Distributed Systems
Master of Science in Engineering in Computer Science

AA 2018/2019

LECTURE 22: BLOCKCHAIN

Definition

A blockchain is a **decentralized**, **distributed** and public digital ledger that is used to **record transactions** across many computers so that any involved **record cannot be altered retroactively**, without the alteration of all subsequent blocks

… A Blockchain is a decentralized fully replicated DB on a trustless p2p network containing a history of transactions

Blockchain features

- Public
- Immutable
- Non-repudiable

Bitcoin Blockchain

Blockchain born with Bitcoin [1] to support payment

Bitcoin: virtual currency without a centralized authority (bank)

- The transactions' validity is verified by the network

Bitcoin Public Ledger: the Bitcoin Blockchain contains the list of all transactions ever made

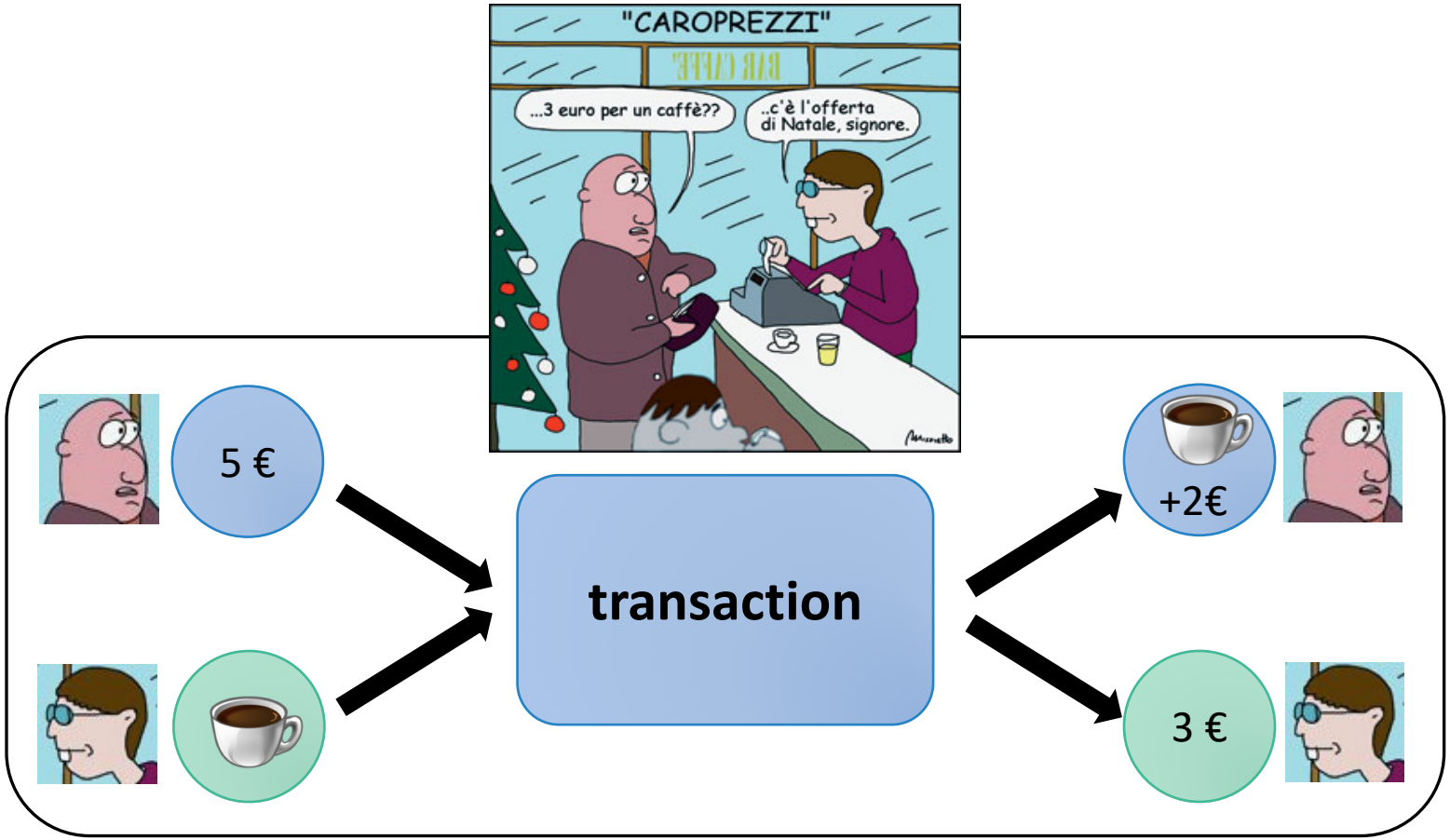
Bitcoin transaction (txn)

- Each transaction cost an amount of crypto-currencies (coins)
- Each transaction is broadcasted to the whole p2p network
- Each node verifies on his own all transactions and stores them to his ledger copy
- Must be achieved consensus between nodes on transactions in the ledger

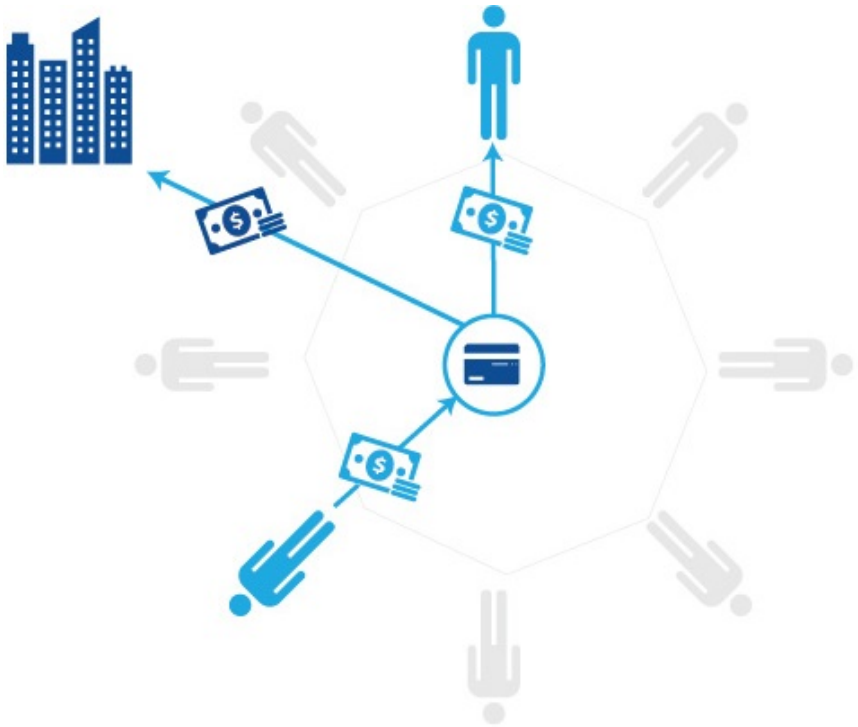
[1] Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto, 2008

Let’s start with a coffe…

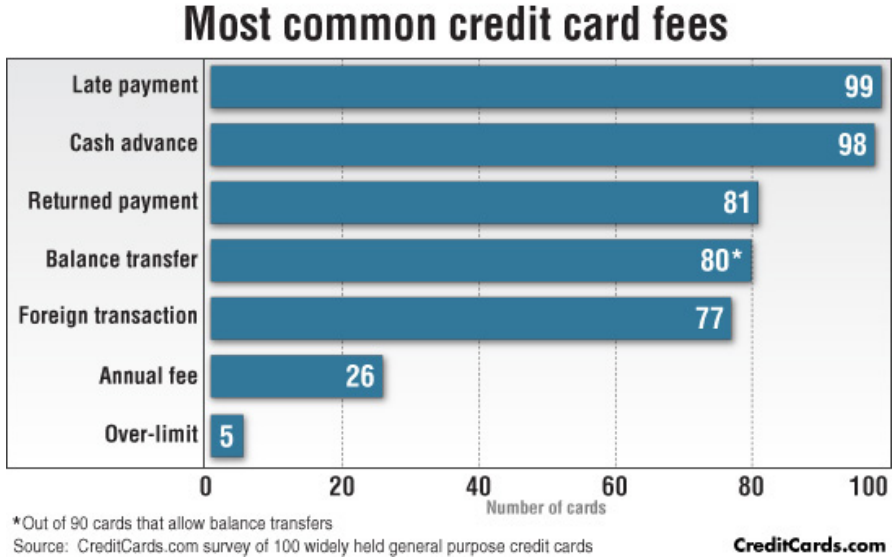
Coffee for money .. A transactions



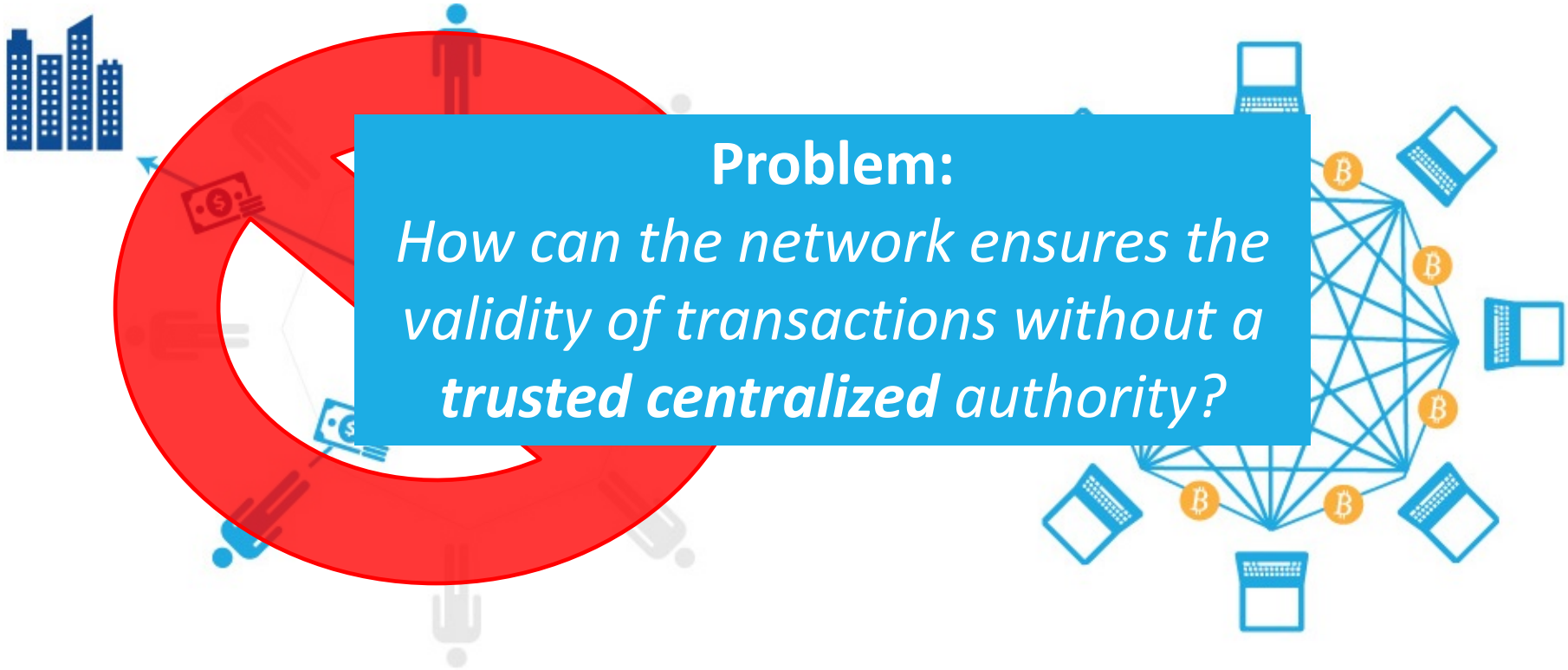
Why Bitcoin uses a Blockchain?



Current payment systems require third-party intermediaries that often charge high processing fees ...



Why Bitcoin uses a Blockchain?



Problem:

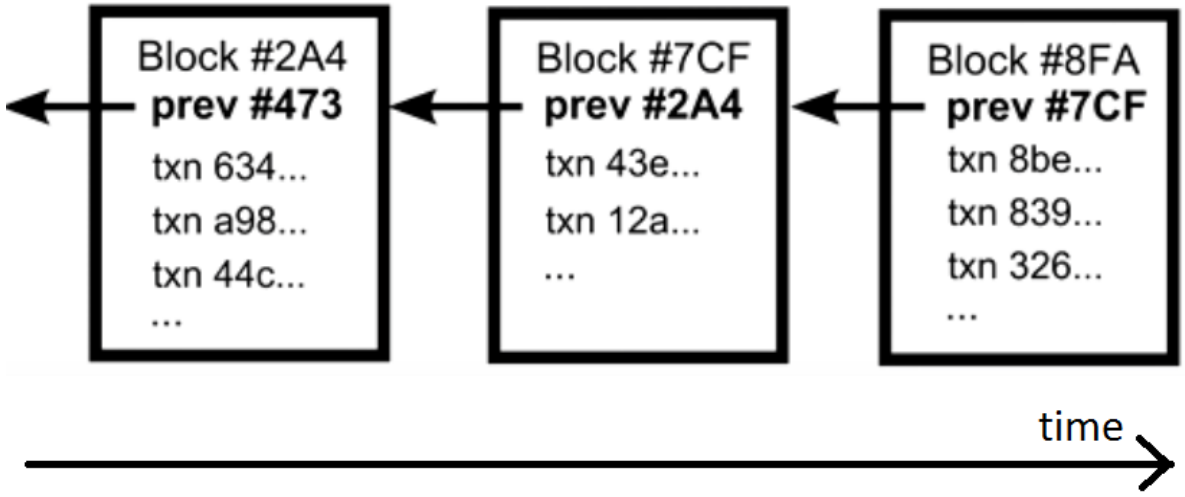
How can the network ensures the validity of transactions without a ***trusted centralized*** *authority?*

Current payment systems require third-party intermediaries that often charge high processing fees ...

... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

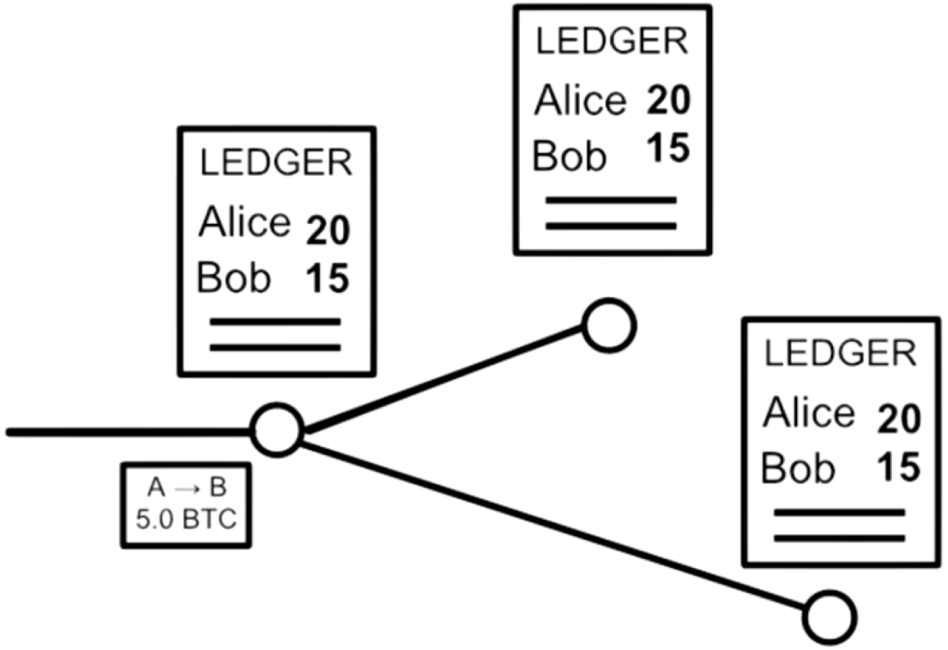
Blockchain Concepts

- Why “Block”-“Chain”?
  - Because **transactions** are grouped in **blocks**
  - … and because the blocks are connected each other in a **chain**



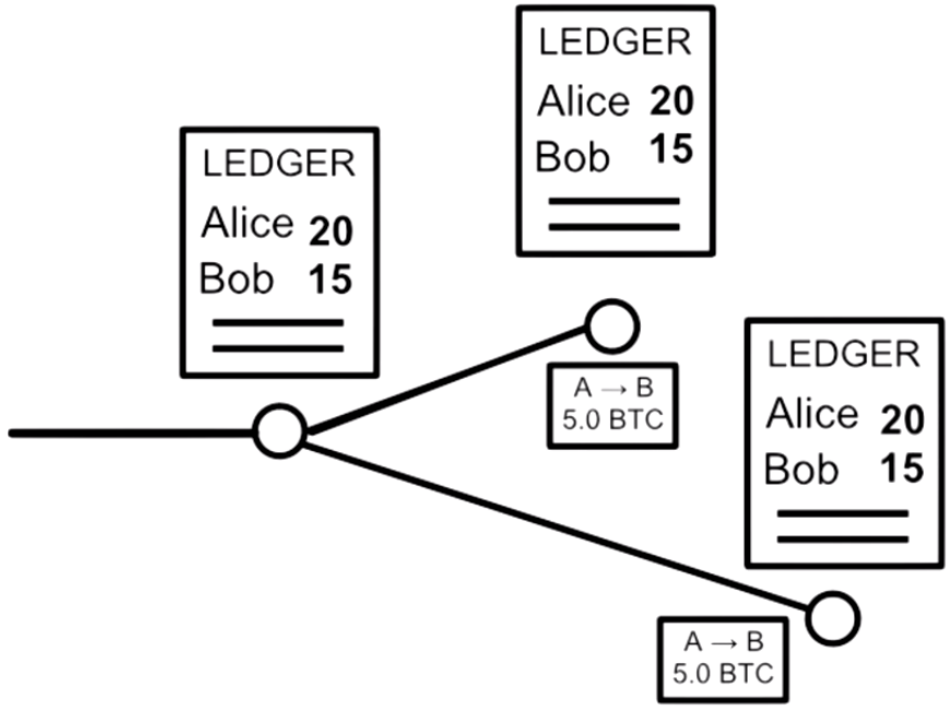
Transaction

- Alice wants to send 5 crypto-currencies to Bob
  - Step 1: she update her ledger



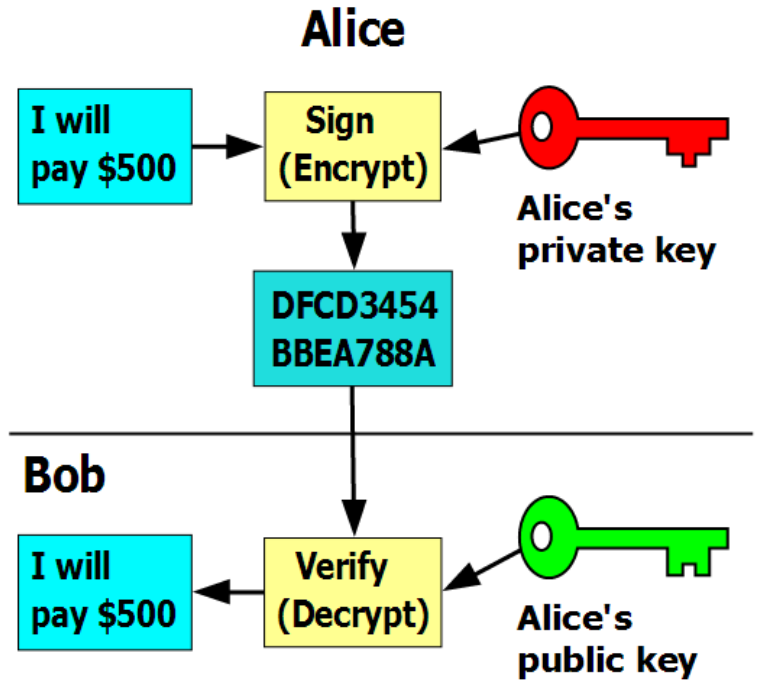
Transaction

- Alice wants to send 5 crypto-currencies to Bob
  - Step 1: she update her ledger
  - Step 2: she broadcast the msg
  - Step 3: all nodes verify the transaction



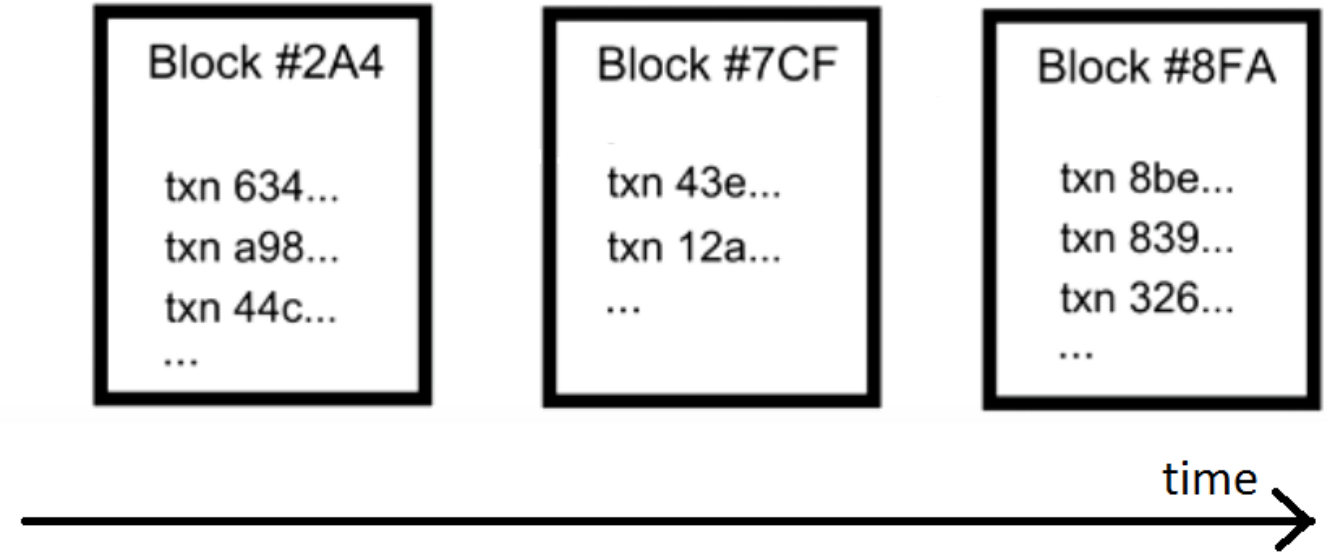
How nodes verify a transaction: Authentication

- **Digital Signature for Authentication**
  - Each message is sent together with the sender's signature
  - Each node in the network verifies the sender of a txn through its digital signature



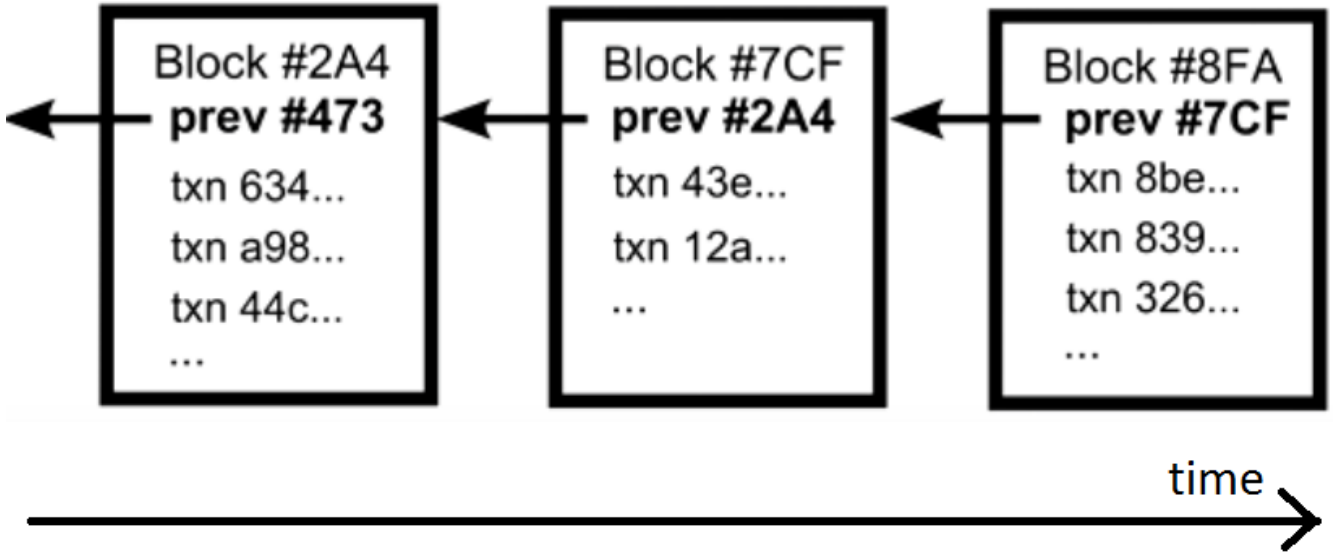
How to create and chain blocks

- The network orders txns by inserting them into groups called **blocks**



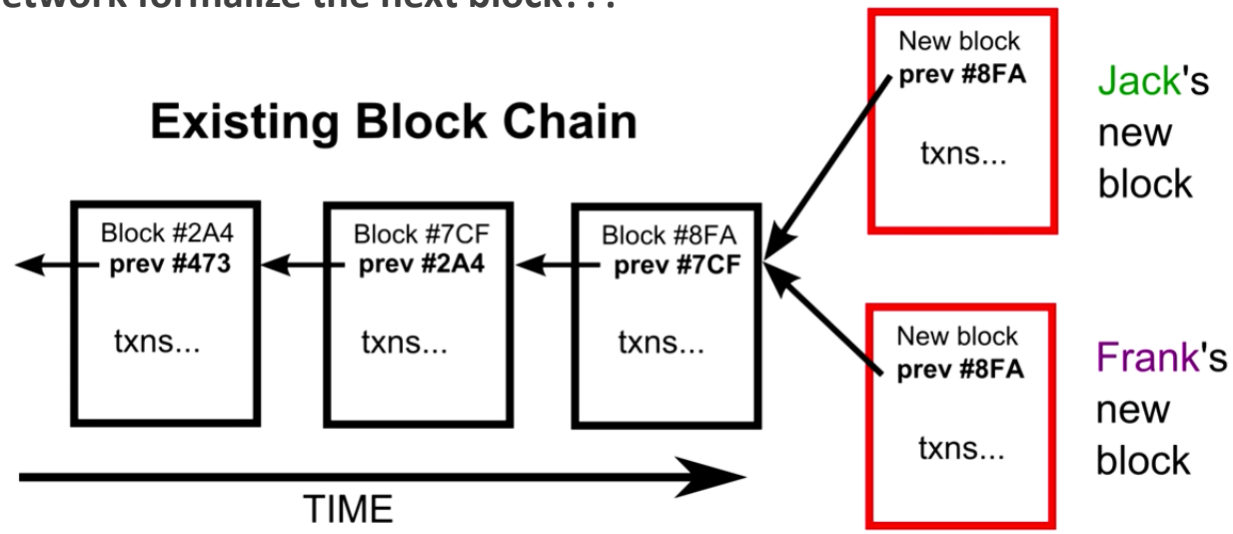
How to create and chain blocks

- Each **block** has a reference to the hash of the previous one
- Txns in the same block are considered made at the same time
- **To define a # txns in a block and block duration**



How to create and chain blocks

- Txns not yet in a block are called **unconfirmed txns**
- Each node can pick a set of unconfirmed txns to build a new block and propose it
- Two blocks still might arrive at the same time:
  - **Each node simply choose the first**
  - **How the network formalize the next block???**



How to create and chain blocks

Attaching a new block requires Consensus

Which Consensus protocol should I use?

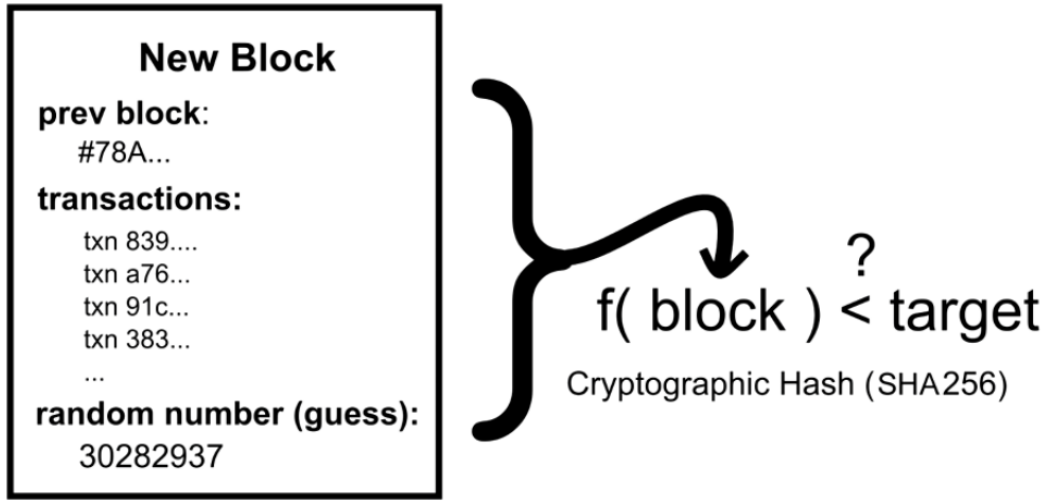
Public Network → **Proof of X**

OR

Private Network → **BFT Consensus**

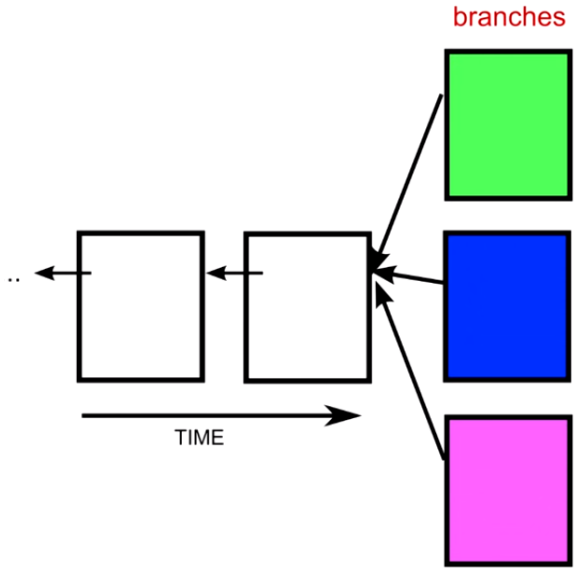
Proof-of-work (PoW) & Mining

- **Proof-of-work:** mathematical challenge to “solve” a block
- **Mining:** find a number s.t. hash(block) < target
- The first node who “solves” a **block** can propose it as next in the blockchain
- Other nodes which receive the block re-compute the hash to check the validity



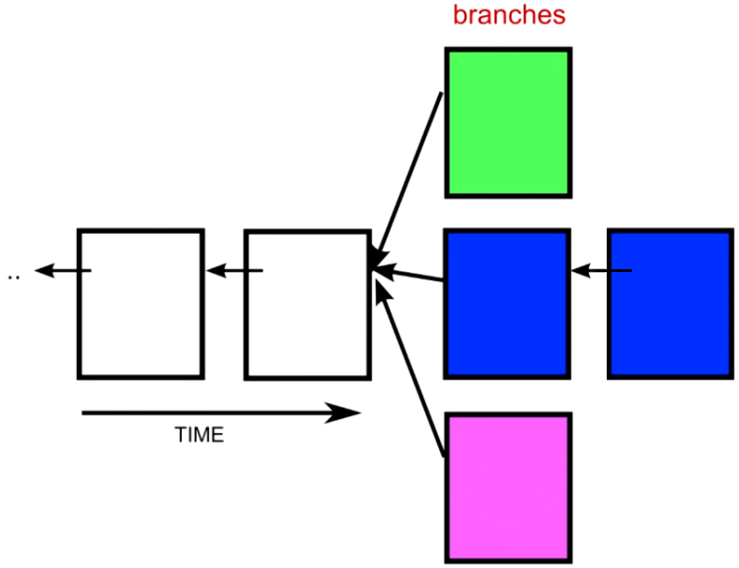
Proof-of-work & Mining: Branches Management

- Occasionally two or more blocks may arrive together → **temporal disagree**
  - The probability that two or more nodes mine a block at the same time is very low
- **RULE**: in case of branches the network has to converge to the longest branch.



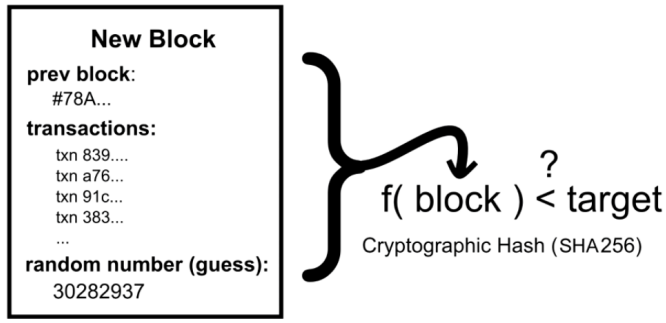
Proof-of-work & Mining: Branches Management

- Occasionally two or more blocks may arrive together → **temporal disagree**
  - The probability that two or more nodes mine a block at the same time is very low
- **RULE**: in case of branches the network has to converge to the longest branch.
  - **Problem solved with next blocks:** *eventually one branch will become the longest (usually after one block) bringing convergence*



Scalability Issues

- Transaction rate depends on two parameters
  - **Block size**: how many transactions to include in a block?
  - **Block interval**: how long to wait for a block to propagate to all the nodes?
    - Change run-time the **difficult of the target** to solve a block according to the computational power of the network

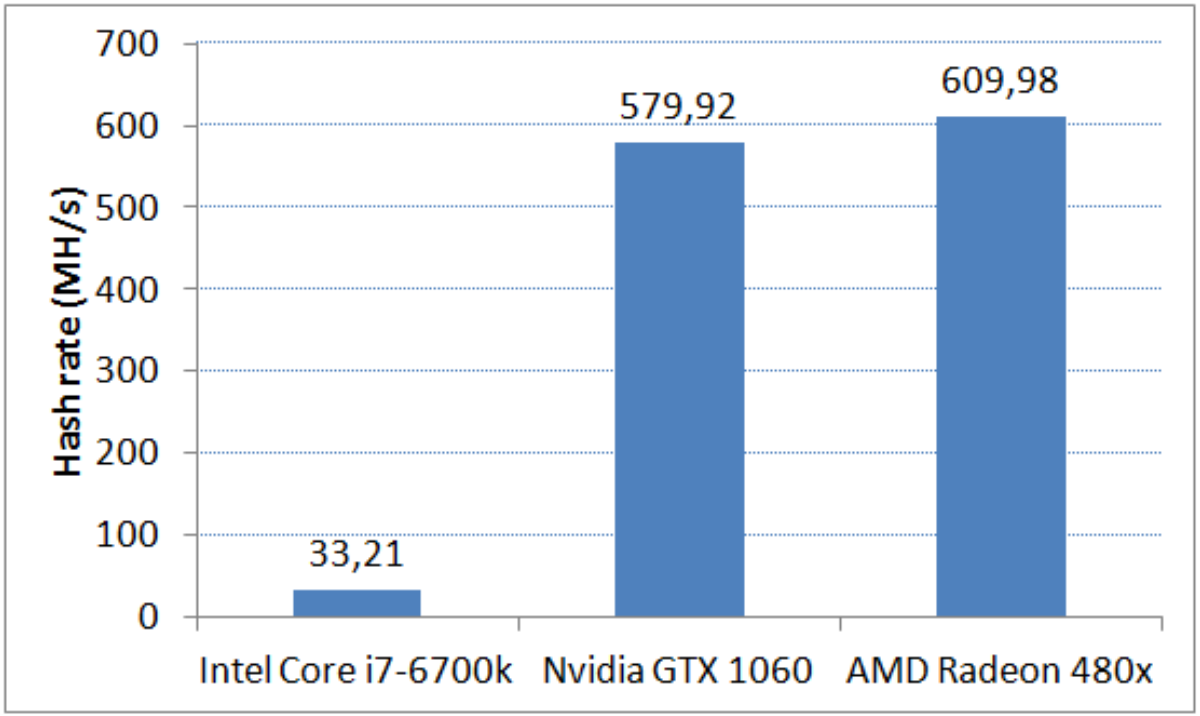


- Metrics
  - **Throughput**: how many transactions per second?
  - **Latency**: how long to wait for a transaction to complete?

- How parameters impact on metrics
  - Increasing block size improves throughput, but the resulting bigger blocks take longer to propagate in the network
  - Reducing the block interval reduces latency, but leads to instability where the system is in disagreement and the blockchain is subject to reorganization

Miner Requirements

- A miner needs a **high computational power** to compute a thousands of hash per seconds (KH/s or MH/s)
- CPUs are ineffective (few cores) better using GPUs



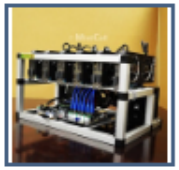
usually Radeon card are better for mining as mining softwares use

than CUDA

* source: cpuboss, gpubooss

Miner Requirements

- Possible to improve performances by employing a cluster of GPU



KADA 6.1 GPU Mining Rig Open Air Frame Case Chassis with 6 USB Risers - Ethereum

99.6 % Positive feedback (★ ★ ★ ★ ★)

235 $

Listing Status: Completed

Country: US

Item condition: New

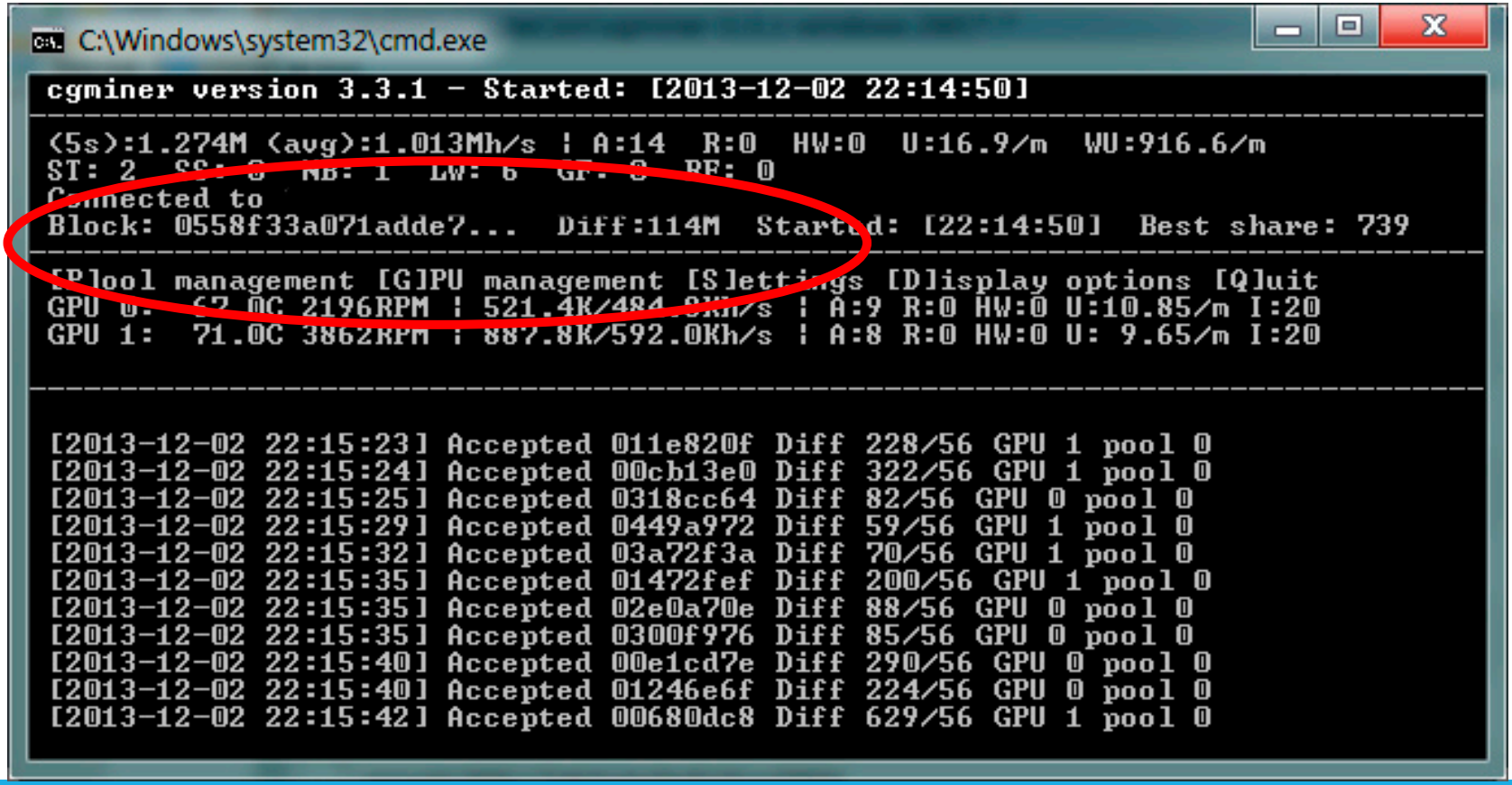
Buy Now!

ebay

PayPal VISA MasterCard DISCOVER

Software for Mining

- CGminer, BFGminer, BitMiner, BTCMiner, DiabloMiner, …



ASIC

- ASIC: alternative specific hardware for mining

- Example: AntMiner S5
  - Hashrate: 1.15GH/s
  - Price: $370
  - Power consumption: 590W
    - Mining for 24 hours/day is expensive!

Question:
Why should an user mine?

Miner Incentive

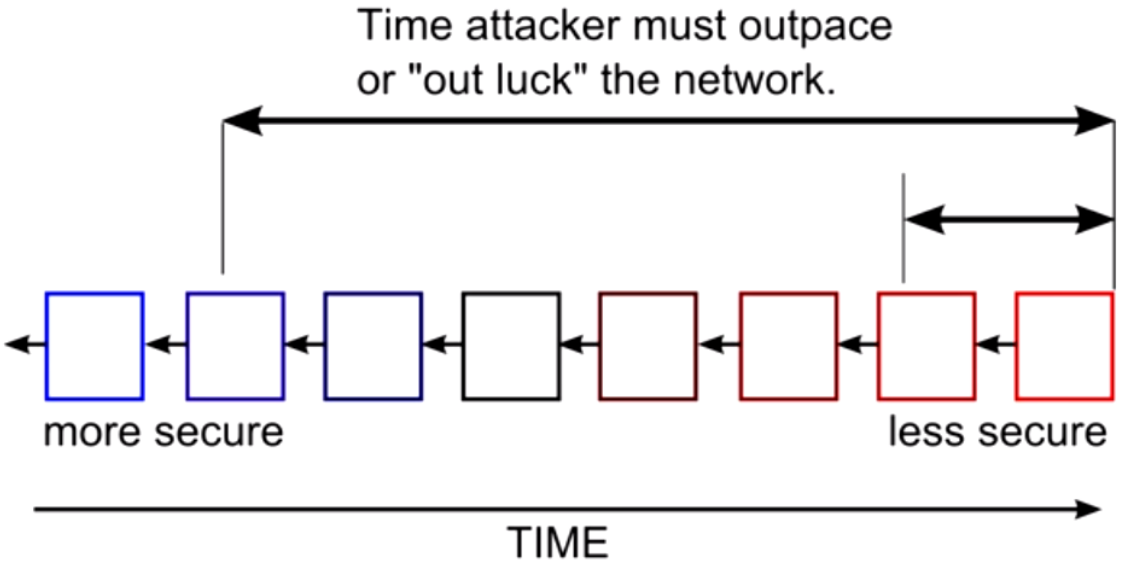
- **Reward**: Solving a block gives coins to node that found the proof-of-work
  - Some txn may bring **additional fee** to node who mines the block containing that txns
  - Currently the txn fees are quasi-zero
  - Miners will be motivated to include in a block txn with a fee
- Rewards are an incentive for nodes to keep them supporting the blockchain and keep nodes honest
  - Invalid txns won't give to miner the reward!
- Furthermore, it is a way to distribute coins into circulation
  - There is no central authority issuing new coins
  - Each crypto-currency platfrom will not erogate new coins to miners forever → currency deflation
    - Is effective to mine whilst you earn more money than those spent for electric power

How the PoW Ensures Integrity: Computational Power

- **Impossible to change a txn in a block *b* in the blockchain:** an attacker should be quicker than the rest of the whole network to mine a block.
- In that case he could be able to re-mine *n+1* blocks (i.e. all blocks next to *b* +1) quicker than the rest of the network to mine a new block.
- If so, the attacker could obtain the longest (modified) blockchain and all network would converge to it.
- But for doing that, he would have the 50% of the computational power of the network to have a 50% probability to solve a block before another node.
- And he would have a higher percentage of computational power to solve more blocks sequently.

How Blockchain Ensures Integrity: Computational Power

- Last blocks are so less secure
- Wait for 5/6 blocks makes a success probability too low for an attacker
- This solution protects from both **Integrity** and **Double Spending Fraud**



Alternative to PoW?

- **PoW pro:** very secure
- **PoW cons:** waste of electric power

- **Proof-of-Stake (PoS)** is the PoW alternative
  - **Secure without mining → no energy wasted**

Proof-of-Stake

- Instead of mine a block, the creator of the next block is chosen in a deterministic way according to its wealth (i.e. stake)
- The reward are not related to the created block but according to your wallet
- The longer you keep the coin in the wallet, the more the reward is high
- The probability to ***mint*** (instead of mine) a block is proportional to your wallet
  - **Minting** process require a lot of coin to attack the network
  - If you have a the *p*% of coins of the network you will mint the *p*% of the blocks
  - Very difficult to mint two consecutive blocks!