BUSINESS LAW TODAY

Blockchain: Tapping Its Potential and Insuring Against Its Risks

By Lorelie S. Masters, Sergio F. Oehninger, and Patrick M. McDermott

Blockchain is the distributed ledger technology (DLT) behind Bitcoin, Ethereum, and other cryptocurrencies. Blockchain is widely believed to be a game-changing trend for global business across sectors. Blockchain has been described by the creator of Bitcoin as a "peer-to-peer network using proof-of-work to record a public history of transactions" and by *Forbes* as "a distributed and immutable (write once and read only) record of digital events that is shared peer to peer between different parties (networked database systems)." In other words, Blockchain is a record of peer-to-peer (P2P) digital transactions categorized into blocks by a decentralized network of computers. Each transaction is time-stamped, encrypted, and linked to its preceding block, creating a "blockchain." Each new block added to the chain must be validated by a consensus among the network of participants.

"Disruptive" Potential of Blockchain

The potential disruptive uses of blockchain technology in the marketplace have been compared to that of the Internet. The possibilities of blockchain are said to be endless across all industries, including fintech, health care, analytics, retail, energy, manned and unmanned vehicles, insurance, and the sharing economy. Over time, corporations using blockchain combined with artificial intelligence (AI) and the Internet of Things (IoT) will likely be able to better integrate their business partners and suppliers into the network, giving them a complete view of the supply chain and enabling them to conduct all transactions inexpensively, transparently, and securely through blockchain.

In June, a number of international banks selected a multinational technology company to use blockchain technology to build an international trading system called Digital Trade Chain. According to an Accenture and McLagan report, blockchain may "reduce infrastructure costs for eight of the world's 10 largest investment banks by an average of 30 percent, translating to $8 billion to $12 billion in annual cost savings for those banks."

A major automobile manufacturer has partnered with MIT's Media Lab and others to identify the uses of blockchain technology in the automobile industry. A global retailer teamed up with a multinational technology company and recently announced the results of a test using blockchain technology in which it traced a food product from farm to shelf in seconds, as compared to the days-long process without blockchain technology.

The Blockchain Insurance Industry Initiative B3i, which includes global banks and financial services companies, is exploring the application of blockchain technology in the insurance sector. In June, a major insurer and a major multinational technology company announced a successful pilot program of a blockchain-powered "smart insurance policy." Such smart insurance policies would be designed to execute the contract terms when specified conditions are met, provide for data continuity, trace the origin of a risk, and reduce fraud, among other benefits. In addition, numerous start-ups are marketing their blockchain-based platform to health care companies.

Security of Blockchain?

Because changes to a blockchain are displayed in real time and no central user controls the record, blockchain is said to be much less susceptible to hacking than a traditional database. For instance, if hackers wanted to modify information in a blockchain, they would first need to hack into both the specific block and all of the preceding and ensuing blocks in the blockchain across every ledger in the network at the same time.

Because consensus among the network participants is required, the hackers' change would likely be rejected as it would conflict with the other ledger entries on the network. Many observers believe this leads to an unparalleled level of security.

However, blockchain technology, like the Internet before it, will likely lead to unforeseen risks and exposures. For example, in 2013, Mt. Gox, a Bitcoin exchange handling 70 percent of all Bitcoin transactions at the time, suffered a technical glitch resulting in Bitcoin's temporarily shedding a quarter of its value. That technical glitch was a fork in the blockchain, which resulted from the use of differing versions of the Bitcoin software. In 2015, Interpol identified an opening in blockchain used for cryptocurrencies that hackers could exploit to transfer malware to computers. In addition, blockchain is only as secure as its entry points. If the access systems used for blockchain are vulnerable to attack, the technology's security may be undermined. In sum, blockchain is not risk-free and may not be hacker-proof. Given the value and potential high profile of transactions that may take place using blockchain technology, hackers will have incentives to invent new ways of using the technology for malicious purposes despite its protections.

Insuring the Blockchain

Because blockchain technology is not risk-free, companies should consider how their insurance policies, especially their cyber insurance policies, can protect against risks arising out of the use of blockchain technology—and whether they include provisions that could be used to deny coverage for claims with a connection to blockchain technology. For instance, one insurer's cyber insurance policy form insures against disclosure of personally identifying information that results from unauthorized access into a system owned by either (a) an insured; or (b) "an organization that is authorized by an Insured through a written agreement to process, hold or store Records for an Insured." Because blockchain is peer-to-peer, the insurer may argue it is not owned by any insured or any other "organization." Thus, a policyholder experiencing losses due to the disclosure of personally identifying information arising out of the use of blockchain technology may face a coverage dispute with its insurer.

As another example, another cyber insurance policy form provides coverage for the "failure or violation of the security of a Computer System," and defines "Computer System" to include "cloud computing" and "other hosted resources operated by a third-party service provider." It is not clear whether the insurer would consider blockchain technology to fall within this definition, particularly because blockchains are peer-to-peer networks not operated by a central administrator. Policyholders also should review exclusions in cyber policies carefully, including those for accessing unsecure websites, self-inflicted losses, terrorism, and others.

Finally, policyholders should consider whether coverage for blockchain-related risks remains available under their traditional policies, such as technology professional liability policies, commercial crime policies, and specialty coverage forms. They should specifically review cyber, computer or technology, and data-related exclusions.

Conclusion

As the use of blockchain technology grows, cyber policies will adapt and begin to incorporate language addressing blockchain technology. However, the complexity of the technology, the lack of understanding of it, and the scarcity of data about its use may impede the development of the market for insurance covering operations or transactions involving blockchain. Nonetheless, as insurers increasingly conduct blockchain scenario analyses, follow developments in blockchain and related technologies, and improve their own understanding and analysis of blockchain's risks, policyholders can expect them to offer new policies covering such risks. In the meantime, policyholders looking to conduct business using or involving blockchain should consider consulting experienced coverage counsel and carefully reviewing the policies they buy to ensure that those policies provide the insurance protection they need.

Lorelie S. Masters is a partner with Hunton & Williams based in Washington. A nationally recognized insurance coverage litigator, she handles all aspects of complex commercial litigation and arbitration. Lorie has advised clients on a wide range of liability coverages, including insurance for environmental, employment, directors and officers, fiduciary, property damage, cyber, and other liabilities.

Sergio F. Oehninger is counsel with Hunton & Williams based in Washington. He counsels multinational corporations on insurance coverage and risk-management issues arising in various industries, including financial services, retail, manufacturing, energy, technology, and real estate.

Patrick M. McDermott is an associate with Hunton & Williams based in Washington. His practice focuses on complex civil litigation matters, with an emphasis on insurance coverage disputes.