**What is Blockchain Technology?**

"The practical consequence […is…] for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate."

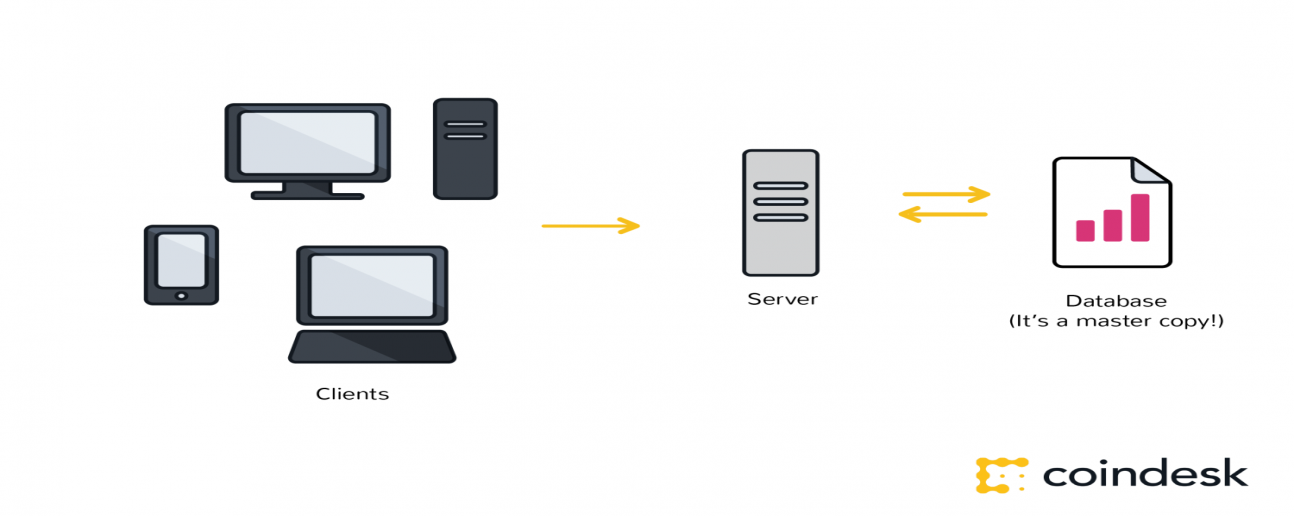
*- Marc Andreessen*

From a cruising altitude, a blockchain might not look that different from things you're familiar with, say Wikipedia.

With a blockchain, many people can write entries into a record of information, and a community of users can control how the record of information is amended and updated. Likewise, Wikipedia entries are not the product of a single publisher. No one person controls the information.

Descending to ground level, however, the differences that make blockchain technology unique become more clear. While both run on distributed networks (the internet), Wikipedia is built into the World Wide Web (WWW) using a client-server network model.

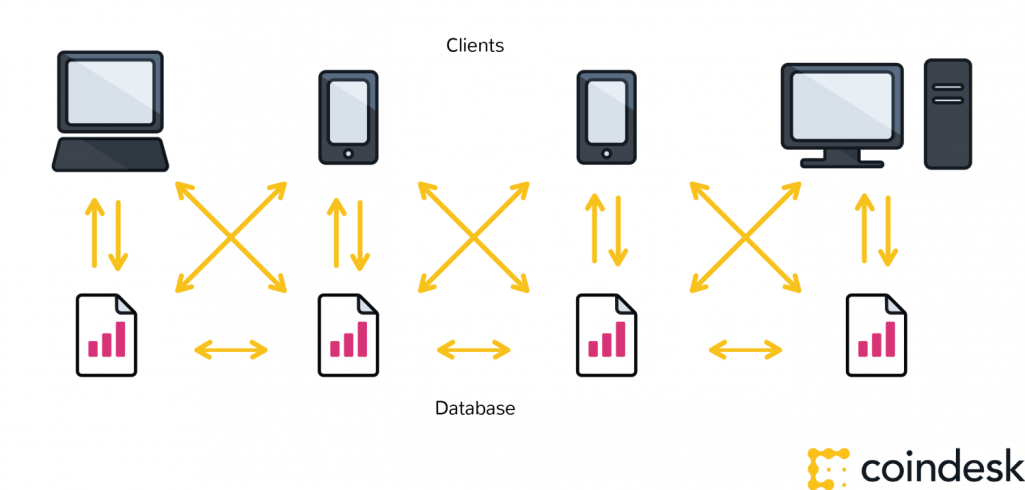
A user (client) with permissions associated with its account is able to change Wikipedia entries stored on a centralized server.  
  
Whenever a user accesses the Wikipedia page, they will get the updated version of the 'master copy' of the Wikipedia entry. Control of the database remains with Wikipedia administrators allowing for access and permissions to be maintained by a central authority.



Wikipedia's digital backbone is similar to the highly protected and centralized databases that governments or banks or insurance companies keep today. Control of centralized databases rests with their owners, including the management of updates, access and protecting against cyber-threats.

The distributed database created by blockchain technology has a fundamentally different digital backbone. This is also the most distinct and important feature of blockchain technology.

Wikipedia's 'master copy' is edited on a server and all users see the new version. In the case of a blockchain, every node in the network is coming to the same conclusion, each updating the record independently, with the most popular record becoming the de-facto official record in lieu of there being a master copy.

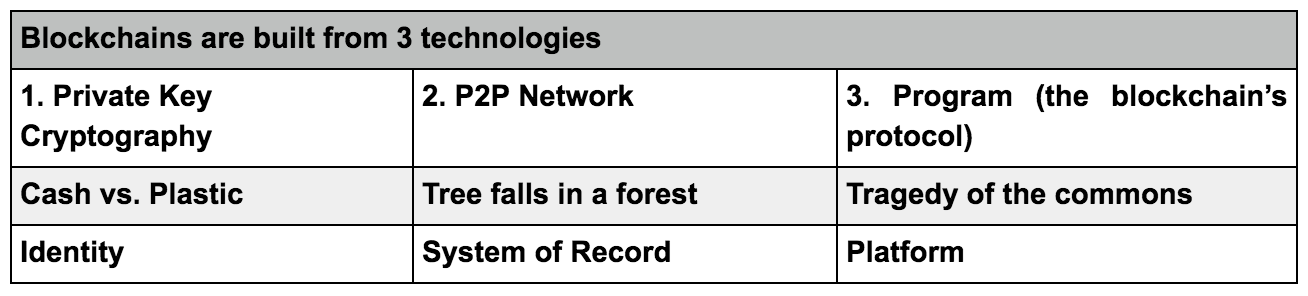


**Transactions are broadcast, and every node is creating their own updated version of events.**

It is this difference that makes blockchain technology so useful – It represents an innovation in information registration and distribution that eliminates the need for a trusted party to facilitate digital relationships.

Yet, blockchain technology, for all its merits, is not a new technology.

Rather, it is a combination of proven technologies applied in a new way. It was the particular orchestration of three technologies (the Internet, private key cryptography and a protocol governing incentivization) that made bitcoin creator Satoshi Nakamoto's idea so useful.



The result is a system for digital interactions that does not need a trusted third party. The work of securing digital relationships is implicit — supplied by the elegant, simple, yet robust network architecture of blockchain technology itself.

## Defining digital trust

Trust is a risk judgement between different parties, and in the digital world, determining trust often boils down to proving identity (authentication) and proving permissions (authorization).   
  
Put more simply, we want to know, 'Are you who you say you are?' and 'Should you be able to do what you are trying to do?'  
  
In the case of blockchain technology, private key cryptography provides a powerful ownership tool that fulfills authentication requirements. Possession of a private key is ownership. It also spares a person from having to share more personal information than they would need to for an exchange, leaving them exposed to hackers.  
  
Authentication is not enough. Authorization – having enough money, broadcasting the correct transaction type, etc – needs a distributed, peer-to-peer network as a starting point. A distributed network reduces the risk of centralized corruption or failure.  
  
This distributed network must also be committed to the transaction network’s recordkeeping and security. Authorizing transactions is a result of the entire network applying the rules upon which it was designed (the blockchain’s protocol).   
  
Authentication and authorization supplied in this way allow for interactions in the digital world without relying on (expensive) trust. Today, entrepreneurs in industries around the world have woken up to the implications of this development – unimagined, new and powerful digital relationshionships are possible. Blockchain technology is often described as the backbone for a transaction layer for the Internet, the foundation of the Internet of Value.   
  
In fact, the idea that cryptographic keys and shared ledgers can incentivize users to secure and formalize digital relationships has imaginations running wild. Everyone from governments to IT firms to banks is seeking to build this transaction layer.

Authentication and authorization, vital to digital transactions, are established as a result of the configuration of blockchain technology.

The idea can be applied to any need for a trustworthy system of record.

# How Does Blockchain Technology Work?

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.

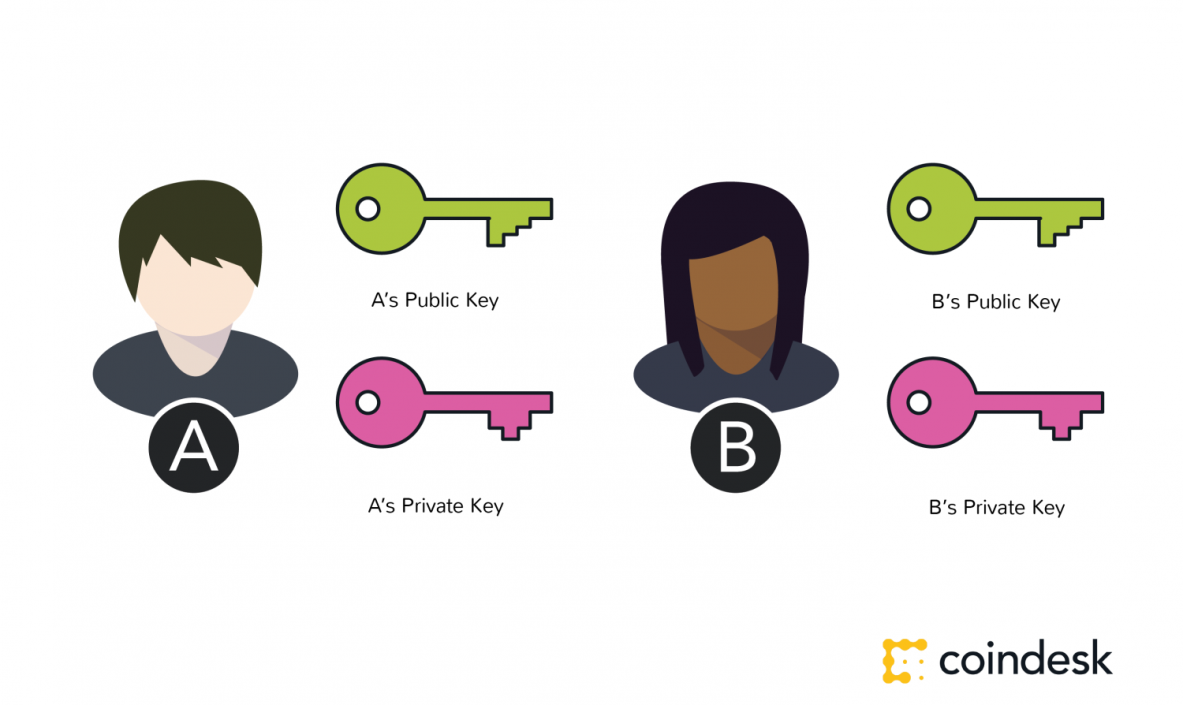
The following is an explanation of how these technologies work together to secure digital relationships.

## Cryptographic keys

Two people wish to transact over the internet.



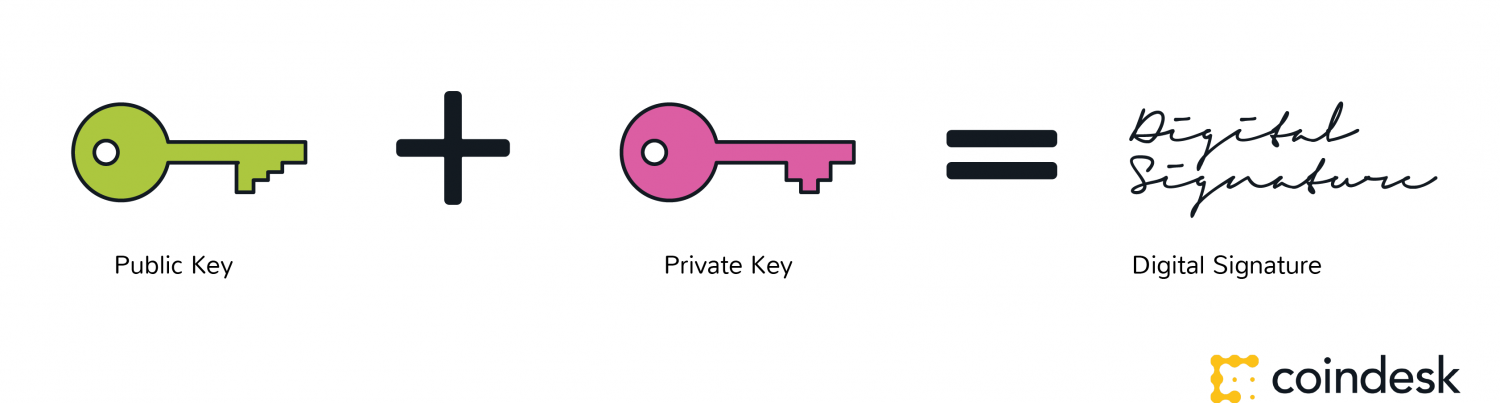
Each of them holds a private key and a public key.



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.



## Identity

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.

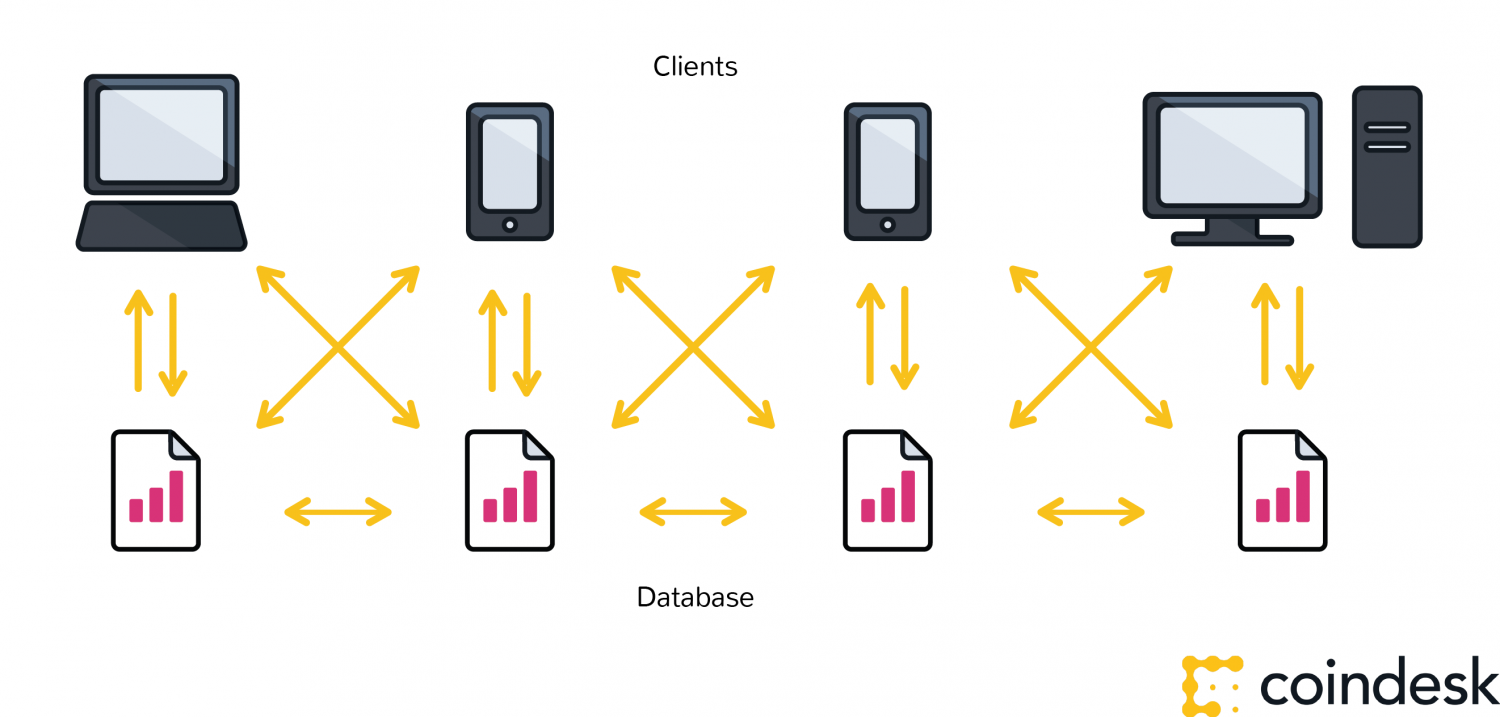
If a tree falls in a forest, with cameras to record its fall, we can be pretty certain that the tree fell. We have visual evidence, even if the particulars (why or how) may be unclear.

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.

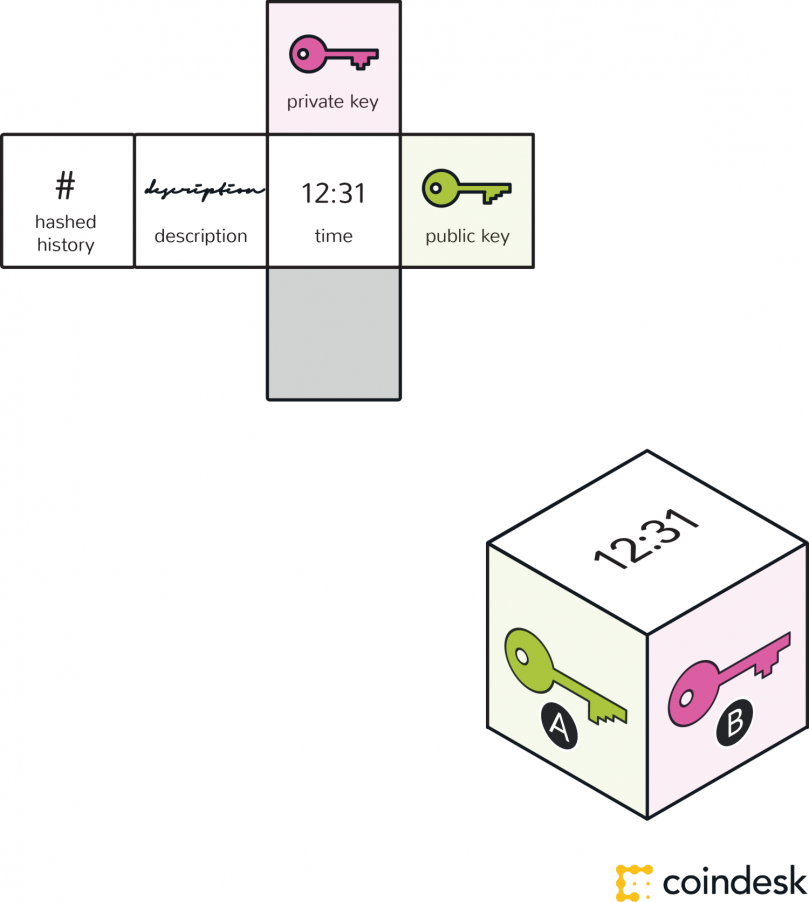
That is one of the bitcoin blockchain’s most attractive qualities — it is so large and has amassed so much computing power. At time of writing, bitcoin is secured by 3,500,000 TH/s, more than the 10,000 largest banks in the world combined. Ethereum, which is still more immature, is secured by about 12.5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

### System of record

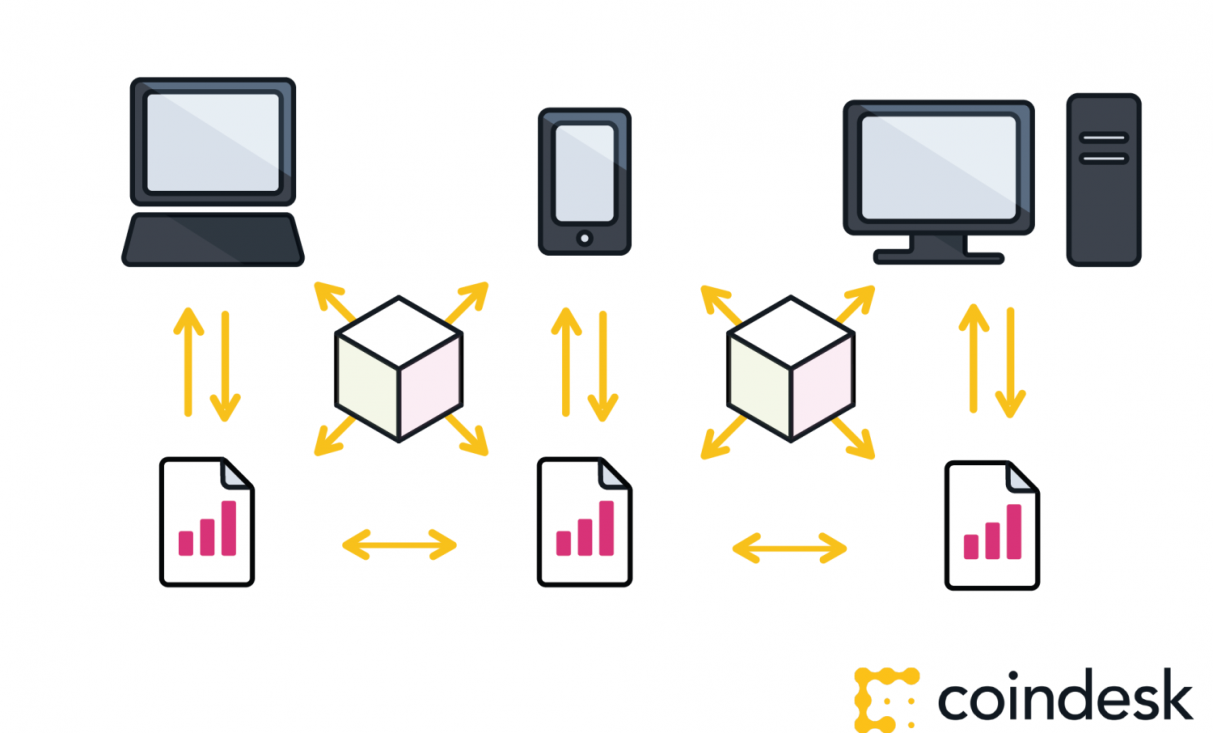


When cryptographic keys are combined with this network, a super useful form of digital interactions emerges. The process begins with A taking their private key, making an announcement of some sort — in the case of bitcoin, that you are sending a sum of the cryptocurrency — and attach it to B’s public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

### Protocol



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



### Network servicing protocol

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.

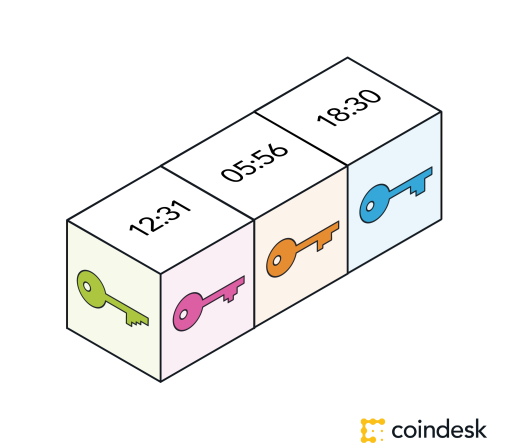
With blockchains, by offering your computer processing power to service the network, there is a reward available for one of the computers. A person’s self-interest is being used to help service the public need.

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.

They basically vote with their CPU power, expressing their agreement about new blocks or rejecting invalid blocks. When a majority of the miners arrive at the same solution, they add a new block to the chain. This block is timestamped, and can also contain data or messages.

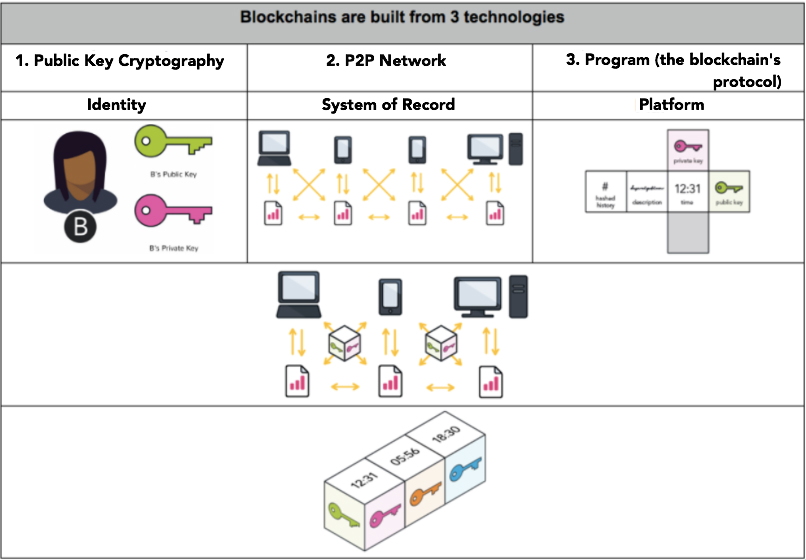
Here’s a chain of blocks:



The type, amount and verification can be different for each blockchain. It is a matter of the blockchain’s protocol – or rules for what is and is not a valid transaction, or a valid creation of a new block. The process of verification can be tailored for each blockchain. Any needed rules and incentives can be created when enough nodes arrive at a consensus on how transactions ought to be verified.

It’s a taster’s choice situation, and people are only starting to experiment.

We are currently in a period of blockchain development where many such experiments are being run. The only conclusions drawn so far are that we are yet to fully understand the dexterity of blockchain protocols.



**Example Link (Demo) :**

[**https://anders.com/blockchain/**](https://anders.com/blockchain/)

[**http://blockchaindemo.io/**](http://blockchaindemo.io/)

**Reference link:**

[**https://blockgeeks.com/guides/what-is-blockchain-technology/**](https://blockgeeks.com/guides/what-is-blockchain-technology/)

[**https://en.wikipedia.org/wiki/Blockchain**](https://en.wikipedia.org/wiki/Blockchain)

[**https://www.coindesk.com/information/what-is-blockchain-technology/**](https://www.coindesk.com/information/what-is-blockchain-technology/)