The miner will go through the hashes and essentially brute force a solution for x. As a reward for this effort, miners are allocated Bitcoins at the conclusion of a successful block.

So how does proof-of-work relate to what is known as the Byzantine Generals Program, also referred to as “practical Byzantine fault tolerance”? The description of the problem begins with several Byzantine generals surrounding an enemy encampment. These generals must coordinate their strategic choices and agree to attack at midnight. Without solidarity, their attack will fail so it is essential that the generals must all receive the same instructions. However, messages may be intercepted by enemy scouts who will change the message to say, “attack at dawn,” a sub-optimal strategy. How can the generals’ leader send messages over an open network to ensure that the messages will not be changed? The general who sends out the order to attack at midnight first tells all the other generals that the message must have five zeros in its hash in order to be valid. This is accomplished by pairing the text of the message, “attack at dusk” with a nonce that makes the hash begin with five zeros (hash of “Attack at midnight! Kdn40kn5D2” = 0000083750187591).

This nonce (Kdn40kn5D2) is found through proof-of-work, and in this hypothetical we will assume it took the general's interns ten hours to compute. The scout who intercepts this message can try to change the text to read “attack at dawn! Kdn40kn5D2,” but the resulting hash will not begin with the required five zeros since the text of the message has been changed. However, assume the scout buys himself a faster computer than the general which can solve for the nonce in only five hours, which is well within the time limit to confound the generals’ plans. To combat this, the generals all buy computers that can compute the nonce in five hours. They combine their computing power to find a nonce that allows the hash to begin with fifteen zeros. This increase in computational difficulty means that the individual scout would need hundreds and hundreds of years to solve for the new nonce. By the time the scout can produce a nonce, the attack has already occurred. These generals could also send their own individual messages which would be combined as a block. They would then work together in finding a nonce that makes the required number of zeros for their messages, verifying that block. The scout could try to assemble a computer or network of machines that would compute the nonce faster than the generals. This is known as the “51% Attack,” and, although in theory it would work, the difficulty in amassing the network often renders the option unviable.

A variation on the proof-of-work method is the proof-of-stake algorithm. Instead of using hash functions like in the PoW method, digital signatures are used to prove ownership of the transaction. Rather than miners solving complex and resource-consuming tasks, a user is chosen at random (or pseudo-random)

to validate the addition of a new block. The chance of a particular user, or node, to be chosen to validate the transaction increases based on their proportional wealth in the system. In this case, users that have more wealth, or "stake," in the transaction have a higher chance of being chosen to validate the transaction. However, by favoring those with higher stakes, this method does create a somewhat more centralized system.

The most centralized version of the proof-of-stake function is the delegated proof-of-stake system. Instead of just giving weight to bigger stakeholders, the users select from among themselves a single user (or small group of users) to validate the transactions. Real-time voting and trust algorithms can both be used to allow users to choose who validates the system. This allows smaller stakeholders to band together and wrestle some control away from the dominant stakeholders.

Private networks work well for smaller communities that would rather have a centralized system that verifies transactions. Ledgers on a private network may not necessarily need extensive consensus building measures, and could instead use limited, trusted sources to validate transactions. Companies choose their consensus methods based on desired speed and security. There are also methods in which consensus can be reached without completing computational problems in a process called "virtual mining." This would eliminate the need for expensive machines that require tremendous amounts of energy.

Private networks can have their rules changed quickly, allowing for more difficult or easier proofs, according to the type of data and the desired transaction time. The chances of a 51% attack are low, since all the validators are known and trusted. Even if the validators are not all trusted, like in a consortium network, it would take a large amount of computing power and that party would need to have hidden that capability from the others in the network. Private networks may also be cheaper and faster since blocks only need to be verified by a few, trusted nodes with high computing power rather than thousands of individual, small-powered computers. Finally, private networks are more private than public networks since only a few users are able to access the transactions.

II. Current Financial Privacy Laws

Under law and regulations governing the U.S. Security and Exchange Commission (SEC), financial transactions have stringent regulations that protect the privacy of users and that verify the validity of each transaction. The SEC's consumer privacy rules are found at 17 C.F.R. Part 248 ("Part 248"), under Regulations S-P, S-AM, and S-ID. Regulation S-P contains rules on privacy and opt-out disclosures, disclosure limitations, and exceptions for lawful disclosure. Regulation S-AM pertains to limitations on affiliate marketing, while Regulation S-ID explains how identity theft should be disclosed to customers. Many of these rules come from the 1999 Gramm-Leech-Bliley Act, which lays the groundwork for modern financial data protection.

A. The Gramm-Leech-Bliley Act

The Gramm-Leech-Bliley Act ("GLBA"), also known as the Financial Services Modernization Act of 1999, regulates the privacy protections of financial institutions that engage in banking, insuring, stock and bond trading, financial advice, and investing. The SEC has incorporated GLBA under Regulation S-P. This legislation was passed after a series of incidents in which credit card companies sold personal information, including credit card numbers, to companies that used this information in a fraudulent manner. Also, the European Union had enacted its own data privacy regulations in the form of the 1995 European Data Protection Directive. The Data Protection Directive required that when personal

information of EU citizens is transmitted abroad, the receiving country must afford the same protections as offered in the citizen's host country. This combination of domestic and international factors encouraged Congress to create legislation that protects the personal information of financial customers.

Under GLBA, financial institutions must take measures to protect the security and confidentiality of their customers' private information. This includes administrative, technical, and physical measures that will protect private information against any anticipated threats and unauthorized access. Financial institutions must provide all customers with information pertaining to their third-party disclosure policies. GLBA also requires that before financial institutions can release private information, they must first "clearly and conspicuously" offer customers an opt-out agreement. This gives more power to the consumer who can make the final and conscious decision whether he or she would like to share private information. However, disclosing complex privacy structures can be complicated for users to understand, due to consent forms being too long or too convoluted.

Even if a consumer does not opt-out and allows the institution to share private information, financial institutions are still prohibited from transferring account numbers or access codes, such as credit card and PINs, to any third party for marketing purposes. This safeguard is the result of multiple incidents of fraud emerging from companies buying credit card numbers and PINs from banks. As one example, concerns over the protection of sensitive customer information arose after the California-based Charter Pacific Bank of Agoura Hills sold the credit card information of hundreds of thousands of its customers to an adult website in 1999. The owners of the adult website stated that they intended to use the information to determine if their account holders had valid credit cards. Instead, the company charged the accounts for web-services they did not provide. In almost fifty percent of the cases, the credit card holders did not even own a computer. The FTC determined that over ninety percent of the company's total sales came from these unauthorized charges, totaling around $43 million. In 2000, the FTC won a $37.5 million judgment, representing the total amount of illegal charges minus the amount consumers received through chargebacks and credits.

There are still some pieces of information that consumers cannot prevent their financial institutions from sharing. Financial institutions may disclose personal information to regulatory agencies such as the Bureau of Consumer Financial Protection, the Secretary of the Treasury, a state insurance authority, the Federal Trade Commission, a self-regulating organization, or any law enforcement agency. Credit reporting agencies may also receive private information under the Fair Credit Reporting Act. Under The Fair and Accurate Credit Transactions Act of 2003, credit reporting organizations have strict guidelines on how long they can hold personal information and that they must destroy the information after a given time. Private information acquired through legal means by third parties may not be sold to additional parties. However, that information may be shared within the third party's own corporate family. Large corporations could use such private information within their own corporate structure, allowing for information to be used in ways the original customer did not intend.

B. SEC and the Securities Exchange Act Rules 17a-3 and 17a-4

Aside from consumer protection regulations, the SEC requires that financial records themselves are secure and private. Financial records must be sufficiently secure to satisfy the technical safeguard requirements of the Gramm-Leech-Bliley Act and Subsection 30 of Part 248, in other words, secure enough to "ensure the security and confidentiality of customer records and information." Pursuant to the Security Exchange Act of 1934 ("SEA"),Rules 17a-3 and 17a-4 describe the types of records and the data retention systems used by each member of the SEC that "transacts a business in securities through the medium of any such member, and every broker or dealer registered pursuant to section 15 of the

[SEA].” These rules give both an understanding of the type of transactions that must be recorded, how they are recorded, and the amount of time that these records must be kept.

1. How Data is Recorded

Rule 17a-4 states that records being preserved under 17a-3 and 17a-4 must be stored on either micrographic media or electronic storage. Micrographic media is defined as microfilm, microfiche, or any similar medium. While some financial institutions, such as Visa, Inc., still recognize microfilm and microfiche, those are increasingly uncommon media in the modern financial industry. The more prevalent storage method, electronic storage, has a far more complex set of regulations.

Electronic media storage is loosely defined as any digital storage medium or system that complies with SEA Rule 17a-4(f). This data must be stored in a non-rewritable, non-erasable format. The original data must be serialized and, if applicable, be stored on duplicate storage devices. The data must also be in a format which can be downloaded and handled by the Commission or any self-regulatory organization of which the data holder is a member. These regulations are fairly straightforward: original data should not be vulnerable to tampering, the data should be sequentially labeled with time-stamps, the data should have redundant storage options, the accuracy of data copied to another storage device should be verified, and the data should be searchable by approved third parties.

Data, as listed by 17a-4(f), is primarily recorded in WORM (write-once-read-many) media. WORM is a type of digital storage technology that only allows data to be written to a disk without the opportunity to modify or erase the data. Data is etched onto WORM disks which are then archived by the financial institution or third party company. The physical storage of these disks are costs borne by the financial institutions. Cloud service providers, such as Amazon Web Services, have begun offering off-site data storage options on servers that Amazon will lock themselves.

In late 2016, the Financial Industry Regulatory Authority (FINRA) imposed a $14.4 million fine on twelve financial institutions for failing to maintain WORM records. FINRA requires WORM formats as it prevents alteration of the firm's books and records. WORM formatted records also protect consumers’ private information from being overwritten or altered. In the case against the twelve financial institutions, FINRA noted that the exponentially increasing volume of electronic financial information has led to an increase in attempts to hack into electronic data repositories. These companies all had procedural deficiencies in their recordkeeping and three firms failed to retain certain broker-deal records that the company was required to retain.

2. What Data is Recorded

The minimum requirements for the types of transactions that must be recorded are listed under SEA Rules 17a-3 and 17a-4. There are many rules and requirements of what books and records must be maintained, as well as multiple exceptions to these rules. Generally, books and records are “books, accounts, records, memoranda, correspondence and other documentation or information,” that must be stored “in accordance with the federal securities laws, MSRB rules, FINRA rules and all other applicable laws, rules and regulations.” The recorded data is typically day-to-day business, or “business as such.” Recorded day-to-day business is a broad category and includes trade blotters, asset and liability ledgers, income and expense ledgers, capital account ledgers, customer account ledgers, securities records, order tickets, and trade confirmations.

3. How Long is the Data Retained?

There are not only requirements on how long data must be retained but also mandatory posting guidelines, i.e., how soon the financial transactions must be posted. Rule 17a-3(a) lists specific requirements for how fast books and records must be posted. Under the definition of "make and keep current," books and records must be posted "no later than the first business day following the transaction." Records should be maintained daily and updated to "maintain compliance" with the Customer Protection Rule and the Net Capital Rule. The Consumer Protection Rule states that a broker-dealer must keep a customer's assets separate from the broker-dealer's own proprietary activities. This rule protects customers from losing their assets should a broker-dealer suddenly fail. The Net Capital Rule requires that broker-dealers keep more liquid funds than the dollar amount of total customer assets. This ensures that broker-dealers will be able to cover customers for all liability if a broker-dealer fails.

The latest a transaction may be posted for "subsidiary ledgers relating to securities transactions, dividends, interest and securities borrowed and loaned," is two days following the movement of the money. Given the rules in 17a-3(a), it is clear that transactions must be posted quickly.

There are also many records that must be stored for years at a time. The broker-dealers under 17a-3 are required to retain certain records for at least three years, with the first two years "in an easily accessible place." Other records are required to be kept for not less than six years. The definition of "easily accessible place" is not precisely defined in Rules 17a-3 and 17a-4. The Broker-Dealer & Investment Management Regulation Group states that "easily accessible place" generally means that the records must be kept on the premise of the financial institution and are organized in such a way that finding specific records can be done quickly.

The regulatory length of time that these financial records are stored is best considered a balancing act by the SEC. On one side, the Self-Regulating Organizations and other investigatory agencies that conduct audits and investigations need access to files, including those over a period of several years. On the other, the extensive length of storage time may lead to greater risk for private information, spanning over a longer period of time, to be stolen.

III. Do Distributed Ledgers Comply With Financial Regulations?

Currently, WORM is the industry standard for compliance with financial recordkeeping regulations. It is striking how similar WORM is to previous storage methods such as microfiche or microfilm. Data storage has followed a similar trend since its origin on paper. Microfilm and microfiche records were smaller than paper and thus allowed for more data to be physically stored in one location. CD-R and DVD-R can hold more information than micro-documents and storage drives can hold more than CDs. The drive behind this trend is to first have a physical etching of the data and then to minimize the amount of space that etching takes up.

Distributed ledger technology may be a way to replace physical etching with cryptologic assurance. Rather than having a physical copy of the data, or multiple physical copies as regulations apply, data could be '"locked down" using math. Companies such as Amazon Web Services have already started this general trend. Amazon's Web Services offer Amazon Glacier as a remote data-storage option for SEA Rules 17a-3 and 17a-4 records. Amazon does not clearly state that the data it stores is physically written to a traditional WORM disk. Instead, Amazon assures the customer that his or her data is safe in Amazon's "vault." Data is locked by the customer after calling the Glacier API and initiating a remote VaultLock command. After

the data is locked, Amazon suggests that customers can “dust off [their] hands and stroll off into the sunset,” as their data will be stored “until the heat death of the universe.” Theoretically, Amazon is already using technology like distributed ledgers to store this financial information.

There are some benefits of using WORM storage methods. For example, WORM allows for real-time and permanent storage of data on a local device. Emails with financial details are required to be stored in WORM media. This is to prevent the deletion of any emails from the official record. A financial institution cannot have a system that collects all emails through the day but stores them only at the end of day, as users could delete emails mid-day. This is also why a company may not just compile a list of emails and then create a hash, later checking the hash to see if edits to the data have been made. This method is not WORM compliant since data may be deleted mid-compilation and the data itself is not secure. A WORM system will write the email's data to the disk as soon as it is processed. This is a nearly instantaneous process that allows for secure storage. Using distributed ledger technology for the secure storage of emails would be a more time-consuming process. In the case of creating an email blockchain, emails could not be received or recorded on the ledger until a nonce was created for a block of emails. This could take several seconds to minutes depending on the difficulty setting.

One problem that distributed ledger technology has when compared to WORM technology is delay. Bitcoin is a popular electronic trading commodity, but transactions may take half an hour or more to complete. This is on a public ledger with a tremendous amount of computing power being used to establish consensus. There are also only around 300,000 transactions over Bitcoin per day. Granted, the difficulty setting could be higher for Bitcoin than for other distributed ledger platforms. Still, the amount of time to complete consensus building for transaction blocks would likely be prohibitive. This is especially true for transactions such as stock trades, where transactions are measured on the millisecond. This could also be true for emails. Email users have become accustomed to sending and receiving emails instantaneously. Having emails written to a distributed ledger would require the emails to be delayed until consensus was reached.

A traditional ledger is a good example of how blockchain could be considered a retention method for financial documents. A ledger is a detailed compilation that records the final trades and transactions made over the course of the day. Ledgers include information on trades such as the price, time, order size, and if it was a buy or sell trade. Ledgers are a required record and are used by firms to review and confirm the transactions made over the past few hours or days.

Distributed ledger technology could be used to verify the validity of the transactions that have already occurred, creating an immutable record. The SEC and other self-regulating organizations must ensure that the records they are reviewing are accurate and have not been changed by anyone, including the bank itself. In this example, a bank has a few hundred thousand transactions that will be compiled by the ledger. Each transaction, after it is completed, is combined into a block. The bank's network then mines the block, creating a nonce for the series of transactions. Once the block has been mined, it will become practically impossible to alter.

These blocks would then become a trusted record for organizations such as FINRA and other self-regulating organizations. The bank itself will also be able to analyze the data in order to observe financial trends or to further other proprietary activities. The data will also remain private if it remains on a private network. Banks, especially big banks, typically have many branches with many computers. This property increases the privacy of the bank's customers. Bank branches may act as shared networks, combining computing power to complete nonces and verify the daily transactions. The banks will be more likely to have enough computing power to find nonces without outside help. Even if third parties add computing

power to find the nonce, existing regulations from the SEC and self-regulating organizations allow for third parties to hold private information of customers. Given sufficient computing power, banks would certainly be able to maintain records using distributed ledger technology.

Data maintained digitally using distributed ledger technology would be easier to store and analyze than WORM media. Data stored on WORM devices is limited and unless the WORM storage nodes are always connected to the same network, the bank must find and bring the data in separately. Data stored on the blockchain is not only immutable, like WORM media, but easily accessible by the owners of the data. This means that financial institutions and trusted third parties can use stored data for big data analytics or other products.

Conceivably, ledger blocks can also be on private networks to maximize customer privacy. In such circumstances, only nodes that are trusted by the banks may compute the blocks and would be the only ones that may view the data. The network might also extend to third parties in a consortium network. These third parties could include large corporations such as Amazon and Google, both with enough computing power to complement the financial institutions. These companies would be subject to the financial privacy regulations that the financial institutions must follow to ensure customer privacy. This model is arguably no less private or secure than the current WORM method. The greatest concern of using distributed ledger technology will likely be cost or transaction time.

Another idea would be to have the U.S. government give an incentive for financial corporations to use distributed ledger technology. Banks share computational cost with the government, which can then allow organizations such as FINRA and other self-regulating organizations to have access to the records. This would raise significant issues in customer privacy since the government would be a trusted node in the verification of transaction blocks. However, the government would also be able to conduct snap audits of financial institutions, increasing the overall privacy protection of companies for their customers. This might help solve a problem inherent in GLBA, namely: GLBA allows for financial institutions to have both “savings” and “investment” options for their customers, generously increasing the amount of business in which these corporations are able to participate. Allowing banks to grow so big so rapidly has been cited as one of the reasons banks are currently “too big to fail.” By allowing the government to conduct snap audits, banks and other financial institutions would be incentivized to take extra care in following the privacy regulations that already exist. On the other hand, customers may have concerns that the government will have access to their financial information. While this concern is understandable, customers currently do not have many privacy protections against government audit currently, and existing regulations protect against intrusion from private third parties, not the U.S. government.

IV. Distributed Ledgers in State Information Governance Policies

Perhaps the SEC and FINRA may draw inspiration from how other institutions are using distributed ledgers to solve problems with existing financial record keeping systems. The use of distributed ledgers and blockchain for information governance is not just a federal issue, and states are passing special legislation that will legitimize the use of these new technologies. For example, Colorado and Delaware are taking strides to encourage the use of distributed ledger technology within their states’ record keeping systems. It is important to note that although the use of distributed ledger technology is being encouraged, it by no means is ready to immediately replace existing systems. Instead, these new pieces of legislation are meant to supplement existing standards and to legitimize the use of new technologies as older systems are phased out. Legislators increasingly seemed inclined to accept that blockchain technology may well lessen existing issues inherent in current record keeping systems, while also allowing for newer concepts, such as smart contracts, to be more effectively utilized.

One goal of this legislation is to avoid the problem one Delaware court faced in 2013, involving a company's going private and buying back on the order of 36.7 million outstanding shares. However, due to “short selling and the high volume of trading during the three days before the closing of the merger,” eligible claims were made for over 49 million shares. In a 2017 memorandum opinion, Vice Chancellor Laster described the time and effort it would take within the existing system to determine actual ownership of shares as a “forensic audit of herculean proportions.” In the memo, Laster directly references distributed ledger technology as a “potential technological solution” for the problems inherent within the existing record keeping systems. As brokers and the Depository Trust Company (DTC) use distributed ledger technology more effectively, the previously herculean task may be reduced to days or even hours.

Delaware's recent legislation allowing corporate shares to be recorded on a blockchain has been effective since August 1, 2017. When a company decides to issue shares on Delaware's distributed ledger, those shares are validated by the Division of Corporations. In that genesis block, a perfect record of shares is created and subsequently tracked. In the current system, DTC tracks the ownership of shares through a Fast Automated Securities Transfer (“FAST”) Account, which digitally moves securities between DTC and transfer agents by holding the shares as a “fungible bulk.” FAST was implemented in 1975 after trade volume grew to the point where the physical movement and transfer of paper shares became physically impossible. At a high level, the problem is that Delaware's corporate law is “inherently inconsistent.” In a 2016 speech to the Council of Institutional Investors, Vice Chancellor Laster explained that Delaware state law is not designed for tracking shares held in fungible bulk and instead “assumes that stockholders own shares directly. . . .” Laster argues that distributed ledger technology would eliminate the need for an intermediary and instead shares would be openly tracked on Delaware's distributed ledger. Not only would this clarify property rights, but it would also make proxy voting more transparent and allow the distribution of dividends to be automated and accurate.

To stay ahead of the technological curve, the Colorado Senate has proposed a Bill which supports the use of distributed ledgers to improve a variety of industries within the state. In this proposed legislation, a director of the State's Office of Information Technology (OIT) would “annually assess the data systems of each public agency for the benefits and costs of adopting and applying distributed ledger technologies such as blockchains.” Privacy and security are in the forefront of this conversation, and the OIT will examine how blockchains are shared across jurisdictions. Government offices, including the department of state and the department of regulatory agencies, will also be required to consider adopting distributed ledger technologies.

While Colorado's legislation does not address any specific issue, it may serve to prevent problems like the ones faced by Vice Chancellor Laster in Delaware. Again, it is important to recognize that, from an overall perspective, existing systems of information governance employed by Delaware and Colorado are not failing, nor that blockchain technology acts as a silver bullet. However, as transactions grow more complicated and other technologies such as smart contracts become more prevalent, existing information governance systems will become obsolete and more akin to a “daisy-chain.” As explained by Laster, “[a daisy-chain] generally works under normal circumstances, but when the system comes under pressure, it breaks down. That should not be surprising. After all, what is a daisy chain? It's a chain of flowers. Under stress, daisy chains break.”

Conclusion

Distributed ledgers should be considered a valid storage method for particular financial records under the privacy regulations stated in SEA Rules 17a-3, 17a-4, the Gramm-Leech-Bliley Act, and other rules promulgated by financial authorities. The two main issues facing distributed ledgers are time and cost.

Unlike WORM media, creating blocks on a ledger takes time; a resource vital to many financial transactions. The cost of building the computational network to reach consensus may also be greater than storage costs imposed by traditional WORM methods. If this is the case, then it is may turn out that some companies will not be willing to adopt distributed ledger technology. These costs, however, may be negated due to the newfound ease in analyzing data on a network of distributed ledgers rather than on WORM storage media. Undoubtedly, the SEC and FINRA will be spending time examining this potential use of this new technology, and will take note that as the number of global transactions increase, distributed ledgers may step up to fill a future void. So too, the rapid rise of distributed ledger technology heralds a disruptive change in recordkeeping practices that institutions in all sectors of the economy will undoubtedly be examining in the very short term future.

Notes

No Notepad Content Found