BLOCKCHAIN 101

Authors
Fanny Karaman
Galia Antebi

Tags
Bitcoin
Blockchain

Blockchain has recently been in the spotlight, mostly due to the 2017 surge in cryptocurrency values and the rise of initial coin offerings ("I.C.O.'s"). Many legal advisors have clients who use or wish to use blockchain in their businesses, and yet, the actual technology is often not discussed in the legal field.

Blockchain is notable because it allows different parties to collaborate without trusting each other. No trust is required because the technology is designed to (i) validate the information stored on the blockchain and (ii) make that information difficult to alter retroactively.

HISTORY OF BLOCKCHAIN

Q 1: How Did the Technology Develop?

The idea behind blockchain was originally developed in 1991 by a group of individuals attempting to timestamp digital documents.[1] As such, blockchain is based on a timestamp server, which works by widely publishing information to a decentralized network that collectively checks the validity of the timestamp.

After the 2008 financial crisis, confidence in financial institutions was low, and as an alternative, the idea of a decentralized payment network was seriously considered. Around this time, Satoshi Nakamoto used the blockchain concept to create the decentralized digital currency Bitcoin.[2]

DEFINITION OF BLOCKCHAIN

Q 2: Are Blockchain and Cryptocurrency the Same?

No. Blockchain is the technology behind cryptocurrency.

Q 3: Technically Speaking, How Does Blockchain Work?

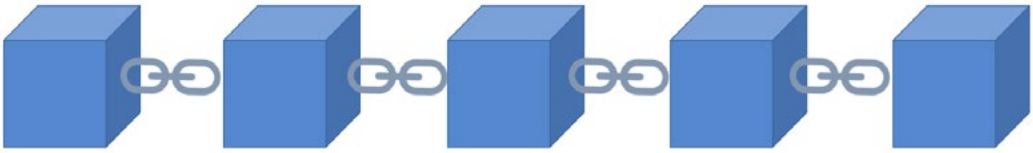
Blockchain is a distributed database that maintains a list of blocks.

As explained later, every block is composed of a certain number of records, including the history of every previous block up until its creation. This results in the blocks essentially being linked, or "chained," to each other, hence the term "blockchain." It can best be illustrated as follows:

---

1 Stuart Haber, W. Scott Stornetta, "How to Time-Stamp a Digital Document," *Journal of Cryptology 3,* no. 2 (1991): pp. 99-111.

2 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Nakamoto Institute, October 31, 2008. For a discussion of cryptocurrency, see "Tax 101: Virtual Currency - What Is It? And How Is It Taxed?" *Insights 4,* no. 12 (2017).



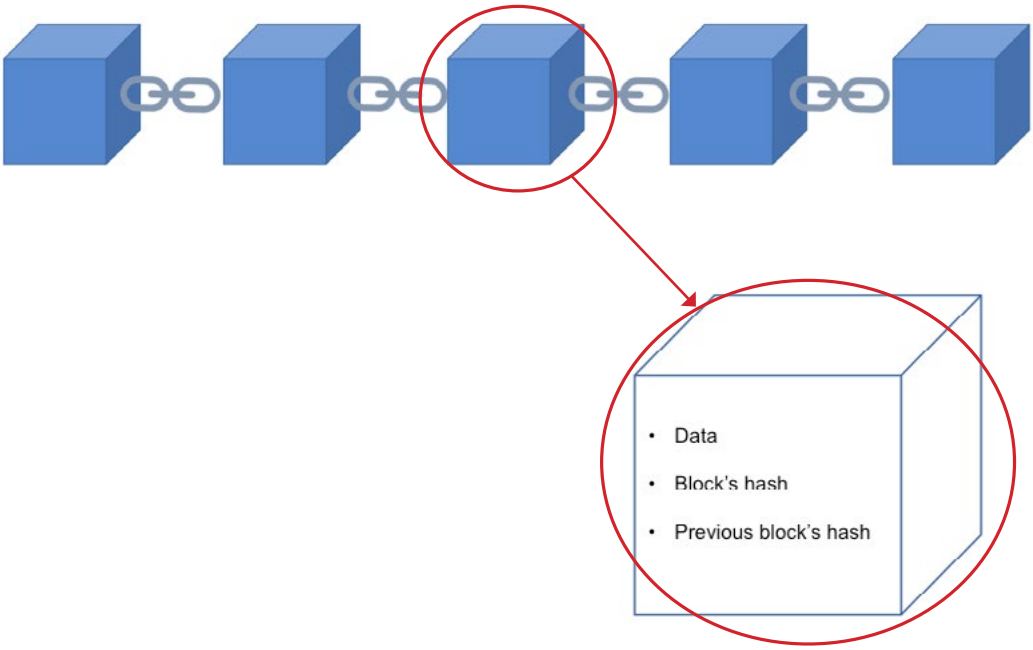
The entire chain is encrypted and every transaction is linked to a unique hash (discussed below) that is easy to verify and almost impossible to falsify because blockchain is maintained by a network of computers, also called "nodes." The nodes within a network work independently to process mathematical formulas and update the database. Once one node has solved an equation, the result is shared within the network, and if a certain level of consensus is reached, the blockchain is updated. This is known as proof of work (discussed in detail below).

Depending on the relevant blockchain, the network can be decentralized, or it can be kept among a group of accredited users.[3] This is often referred to as a "blockchain network." Similarly, a blockchain can be public or private, depending on the intended use.

Q 4: What Is a Block?

A block is composed of three items:

- Data
- The hash of the block
- The hash of the previous block



[3] See, for instance, the Australian stock exchange ("ASX Chess Replacement," ASX.).

Blocks contain previous transactions (if any) in the chain and incomplete transactions that are waiting for validation from the nodes. Once approved, these transactions become the data stored on a particular block.

Q 5: What Type of Data Is Contained in a Block?

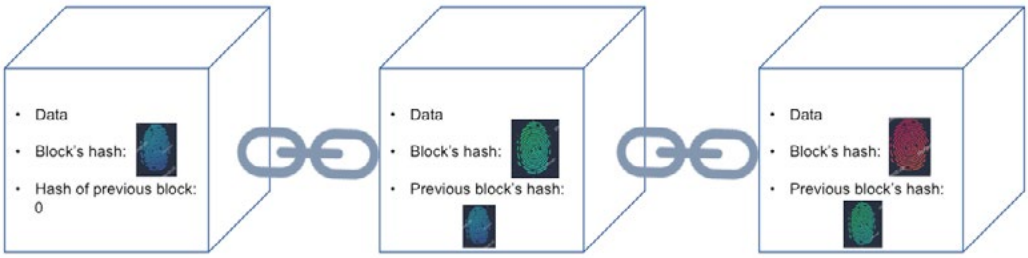
The type of data stored in a block depends on the blockchain it is a part of. For instance, if the block is part of the Bitcoin blockchain, the data it contains will include the sender, the receiver, and the number of transferred Bitcoins.

"Blockchain allows for transparency, immutability, traceability, auditability, and authentication of a specific transaction."

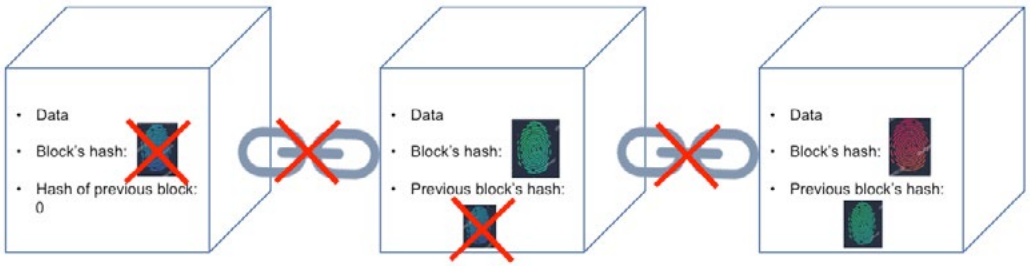
Q 6: What Is a Hash?

A hash is a unique series of letters and numbers that identifies a validated block. As such, it constitutes a cryptographic signature, similar to a fingerprint. When the block's underlying transactions are validated by the network, its hash is calculated.

The hash of the previous block is always contained in a block, along with its own hash.



This constitutes one level of blockchain security. If a block is altered, its hash will change, and the chain will be broken because the subsequent block contains a historical reference that no longer matches with the previous block's new hash.



Given that computers nowadays are very powerful, it is possible to recalculate the hashes of the blockchain to recreate the subsequent blocks. To enhance its security, the technology also contains a proof of work system.

Q 7: What Is Proof of Work?

Proof of work is a security mechanism that slows down the creation of new blocks, by requiring formulas to be solved and verified before the database is updated. It is the reason why blockchain does not require the parties' trust.

Proof of work is best illustrated through the example of Bitcoin. On average, the Bitcoin blockchain is updated every ten minutes with a new block of transactions. Bitcoin blocks contain several Bitcoin transactions that are waiting for approval from the network in order to be validated and completed. All the nodes compete against each other to solve a mathematical formula in order to approve the transactions contained in the block. The first node to solve the formula adds in a specific block of transactions. All other computers check and verify that the formula was solved correctly. If more than 50% of computers agree, the block of transactions is included in the chain.

USE OF BLOCKCHAIN

Q 8: What Is the Purpose of Using Blockchain Technology?

As explained earlier, blockchain allows for certain transactions to be carried out in a safe and almost unalterable way. As a result, blockchain allows for transparency, immutability, traceability, auditability, and authentication of a specific transaction.

Q 9: What Is the Link Between Smart Contracts and Blockchain?

A smart contract is the coded version of contractual-like arrangements. These codes are stored inside the blockchain and result in self execution of the contract, through the blockchain, if the terms of the coded agreement are met.

Q 10: What Are Other Potential Applications?

In addition to cryptocurrencies and smart contracts, potential examples of how blockchain can be used are the following:

- Food safety – Walmart and IBM use blockchain technology to increase the transparency and the traceability of the food supply chain.
- Diamond sourcing – Everledger and IBM use blockchain to track and reduce fraud in the diamond industry by tracing a diamond's origin, quality, and history.
- Stock markets – The Australian stock exchange has announced it will replace its traditional clearing system with blockchain technology.[4]
- Venture capital – In 2017 dozens of small companies raised millions in I.C.O.'s that use blockchain technology. In July 2017, the S.E.C. announced that some of the coins issued through these I.C.O.'s are securities and are subject to securities laws.[5] As a result, I.C.O.'s may now be subject to securities laws.
- Corporate records – Delaware has amended Delaware General Corporation Law to provide statutory authority for Delaware corporations to use networks of electronic databases, such as the blockchain, for the creation and maintenance of corporate records, including a corporation's stock ledger.[6]

---

4 "ASX Chess Replacement."

5 S.E.C., "The Treatment of These Coins as Stock for Tax Purposes Depends on Their Rights and Powers," release no. 81207, July 25, 2017. See "Tax 101: Virtual Currency."

6 See §§151(f), 224, and 232(c) of the Delaware General Corporation Law.

CONCLUSION

Because it is a decentralized system, blockchain can eliminate the need for intermediaries, such as banks, lawyers, and brokers – which can have a wide appeal to clients. Advisors should continue to monitor the evolution of this technology and the potential implications for clients, as well as the legal industry.