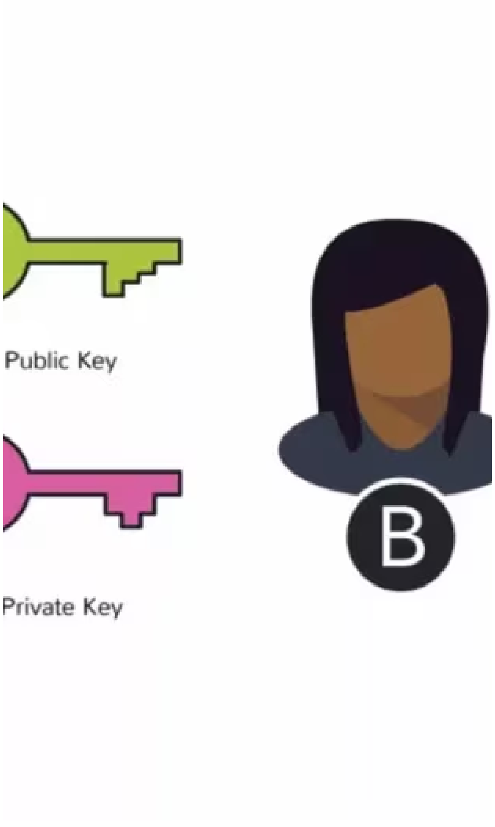


Cryptographic Keys

Technology

How Does Blockchain Technology Work?

By Nolan Bauerle

Updated May 29, 2023 at 7:06 p.m.

Beginner

As stated in our guide “What is Blockchain Technology?”, there are three principal technologies that combine to create a blockchain. None of them are new. Rather, it is their orchestration and application that is new.

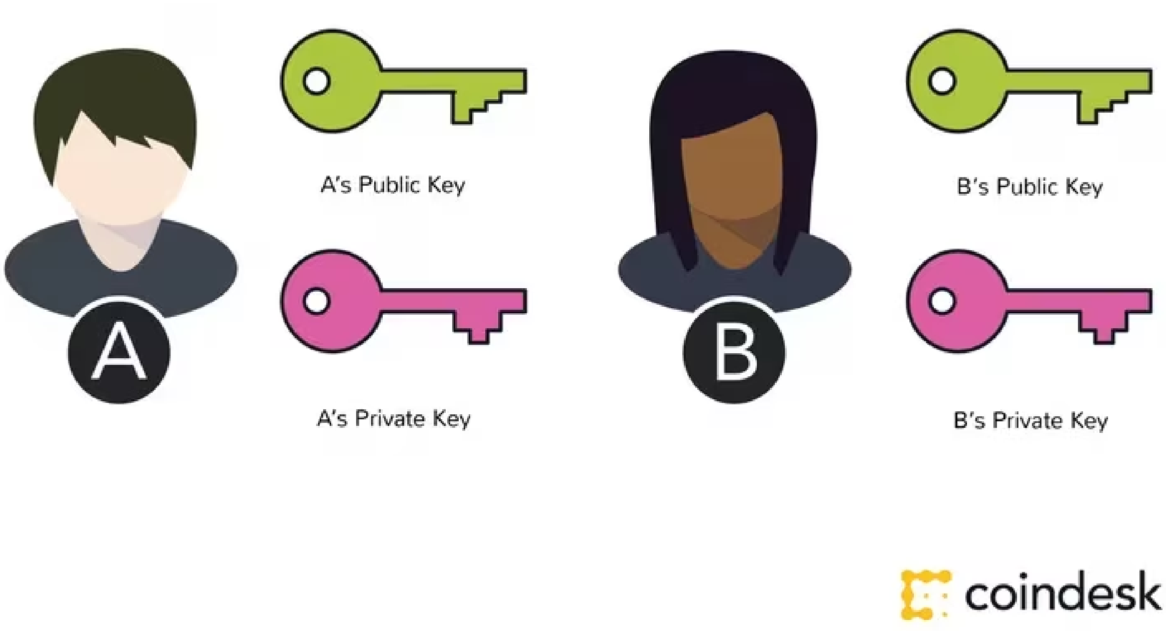
These technologies are: 1) private key cryptography, 2) a distributed network with a shared ledger and 3) an incentive to service the network’s transactions, record-keeping and security.

The following is an explanation of how these technologies work together to secure digital relationships.

Cryptographic keys

Two people wish to transact over the internet.

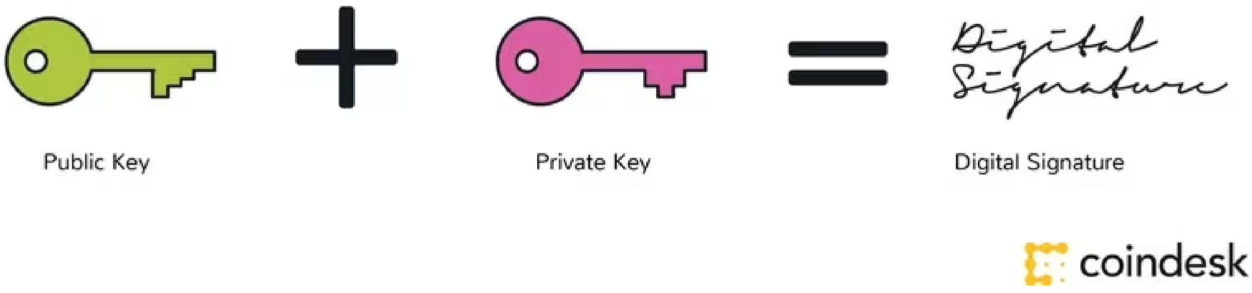
Each of them holds a private key and a public key.



The main purpose of this component of blockchain technology is to create a secure digital identity reference. Identity is based on possession of a combination of private and public cryptographic keys.

The combination of these keys can be seen as a dexterous form of consent, creating an extremely useful digital signature.

In turn, this digital signature provides strong control of ownership.



But strong control of ownership is not enough to secure digital relationships. While authentication is solved, it must be combined with a means of approving transactions and permissions (authorisation).

For blockchains, this begins with a distributed network.

A Distributed Network

The benefit and need for a distributed network can be understood by the ‘if a tree falls in the forest’ thought experiment.

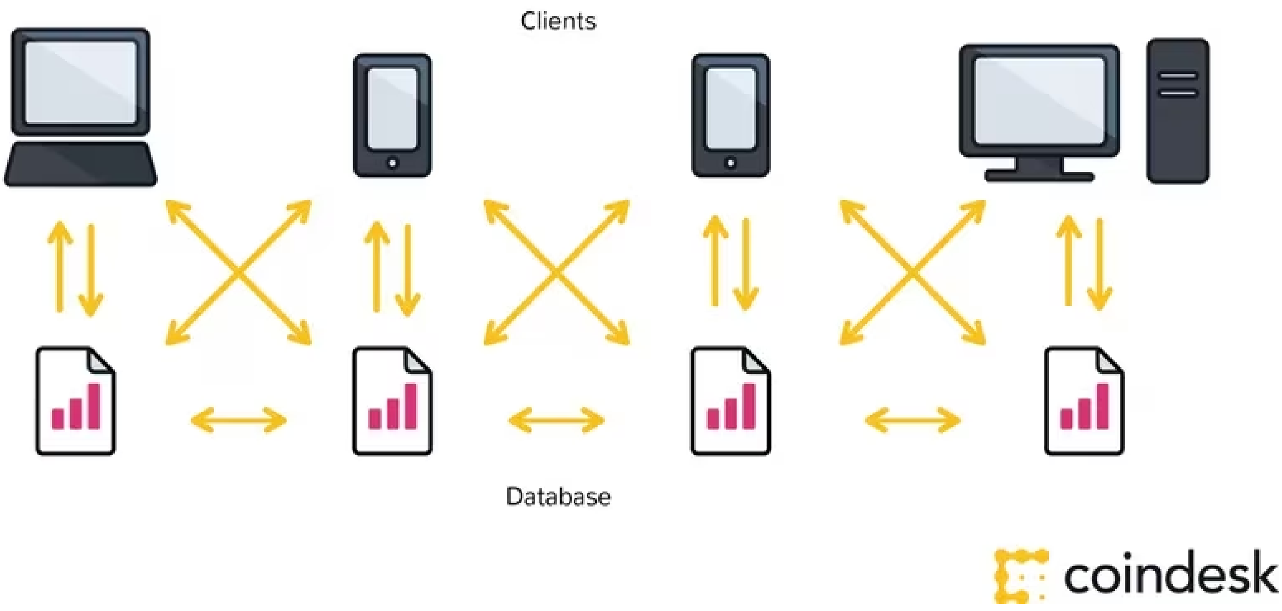
If a tree falls in a forest, with cameras to record its fall, we can be pretty certain that the tree fell. We have visual evidence, even if the particulars (why or how) may be unclear.

Much of the value of the bitcoin blockchain is that it is a large network where validators, like the cameras in the analogy, reach a consensus that they witnessed the same thing at the same time. Instead of cameras, they use mathematical verification.

In short, the size of the network is important to secure the network.

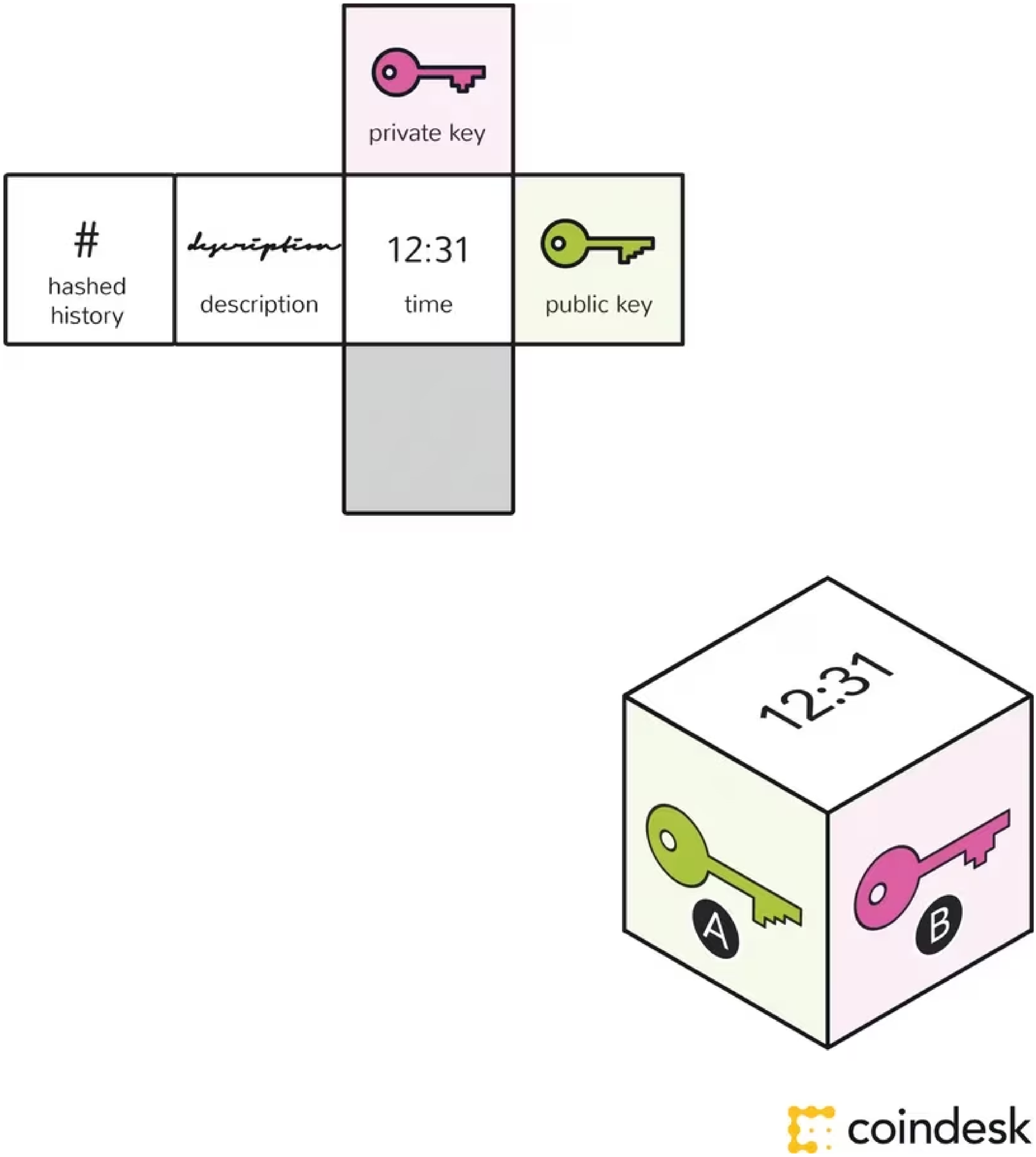
That is one of the bitcoin blockchain’s most attractive qualities – it is so large and has amassed so much computing power. At time of writing, bitcoin is secured by 3,500,000 TH/s, more than the 10,000 largest banks in the world combined. Ethereum, which is still more immature, is secured by about 12.5 TH/s, more than Google and it is only two years old and still basically in test mode.

System of record

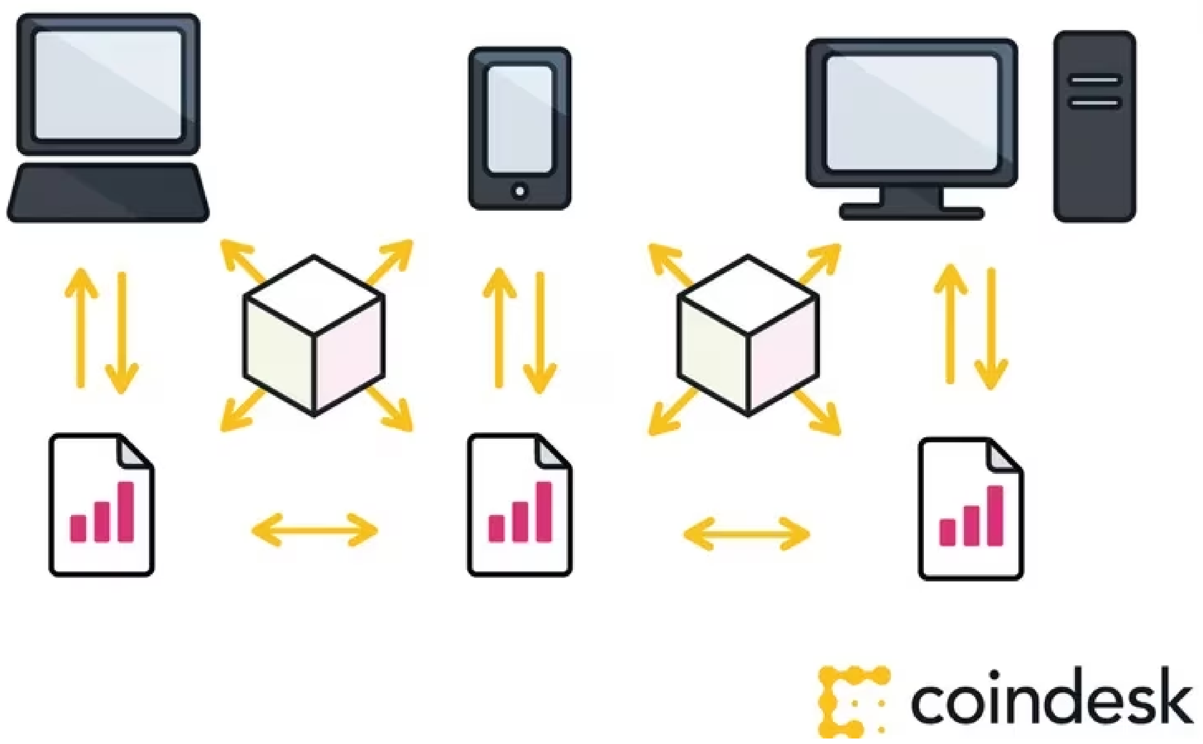


When cryptographic keys are combined with this network, a super useful form of digital interactions emerges. The process begins with A taking their private key, making an announcement of some sort – in the case of bitcoin, that you are sending a sum of the cryptocurrency – and attach it to B's public key.

Protocol



A block – containing a digital signature, timestamp and relevant information – is then broadcast to all nodes in the network.



A realist might challenge the tree falling in the forest thought experiment with the following question: Why would there be a million computers with cameras waiting to record whether a tree fell? In other words, how do you attract computing power to service the network to make it secure?

For open, public blockchains, this involves mining. Mining is built off a unique approach to an ancient question of economics – the tragedy of the commons.

With blockchains, by offering your computer processing power to service the network, there is a reward available for one of the computers. A person's self-interest is being used to help service the public need.

With bitcoin, the goal of the protocol is to eliminate the possibility that the same bitcoin is used in separate transactions at the same time, in such a way that this would be difficult to detect.

This is how bitcoin seeks to act as gold, as property. Bitcoins and their base units (satoshis) must be unique to be owned and have value. To achieve this, the nodes serving the network create and maintain a history of transactions for each bitcoin by working to solve proof-of-work mathematical problems.