A Brief History of Blockchain

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.

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-toPeer 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.

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.

Excerpt taken from an article by Lewis Popovski and George Soussou.