Understanding the Risk of "Immutable" Blockchain Applications

by Stephen Palley

When faced with new technological risks and problems that they pose, courts have historically risen to the challenge. Take electricity, for example, and more particularly, the liability for exposure to uninsulated electrical wires, which was the subject of a case decided by the Kentucky Supreme Court in the first year of the 20th century. Although the fact pattern was new, the court was still able to rule. It presented the issue thus: "Did the fact that the gas company supplied the harmless wires with the force that converted them into a death-dealing agency make it responsible for the inury which resulted in the death of the intestate? The exact question submitted has not, so far as we are aware, been answered by any court of last resort." (*Thomas v. Mayville Gas Co.* 108 Ky. 224 (1900)). The court applied existing precedent and concluded that the gas company should have insulated the wires and was in fact negligent.

Risk managers have it harder than courts, who sit in judgment after the fact. One of the challenges a corporate risk manager faces is to anticipate risk and responsibility without clear precedent or a specific fact pattern. This task is made easier by understanding how new technology operates and where unanswered questions may exist. To that end, we focus here on emerging technology risk associated with blockchain technology, in particular the creation of so-called "unstoppable" and "immutable" blockchain-based software.

At its simplest, blockchain can be thought of as an "append-only" distributed database, with no central server, and with no ability to change or modify a record once added. Depending on the blockchain protocol used, the technology can be used to store static data—raw information—as well as executable code that will be triggered after certain amount of time passes or an external event triggers. The inability to change information or code once added to blockchain is sometimes referred to as "immutability."

Blockchain technology has many potential use cases for enterprises. The simplest, and perhaps best known, is as a substitute for state-issued money. Bitcoin, Ethereum and other cryptocurrencies have been touted as a means to expedite electronic payment and to make cross-border remittance without bank intermediaries possible.

The technology has also been touted as a way to bring transparency to business relationships. Supply chain applications are an example. Using a blockchain infrastructure to track production, delivery and sale of products, all participants can have equal access to the same data and (at least in theory) the ability to reduce commercial friction and speed payments. Corporate giants as varied as Walmart and Maersk, to name a few, have thus announced blockchain projects.

Another way that blockchain technology has been touted for businesses is in the use of so called "smart contract" technology. Just like a centralized database system, blockchains can contain executable code in addition to static data. This provides users with the ability to create unstoppable, unchangeable applications that can guarantee certain types of contract performance upon the occurrence of specified events. There are a number of existing examples in the insurance industry. For example,

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

October 2018

the blockchain-based insurance company Etherisc offers "smart contract" flight insurance policies built on the Ethereum blockchain that guarantee claim payments in the event that flights are late. Because of the use of blockchain technology that cannot be altered by the insurance company, claims are paid automatically where an insured's flight is reported as late by a trusted third-party data source (sometimes referred to as oracles).

THE RISKS OF IMMUTABILITY

On the one hand, there are powerful advantages to a distributed programmable database that all participants have equal access to and that no one can unilaterally change after the fact. On the other hand, a database that cannot be edited and software that cannot be turned off present unique and, in some in cases, potentially troubling risks.

One example of immutability risk involves something called "the DAO Hack," in which a decentralized investment fund, created on the Ethereum blockchain in 2016, raised more than $150 million in cryptocurrency. Soon after its launch, however, an error in the DAO code allowed a user to move nearly a third of those funds to their own control. Because the code was public but "immutable" it was impossible to stop the hack while it was happening while remaining true to the concept of immutability.

In order to make investors whole, participants in the Ethereum ecosystem agreed to "hard fork" the Ethereum protocol, effectively reversing time and returning the blockchain to a prior state (where the hack had not occurred). This was a controversial decision among members of the Ethereum community, and resulted in the creation of two rival Ethereum blockchains—Ethereum and Ethereum classic.

The creation of a second blockchain was a financial windfall to some, as holders of ether (the native cryptocurrency of Ethereum) at the time of the hack were suddenly also holders of ether class (the native crypto-currency of the Ethereum Classic blockchain). But the ability to "fork" a distributed "immutable" blockchain creates a quandary: Imagine immutable and "unstoppable" code on one blockchain that has now been copied to a new blockchain. If that code interacts with assets that are not contained on the blockchain, users face the risk of the same automatic contract performing multiple times.

Another example of immutability risk involves a cryptocurrency wallet called Parity. Crypto-currency like bitcoin and ether is in effect a bearer instrument, where control over the asset is determined by whoever knows and has possession of a cryptographic private key—a series of letters and numbers. In order to manage cryptocurrency assets, users rely on software and hardware wallets to hold, receive and send their holdings. Parity is one of the major software crypto-currency wallet providers for ether. Due to a vulnerability in a software library many wallets relied upon, approximately 514,000 ether wallets were permanently frozen and lost to users in the fall of 2017, resulting in a loss of approximately $150 million. As with the DAO hack, this hack involved "immutable" distributed software—the only way to recover funds would be to convince participants in the Ethereum community to again fork this supposedly immutable blockchain. To date, that has not happened.

A third risk arises from active participation in a blockchain as a "miner" or "node." While this seems like it might not apply to enterprises, depending on the technology used, the nature of participating in a blockchain project can actually entail involvement in this capacity. This is particularly true when private blockchain software is being used to create a proprietary and closed ledger. At the risk of oversimplifying, miners are responsible for adding data to a blockchain. Nodes store that data and make it available to the world. Immutability raises other concerns when we are dealing with data. If adding or possessing certain information or data is illegal, distributing that material globally to a shared distributed database that cannot be edited or revised potentially magnifies risk rather than removing it. If something is infringing or illegal sitting on a private server, or on the cloud, it is hard to understand how distributing it everywhere in the world in an immutable form does anything to limit or restrict that risk.

MANAGING BLOCKCHAIN RISKS

While risks associated with blockchain technology may be new, they can be managed, mitigated and avoided by understanding the way the technology is used. Sometimes the most useful

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

tools in a risk manager's tool kit are "w" questions: What is it? Why are we using it? Where is it located? These questions, along with a basic understanding of the technology, can help manage technology risks in a rapidly moving space like those presented by blockchain.

At a more basic level, one can ask what insurance policies might apply if a business plans to work with blockchain technology. We have begun to see the development, for example, of insurance policies and products for cryptocurrency, for those businesses that choose to accept or hold these assets. In 2015, ISO amended the commercial crime policy form to include a specific exclusion for virtual currencies that applies to "loss involving virtual currency of any kind, by whatever name known, whether actual or physical including, but not limited to, digital currency, cryptocurrency or any other type of electronic currency." Coverage can, however, be added back for scheduled virtual currencies by endorsement. Cryptocurrency exchanges like Gemini and Coinbase have also announced success in securing coverage for virtual currency assets, suggesting that insurance markets may become more comfortable with this risk.

Whether or not insurers become willing to take on more esoteric blockchain risks like the immutability issues raised above remains to be seen, but if the technology is here to stay it seems likely that insurers will adapt with it. ■

Stephen D. Palley is a partner in the Washington, D.C. office of Anderson Kill. He is co-chair of the firm's Blockchain and Virtual Currency Group and a member of the Insurance Recovery Group.