FOLEY & LARDNER LLP

How Does Blockchain Come Into Play in a Pandemic?

Joanne Molinaro
13 April 2020

Legaltech News
While at-home investors and big-dollar funds are keeping their eyes on Bitcoin during the unprecedented economic effects the global pandemic continues to cause across the globe, crypto-experts are contemplating the obvious: Could blockchain—the technology underlying Bitcoin—be the answer to the next bi pandemic?

What Is Blockchain Technology?

A blockchain is an incorruptible digital ledger of transactions that can be programmed to record almost anything of value. Digital data is recorded in "blocks," each of which is assigned a unique "hash." The hash serves as an identifying "seal" that ensures the data on the block have not been corrupted. Each block also contains on it the hash of the *preceding* block, which is what allows for the formation of a "chain." If one attempts to change the data residing on a given block, a new hash will be generated for that block and the chain will be broken, since the hash of the block coming *after* the tampered block will no longer reflect the correct hash. This is one of the features that make a blockchain virtually "unhackable."

A key attribute of a blockchain is that the data is *shared* or "distributed." Imagine a shared spreadsheet (like a Google doc) containing digital data (the digital ledger) that is duplicated thousands of times and distributed to numerous different computers (or "nodes") on a vast network. A copy of that spreadsheet is updated every time a single item is changed. When a change is made to the document, a notification is sent to all the nodes and a new version of the spreadsheet is redistributed to those computers—each of which stores its own copy of the same spreadsheet, including *every* version of that spreadsheet from its creation. Because each node on the network stores its own copies of every single historical version of the entire spreadsheet, there is no *one* "central" repository or administrator of the data. Rather, the distributed ledger is "decentralized."

Here is how blockchain is different from a "shared" spreadsheet: If someone tries to go back into the historical record and delete or change something, each of the nodes will refer back to its own repository of historical data, note the discrepancy that the proposed change would create, and *reject* the data from being written onto the "spreadsheet." Thus, the more "nodes" or computers there are to monitor the integrity of the data being written onto the blockchain, the more secure that blockchain is.

Let's apply the above analogy to a pandemic. Think of a Pandemic [P-1] blockchain as a very large

spreadsheet that contains each instance when a new case of P-1 is contracted. Each new transaction of P-1 contains a cryptograph (to ensure some privacy) of the person who contracted P-1, when it was contracted, where they reside, and information regarding with whom they've been in contact.
The transaction also includes the entity that wrote to the blockchain, as well, to ensure some mechanism for verifying the data. This is key—the utility of blockchain (like any other digital ledger) is only as good as the data written onto it—and given the nature of the data that would reside on the P-1 blockchain, one important way of ensuring integrity would be to "validate" the users writing onto it.

Let's assume that the data is verified and ultimately written onto the P-1 blockchain. Once that "block" of data is added to the chain, all the nodes to that blockchain (i.e., the computers that keep a record of the sprawling spreadsheet) instantly receive an updated record of an unbroken chain of all P-1 transactions. No one can subsequently change the data written onto that block without breaking the chain, and anyone with access to the blockchain will be able to trace where and how quickly P-1 travels.

Real Use Cases in Light of COVID-19

Acoer, a startup located in Atlanta, Georgia, is a software development firm specializing in open source and blockchain solutions. Recently, Acoer has pivoted its HashLog data visualization engine—originally designed for data analytics about clinical trials, dementia, and mortality data—to provide insight on the spread of COVID-19.

As the coronavirus pandemic has revealed, contact tracing is just one facet of data that can be useful in fighting a public health crisis. For instance, price gouging has not only made it impossible to find things like hand sanitizers and toilet paper, in some hospitals medical professionals are being forced to care for patients without proper protective equipment.

In order to counteract this pernicious effect of COVID-19, the Dutch government has deployed blockchain technology to bring transparency to the medical equipment supply chain. Specifically, the blockchain will provide an ecosystem that helps to "match supply and demand," thus "preventing predatory value extraction, such as price gouging, amid the coronavirus pandemic." Given the extraordinary disruption to supply chains across nearly all industries, blockchain can be used not only to combat COVID-19 directly, but the indirect economic effects as well.

Potential Issues with Blockchain Deployment

The security of any blockchain and the reliability of that data written onto a block is, in large part, a function of immutability and transparency. Unfortunately, these two factors run, headlong, into privacy laws. Once written onto a blockchain, the data resides on the blockchain forever. But regulations like the GDPR require that personal data be retained for no longer than is necessary for the purposes for which it was processed. How can blockchain square with patients' rights to have their data deleted?

The immutability of data is a function of decentralization. Therefore, to provide for a "delete button" on

blockchain data, the blockchain would need to become less decentralized. These blockchains are dubbed "permissioned" blockchains or "consortiums," where the nodes are not anonymous, access to the blockchain is subject to the consent of other participants, and the data may be more susceptible to change. However, as decentralization diminishes, so too will all its benefits, namely security. With fewer nodes tasked with maintaining the integrity and security of the data, the more vulnerable to hacking the data become.

Still, as evidenced by startups like Acoer, consortiums appear to be the best answer in times of crisis. And, as the saying goes, beggars cannot be choosers.