How does the technology behind cryptocurrency work?

Craig Godden-Payne
Oct 3, 2018 · 9 min read ★

Cryptocurrency and Cryptoeconomics

Blockchains have recently gained popularity in several industries, and the aim of this post is to discuss the technology behind cryptocurrency, on both permissioned and permissionless blockchains.

. . .

An Introduction…

Blockchains can solve problems and create efficiencies in tech areas such as privacy, security and data sharing.

We are going to talk about various aspects, such as:

- Blockchain
- Decentralisation
- Transactions
- Bitcoin
- Database comparisons
- Smart Contracts (Ethereum)
- Cryptoeconomics
- Consensus Algorithms
- Challenges in adoption

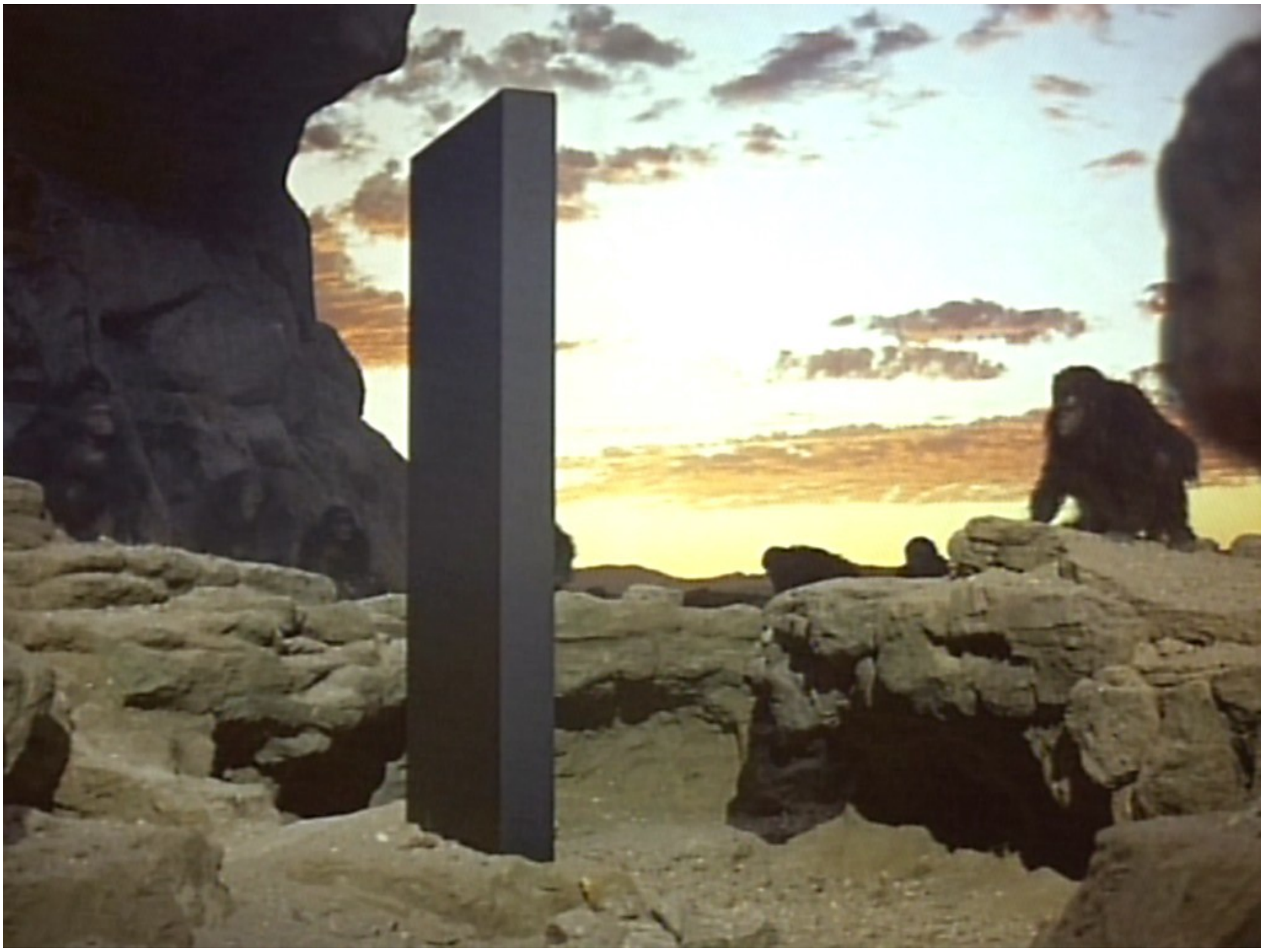
. . .

Blockchain

Blockchains help to move away from the centralised “one source of truth” monolith database, that most companies have.

For as long as software and databases have existed, there have been huge shifts between different models of how the two interact, with a big push to try and move away from centralised computing.

Splitting software into smaller chunks, microservices and moving into the cloud improves reliability and scalability, but one thing that usually remains is a huge monolith database.

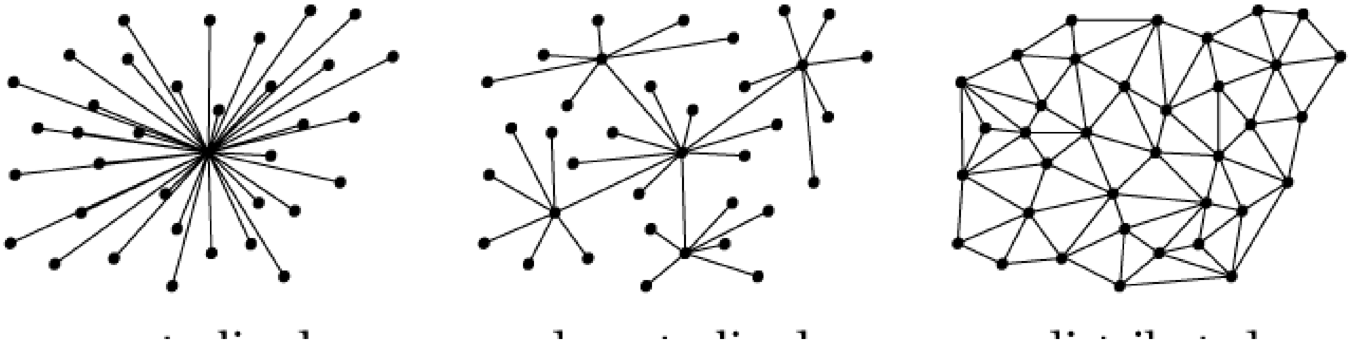


Monolith

• • •

Decentralisation

This can be improved with a decentralised system, but the ultimate goal would be a fully distributed system.



Visual representation of centralised, decentralised and distributed models.

A blockchain is a type of distributed ledge technology, which basically means it is a data structure which resides across multiple computing devices, typically spread across multiple devices and regions.

Distributed ledger technologies existed before bitcoin, but bitcoin brought together some of the core ideas, with regards to time stamping, P2P, cryptography and sharing the computing power.

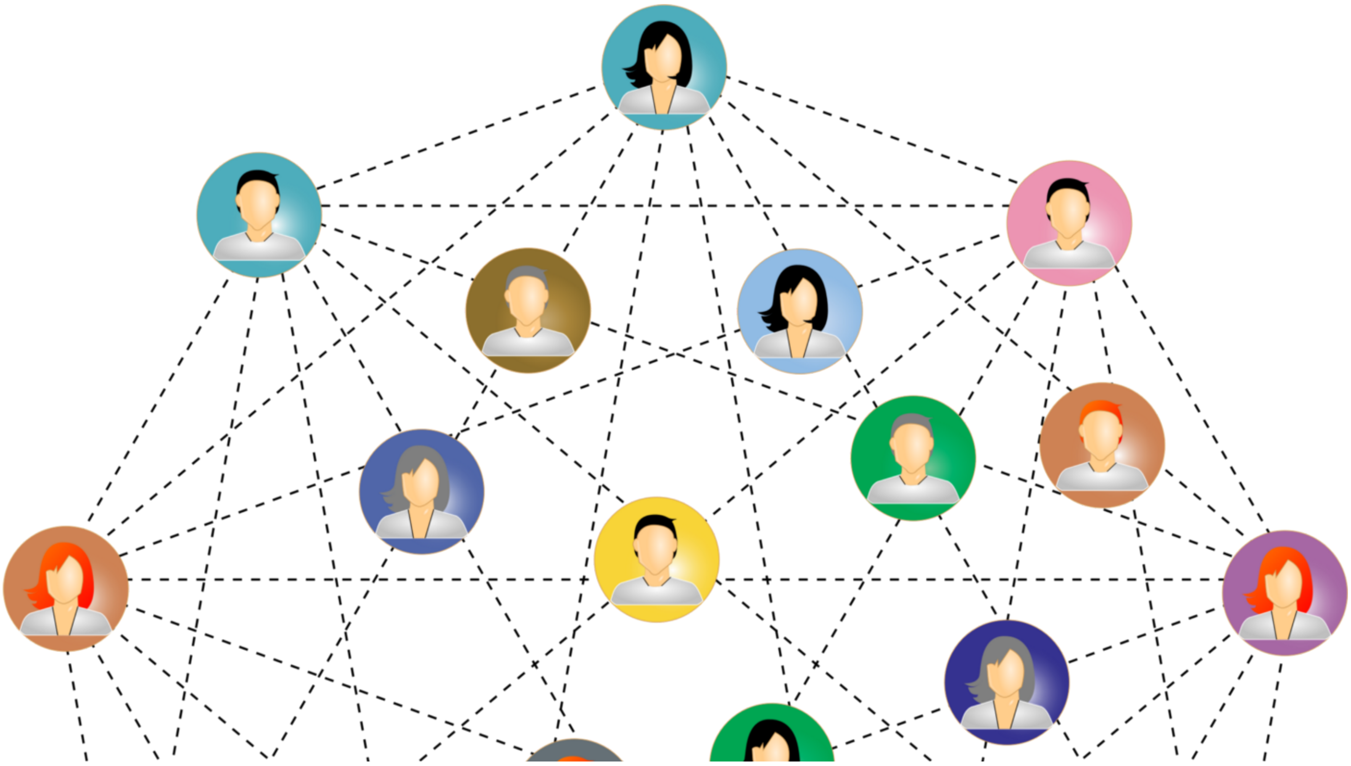
Azbit aims to connect traditional finance and cryptocurrency | Data Driven Investor

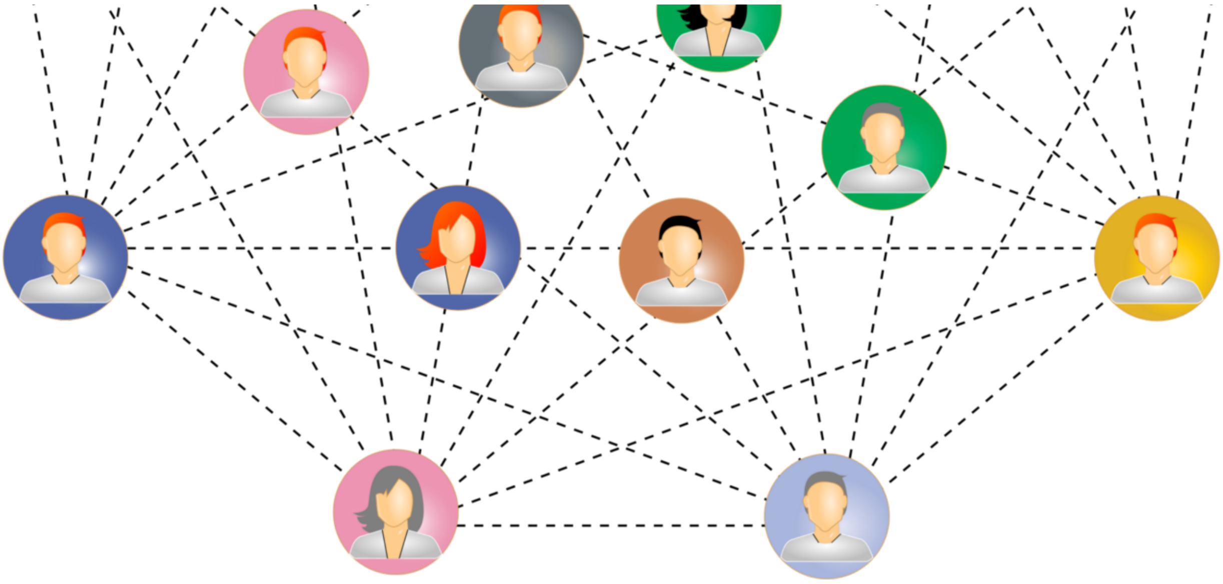
Azbit is the next crypto project providing an exchange platform offering margin and algorithmic trading. As numerous...

www.datadriveninvestor.com

A good description of a Distributed ledger technology could be summed up as:

- A Data structure that captures the current state of a ledger
- Transactions that change the ledger state
- A Protocol to allow transactions to be accepted





Connected

. . .

Transactions

A blockchain will track various assets transactions, and group them into blocks. There be any number of these transactions in a block.

Nodes on the blockchain network group upload the transactions and send them through the network.

The transactions are synced up by an agreement by all peers, and eventually each node will contain an up to date version of the ledger.

Some blockchains have a concept of smart contracts. Smart contracts are just predefined actions that are performed when certain conditions are met.

Transaction

. . .

But what is a blockchain?

Blockchain is a very wide term, and is comparable to the word Internet, the way it is a description of the wider concept rather than actual technology.

Blockchain is in a basic form, a chronological chain of blocks of transactions, that are bundled together and added to a chain, at the same time across a distributed network.

Blockchains used to be referred to as the specific data structure within a distributed ledger technology, but now a lot of people use the term blockchain to refer to anything, from cryptocurrencies to enterprise deployments of distributed ledger technologies.

Blockchain

. . .

Lets mention a bit about Bitcoin

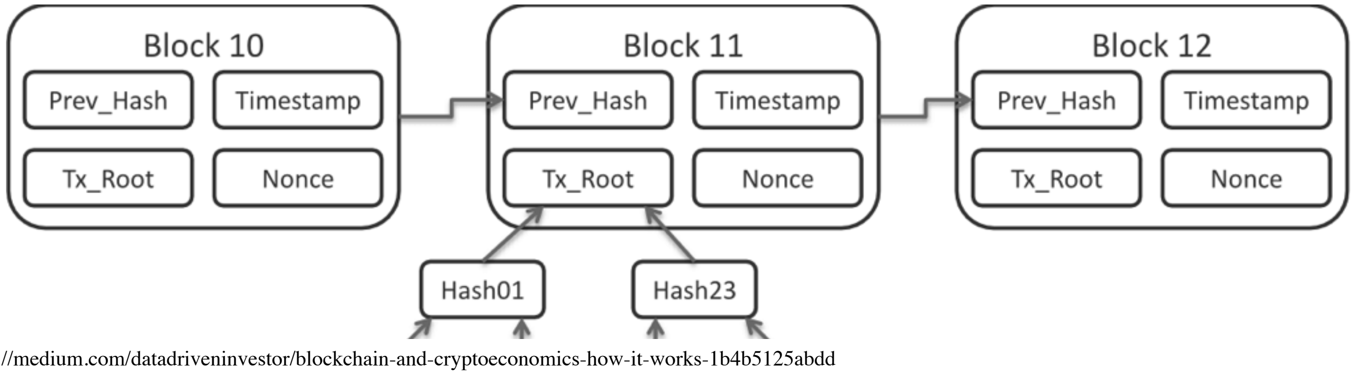
Bitcoin is a cryptocurrency. It is a decentralised digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries

Miner nodes bundle unconfirmed and valid transactions into a block. The miners must then solve a cryptographic challenge, to propose the next block. People refer to this as "proof of work".

Bitcoin

A block consists of 4 pieces of metadata.

- A reference to the previous block
- A proof of work (known as nonce)
- A timestamp
- A reference to the merkle tree root of transactions



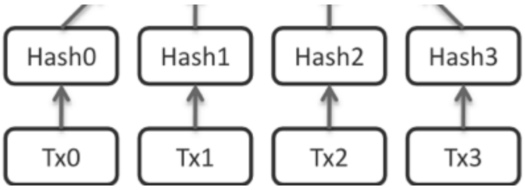


Diagram of how bitcoin stores its metadata

. . .

Why is blockchain technology so good?

Blockchain creates a distributed consensus between mutual distrustful parties, whilst creating a shared instantaneous source of truth.

In comparison, some banks will reconcile at the end of the day, and some shops will process all sales at the end of the day and update stock levels, ready for the next day.

In theory, you view the entire chain of transactions, at any time, from any node and know the information you receive is good.

Transactions

. . .

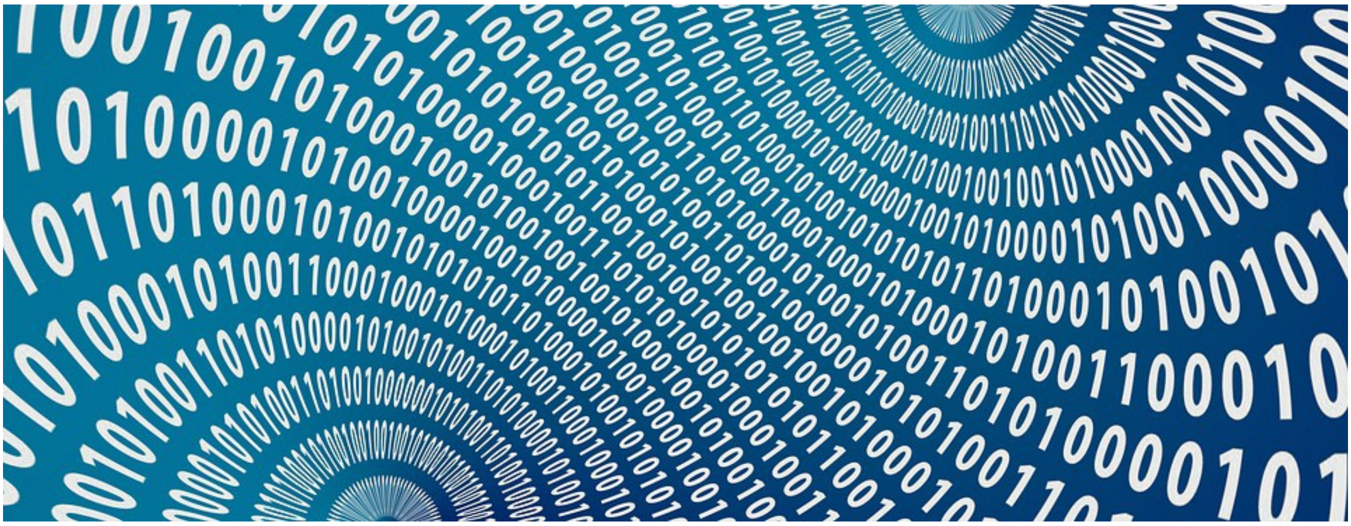
What is the difference between a blockchain and a database?

A blockchain is a write only, data structure, where the next record is always written at the end of the chain.

This is achieved by each block referencing the previous block, meaning there is not an easy way to have to edit or delete data from the blockchain, and an attempt to do this, would be extremely easy to detect.

In comparison, a database can easily be manipulated and changed by a database administrator, or an application which may change the state of some data.

Blockchains we designed to be decentralised, where databases are usually designed to be centralised, or tend to have a single "master" node, which controls the data.



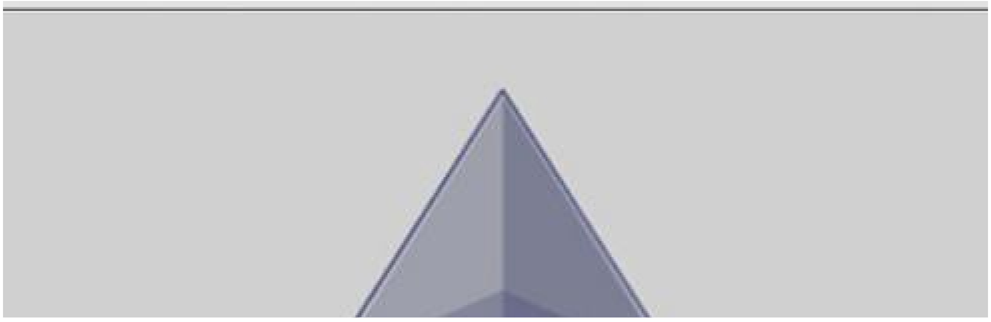
Data transfer

. . .

Smart Contracts

Smart contracts are pieces of code, that execute pre-defined actions, when certain conditions are met.

This allows the ledger state to be modified, or facilitates the transfer of some kind of asset, or can verify or negotiate a legal contract of some kind. They were made popular by the Ethereum blockchain.



Ethereum

Example of an Etherum smart contract

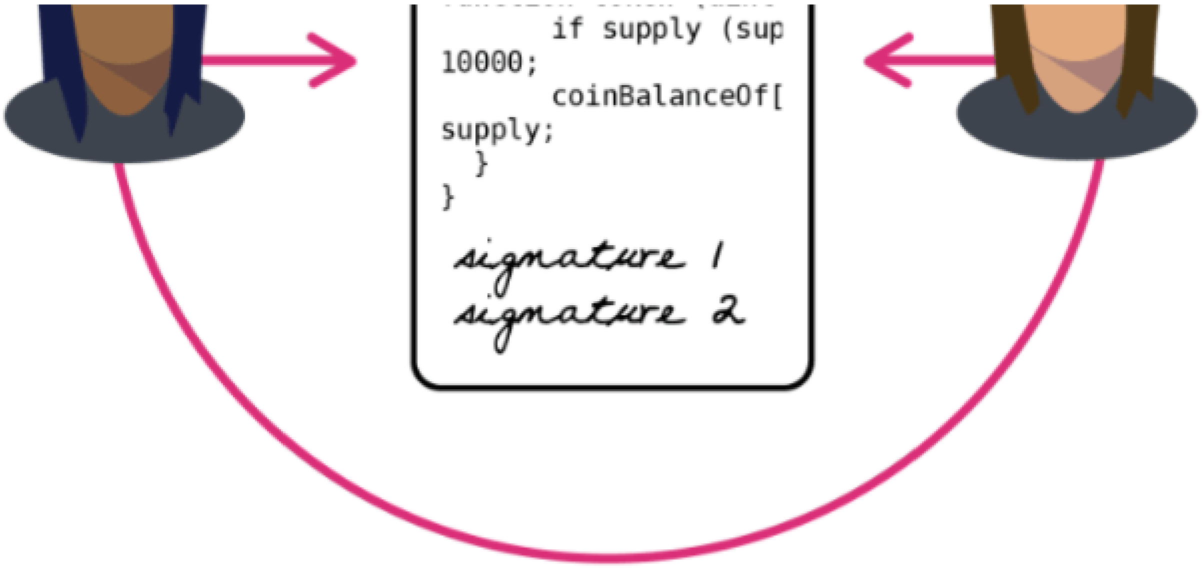
In an equity raise, transfer X amount from the investor, to the company on receiving the shares from the company.

The monetary value of X has been pre-validated by the company for the transaction. The amount is held by the smart contract until the shares are received.

- The smart contract encodes the agreement between a company raising funds and its investors
- The smart contract sits on the Ethereum public blockchain. Once an event is triggered, for example an expiration date, or a strike price that has been pre-coded, the smart contract executes its logic.
- If needed, regulators can scrutinise the market activity without compromising the identity of the specific parties involved.

```
contract token {
        mapping  (addr
public coinBalanceOf;
        event CoinTran
sender, address rece:

function token (uint
```



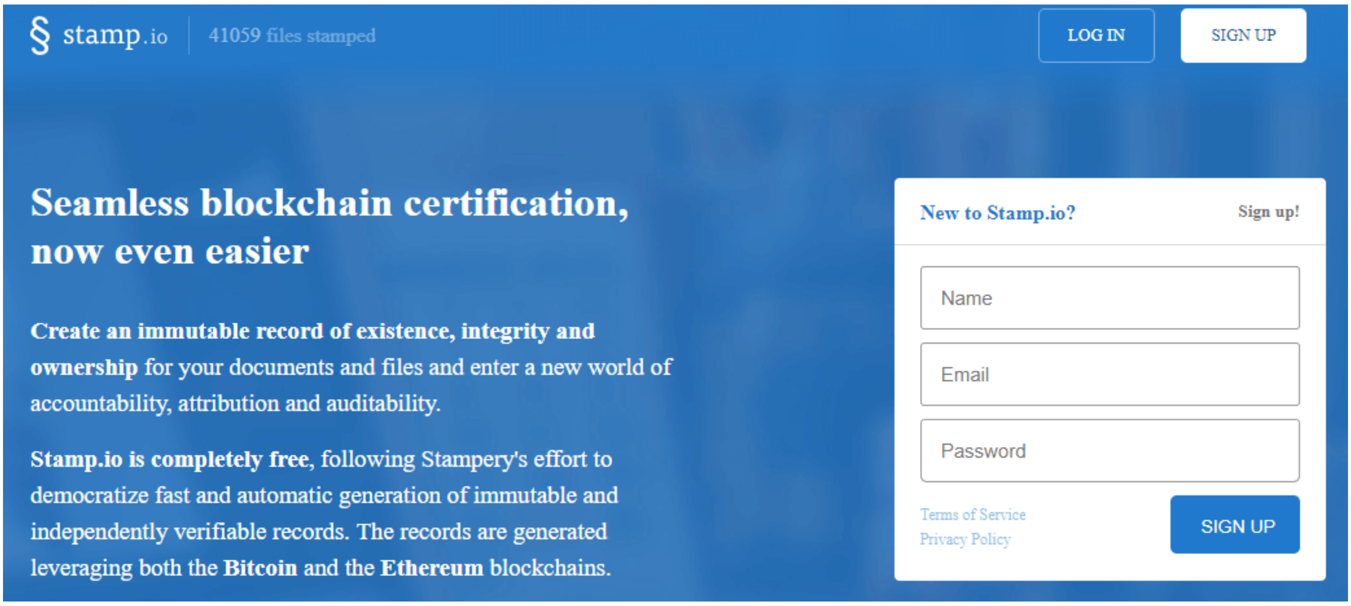
```
        if supply (sup
10000;
        coinBalanceOf[
supply;
   }
}
```

Another example of use of the Ethereum blockchain

Check out the website https://stamp.io

You can take a document and upload it to the Ethereum blockchain.

Stamp.io will then return a certificate, and you can view your transaction then on the public Ethereum blockchain



Seamless blockchain certification, now even easier

Create an immutable record of existence, integrity and ownership for your documents and files and enter a new world of accountability, attribution and auditability.

Stamp.io is completely free, following Stampery's effort to democratize fast and automatic generation of immutable and independently verifiable records. The records are generated leveraging both the **Bitcoin** and the **Ethereum** blockchains.

stamp.io

. . .

Why were these technologies created, and what problem do they

solve?

Bitcoin was released in 2009, in response to the global financial crash at the time. The idea was to transfer value, over the internet without an intermediary. Bitcoin is essentially programmable money.

Ethereum was created in response to Bitcoin, and it has a more extensive set of APIs, and allows for smart contracts.

At the core of the Ethereum blockchain are EVMs (Ethereum virtual machines), which run on the Ethereum network. Unlike Bitcoin, Ethereum does not just track transactions.

. . .

What is Cryptoeconomics?

Cryptoeconomics is about building systems, that have certain desired properties, which use cryptography to prove properties about messages, that happened in the past, while using economic incentives, defined inside the system.

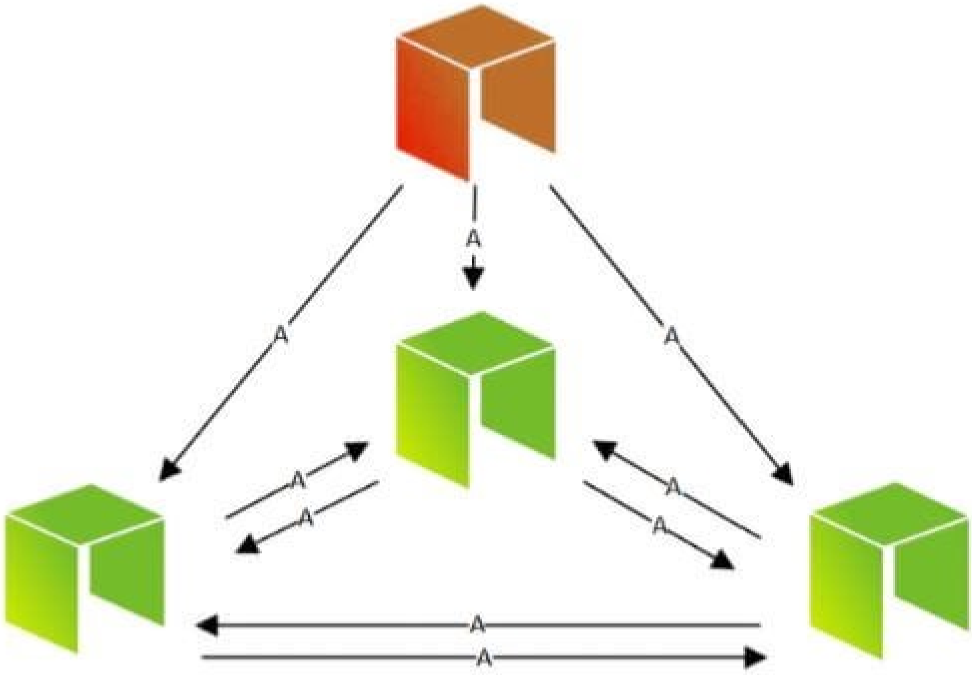
Rather than imposing barriers to entry, permissionless blockchains, such as bitcoin are public and open. Although, this can also mean they are open to malicious attackers.

This is prevented by having good behaviour incentivised so that:

- malicious attackers cannot take over the system with an escalated attack

- malicious attackers cannot undertake an organised majority attack
- the payoffs of securing are higher than the payoffs for attacking

Consensus Algorithms



Consensus Algoritms

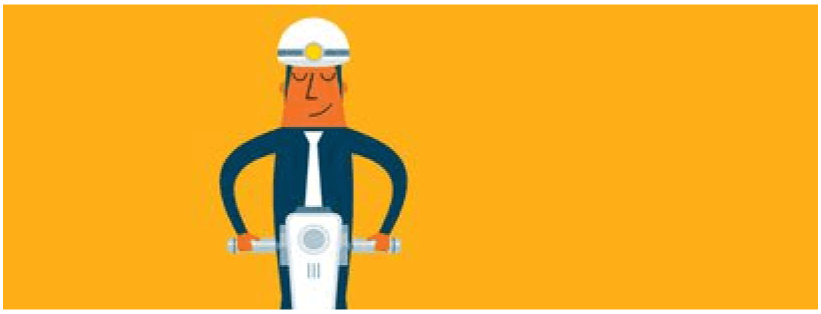
Consensus is the process of achieving agreement among network participants as to the correct state of the data in a system.

It does two things:

- Ensures data is the same for every node on the network
- Prevents malicious actors from changing the information.

Bitcoin mining is one example of a consensus algorithm, although there are others.

Proof of work



PoW is used within bitcoin, and is usually referred to as mining. In order to add a new block onto the block chain, a computational challenge must be solved.

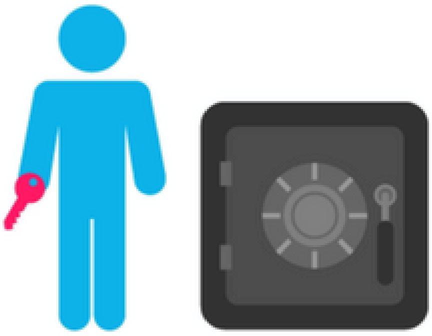
The incentive for “mining” is an economic payoff.

Proof of work is hard to create, but easy to verify, you could compare this to a combination lock. It’s really difficult to guess the correct sequence of numbers of a combination lock, but once you know the combination, it’s easy to verify, because it opens the lock.

Proof of work requires a huge amount of energy to be expelled, and each block usually takes about 10 minutes to mine.

Mining is concentrated in countries where energy is cheap.

Proof of stake



In PoS, nodes are known as validators, rather than miners. When a node validates, it earns a small transaction fee.

Nodes are randomly selected to validate blocks, and the probability of selection is based on the stake already held. This saves the massive amount of computational resource involved to create the next block.

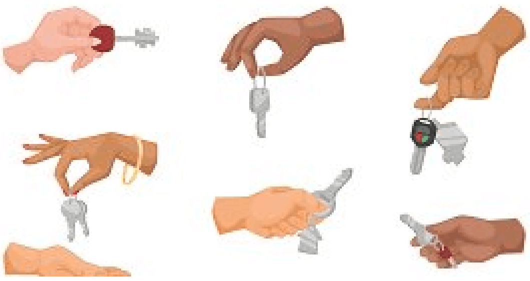
Example of how selection works: If node X already has validated and earned 2 coins, and node Y has 1 coin, node X is twice as likely to be called upon to validate a block of transactions.

Proof of elapsed time

PoET emulates the mining style of bitcoins proof of work, but instead of competing to solve a cryptographic challenge, there is a random lottery, and works on a first come first serve basis. Each validator is given a random wait time.

The winner creates the next block on the chain.

Proof of Authority



PoA uses a set of authorities, which are designated nodes, who are allowed to create blocks on the chain. Ledgers using PoA require sign off by the majority of the authority nodes in order for the block to be created.

. . .

Challenges in Adoption, and deployment of Distributed Ledger Technologies.

At the moment, there are a lot of challenges.

- Lack of Standards
- Regulatory challenges
- Lack of knowledge

Standards

Standards need to be in place to ensure interoperability and prevent a fragmented ecosystem. Standards do not just need to be created for the blockchain, but also services used on it, like privacy, identity and data governance.

In 2016 the International Organisation of Standardisation for Blockchain and Distributed Ledger Technologies was created.

Regulations

Lack of regulation creates uncertainty for everyone involved. Highly regulated sectors, such as finance are treading very carefully with distributed ledger technologies, as there are no regulatory guidelines at this time for smart contracts.

This is most likely one of the major reasons that is preventing the rapid adoption of DLTs.

Lack of know-how

Blockchain is general is gaining more traction, and people are becoming more interested in it, but there is still a lack of technical talent of people in blockchain

Blockchain Bitcoin Ethereum Crypto Smart Contracts