LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Insurance And Regulatory Hurdles To Blockchain Adoption

By **Brian Scarbrough and Justin Steffen**
September 13, 2017, 2:18 PM EDT

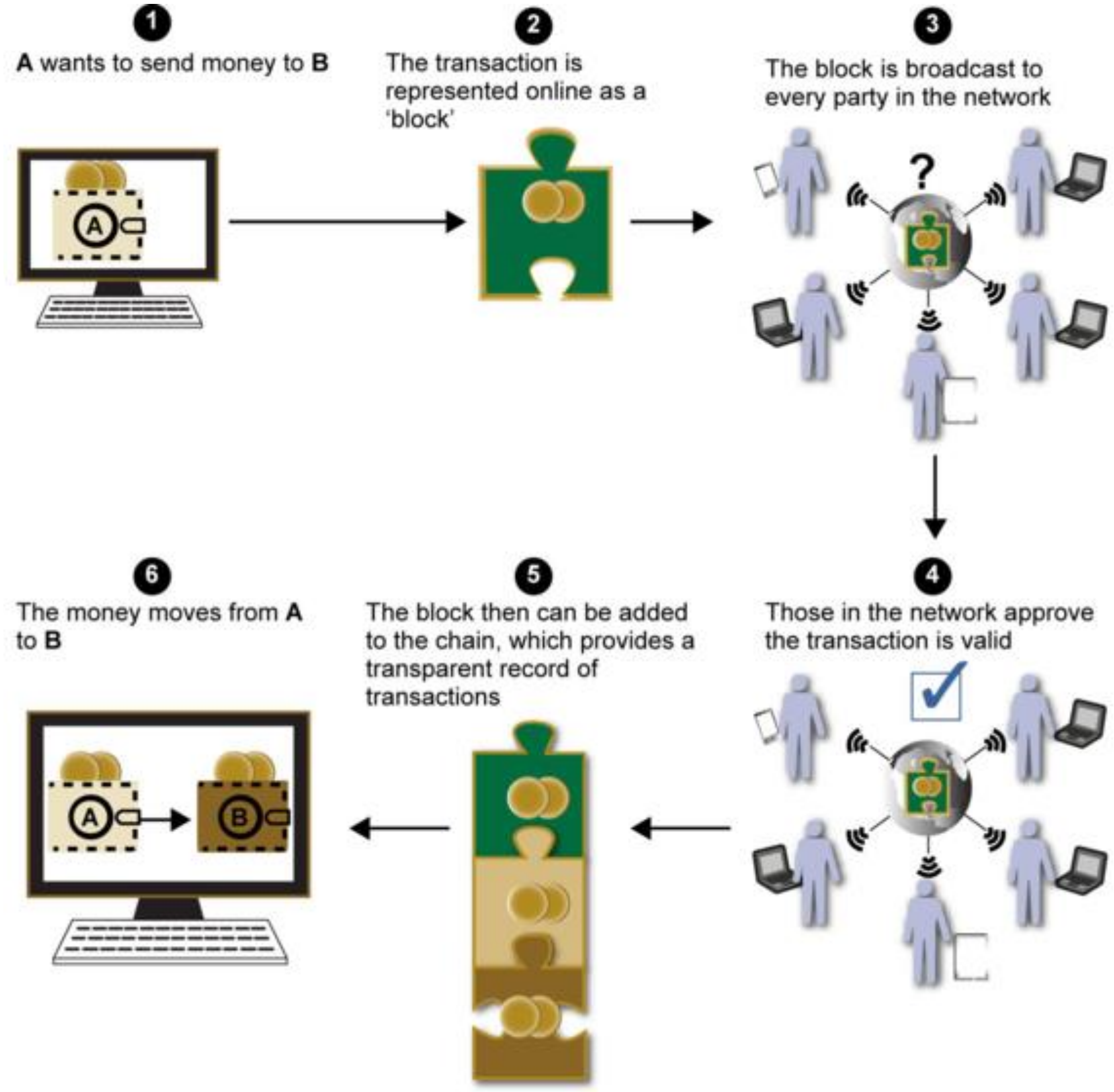
The blockchain craze is in full swing with diverse companies ranging from financial intuitions to auto manufacturers all seeking to utilize this exciting new technology. Blockchain, a type of distributed ledger technology (DLT), refers to a database that is shared across a network and was originally designed to record transactions of the cryptocurrency bitcoin.[1] Blockchain, however, has grown well beyond its cryptocurrency roots, leading proponents to suggest that the technology can aid in everything from securities settlement to voter registration to supply chain tracking. The excitement for enterprise uses of blockchain technology is palpable. But will insurability and regulatory issues derail this momentum? Not if institutions seeking to deploy this technology recognize the risks.

Brian Scarbrough

The Rise of Blockchain

Justin Steffen

Blockchain technology was born out of Bitcoin. In 2008, Satoshi Nakamoto penned a white paper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System.” In addition to describing the digital currency, Bitcoin, the paper also described the blockchain technology that supported it and would prevent individuals from spending their bitcoin more than once. In brief, a blockchain is a digital ledger that is distributed across a network of replicated databases known as nodes. Once a digital transaction is carried out, that transaction is grouped with other transactions and transmitted to the network.


1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
A
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides a transparent record of transactions
6
The money moves from A to B
A
B

Source: GAO. | GAO-17-361

Although there are different blockchains and different types of blockchains (permissioned, public, etc.), when most people use the term “blockchain,” they are referring to public blockchains such as Bitcoin. Blockchain derives its name from the method of validating and memorializing transactions that the Bitcoin blockchain utilizes. For Bitcoin, network members, known as miners, compete to record transactions by solving complex coded problems. Once a miner solves the problem and validates the block, the solution and block are sent out to the network. If the majority of miners agree, the miner that solved the problem receives a reward, the block of transactions is added to the encrypted ledger of previous transactions blocks, and a new transaction block is begun.[2] Blockchain is often used to generically describe all forms of distributed ledgers, regardless of whether transactions are validated and stored in a way similar to the Bitcoin blockchain.

Blockchain technology has many advantages. Blockchains can streamline burdensome, manually intensive reconciliation processes, thereby reducing overhead costs. Blockchains can improve resilience by spreading information among multiple hubs or “nodes” that are unlikely to crash or be hacked simultaneously. In addition, blockchains are transparent and therefore render information verifiable by numerous parties, and blockchains offer efficiency and allow for the elimination of third parties from many transactions. Blockchains may also enable faster and more accurate transaction settlement and could enhance security by ensuring that records cannot be altered.

Given these advantages, companies have adopted and augmented the original blockchain technology. The Ethereum blockchain, for example, is an open-source, blockchain-based platform that facilitates smart contracts (computer coded contracts in which the parties have defined functions that will automatically execute upon the happening of predetermined criteria). Indeed, blockchains are no longer one-size-fits-all. Rather than being public like Bitcoin, there also are permissioned or private ledgers, which may provide the security that regulated entities like banks prefer. And there are hybrid blockchains, blockchains that allow for dispute resolution, tokenless blockchains (ledgers that do not require a currency or token to function), and more.

Although commonly associated with Bitcoin, blockchain technology is not merely a ledger for recording digital currency. The possible uses for the technology are truly dizzying. Blockchain technology could enable pharmaceutical companies to track the movement of prescription drugs throughout the country, facilitate instantaneous clearing and settling of securities transactions, provide for a digital identity that will protect consumer privacy, and allow healthcare providers a means of maintaining a decentralized patient records system, just to list a few possible applications. Proponents have gone so far as to suggest that blockchain can change the world, representing an “internet of value” — where currency and other digital assets can move as freely as information does today.

Blockchain or DLT, however, is not without its drawbacks. Blockchains, for example, may still be subject to hacks and unforeseen occurrences, or experience bugs as demonstrated by the 2016 DAO hack in which a hacker exploited a vulnerability in the source code to misappropriate millions in Ether.[3] Blockchains based on the limitations of the Bitcoin blockchain may have issues with scale, and blockchains face regulatory uncertainty as regulators have almost universally adopted a wait-and-see approach with the technology. The relative newness of this technology may also be a drawback as companies’ legacy insurance policies may predate blockchain or DLT or may not have been drafted with an understanding of blockchain’s import.

Where Are All The Regulators?

For years, regulators in the United States abstained from regulating blockchain and DLT. Where agencies offered guidance, that guidance was often disjointed. Bitcoin and other virtual currencies, for example, are property according to the IRS, currency according to FinCen and a commodity according to the CFTC.[4] Regulators’ initial inaction, however, should not be mistaken for a lack of interest. The CFTC, SEC and the Federal Reserve all created blockchain working groups.

Recently, the SEC examined The DAO, an unincorporated organization with the objective of operating an Ethereum-based for-profit entity that would fund projects curated by Slock.it UG, described above in more detail. In its July 25 report, the SEC concluded that The DAO token sales violated federal securities laws and warned industry participants that “the federal securities laws apply to those who offer and sell securities in the United States, regardless whether the issuing entity is a traditional company or decentralized autonomous organization, regardless whether those securities are purchased using U.S. dollars or virtual currencies, and regardless whether they are distributed in a certificated form or through distributed ledger technology.” The SEC’s report portends regulation of token sales or initial coin offerings and of cryptocurrency exchanges.

State regulators, likewise, have begun promulgating laws and regulations aimed either at promoting, defining or limiting blockchain technology, primarily in the cryptocurrency space. Delaware, Arizona, Nevada and Vermont have all pursued blockchain initiatives. Nevada, for instance, recently passed a bill that would prevent the taxation of blockchain, and the Delaware assembly passed a law legalizing blockchain-based stock trades.

Mirroring regulators' increased interest in cryptocurrency and token sales, regulators' interest in blockchain will only intensify, and they will begin to issue more regulations aimed at companies employing blockchain or DLT. What those regulations will ultimately look like is still unclear. Forthcoming regulations, however, will likely focus on a couple of key areas: security, privacy and confidentiality, and know-your-client and anti-money laundering requirements.

First, regulators may focus on whether businesses are protecting consumers and properly securing digital assets. Blockchains, such as Bitcoin, often use public and private keys. Individuals who wish to transact in bitcoin, for example, may maintain their own private keys or they may rely on a third party vendor to secure their private keys. These third parties are subject to attack, and there have been several high-profile hacks. Crypto-exchange Bitfinex announced a security breach in August 2016 that resulted in the loss of 120,000 bitcoin — then valued at $72 million. Bitfinex was fined by the CFTC and the exchange offered its own BFX tokens in exchange for the losses suffered by its customers.

Second, although individuals on public blockchains can remain anonymous, the public nature of the transactions themselves pose privacy and confidentiality issues that may draw regulators' attention. Perhaps anticipating these concerns, a number of innovators have sought to create technological solutions to preserve confidentiality and privacy on public blockchains. Some, for example, utilize zero-knowledge proofs that could preserve the confidentiality of certain data. Similarly, the R3 Consortium announced that it has partnered with Intel to use Intel's new Xeon Scalable Processors and will incorporate the hardware into its open-source Corda platform. The Xeon Processors are designed to provide a layer of hardware security. Regulators may demand that such technologies be utilized by or made available on open blockchains and may exercise oversight over participants in permissioned or private blockchains to ensure that all participants are complying with data privacy and other regulations.

Finally, for those financial institutions that utilize blockchain technology for money transfers, money transmission, securities settlement and smart contract transactions, regulators will almost certainly require that companies ensure that they comply with know-your-client and anti-money laundering requirements. Having a robust compliance program, therefore, will continue to be a must — even for companies dealing with crypto assets.

Not only is the nature of domestic regulation uncertain, but the means by which regulation will be conducted is also unclear. Regulators may interpose themselves directly onto a blockchain by, for example, maintaining a node on a network — enabling the regulators to observe transactions in real-time. Regardless of what form regulations take or how those regulations are enacted, however, regulators will take action. Once they act, companies using blockchain technology will have to accommodate new rules and navigate the heightened scrutiny. Increased regulation will unquestionably entail increased expenses, at least in the near term.[5]

Do I Have Insurance For Blockchain or DLT Exposures and Value?

Blockchain and DLT also may raise a number of questions as to insurance coverage. For example, is there a difference in exposures or value in insuring a decentralized business or business process relying on blockchain technology rather than a centralized one? Does possible lack of control over all nodes on a blockchain impact this exposure and value? Relying on software and hashing functions built into blockchain or DLT code may raise privacy and confidentiality exposures, which a company may want insurance to cover. And then there is the question of how to value cryptocurrencies like bitcoin relying on blockchain or DLT.

Various types of insurance policies could be relevant to cover these exposures and value. Below is a brief list.

- Cyberinsurance policies (both first-party and third-party), including for data breach response costs, system failure, system interruption, cyberextortion, data corruption or lost digital assets certainly could be relevant. For example, some insurers already have added language to cyberextortion / ransomware policies to include Bitcoin, other cryptocurrencies and the use of blockchain technology as a covered form of ransom payment.

- Commercial crime insurance policies covering loss through computer fraud, theft and social engineering by employees or third parties also could be relevant. If digital assets are stolen, will these policies respond?

- Errors and omissions and professional liability insurance policies for loss resulting from services provided to customers are another type of insurance to consider. This could be relevant for instance if you are implementing or servicing via blockchain or DLT and there are coding errors.

- Directors and officers insurance policies for liability at the board level or key executive level also should be considered. Management or company boards could face liability exposures for their involvement, or lack of involvement, in implementing and overseeing a company's use of blockchain or DLT, particularly if hacking or other security incidents occur.

- Finally, property and business interruption insurance policies should be considered if blockchain or DLT is integral to the functioning of your business. While cyberinsurance policies may cover loss from network or computer system interruption, if a company suffers physical damage to its computer systems components or other tangible property or suffers business interruption loss due to physical damage to such property or the property of others (for example due to fire or natural disasters), commercial property insurance may cover the loss.

As to any type of insurance policies, there are a number of key considerations. Do the policies exclude coverage for cryptocurrencies or digital assets? Are cryptocurrencies or digital assets affirmatively included in coverage (e.g., in the definition of money in crime policies or cyberextortion policies)? Are there electronic data exclusions? Are contractual exposures excluded? In addition, it is crucial to examine whether there is the ability to transfer risk through contracting with third parties rather than relying solely on insurance.

Given the broad applications for blockchain, this is not just a fintech issue. Indeed, any business that incorporates, relies upon or is considering the use of blockchain and DLT, including smart contracts, should consider their insurance situation. This includes insurance brokers, who increasingly are utilizing this technology as part of their brokering and risk management servicing platforms.

Conclusion

It’s still early, but blockchain and DLT offer promise to truly alter the financial services landscape, as well as change a diverse array of traditional businesses outside the financial arena. Regulators are already interested, and will continue to act, and companies will need to be ready. Similarly, companies can prepare by reviewing their current insurance policies to understand if they would cover blockchain and DLT exposures or risks and if not, broadening them or placing separate coverage to include this technology and the value and exposures that come with it.

Brian S. Scarbrough is a partner with Jenner & Block LLP in Washington, D.C., and Justin C. Steffen is a partner at the firm's Chicago office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] “Bitcoin” with a capital “B” is used to refer to the Bitcoin ecosystem as a whole, whereas “bitcoin” with a lower case “b” refers to the cryptocurrency.

[2] This is known as a “proof-of-work” system. Other blockchains may utilize a “proof-of-stake” system or another means of validating transactions.

[3] The Distributed Autonomous Organization (DAO) was an investing fund set up on the Ethereum blockchain through a smart contract. The terms of the smart contract governing the DAO provided that the entirety of the relationship between the parties was set forth in the computer code. A hacker did not alter the code but simply identified a way under the existing code to expropriate $60 million for himself. Ethereum performed a hard fork to return the ill-gotten Ether value from the hacker to the DAO, resulting in two distinct blockchains.

[4] Regulators’ varying definitions for virtual currencies are not surprising as tokens and cryptocurrencies have a variety of potential uses: currency, communications networks, a means to transfer value, etc.

[5] Although regulation often has necessitates additional costs in the short term, it may also have many long-term benefits. If regulators have their own node on the network or regulate platforms instead of individual participants, for instance, regulators may be able to more efficiently enforce their regulations and individual companies’ compliance costs in the long-term may actually decrease. In addition, clear regulation can actually increase investment in technology as many investors may be waiting until there is more regulatory certainty. After Japan issued a bill mandating the regulation of bitcoin and other virtual currencies last May, trading rose exponentially.
