PWL # 7:
"**Bitcoin: A Peer-to-Peer Electronic Cash System**"
Satoshi Nakamoto

Papers We Love ❤ Brasília

Presenter: Alessandro Leite

February 22, 2018

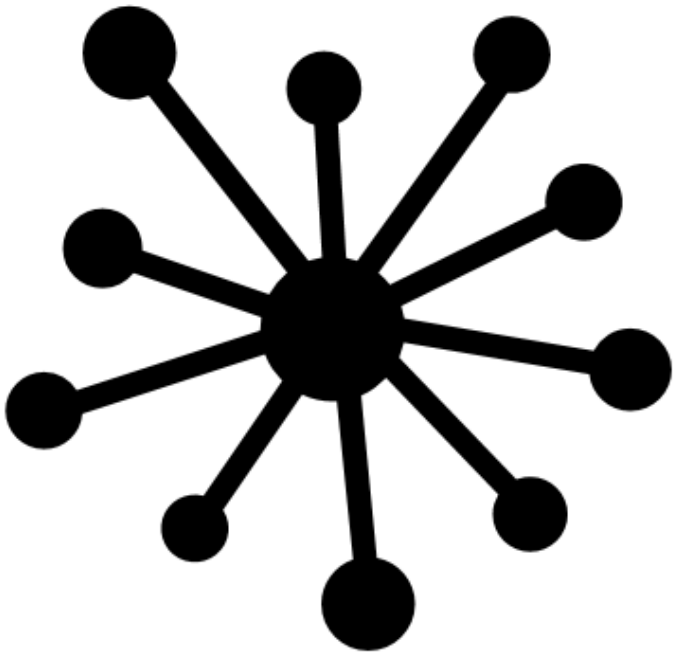
Outline


BITCOIN·DIGITAL·DECENTRALIZED·PEER
METALS
1OZ 999 FINE COPPER

What is Bitcoin?

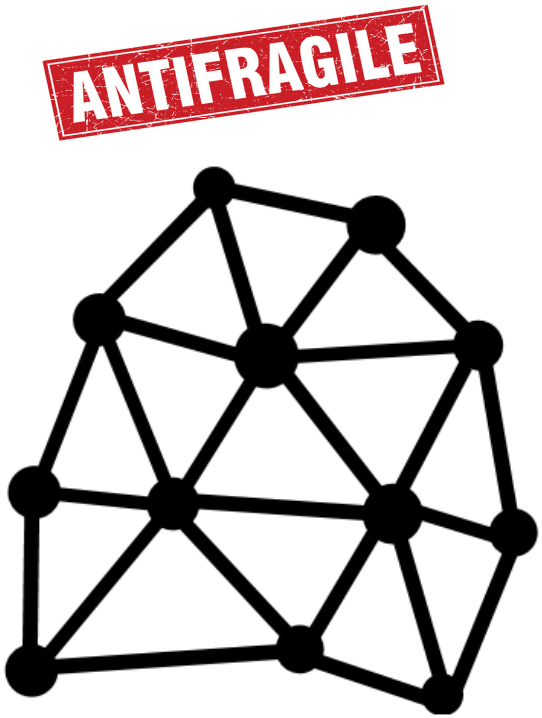
- First decentralised cryptocurrency
- An electronic payment system based on cryptographic proof instead of trust
- Developed by a person or a group under the pseudonym of **Satoshi Nakamoto** in 2008
- It is in operation since early 2009
- It works without the management of any financial institution

What are the characteristics of a **centralised network**?



- Requires huge amount of storage
- Demands high computing power
- It is a bottleneck
- Fallible to a physical or viral attack

What are the characteristics of a **distributed network**?



- The nodes are independent
- The computing power is distributed
- It is a robust network
- The role of the peers is symmetric

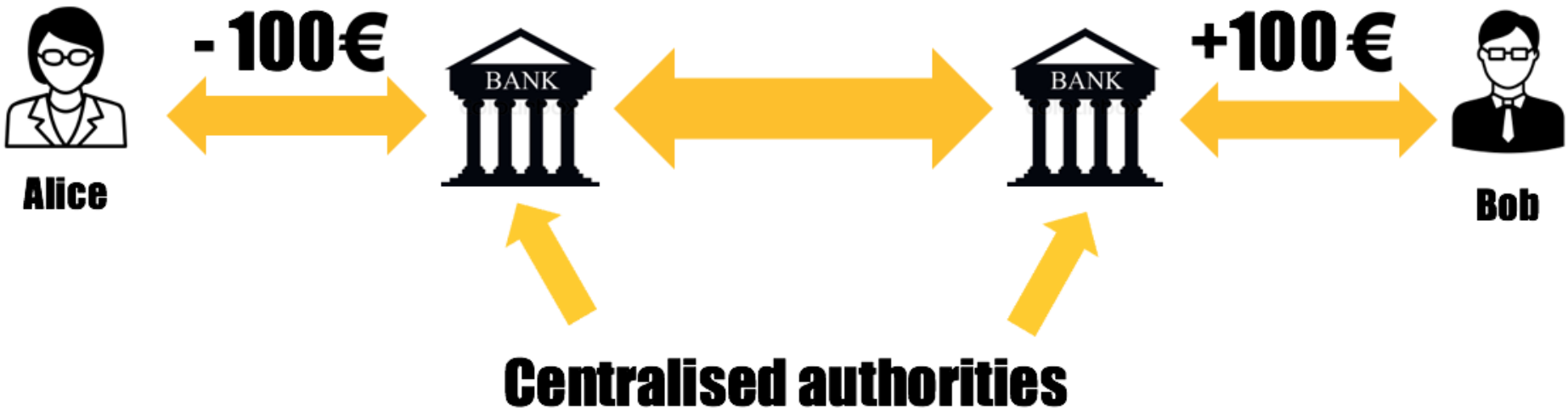
Bitcoin relies on a distributed (i.e., Peer-to-Peer (P2P)) network

What is a Peer-to-Peer (P2P) system?

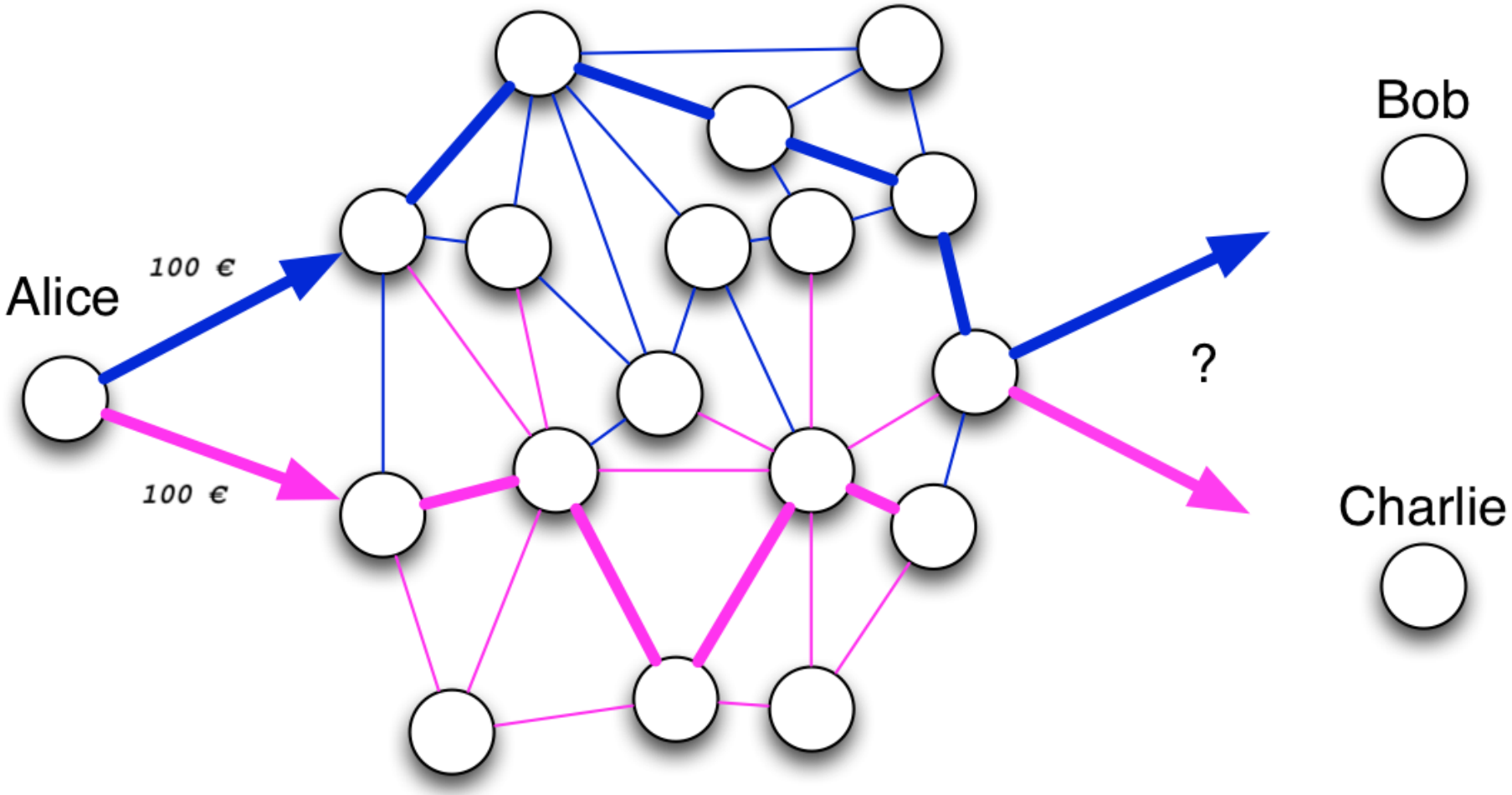
Peer-to-peer systems are **distributed systems** where the nodes (i.e., peers) **autonomously** organise the system topology and respond to external usage in a **decentralised fashion** to share resources **without any central control**[a].

[a] Stephanos Androutsellis-Theotokis and Diomidis Spinellis. "A Survey of Peer-to-peer Content Distribution Technologies". In: *ACM Computing Survey* 36.4 (2004), pp. 335–371.

What is the problem of double-spend coin in the currently financial system?

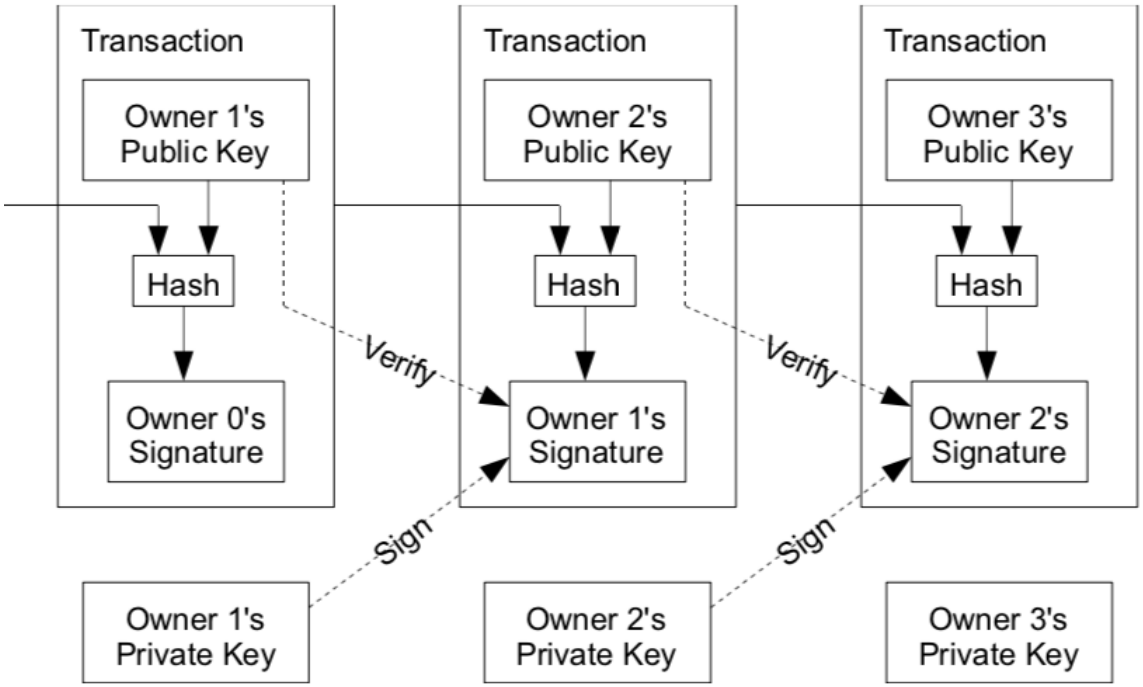


What are the challenges of solving the problem of double-spend coin in a distributed scenario?



What is an electronic coin?

- It's a chain of digital signatures
- In Bitcoin, coin's **ownership** and **transfer** are **ensured** by **digital signatures**
- Coins ownerships are **broadcasted** through the **P2P network** following a **best-effort** approach.



In Bitcoin, all the transactions are public but anonymous

- Nodes collects the transactions into **blocks**
- A **block** contains information about the transactions and the **previous block** linking to the first block when the Bitcoin network started.
- In other words, all the transactions are written in a data store known as **blockchain**.
- The blockchain file is maintained on every node.
- Each block carries a **proof-of-work**

So ... what is the Bitcoin's Blockchain?

- Blockchain is:
  - **a transaction log** (= database)
  - **distributed** (= shared through a P2P network)
  - **secure** (= protected by cryptographic primitives)
  - **indestructible** (= or almost ..., as there are multiple copies distributed across the network)
  - **open** (= even if there is the option to store encrypted data)
  - **formed by blocks successively validated**, **timestamped**, and **chronologically organised**.

How to deal with untrusted nodes?

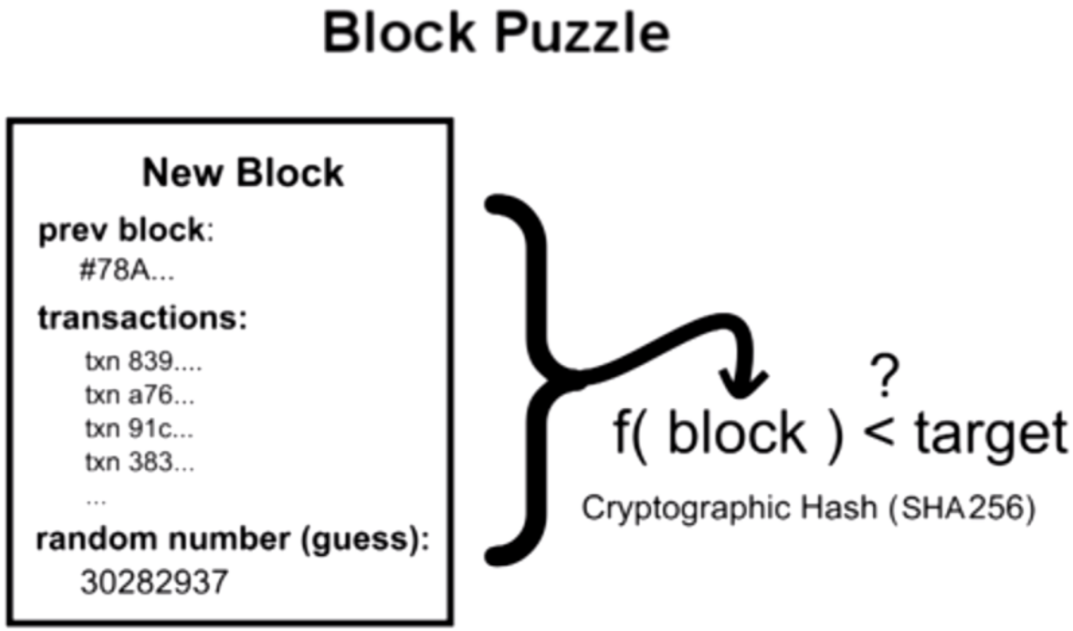
- **Transaction** history **cannot be changed** unless **redoing** all the **proof-of-work** of all blocks in the blockchain.
- Redoing blocks' proof-of-work means recalculating all the proof-of-work from successors.
- Thus, the **double spending problem** is solved using a **P2P timestamp server** to generate **computational proof** of the chronological order of the transactions.

What does characterise the **proof-of-work**?

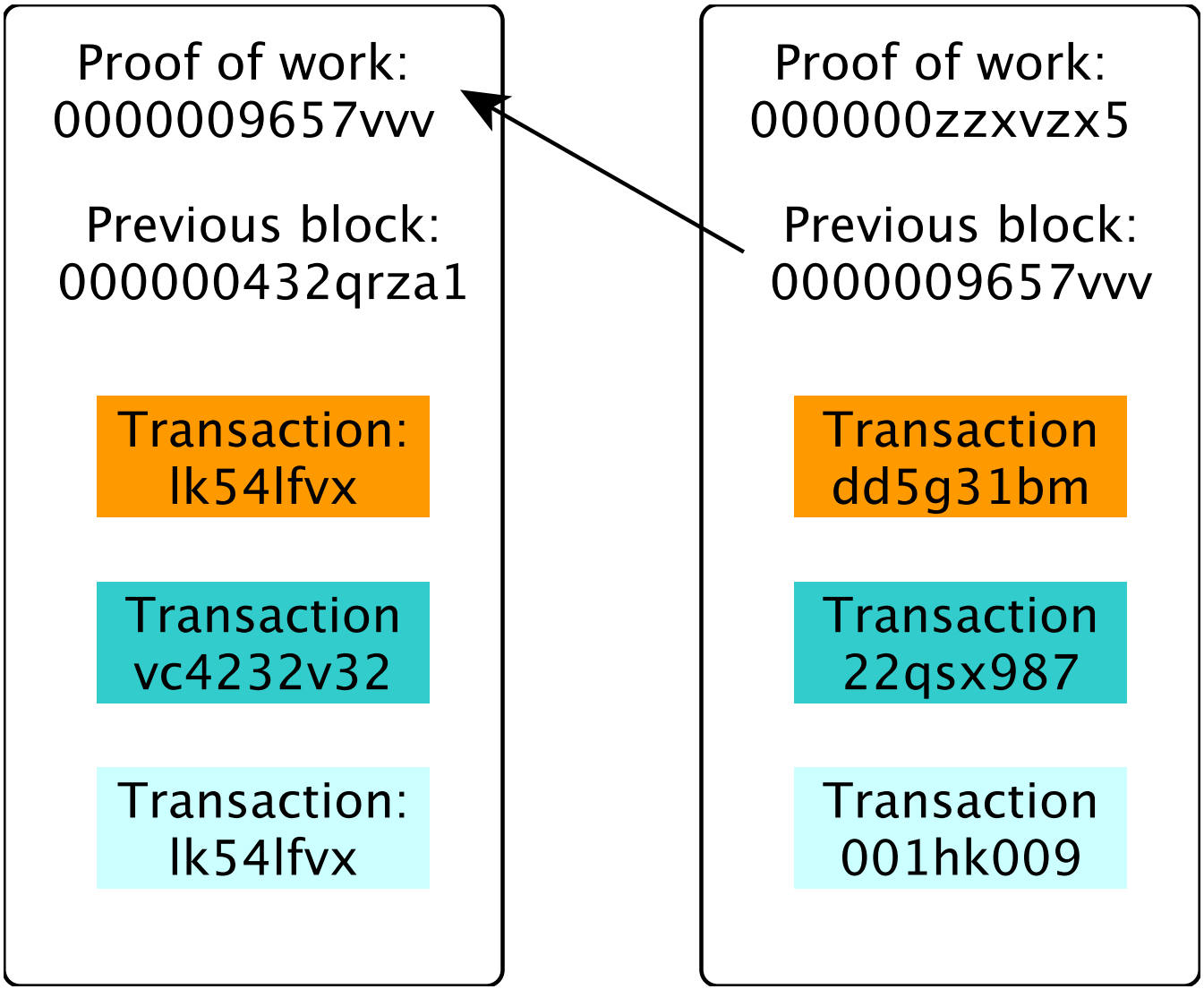
- It specifies a **protocol challenging** the **mining** nodes
- It's a puzzle that is very hard to solve (i.e., it's a CPU intensive task), **but** it's very **easy** to **verify**.
- The difficulty **increases** or **decreases** according to the available **CPU power**.
  - It targets 10 minutes block generation
- Solving the puzzle means winning a lottery

What kind of proof-of-work does Bitcoin relies on?

- Bitcoin transactions use Adam Back **Hashcash** proof of work with configurable amount of work to compute.
- Uses cryptographic hash **SHA256**

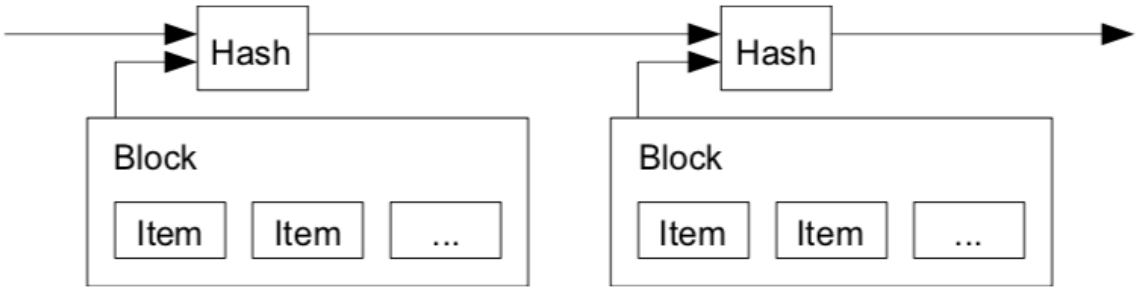


Example of a block



Bitcoin relies on timestamp server

- **Timestamp server** works by taking a hash of all data in a block including the hash from previous block.
- It is also the solution to order the **transaction blocks**.



Can everyone solve the Bitcoin's proof-of-work puzzle?

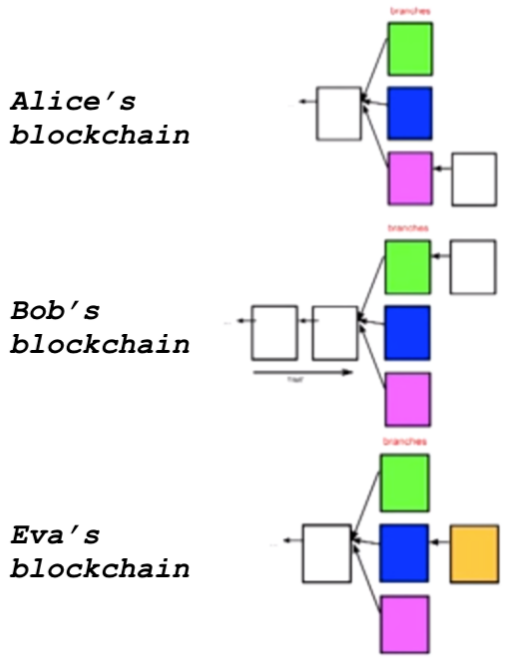
- An ordinary PC may take several years to solve the puzzle
- It is usually solved in 10 minutes using the Bitcoin network

What are the network protocol implemented by Bitcoin?

- New **transactions** are **broadcast** to **all nodes**
- Each node collects new transactions into a block
- Each node works on finding a difficult proof-of-work for its block
- When a node finds a proof-of-work, it broadcasts the block to all nodes
- Nodes accept the block only if all transactions in it are valid and not already spent
- Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash

What are the characteristics of Bitcoin network?

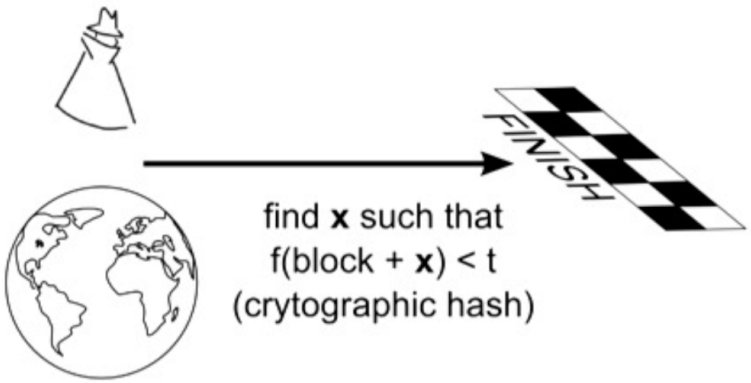
- It is extremely unlikely, but two or more nodes may solve the proof-of-work at same time



- In this case, **branches** in the **blockchain are created**
- It will be broken when someone solves the next block
- Nodes will switch to the longest branch
- Blocks will be discarded and respective transactions will be handled by the wining branch

Bitcoin uses game-theory concepts to incentive nodes to stay honest

- **Nobody can change a transaction** or the Bitcoin protocol's implementation **without the majority** of the entire network of the users accepting the change.
- While the majority of the nodes are honest, attackers cannot harm the system.
- An attacker would need astronomical computing power to corrupt the blockchain.



Conclusion

- Bitcoin is a **cryptocurrency** based on **mathematical theories**
- It **works without** needing to rely on **any central authority**
- It may **guarantee** users **anonymity**
- It uses **proof-of-work** to avoid **untrusted** users and to **encourage** nodes to **stay honest**.
- The **proof-of-work comprises** a **computing problem** that is **difficult** to solve but that is **very easy** to **verify**.


That's all Folks!