BLOCKCHAIN | BLOCKCHAIN NUTS & BOLTS

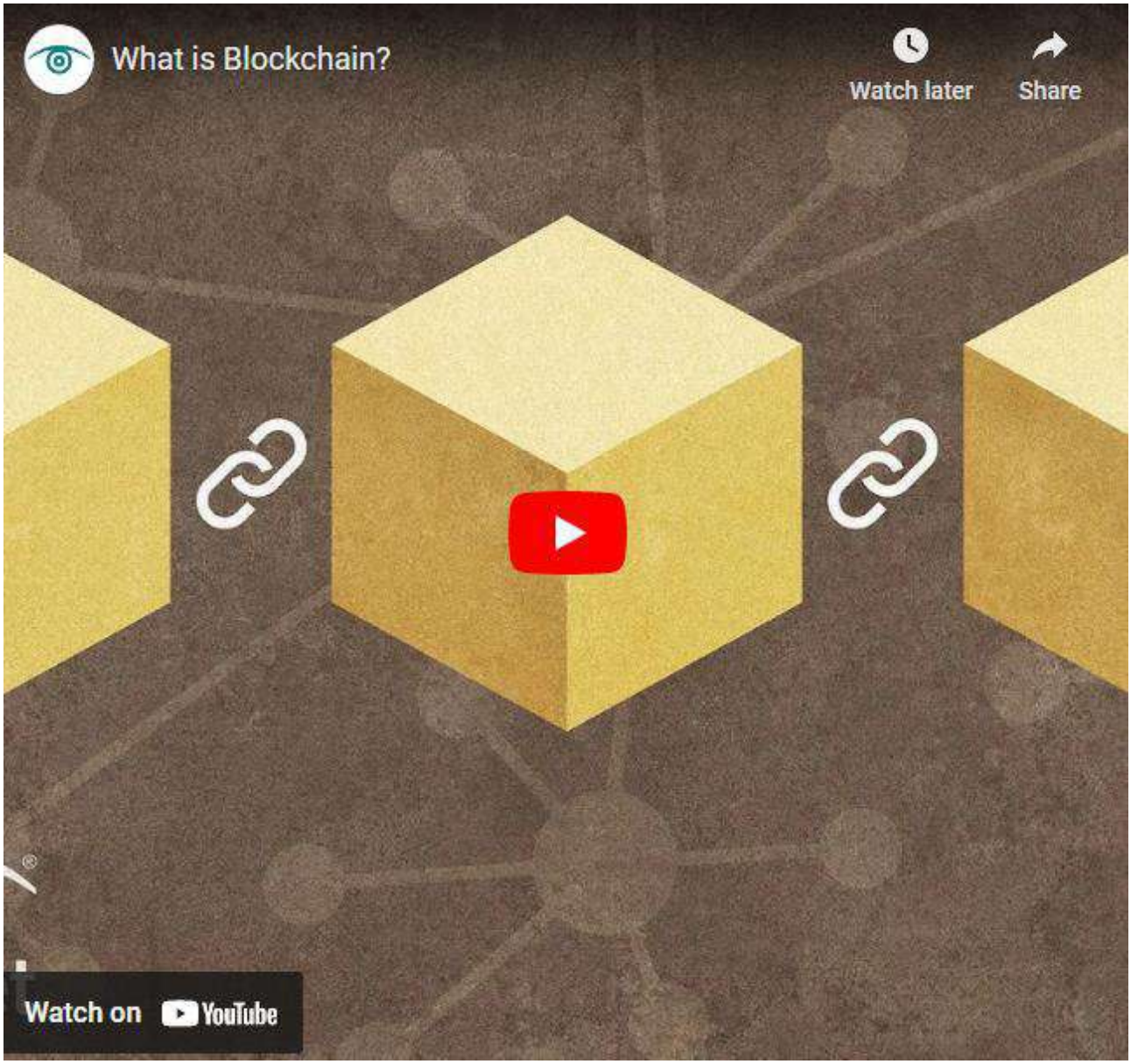
What Is Blockchain Technology and How Does It Work?

What is Blockchain? American comedian Stephen Colbert says that “it’s gold for nerds.” Well, the nerds are now the popular kids on the block, and blockchain technology is becoming one of the most prominent trends in finance and digital innovation since the creation of the Internet.

Table of CONTENTS

Blockchains are databases. Instead of being stored on a central server that's accessed by all users, blockchain records are stored on users' computers all over the world. That makes blockchain a distributed database with a peer-to-peer architecture. "Distributed" means that the data is stored in multiple locations and "peer-to-peer" means that there is no central authority that holds a master copy of the data.

Satoshi Nakamoto's Bitcoin blockchain is not the first distributed database and it is not the first peer-to-peer database. It isn't the first blockchain. But it serves as the basis for the first modern cryptocurrency and it is the starting point for the blockchains that have come after it.



How Does Blockchain Work?

Let’s say we want to store data about a poker hand in a database. We’ll start by assigning each of the cards in the deck a number: 1 is the ace of spades, 2 is the 2 of spades, 3 is the 3 of spades, all the way up to 52, the king of hearts. Your hand might look like this:

Record	Card value
1	12
2	44
3	4
4	31
5	27

Think of record numbers as the row numbers in a spreadsheet. Database programmers call them records, and blockchain programmers call them blocks. Row, record, block – they all refer to a single chunk of data.

Your opponent’s hand would occupy rows 6-10, another hand might be stored in 11-15, and so on. So if you want to specify which hand you’re talking about, you need only tell the database which row holds the first card.

Links in the Chain

Of course, in a distributed peer-to-peer database, other users may be dealing hands at the same time you are. Your cards are unlikely to appear in consecutive rows. So we can add pointers to the previous and next cards to link the data in a chain:

Record	Card value	Prev card	Next card
15	12	0	37
37	44	15	118
118	4	37	121
121	31	118	199
199	27	121	999

The first card in your hand is stored in row 15. The card value is 12, which makes it the queen of spades. There's no previous row in your hand, so we put a 0 in the "Prev card" column. The next card is stored in row 37.

So we take a look at row 37. It, too, specifies a single card, points to the row where the previous card can be found (15) and points to the next card, which is stored in row 118.

In computer science, this structure is known as a doubly linked list because it links both forward and backward. The pointers are stored in the database as data along with the card values.

Securing the Data

There is nothing to stop us – or hackers – from changing card values. This database makes cheating easy. Anybody with access to the database could change the values of your hand's first four cards to 1, 14, 27, 40 – that's four aces.

We can guard against data errors and hackers by adding a column. For each row, we'll add a column that contains the sum of card values, like this:

Record	Card value	Prev card	Next card	Checksum
15	12	0	37	12
37	44	15	118	56
118	4	37	121	48
121	31	118	199	35
199	27	121	999	58

See how this works? For our second card, the checksum value is 56, which is the sum of the values of the first two cards, 12 and 44. The checksum for card three is the sum of the next two cards. Every time we read a card value we can calculate the checksum and compare it to the checksum stored in the database. If they aren't the same, we know the data has been tampered with.

The memory chips inside your computer and smartphone detect errors using this system. This system is also used for finding errors on your hard drive.

This simple checksum system is an essential part of blockchain technology. It is well known to first-year computer-science students.

It's also laughably vulnerable to hackers. Anyone who has sufficient access rights to change card values could also alter the checksums to cover up his work. Or the hacker could alter the "previous card" and

“next card” pointers to replace a card in your hand with a card stored in a different row.

Nakamoto anticipated these vulnerabilities in his blockchain architecture. Instead of employing simple addition to create checksums and track links in the chain of data, he used a cryptographic process called “hashing.”

Hashing and Encryption

Hashing creates a unique identifier by combining the previous record’s value with the current record’s value in a one-way mathematical process resulting in a hash value like 06C4D99F32047. It’s called one-way because there is no matching mathematical process to turn 06C4D99F32047 back into the original data.

In a blockchain, the hash value for each block is based on the previous block’s hash value, which is based on the hash value of the block before that, all the way back to Nakamoto’s block 0. You can compute the hash value for any block and compare it with the hash value that is stored in the block. If they don’t match, the data has been tampered with.

In a conventional database, one could tamper with data, then compute new hash values and inject them into subsequent blocks or records to hide the effects. That doesn’t work with a distributed peer-to-peer blockchain database, because the hacker would have to simultaneously change copies of the database that are stored on hundreds or thousands of computers.

One consequence is that although it is possible to add new data blocks to the blockchain, previous blocks can’t be deleted or altered. This means that you can’t send yourself $100,000 in Bitcoin and erase the transaction.

Every transaction on the blockchain is validated using this hash mechanism.

In addition, Nakamoto set encryption in place to ensure that data stored in the blockchain would be viewable by every user but decipherable only by those who had the proper decryption keys. Without the key, all you see is a stream of nonsense characters.

The Power of Blockchain Technology

Blockchain technology makes data private, permanent, and verifiable. The record of data and transactions is public, but encryption protects it from prying eyes and alteration. This is why the Bitcoin blockchain is often referred to as Bitcoin's "open ledger."

All that hashing and encryption takes a lot of computing resources. It's slow. Worldwide, the entire Bitcoin blockchain network is limited to processing 4.6 transactions per second. Credit card companies routinely process an average of 1,700 TPS and claim they are capable of handling 56,000 TPS. The 4.6 TPS limit is the main source of Bitcoin's scalability problem. Computer scientists are working on it.

The network of computers validating Bitcoin transactions is said to be consuming more electrical power than Switzerland.

Many of Bitcoin's transaction-validating nodes hold the entire blockchain, which is currently about 250 GB of data. These are known as full nodes. The network also includes SPV nodes that perform simplified payment verification. There is no straightforward way to count the nodes. A website called Bitnodes provides an updated count of nodes currently online and reachable, but a quick Google search demonstrates that experts provide estimates of the number of nodes ranging from 6,000 to 200,000. No one really knows how many there are.

All About Ethereum

The most widely used blockchain is Ethereum, which includes modifications that make it more flexible than the Bitcoin blockchain. Ethereum has its own cryptocurrency – Ether – but developers have created many additional cryptocurrencies that run on the Ethereum blockchain. The platform is also used for many kinds of applications in addition to virtual money.
One of the main benefits of Ethereum is that it can hold executable programs in addition to data. These programs are known as "smart contracts." For example, a smart contract for tithing could add up all the Ether added to your account this month and send 10% to the church as a donation.

Like the Bitcoin blockchain, Ethereum is tamper-proof. Luxury watchmaker Breitling gives owners of its watches digital certificates that prove authenticity. If you sell the watch, you can transfer the certificate to the new owner, establishing a verifiable chain of ownership. The technology can also be used to trace the provenance of food in the grocery store, tracking every transfer. More and more people care about ethical sourcing, and blockchain can be part of that.

In 2020, the Associated Press posted minute-by-minute American presidential election results to the Ethereum blockchain to create an immutable record of verified official vote counts.

The Ethereum blockchain handles about 30 TPS. Developers are hard at work on future versions of Ethereum that will use a technique called sharding to run multiple blockchains at once, with consolidated transactions posted asynchronously to the central blockchain. Developers hope new versions of the Ethereum blockchain will handle as many as 100,000 TPS.

Because Ethereum runs smart contracts, it serves as a platform for many blockchain-related applications. Most blockchain-based decentralized applications – especially decentralized financial apps – are based on the Ethereum main chain or private Ethereum blockchains.

Ethereum is also a top choice for corporations looking to implement token-based economies. For example, a company might implement a loyalty program in which customers receive Acme Coins with every purchase. Then there could be a gift shop in which Acme Coins could be traded for benefits. The company could create a network of companies that also accept Acme Coins, giving the tokens a de facto value although they cannot be exchanged for dollars or euros.

And Ethereum specification ERC-721 defines a protocol for creating non-fungible tokens. It is the basis for the NFT market.

Image source: QuoteInspector.com, License: CC BY-ND 4.0

Other Blockchains

Bitcoin and Ethereum are the most widely used blockchains, but there are now hundreds or thousands more, all based on Nakamoto's original concept. Blockchains can be public like the Bitcoin blockchain or private, used for internal data management.

Researchers have created many variations on the basic blockchain architecture. Many include innovations to support faster processing, greater scalability, or lower transaction fees. Consensus mechanisms, coordination of subordinate subchains, private blockchains, and other key technologies are being addressed in projects across the crypto world.

What is a Blockchain? Now You Know

What is blockchain’s definition? How does blockchain technology work? We hope this blockchain explanation has increased your understanding and appreciation of this remarkable, revolutionary peer-to-peer database architecture and its applications.

NOTE