

## A BRIEF HISTORY OF BLOCKCHAIN

While many have invested in bitcoin, few really understand the underlying blockchain technology, which could be 'the largest technological expansion since the Internet.'

BY LEWIS POPOVSKI AND GEORGE SOUSSOU, PATTERSON BELKNAP WEBB & TYLER

When Bitcoin entered the market in 2009, the value of one bitcoin was \$.06 and few noticed. When the price of one bitcoin rose above \$19,000 in December 2017, it and its underlying “blockchain” technology became the newest buzzwords and took the world by storm. Just adopting the word “blockchain” seemingly created value. For example, when Long Island Iced Tea, a company that sells beverages, changed its name to Long Blockchain Corp. in 2017, its stock price rose almost 300 percent in one day even though it had yet to actually be involved with blockchain. While many have invested in bitcoin, few really understand the underlying blockchain technology, where it came from, and where it is going.



### The Beginning

It is widely believed that the first implementation of modern day blockchain technology came from Satoshi Nakamoto. In 2008, a person or group of people identified as Nakamoto published a paper, “Bitcoin: A Peer-to-

Peer Electronic Cash System,” which hypothesized a direct online payment from one party to another without the use of an intermediary third-party. The paper described “an electronic payment system based on cryptographic proof instead of trust.”

The paper sought to solve the problem of double spending. That is, the very nature of digital currency allows it to be easily duplicated and spent more than once. The resulting uncertainty was fatal to the adoption of the technology. The Nakamoto paper solved this problem by linking every transaction to the transaction preceding it in a tamper-resistant manner. The tamper-resistant manner described by Nakamoto was the public ledger. With this ledger, a network can examine the transaction history of an electronic coin that a user submits for payment, and can confirm that the coin has not already been spent, thereby preventing the “double spending” problem.

Blockchain is a type of database that is duplicated on many computers or “nodes.” All of the nodes have the same information on them. This is vital to the success of the blockchain technology. The information is stored in, as the name implies, blocks. Each block can contain multiple transactions, with each transaction having a unique reference number, a time stamp,

a pointer to the immediately previous transaction, as well as information on the transactions themselves. In this way, each node has access to all previous blocks down to the first block of the chain called the “genesis” block. The time stamp gives each block an immutable temporal position in the chain.

A hypothetical transaction exemplifies the way blockchain works. In the context of a sales contract, a seller agrees to sell a widget to a buyer for one “coin.” In a network of computers, one node (buyer) broadcasts code that will automatically deduct one coin from the buyer’s account and add it to the seller’s account as soon as the seller ships a widget to the buyer. A smart contract is born. That is, the execution part of a contract was reduced to code that is implemented by computers and verified by a community of computers before it is immutably added to the database. As soon as the widget is shipped, the smart contract is executed. The other nodes receive the transaction and turn to verify it by ensuring that the buyer in fact

has the coin it has offered to the seller for the widget. The verification may entail looking at the latest transaction of the buyer’s account to make sure it holds sufficient funds for the purchase. The sequence of transactions is recorded in an immutable record, i.e., a blockchain, by forcing the nodes in the network to compete in solving a mathematical problem for the right to add the next block of transactions to the chain, linking the winner’s new block to the previous block, restarting the competition to add the next block each time a solution is found, and rejecting any attempt to insert or replace blocks earlier in the chain. As such, the buyer cannot spend the coin he has provided to the seller again, as everyone in the system knows the buyer no longer has the asset.

### **The Evolution**

While blockchain initially garnered interest because of its ability to be anonymous, such as in the case with cryptocurrencies like Bitcoin, the real appeal of the technology may be due to the complete transparency afforded by it.

Indeed, many have found that the underlying blockchain technology has applications in an ever increasing number of applications in nearly every industry.

For example, in 2013, Ethereum introduced blockchain in the form of “a decentralized platform that runs smart contracts.” It explained that blockchain “enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middleman or counterparty risk.” While Bitcoin is simply a currency, Ethereum “is a ledger technology that companies are using to build new programs.” It is one of the first expansions of blockchain technology outside of currency.

### **The Future**

The Economist recently told the story of Mariana Catalina Izaguirre, and how her life

might have been different with blockchain technology. She had a home in Honduras and was in possession of the official title to the land; however, the Property Institute had paperwork stating that another person owned the land. A judge signed an eviction order, and by the time Izaguirre proved her case, her home was gone. If Ms. Izaguirre’s deed was recorded with blockchain, no one could subsequently claim ownership of her land. Consider also the application to letters of credit. Banks often issue letters of credit to serve as a guarantee for a payment to be made once certain conditions are met. Using blockchain technology, the need for the bank as an intermediary in such a transaction would be removed.

Blockchain technology has evolved and migrated into these fields and continues to grow. It has moved into healthcare, with companies like Hashed Health “leveraging blockchain technologies

to solve the most important problems in healthcare.” Blocktix utilizes “Ethereum-based blockchain [to provide] a simple and secure solution to distribute counterfeit-proof event tickets as well as facilitate trustless [peer-to-peer] transfers of ownership.” Follow My Vote is attempting to “build a secure online voting platform that will allow for greater election transparency” using blockchain technology.

Blockchain can become useful in any field that includes transactions, which is to say that blockchain can become useful in every field. And while it may never reach that potential, we could be witnessing the largest technological expansion since the Internet.

***Lewis Popovski** is a partner at Patterson Belknap Webb & Tyler LLP, where he focuses on intellectual property litigation. **George Soussou** is an associate at the firm, where he also focuses on intellectual property litigation.*