Practical Introduction to Blockchain and the New Era of the Internet: Web3

Boban Sugareski, Senior Software Engineer (Fintech) @ Slice

Brief history of blockchain

1991

A **cryptographically secured chain of blocks** is described for the first time by Stuart Haber and W Scott Stornetta

1998

Computer scientist Nick Szabo works on ‘bit gold’, a **decentralised digital currency**

2000

Stefan Konst publishes his **theory of cryptographic secured chains**, plus ideas for implementation

2008

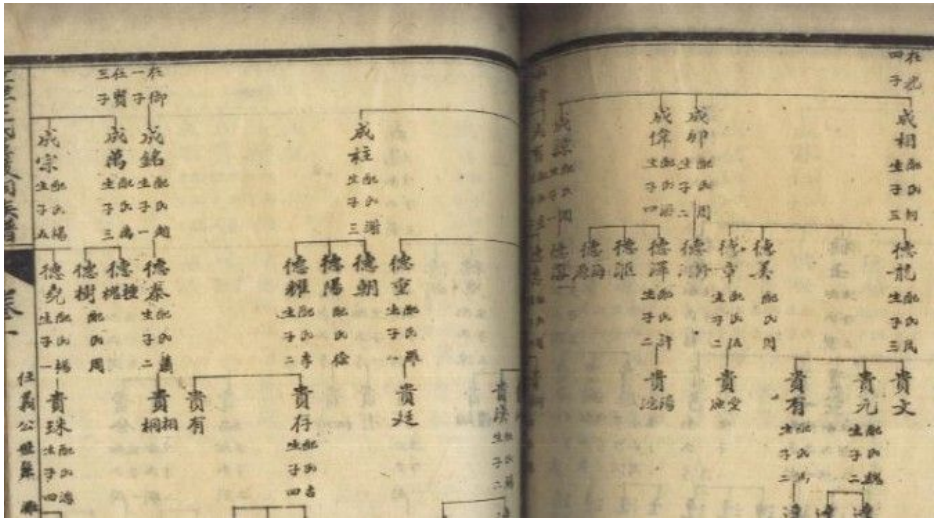
Developer(s) working under the pseudonym **Satoshi Nakamoto** release a white paper establishing the model for a blockchain called **Bitcoin**

Cryptographically secured chain of blocks

Decentralised digital currency

Bitcoin

Old Chinese Genealogy Tradition



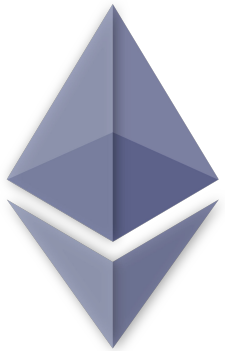
Blockchain

A **blockchain** is a **decentralised database** that is shared among the **nodes of a computer network**

It differs from the traditional databases in **the way data is structured**

Most popular blockchain implementations:

Bitcoin and Ethereum



A **blockchain** collects information together in groups, known as **blocks**

Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a **chain** of data blocks known as the **blockchain**

This data structure inherently makes an **irreversible timeline of data**

Every **block** consists of 1 or more **transactions**

e.g. The Bitcoin blockchain has 1500-2000 transactions per block

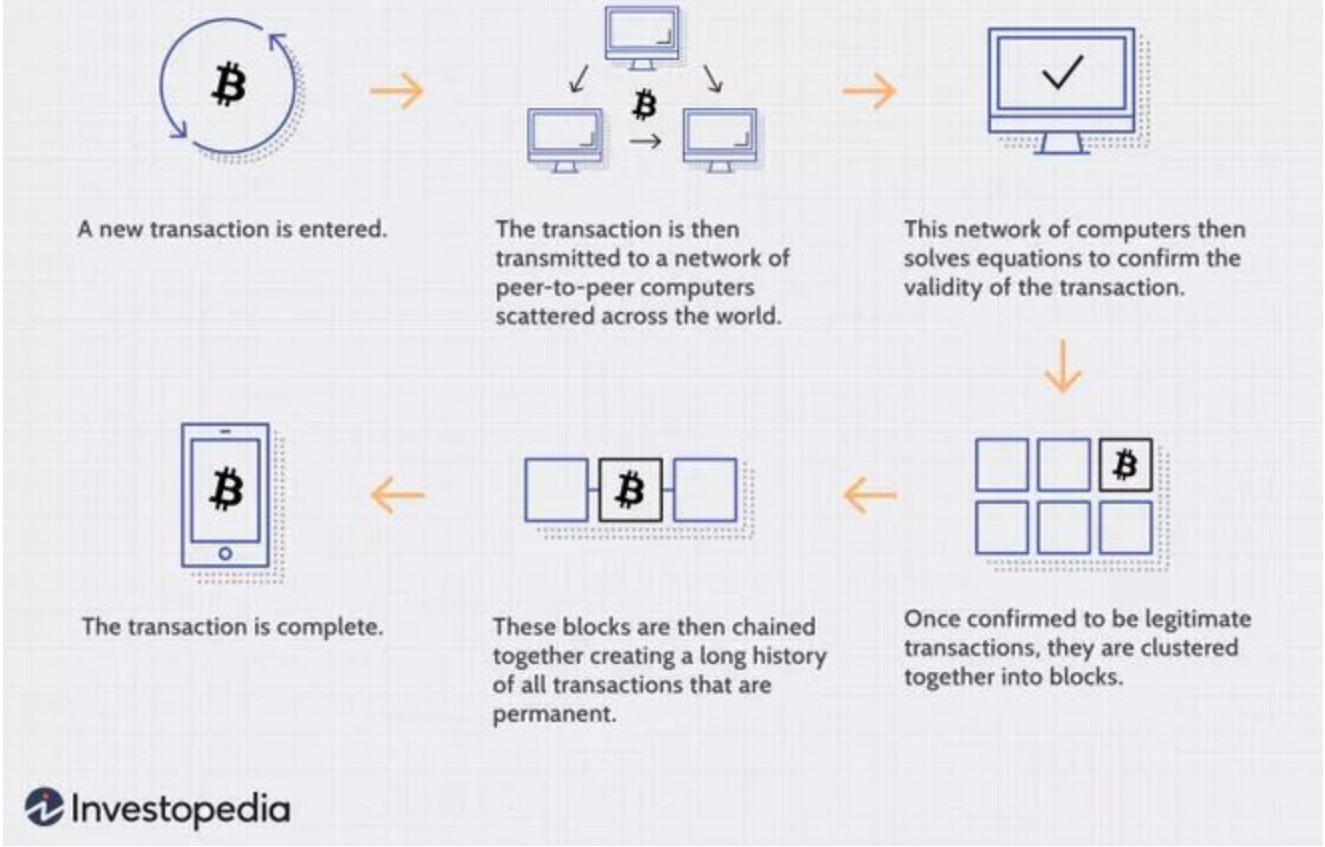
The goal of **blockchain** is to allow digital information to be recorded and distributed, but not edited

In this way, a **blockchain is the foundation for immutable ledgers**, or records of transactions that cannot be altered, deleted, or destroyed

KEY POINT

Changing a transaction requires changing the current block of transactions and all subsequent blocks - which makes hacking the decentralized ledger extremely difficult

The **decentralized ledger** will survive as long as **at least one node survives**


A new transaction is entered.
The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.
This network of computers then solves equations to confirm the validity of the transaction.
Once confirmed to be legitimate transactions, they are clustered together into blocks.
These blocks are then chained together creating a long history of all transactions that are permanent.
The transaction is complete.
Investopedia

“Solving equations to confirm the validity of transactions” is called **mining**

Mining is the way the network confirms new transactions and is a critical component of the blockchain ledger's maintenance and development

It is performed using **sophisticated hardware** that solves an **extremely complex computational math problem**

The **miner** that wins the race, **adds the new block to the chain**, and **earns a reward**

What is the problem with the current world that blockchain is trying to solve?

1. Too much centralized power

A single financial institution can break world’s economy

Bitcoin was published right after the **2008 financial crisis** - caused by **epic failures** by **very few banking giants**

Blockchain is a decentralized system with regulations that deny any single entity to acquire too much power on the network

2. Slow money transfers

Slow cross-border money transfers because of too many intermediaries

A fundamental role played by **financial institutions** is to be an **intermediary entity** and **bring untrusting parties together** to facilitate transactions

It takes 3 days to complete and settle cross-border money transfer and to make it happen, **multiple departments** and **application systems within an institution and across institutions** have to work together

A cross-border Bitcoin transfer completes in no more than 1 hour, or in few minutes with Ripple

No settlement is needed since transaction and settlement are in one action

3. Financial intermediaries charge hefty fees

US bank could charge $10-$30 USD for sending money from the US to another country

A report by Bank of America (BoA) claims **a transfer via blockchain costs 1/6000 of what BoA charges**

4. Security

When **data is stored in centralized area** within an institution, it is **prone to being hacked**

E.g. Equifax (150 million US consumers' information hacked in 2017)

You **cannot steal information from the blockchain**, everything is already public

Users are **anonymous** and only identified by their address

5. Transparency

Financial institution do not give much transaction information to the customers

In the example of cross-border money transfers, **both the sender and the receiver have to wait for three days to know whether the transaction has been completed** successfully or not

If a transaction fails, a lengthy investigation has to be triggered

With blockchain, every **transaction is public and stored forever on the ledger**

Bitcoin vs Ethereum

The Bitcoin blockchain has one job:
trading BTC (the Bitcoin currency)

It is limited only to cryptocurrency transfers

The Bitcoin blockchain has no complete programming language for coding directly on the blockchain, meaning you cannot deploy custom applications on it

But what about:

governance?
elections?
healthcare?
real estate?
media?
supply management?
Auctions?

This is where **Ethereum** comes in

The core idea of **Ethereum** is to be a general-purpose blockchain that could be used for a wide range of business problems not just limited to cryptocurrency transfer

It has a complete programming language called **Solidity**

The programs we write with it and we deploy **on the chain** are called **smart contracts**

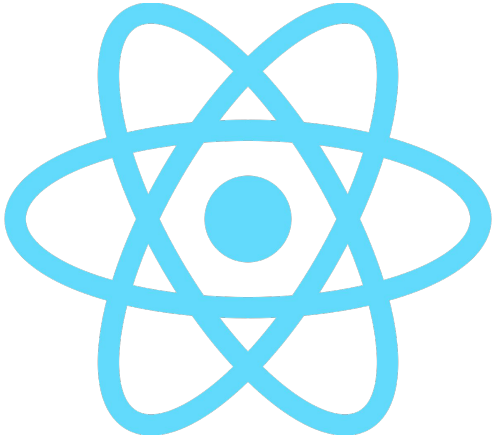
Solidity is an object-oriented, high-level language for implementing smart contracts

Smart contracts are programs which govern the behaviour of accounts within the **Ethereum** state

Demo

React.js

client-side JS library



Ethers.js

JS library for interacting with the Ethereum Blockchain and its ecosystem

Solidity

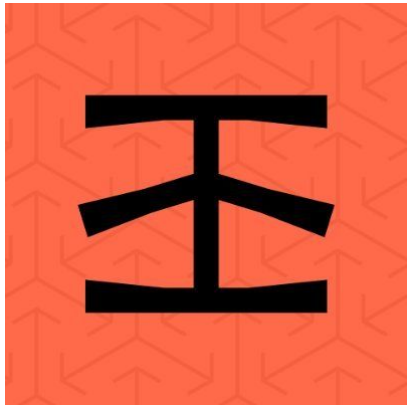
high-level programming language for implementing smart contracts

Hardhat

Ethereum development environment used compiling, deploying, interacting with the smart contracts and the Ethereum blockchain

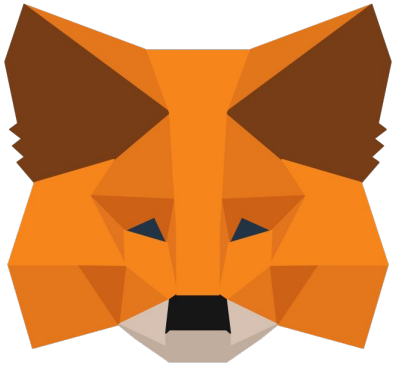
Infura

Ethereum API that offers access to the Ethereum networks (mainnet, testnets)



MetaMask

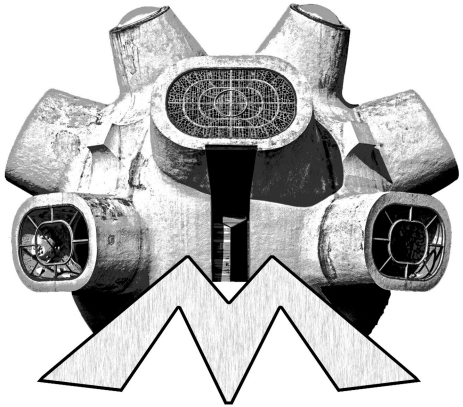
crypto wallet and gateway to blockchain apps



We are building **on-chain elections** (voting dapp) that sends **cryptocurrency** incentive rewards to voters

The cryptocurrency?

Makedonium



Used commands:

npx create-react-app .
npx hardhat
npx hardhat compile
npx hardhat run scripts/deploy --network network_name