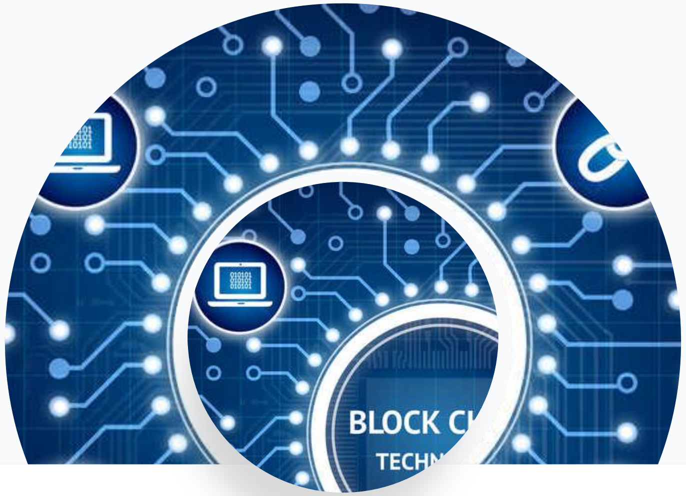


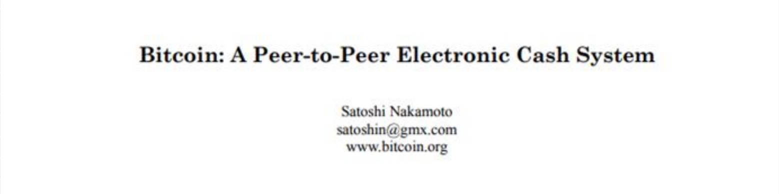
Blockchain

Natalia Milovantseva, PhD

07.02.2018

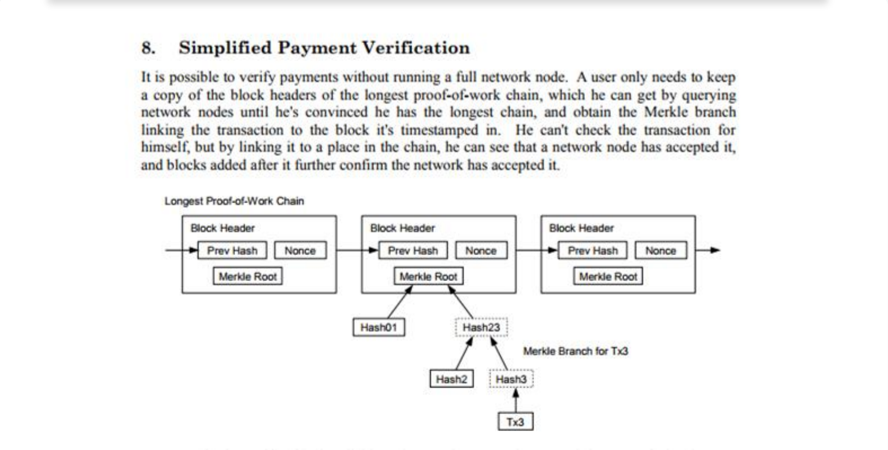
Some history…

- **Satoshi Nakamoto published a paper in 2008**
- **Proposed a system for electronic transactions without relying on trust**
- **No mention of "*blockchain*"**
- **Launched the Bitcoin (bitcoin.org)**
- **Is blockchain a new technology?**
  - P2P networking
  - distributed timestamping
  - cryptographic hashing functions
  - digital signatures
  - Merkle trees



Bitcoin: A Peer-to-Peer Electronic Cash System

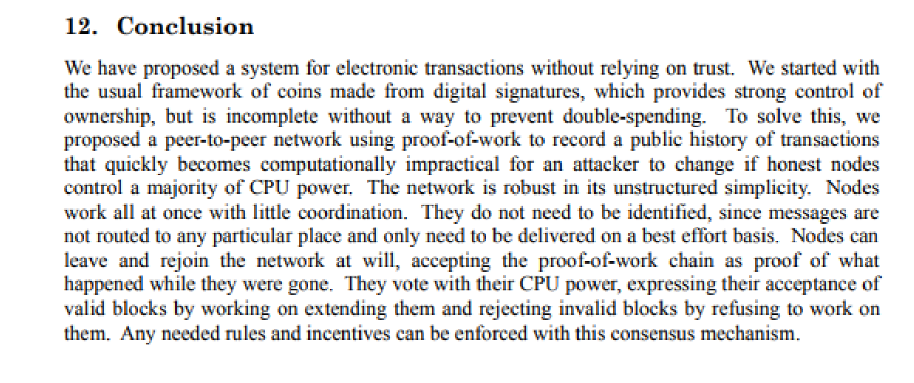
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org



8. Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

Longest Proof-of-Work Chain
Block Header
Prev Hash
Nonce
Merkle Root
Block Header
Prev Hash
Nonce
Merkle Root
Block Header
Prev Hash
Nonce
Merkle Root
Hash01
Hash23
Merkle Branch for Tx3
Hash2
Hash3
Tx3

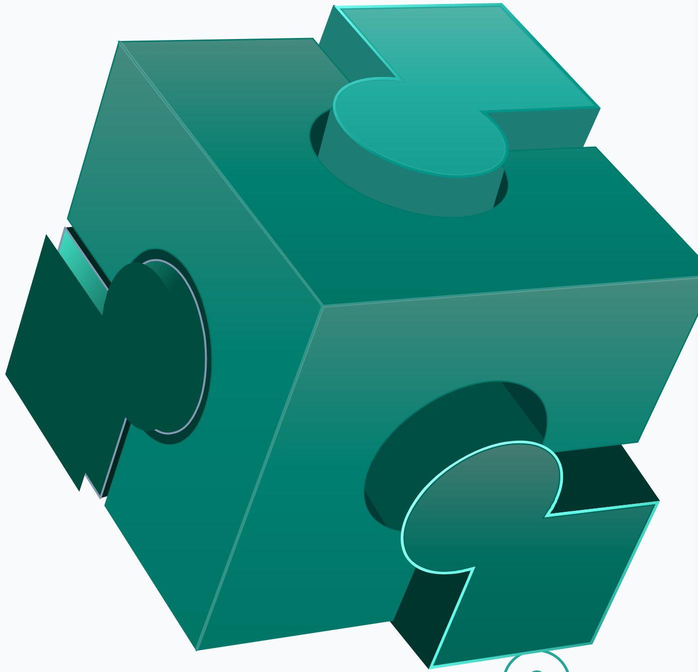


12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

What is blockchain?

- Most of us “go to” a middleman we trust, such as a bank, to conduct a transaction
- Blockchain allows consumers and businesses to remove the need for a third party and connect directly
- Blockchain technology uses cryptography to keep transactions secure and creates a decentralized database of exchanges (distributed ledger), which everyone on the network can see



Just P2P network?

- So, if “blockchain allows consumers and businesses to connect directly” it’s a peer-to-peer (P2P) network. Right?

- But, other types of distributed databases, sold by software vendors, also have no central database manager. Why is blockchain different?

- Blockchain achieves consistent and reliable agreement over a record of events between independent participants

  and the do not need to trust other participants

Blockchain reduces the need for a “trusted middleman”

- A consensus mechanism ensures that each participant’s view of shared database matches the view of all other participants

- “Double spending” problem - same digital file being “copy-and-pasted” and transferred multiple times

- To prevent the “double spending’”problem, a centralized ledger or party needed to stop users from duplicating/spending the same digital file twice.

- No need for a trusted central authority!

General components of a blockchain

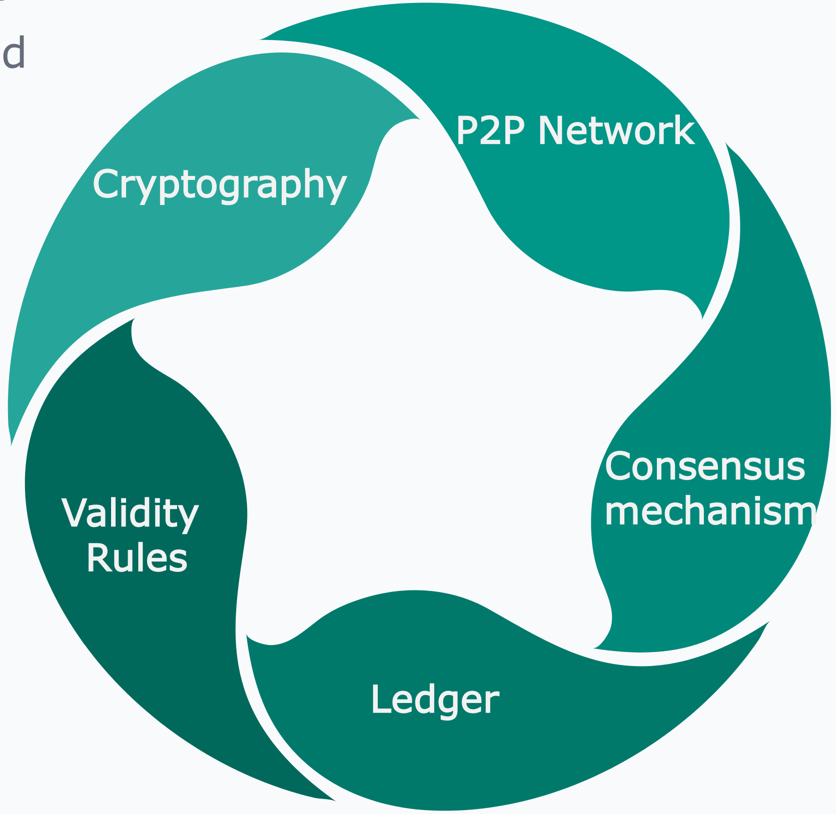
✓ **Cryptography**
-oneway hash functions, Merkle trees, public key infrastructure

✓ **Peer-to-peer network**
-to discover peers and share data

✓ **Consensus mechanism**
-algorithm to determine the ordering of transactions in an adversarial environment

✓ **Ledger**
-list of transactions in “blocks”

✓ **Validity Rules**
-what transactions are considered valid, how the ledger gets updated



Blockchain’s main value proposition

- ✓ All network participants can independently verify the content of the network's database at a specific moment in time

- ✓ This means, all participants have a consistent view of the shared database at a specific moment in time

- ✓ Therefore, any tampering by a malicious actor will be detected and rejected

Benefits of blockchain technology -1

- Shared control over the access to and evolution of data
- Clarity around asset and data ownership
- Can be used as the authoritative data source of ownership claims
- Complete control: the asset or data cannot be transferred without the owner’s explicit consent

Benefits of blockchain technology -2

Using a blockchain may help:

- □ Reduce the need for trust between stakeholders (problem with abuse of trust, such as fraud)
- □ Build a secure value transfer system

Benefits of blockchain technology -2

Using a blockchain may help:

- □ Reduce the need for trust between stakeholders (problem with abuse of trust, such as fraud)
- □ Build a secure value transfer system
- □ Streamline business processes across multiple entities (reconcile)
- □ Increase record transparency and ease of auditability

Blockchain myths and reality

Myth

1) Blockchains are ‘trustless’
2) Blockchains are immutable or ‘tamper-proof’
3) Blockchains are 100% secure
4) Blockchains are ‘truth machines’

Reality

1) Blockchains always require some degree of trust

2) Transactions on a blockchain network can be reversed by network participants under specific circumstances

3) Blockchains are not automatically more secure than other systems (“51% attack”)

4) GIGO applies to every blockchain that uses external data inputs

Open blockchains

- Bitcoin was launched as open public blockchains

  - □ a simple P2P value transfer public blockchain network
  - □ a public infrastructure
  - □ run by anonymous miners
  - □ powered by an unregulated, volatile currency

- - With all the benefits, blockchain was noted as a key innovation

  - However, institutions were uncomfortable with open public blockchains

  - Organizations began developing closed blockchains

Closed blockchains

Closed blockchains are 'private' or '*permissioned*' blockchains in which:

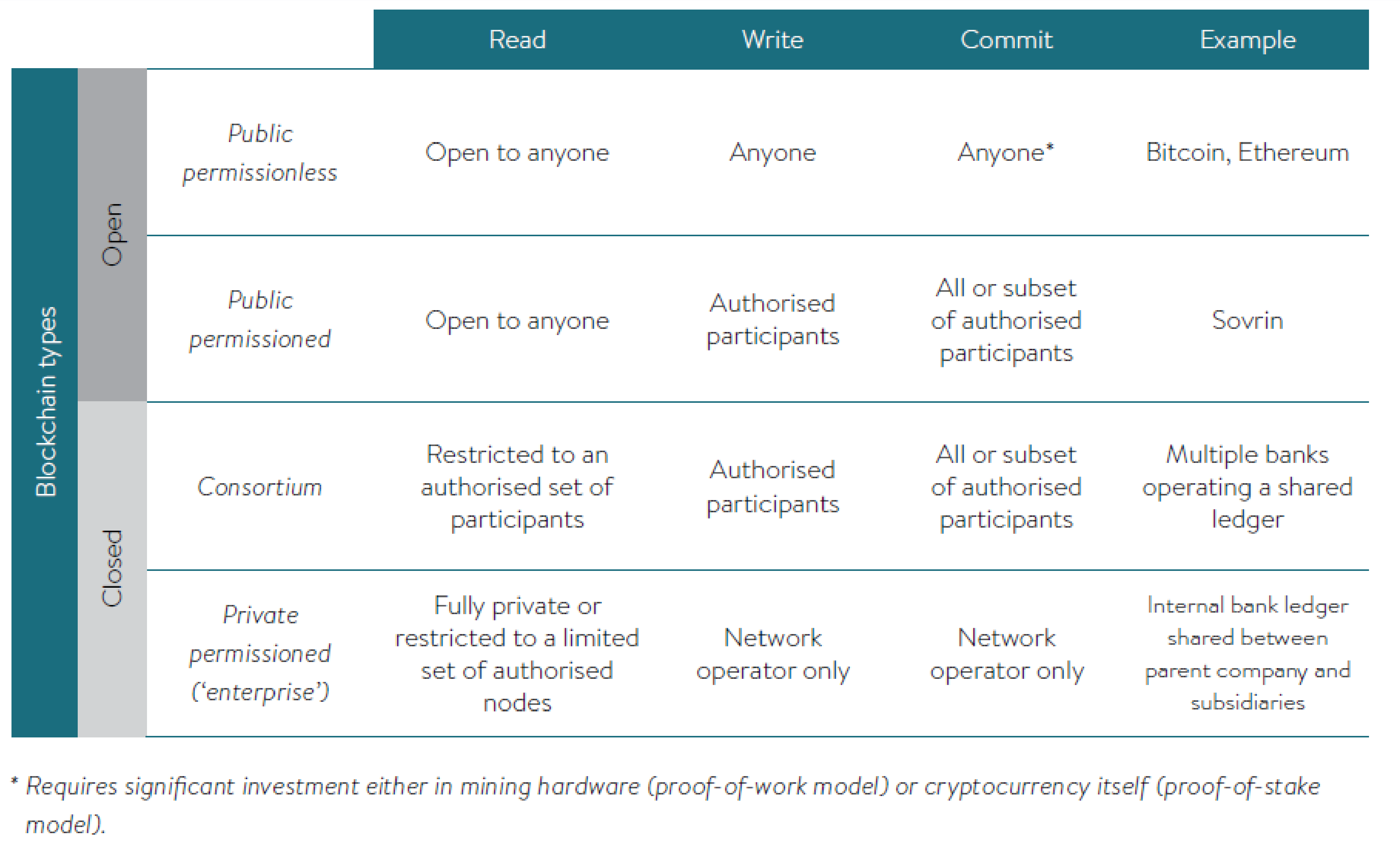
□ access is restricted to a specific set of vetted participants

□ different types of permissions that are granted to participants of a blockchain network

□ 3 major types of permission can be set when configuring a blockchain network:

- □ Read (who can access the ledger and see transactions),
- □ Write (who can generate transactions and send them to the network)
- □ Commit' (who can update the state of the ledger)

Main types of blockchains



			Read	Write	Commit	Example
Blockchain types	Open	*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
	Closed	*Consortium*	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ('enterprise')	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

* *Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model).*

Security and threat model: open vs. closed blockchains

- Public permissionless blockchains
  - □ hostile environment
  - □ unknown actors
  - □ require '*crypto-economics*'
    - □ combination of game theory and economic incentive applied to cryptographic systems to reward miners with tokens , such as bitcoins

- Private permissioned blockchains
  - □ participants are known and vetted
  - □ liable through off-chain legal contracts and agreements
  - □ no need for a token to incentivize good behavior

Blockchains and distributed ledgers are types of distributed databases

Distributed ledgers are a subset of **distributed databases**.
Blockchains are a subset of **distributed ledgers.**

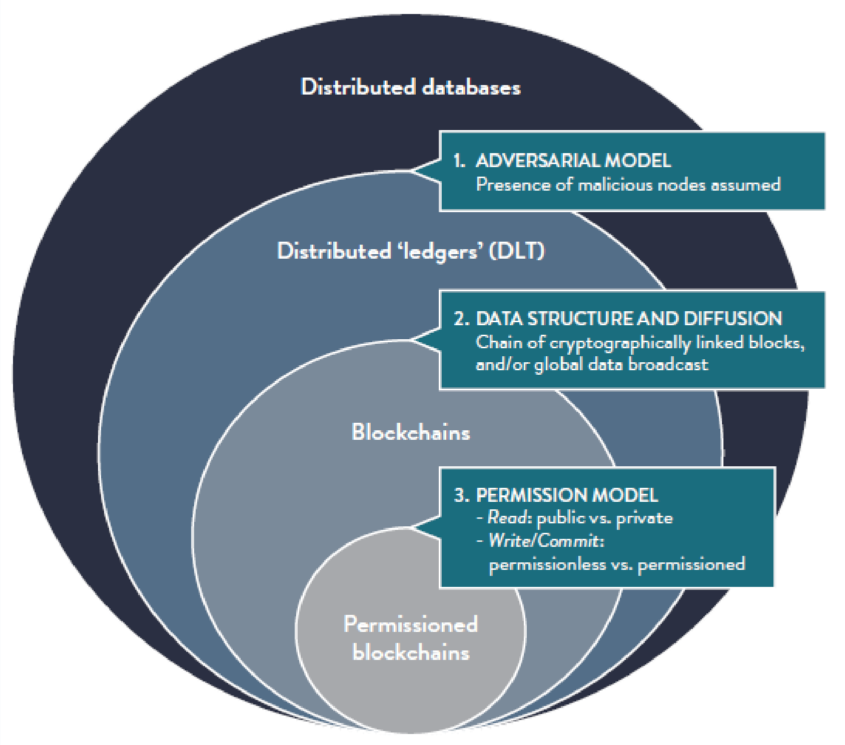
Distributed databases:

□ type of database where data is stored *across multiple computing devices*

□ no central ‘master database’

□ replicated across multiple collaborating devices to maintain a consistent view of the state of the database

□ assumed that *all nodes are honest*



Distributed databases

1. ADVERSARIAL MODEL
Presence of malicious nodes assumed

Distributed ‘ledgers’ (DLT)

2. DATA STRUCTURE AND DIFFUSION
Chain of cryptographically linked blocks, and/or global data broadcast

Blockchains

3. PERMISSION MODEL
- *Read:* public vs. private
- *Write/Commit:* permissionless vs. permissioned

Permissioned blockchains

Blockchains and distributed ledgers are types of distributed databases

Distributed ledgers are a subset of **distributed databases.**
Blockchains are a subset of **distributed ledgers.**

Distributed databases:

□ type of database where data is stored *across multiple computing devices*

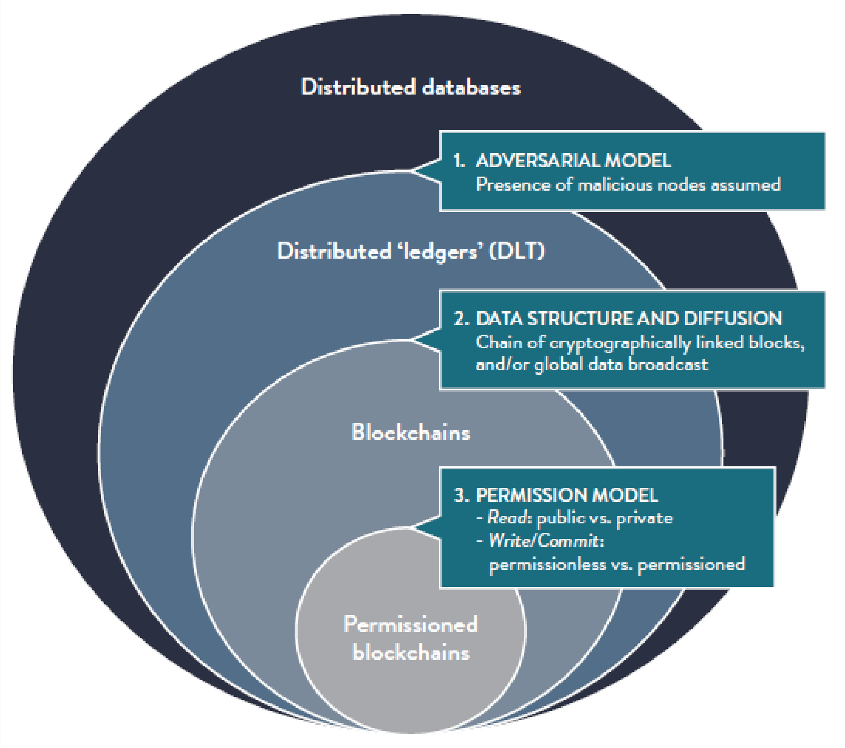
□ no central ‘master database’

□ replicated across multiple collaborating devices to maintain a consistent view of the state of the database

□ assumed that *all nodes are honest*

Distributed ledgers:

□ type of distributed database that assumes the possible *presence of malicious users* (nodes)



1. ADVERSARIAL MODEL
Presence of malicious nodes assumed

2. DATA STRUCTURE AND DIFFUSION
Chain of cryptographically linked blocks, and/or global data broadcast

3. PERMISSION MODEL
- *Read:* public vs. private
- *Write/Commit:* permissionless vs. permissioned

Blockchains and distributed ledgers are types of distributed databases

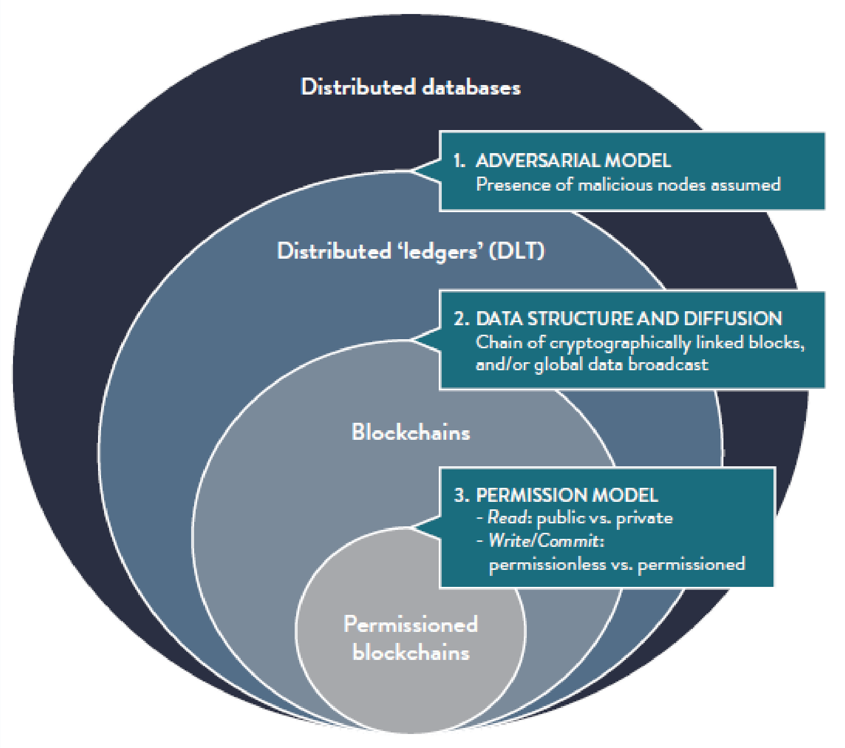
Distributed ledgers are a subset of **distributed databases**.
Blockchains are a subset of **distributed ledgers.**

Distributed databases …

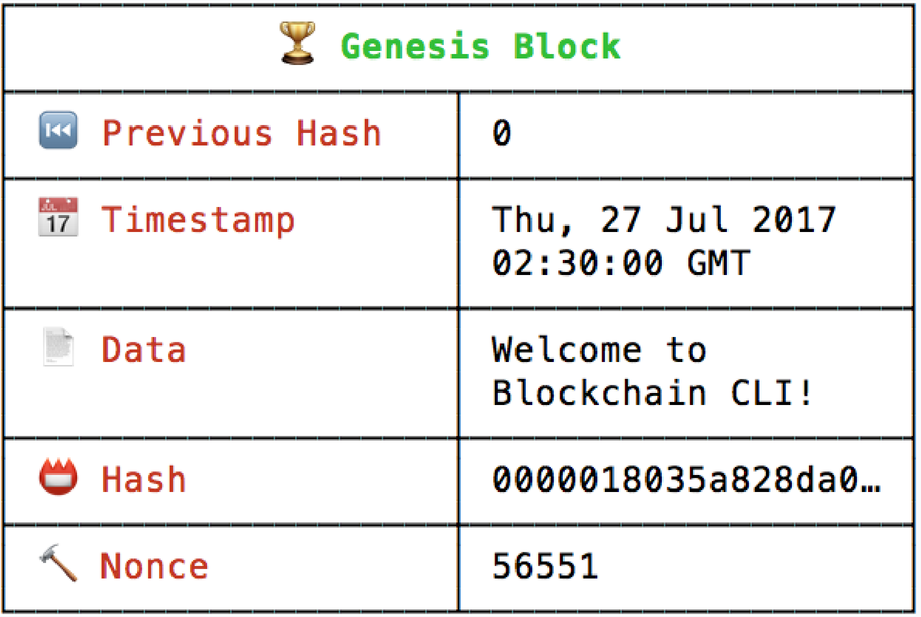
Distributed ledgers …

Blockchains

- □ type of distributed ledger that is composed of a chain of *cryptographically* linked ‘blocks’ containing batched transactions
- □ *broadcasts all data to all participants* in the network


Distributed databases
1. ADVERSARIAL MODEL
Presence of malicious nodes assumed
Distributed ‘ledgers’ (DLT)
2. DATA STRUCTURE AND DIFFUSION
Chain of cryptographically linked blocks, and/or global data broadcast
Blockchains
3. PERMISSION MODEL
- *Read:* public vs. private
- *Write/Commit:* permissionless vs. permissioned
Permissioned blockchains

The proof-of-work system



🏆 Genesis Block	
⏮ Previous Hash	0
📅 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
📄 Data	Welcome to Blockchain CLI!
📛 Hash	0000018035a828da0…
🔨 Nonce	56551

- **The four leading 0's** is a minimum requirement for a valid hash.
- A **nonce** is a number used to find a **valid hash.**

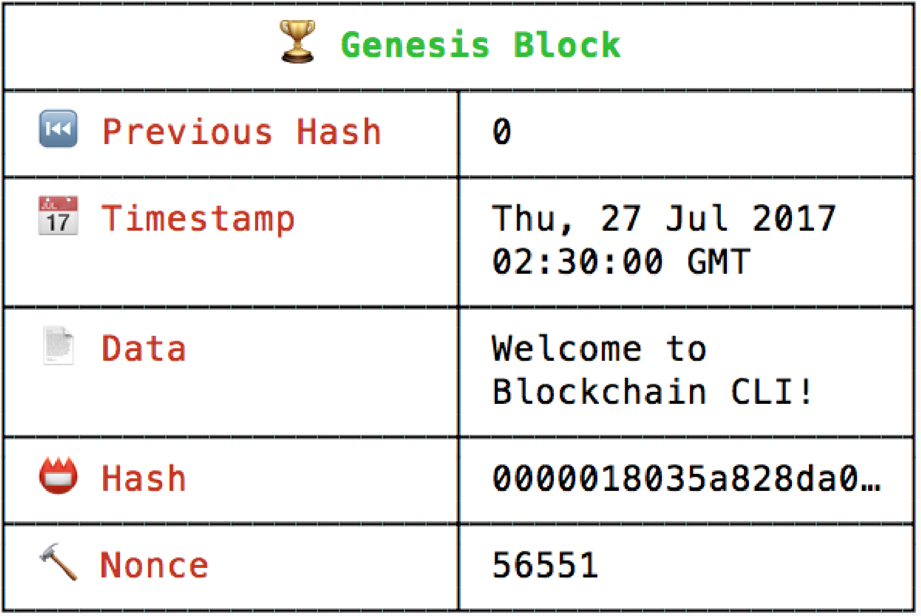
Index (Block #): Which block is it? (Genesis block has index 0)
Hash: Is the block valid?
Previous Hash: Is the previous block valid?
Timestamp: When was the block added?
Data: What information is stored on the block?
Nonce: How many iterations did we go through before we found a valid block?

- Each block on the blockchain is dependent on the previous block
- When a new block is mined, the blockchain looks at the latest block on the blockchain for the index and previous hash
- **A hash value is a numeric value of a fixed length that uniquely identifies data**
- The **hash** is calculated by taking the **index**, **previous block hash**, **timestamp**, **block data,** and **nonce** as input

```
CryptoJS.SHA256(index + previousHash + timestamp + data + nonce)
```

- The **SHA256** algorithm will calculate a unique hash, given those inputs

Mining the first block



🏆 Genesis Block	
⏮ Previous Hash	0
📅 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
📄 Data	Welcome to Blockchain CLI!
📛 Hash	0000018035a828da0…
🔨 Nonce	56551

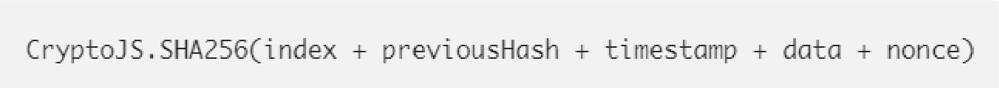
Index: 0+1=1

Previous Hash: 0000018035a828da0…

Timestamp: When the block is added

Data: we ❤this class

Hash: computed



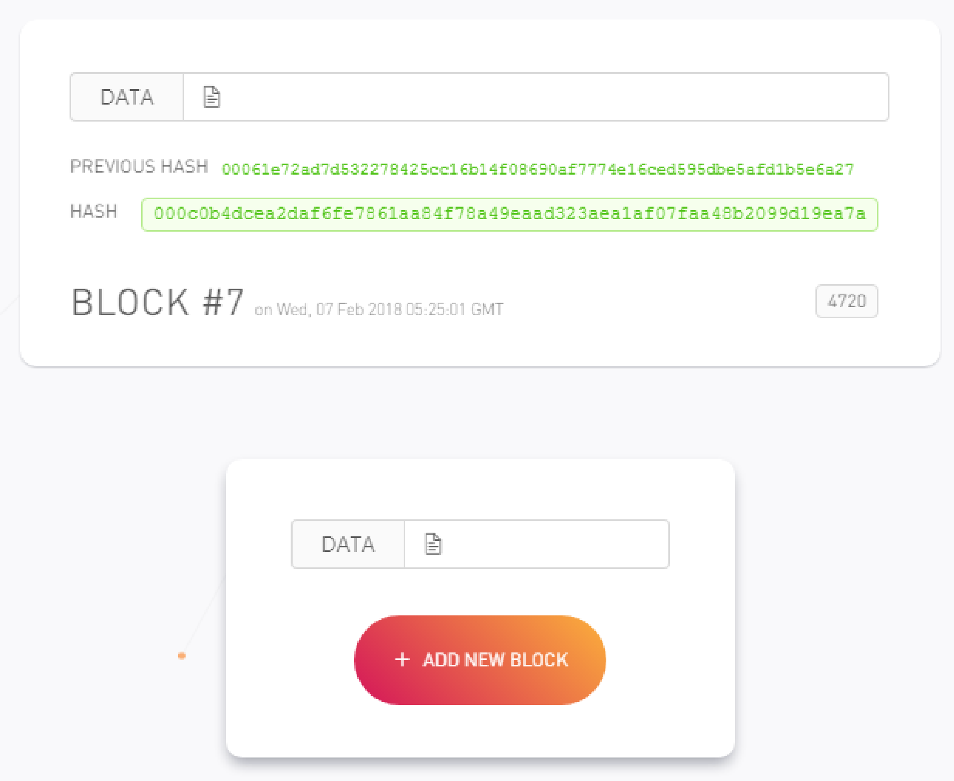
```
CryptoJS.SHA256(index + previousHash + timestamp + data + nonce)
```

A hash value is a numeric value of a fixed length that uniquely identifies data.

Nonce: the number used to find a valid hash.

We have the **following blockchain A → B → C**. Someone wants to **change data on Block A**. This is what happens: Data changes on Block A. **Block A's hash changes** because **data is used to calculate the hash.**
Block A becomes invalid because its hash no longer has **four leading 0's.**
Block B's hash changes because **Block A's hash was used to calculate Block B's hash.**
Block B becomes invalid because its hash no longer has **four leading 0's.**
Block C's hash changes because **Block B's hash was used to calculate Block C's hash.**
Block C becomes invalid because its hash no longer **has four leading 0's.**
The only way to mutate a block would be to mine the block again, and all the blocks after. Since new blocks are always being added, it's nearly impossible to mutate the blockchain.

Blockchain demo



DATA

PREVIOUS HASH 00061e72ad7d532278425cc16b14f08690af7774e16ced595dbe5afd1b5e6a27

HASH 000c0b4dcea2daf6fe7861aa84f78a49eaad323aea1af07faa48b2099d19ea7a

BLOCK #7 on Wed, 07 Feb 2018 05:25:01 GMT

4720

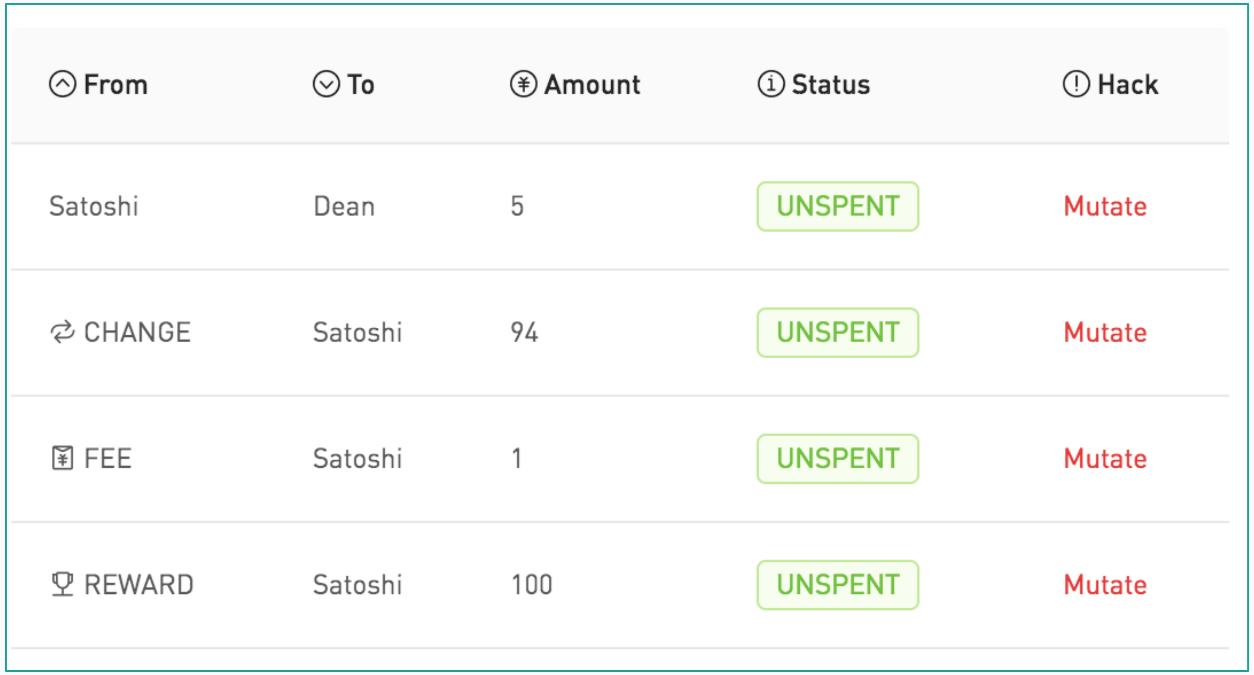
DATA

https://blockchaindemo.io/

Blockchain as a base for cryptocurrency

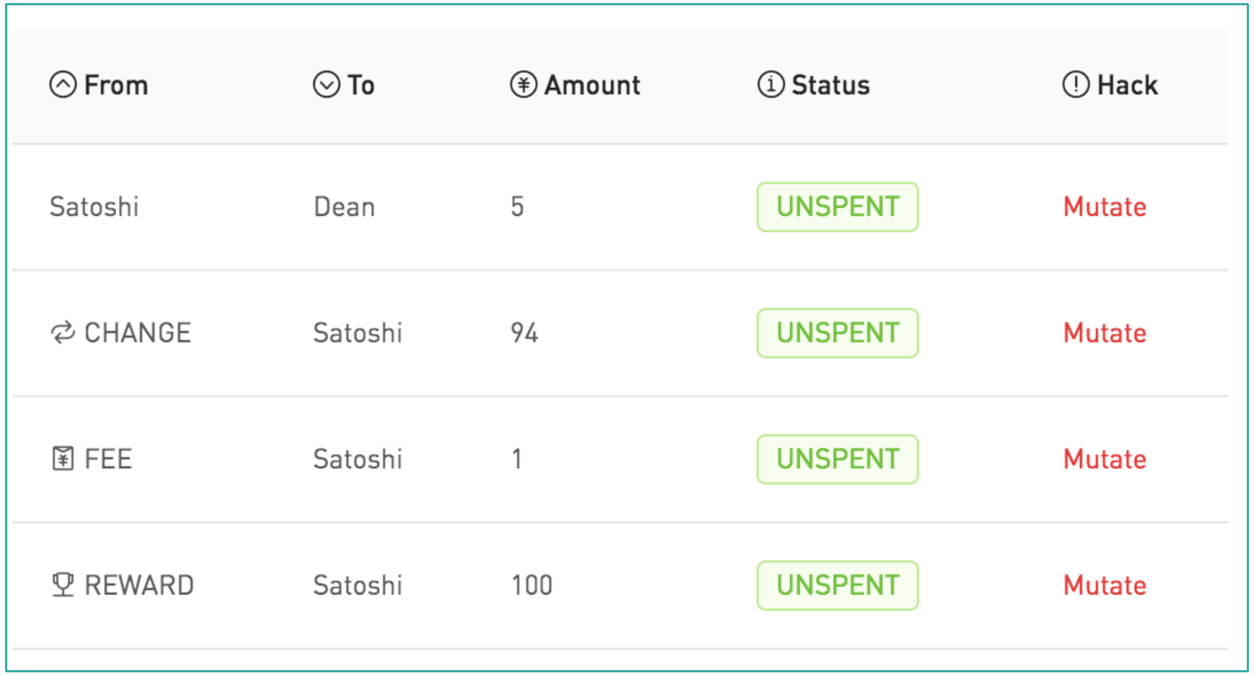
Transaction is created to record an exchange of value

Transaction outputs

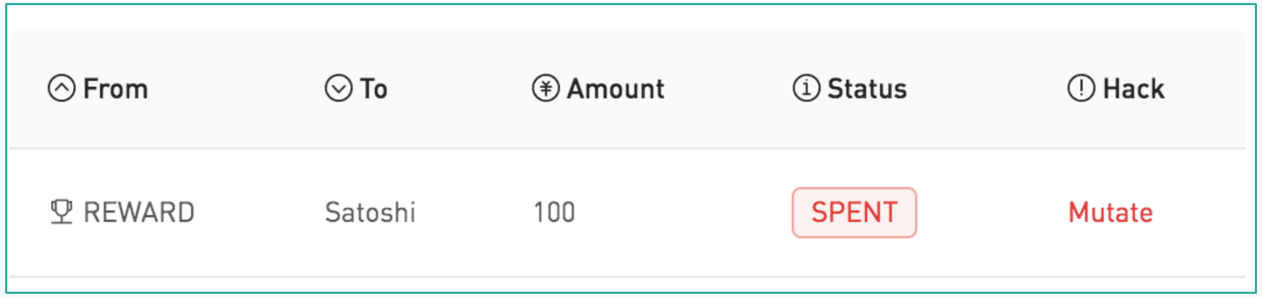


From	To	Amount	Status	Hack
Satoshi	Dean	5	UNSPENT	Mutate
CHANGE	Satoshi	94	UNSPENT	Mutate
FEE	Satoshi	1	UNSPENT	Mutate
REWARD	Satoshi	100	UNSPENT	Mutate

Cryptocurrency transactions



From	To	Amount	Status	Hack
Satoshi	Dean	5	UNSPENT	Mutate
CHANGE	Satoshi	94	UNSPENT	Mutate
FEE	Satoshi	1	UNSPENT	Mutate
REWARD	Satoshi	100	UNSPENT	Mutate



From	To	Amount	Status	Hack
REWARD	Satoshi	100	SPENT	Mutate

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block

Regular — Satoshi paid Dean 5 coins with change of 94 coins

Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from

Outputs — Where value is going to

Hash —Uniquely identifies the transaction (using inputs & outputs)

Type — Reward, Regular, or Fee

Transactions

Satoshi mined a new block with a mining reward of 100.
Type of Transaction: ?

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Satoshi mined a new block with a mining reward of 100.
Type of Transaction: Reward

Inputs: ?

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Satoshi mined a new block with a mining reward of 100.
Type of Transaction: Reward

Inputs: 0

Outputs: ?

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Satoshi mined a new block with a mining reward of 100.
Type of Transaction: Reward

Inputs: 0

Outputs: 100

Hash: ?

A hash value is a numeric value of a fixed length that uniquely identifies data

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Satoshi mined a new block with a mining reward of 100.
Type of Transaction: Reward

Inputs: 0

Outputs: 100

Hash: f(index; previous block hash; timestamp; block data; nonce) = 000abcdefg…

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

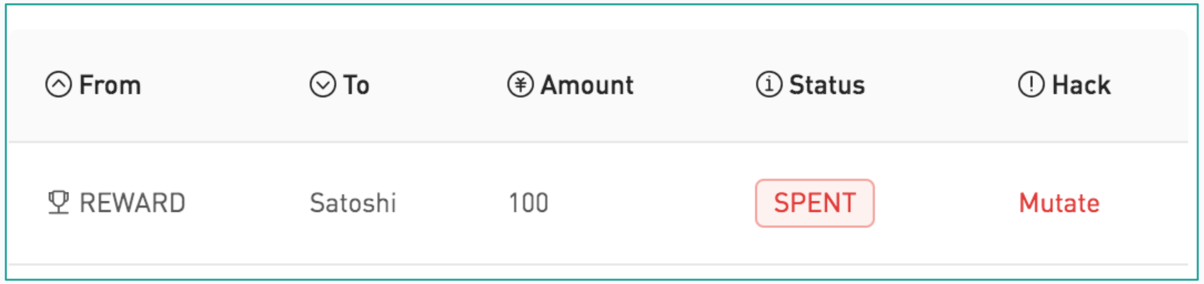
Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Regular Transaction- created when one party pays another.

Satoshi uses the (**unspent**) output from the reward transaction as an input to pay Dean 5 coins. He specifies a **mining fee of 1 coin**.

Type: Regular
Inputs: 100 (output amount)
Outputs:
Output 1: Address: Dean’s address
Amount: 5 coins
Output 2: Address: Satoshi’s address
Amount: 94 coins= 100 - 5 (payment) - 1 (fee)



From	To	Amount	Status	Hack
REWARD	Satoshi	100	SPENT	Mutate

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Regular Transaction- created when one party pays another.

Satoshi uses the (**unspent**) output from the reward transaction as an input to pay Dean 5 coins. He specifies a **mining fee of 1 coin**.

Type: Regular
Inputs: 100 (output amount)
Outputs:
Output 1: Address: Dean's address
Amount: 5 coins
Output 2: Address: Satoshi's address
Amount: 94 coins= 100 - 5 (payment) - 1 (fee)

How does it add up?
The total input amount is
The total output amount is

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Regular Transaction- created when one party pays another.

Satoshi uses the (**unspent**) output from the reward transaction as an input to pay Dean 5 coins. He specifies a **mining fee of 1 coin**.

Type: Regular
Inputs: 100 (output amount)
Outputs:
Output 1: Address: Dean's address
Amount: 5 coins
Output 2: Address: Satoshi's address
Amount: 94 coins= 100 - 5 (payment) - 1 (fee)

How does it add up?
The total input amount is 100.
The total output amount is 5 + 94 = 99.
Input ≠ output . Where is 1 coin?

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Regular Transaction- created when one party pays another.

Satoshi uses the (**unspent**) output from the reward transaction as an input to pay Dean 5 coins. He specifies a **mining fee of 1 coin**.

Type: Regular
Inputs: 100 (output amount)
Outputs:
Output 1: Address: Dean's address
Amount: 5 coins
Output 2: Address: Satoshi's address
Amount: 94 coins= 100 - 5 (payment) - 1 (fee)

How does it add up?
The total input amount is 100.
The total output amount is 5 + 94 = 99.
Input ≠ output . Where is 1 coin?

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Transactions

Regular Transaction- created when one party pays another.

Satoshi uses the (**unspent**) output from the reward transaction as an input to pay Dean 5 coins. He specifies a **mining fee of 1 coin**.

Type: Regular
Inputs: 100 (output amount)
Outputs:
Output 1: Address: Dean's address
Amount: 5 coins
Output 2: Address: Satoshi's address
Amount: 94 coins= 100 - 5 (payment) - 1 (fee)

How does it add up?
The total input amount is 100.
The total output amount is 5 + 94 = 99.
Input ≠ output . Where is 1 coin?
The difference between inputs and outputs of a regular transaction is the mining fee (here – 1 coin)

Types of transactions

Reward — Satoshi rewarded with 100 coins for mining new block
Regular — Satoshi paid Dean 5 coins with change of 94 coins
Fee — Mining fee of 1 for whoever mines the transaction

Parts of transaction

Inputs — Where value is coming from
Outputs — Where value is going to
Hash —Uniquely identifies the transaction (using inputs & outputs)
Type — Reward, Regular, or Fee

Mining

Bob mines Satoshi and Dean's transaction.

Type: Fee

Inputs: None

Outputs: 1 (fee, difference of regular transaction input and output)
Address: Bob's public wallet address

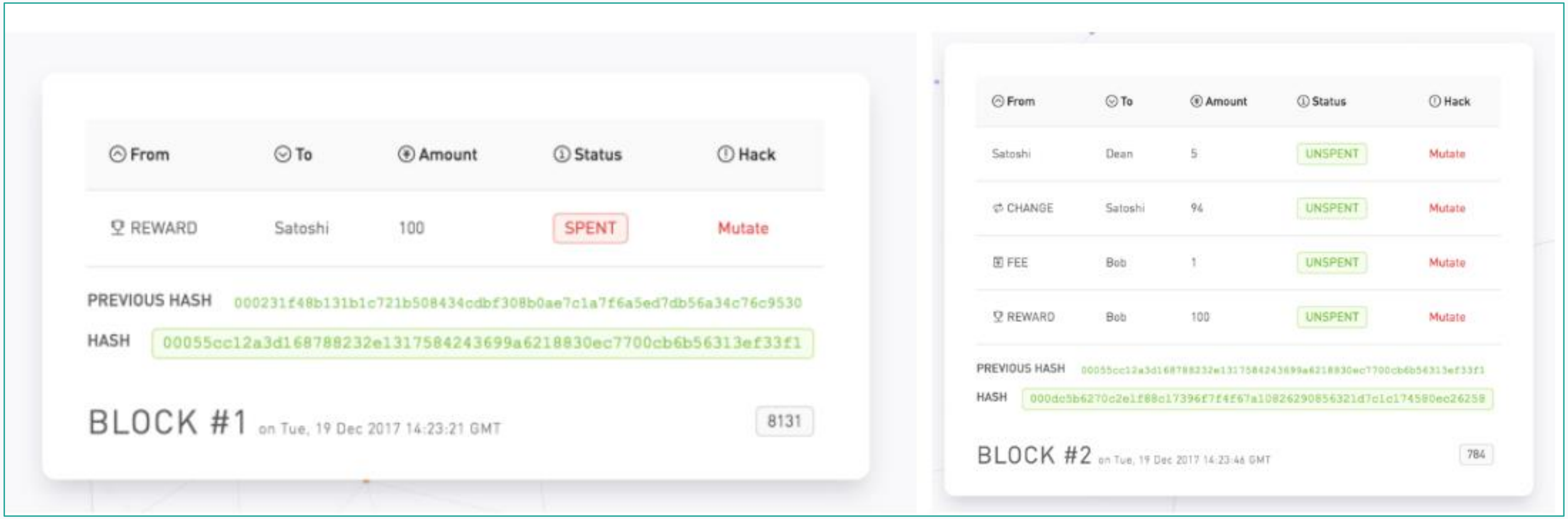
100 Because Bob mined this transaction to the new block, there will be a **reward transaction of 100 to Bob.**

Final Balance

Satoshi: 94 = 100 (reward) - 5 (payment) - 1 (fee)
Dean: 5 (payment from Satoshi)
Bob: 101 = 100 (reward from mining new block with transaction) + 1 (fee)

Total currencies in circulation: 200 = 94 (Satoshi)+ 5 (Dean)+ 101 (Bob)

Blockchain view



From	To	Amount	Status	Hack
REWARD	Satoshi	100	SPENT	Mutate

PREVIOUS HASH 000231f48b131b1c721b508434cdbf308b0ae7c1a7f6a5ed7db56a34c76c9530

HASH 00055cc12a3d168788232e1317584243699a6218830ec7700cb6b56313ef33f1

BLOCK #1 on Tue, 19 Dec 2017 14:23:21 GMT 8131

From	To	Amount	Status	Hack
Satoshi	Dean	5	UNSPENT	Mutate
CHANGE	Satoshi	94	UNSPENT	Mutate
FEE	Bob	1	UNSPENT	Mutate
REWARD	Bob	100	UNSPENT	Mutate

PREVIOUS HASH 00055cc12a3d168788232e1317584243699a6218830ec7700cb6b56313ef33f1

HASH 000dc5b6270c2e1f88c17396f7f4f67a10826290856321d7c1c174580ec26258

BLOCK #2 on Tue, 19 Dec 2017 14:23:46 GMT 784

Two blocks were mined, and each block has a reward of 100, so there should be 200 coins in circulation.

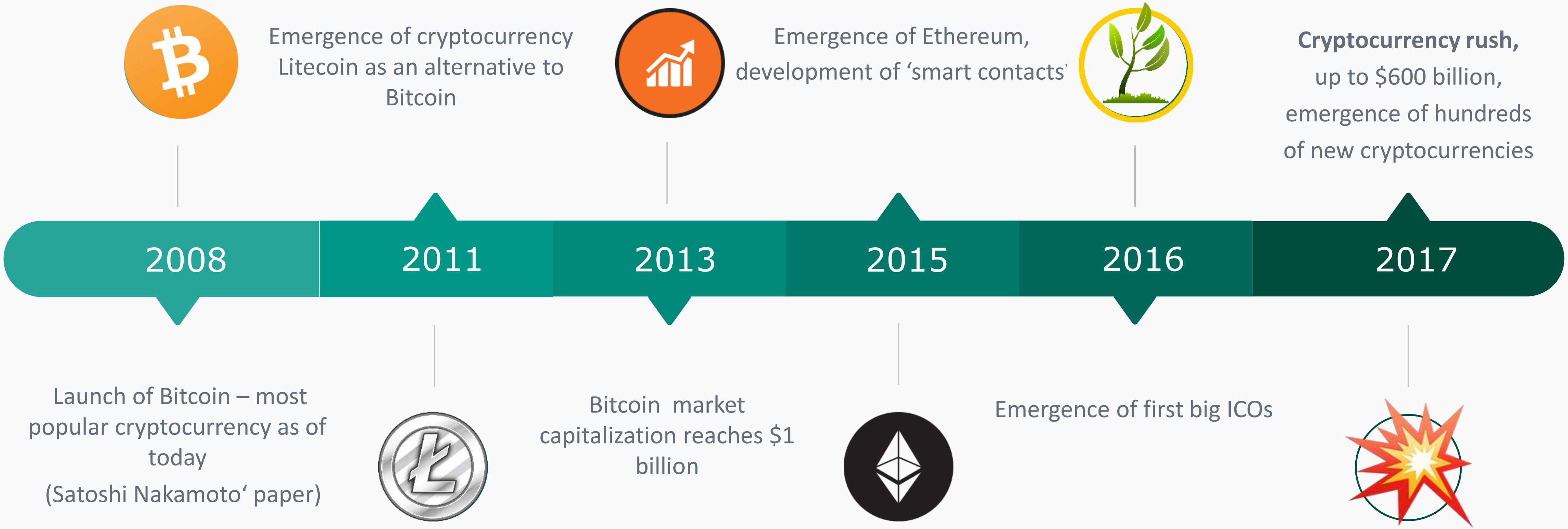
Cryptocoin mining

- Adding transaction records to a cryptocurrency ledger of past transactions .

- It is, as we have examined, a chain of blocks.

- The mining computers collect pending transactions (“blocks”) and turn them into a mathematical equation. The miner who found the solution gets reward.

History of cryptocurrency



2008

Launch of Bitcoin – most popular cryptocurrency as of today

(Satoshi Nakamoto‘ paper)

2011

Emergence of cryptocurrency Litecoin as an alternative to Bitcoin

2013

Bitcoin market capitalization reaches $1 billion

2015

Emergence of Ethereum, development of ‘smart contacts’

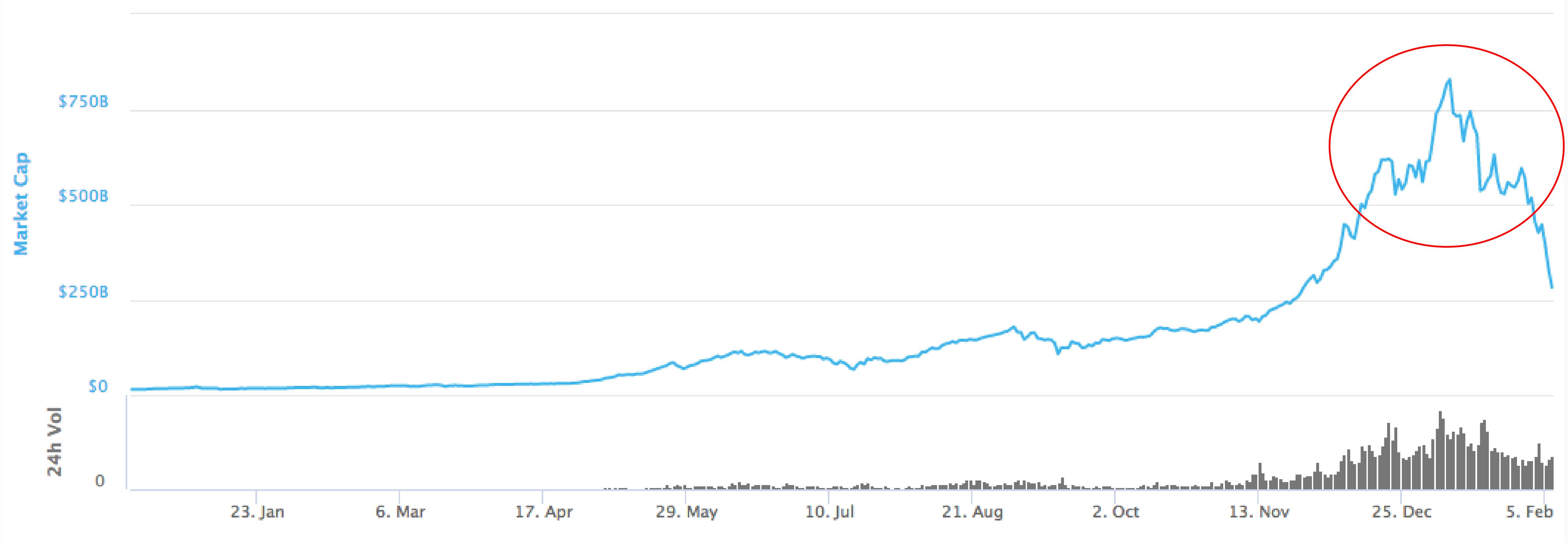
2016

Emergence of first big ICOs

2017

Cryptocurrency rush,
up to $600 billion,
emergence of hundreds
of new cryptocurrencies

Cryptocurrency capitalization, 2017-2018



Blockchain in the digitl economy

□ Network principle of the organization of society, the transition from centralized systems to communities.

□ Changes in the economy – from mass production of goods to individual production for masses

□ The main value is knowledge and the community. Communities are not limited territories and states

□ The ways economic value is created now – creation of profitable networks and new values

□ Decentralized blockchain-networks are the top of this process, which began with social networks and mass Internet services

How cryptocurrency enters the economy

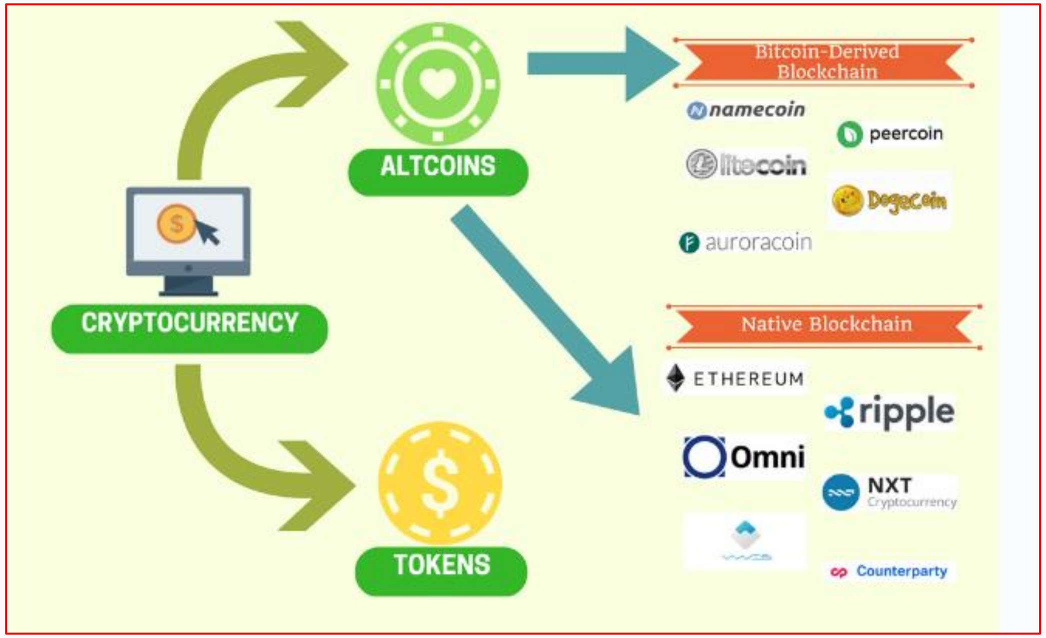
- ICO - Initial cryptocurrency Offerings (*the essence of IPO?)*

- ICO project takes fiat money (another cryptocurrency) and emits new cryptocurrency or allows to generate it to public.
  - Fiat money is a currency without intrinsic value (vs. *commodity* and *representative* money)

- Emitted cryptocurrencies are used as new means of trade or for capital gain.

- Why people trust cryptocurrencies?
  - Vulnerability to cyber-burglary!
  - Popularity depends on what people **expect** from fiat and what **operations** with them are (or **expected to be**) available (capital gain, alternative cryptocurrencies…)

Types of cryptocurrency



- **Altcoins**
  - coins that are an alternative to Bitcoin. Alternative cryptocurrency coins are also called simply “coins”. They’re often used interchangeably.

- **Tokens**
  - representation of a particular asset or utility, that usually resides on top of another blockchain.
  - can represent basically any asset that are fungible and tradeable, from *commodities* to *loyalty points* to even *other cryptocurrencies*

Motivation for crypto money

Individual

Positive

1. Relative anonymity (quasi- anonymity)
2. Relatively easy trading operations, liquidity
3. New means of hoarding
4. Rapid investment growth interest, “cryptocurrency rush”, positive expectations
5. Currently low regulation
6. Possible means for tax evasion
7. Prospective for growth

Negative

1. Low protection in a case of a crypto-burglary
2. Intensive competition with other cryptocurrencies
3. Limited insurance from currency risks
4. High volatility of exchange rate with other currencies
5. Limited conversion into real assets or goods

BLOCKCHAIN