Topic 7 - Blockchain

Eric Casanovas

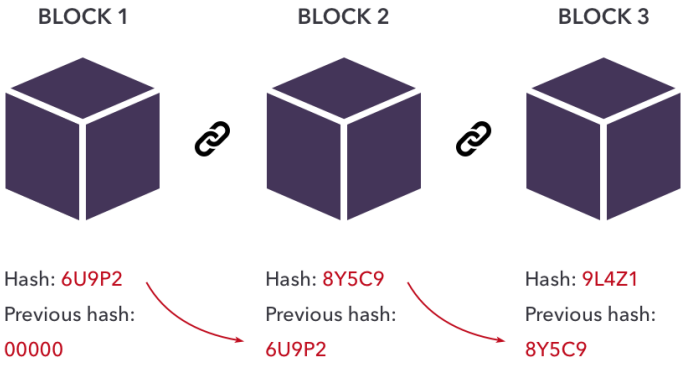
Universitat d'Andorra

18th May, 2022

Introduction I

- A system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system
- The system consists in a growing list of records (blocks) linked using cryptography
- Each block contains a hash of the previous block
- The technology was popularized in 2008 by Satoshi Nakamoto (Bitcoin)

Introduction II



History I

- First blockchain-like protocol was designed in 1982 by David Chaum
- Some people think that the paper written by David Chaum is the basis of bitcoin
- 1992 Stuart Haber and Scott Stornetta described the first cryptographically secure chain of blocks
- 1998 Nick Szabo works on "Bit Gold" the first decentralised digital currency
- 2008 Satoshi Nakamoto releases Bitcoin whitepaper "A Peer-to-Peer Electronic Cash System"
- 2014 Blockchain 2.0 is born, refering to applications beyond currency
- Today, blockchain technologies have many implementations, but the most widely used is for financial purposes. Bitcoin & Ethereum

Types of blockchains

- Permissioned vs Permissionless
- Centralized vs Decentralized

Permissioned vs Permissionless

- **Permissionless** or public blockchains has no access restrictions
- Anyone can send trasactions to this blockchains
- Security relies on incentives
- **Permissioned** or private blockchains has access restrictions
- One cannot join it unless invited by the network administrators
- Hybrid blockchains can also be considered
- Some of the largest, most known public blockchains are the bitcoin and Ethereum

Centralized vs Decentralized

- **Centralized** blockchains mean that the whole chain is controlled by a few participants
- This can cause a single point of failure or a 51% attack
- But, centralized blockchains are faster and can reduce costs
- **Decentralized** blockchains mean that the chain is controlled by a lot of people at the same time
- Decentralized blockchains are considered more secure as there is no single (or few) point of failure and is difficult to perform a 51% attack
- But, it is more expensive for users and slower

Focus

- We will focus on decentralized permissionless blockchains!

Structure

Each blockchain has these 4 parts:

- Networking: Everything related to the communication between the nodes (node discovery, information propagation, verification...)
- Consensus: refers to the methodologies used to achieve agreement, trust, and security across a decentralized network (proof of work, proof of stake)
- Data: blocks and transactions
- Applications: smart contracts, decentralized applications, etc

Consensus

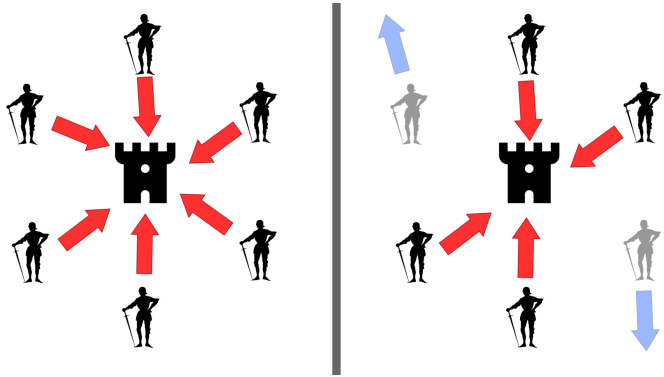
- A fundamental problem in distributed computing
- The goal is to achieve system reliability in the presence of a number of faulty processes
- Some examples:
  - Byzantine Fault or Byzantine Generals Problem
  - PoW
  - PoS
  - etc...

Consensus - BFT I

The dilemma assumes that:

- Each general has its own army and is situated in different locations around a city
- They intend to attack, but the generals need to agree on either attacking or retreating
- If all generals retreat or all attack at the same time it's a victory
- Otherwise, soldiers will die
- The idea is to reach consensus and execute all the same action
- What do you think is the solution?

Consensus - BFT II



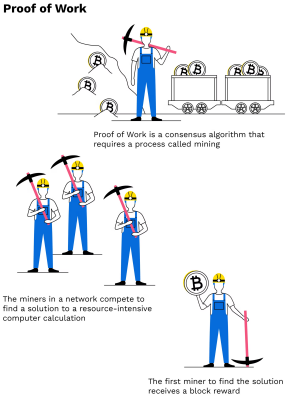
Consensus - BFT III

- The solution consists in follow the majority agreement of the *loyal* generals
- The majority is right
- But what happen if:
  - The generals are not loyal (Possible 51% attack)
  - Some messages didn't arrive i.e. System crashes unexpectedly (ignore its vote)

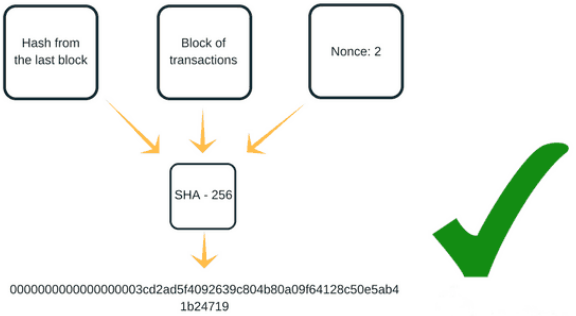
Consensus - PoW I

- Proof of Work is a form of cryptographic proof in which the prover proves to the verifiers that a computational effort has been performed
- This computational effort usually is "reverse a hash" with a given difficulty
- The "winner" receives a reward in compensation for his effort
- PoW is the consensus algorithm used by Bitcoin

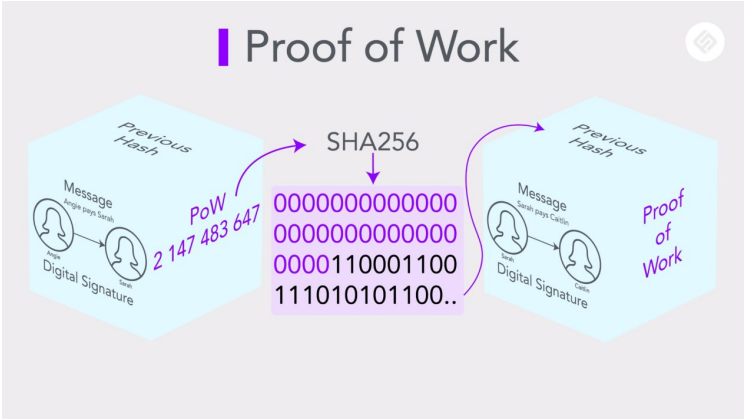
Consensus - PoW II



Consensus - PoW III



Consensus - PoW IV



Consensus - PoS I

- Proof of Stake is a consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency
- No necessity of computational power
- The selected validator receives a reward if he have done his job well
- PoS is the consensus algorithm used by many cryptocurrencies and in the future by Ethereum

Consensus - PoS II

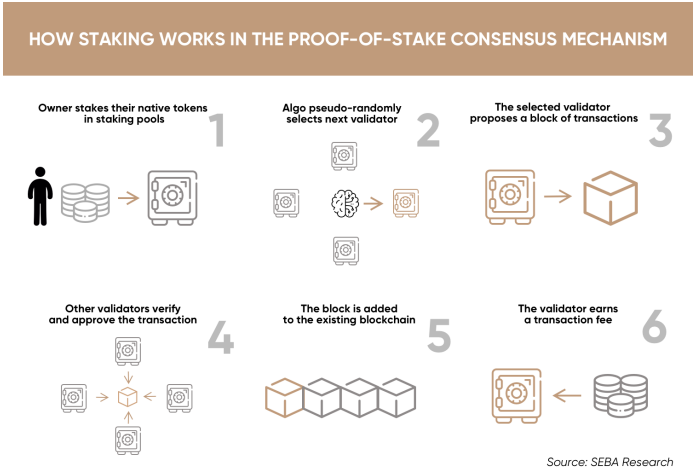
Proof of stake

The probability of validating a new block is determined by how large of a stake a person hold.

The validators do not receive a block reward, instead they collect network fees as their reward.

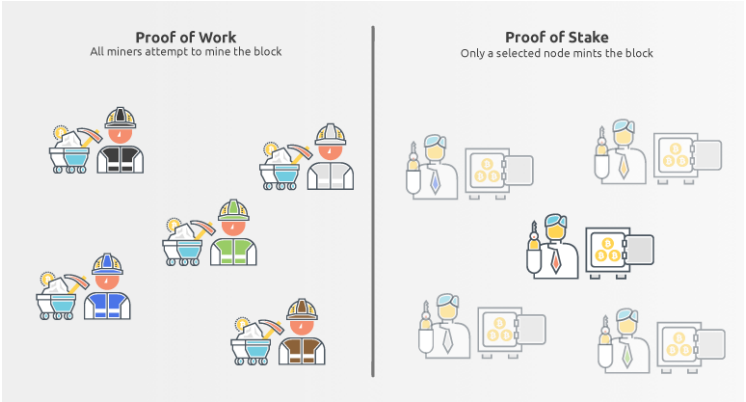
Proof of stake systems can be much more cost and energy efficient than proof of work, but are less proven.

Consensus - PoS III

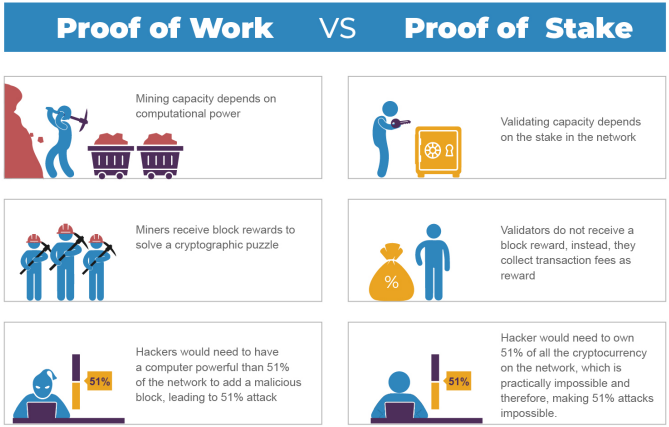


Consensus PoS vs PoW I

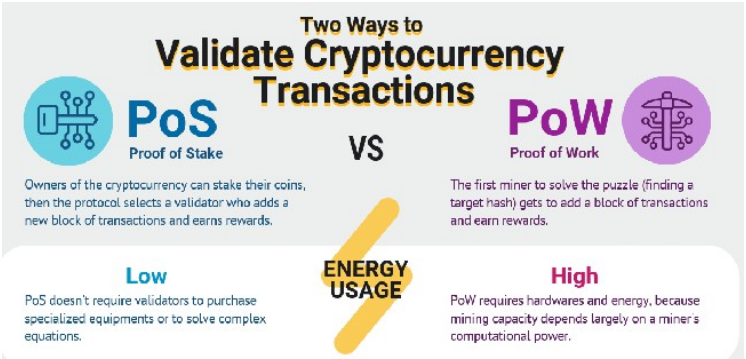
Consensus PoS vs PoW II



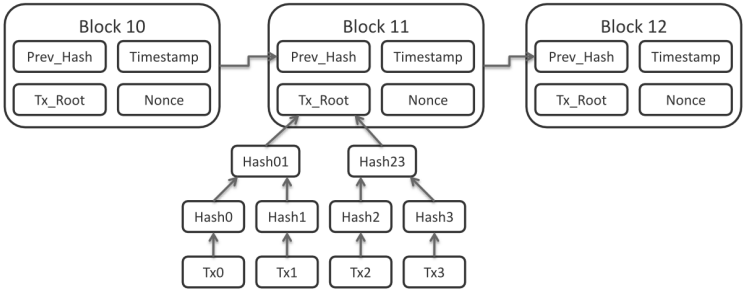
Consensus PoS vs PoW III



Consensus PoS vs PoW IV



Blocks


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Smart Contracts

- Code stored in a blockchain
- Usually public
- Anyone can run this code to perform operations
- The idea is to remove intermediaries
- The most used smart contract platform is ethereum

Smart Contracts - Examples

- Creation of tokens (new currencies on top of the main blockchain)
- Creation of markets
- Trading activities
- Data recording
- Bulk send of transactions

Use Cases I

- The main use case is for financial purposes
- These financial purposes include:
  - Investments
  - Cross-border transactions
  - Trading
  - Payment services
  - And many more...

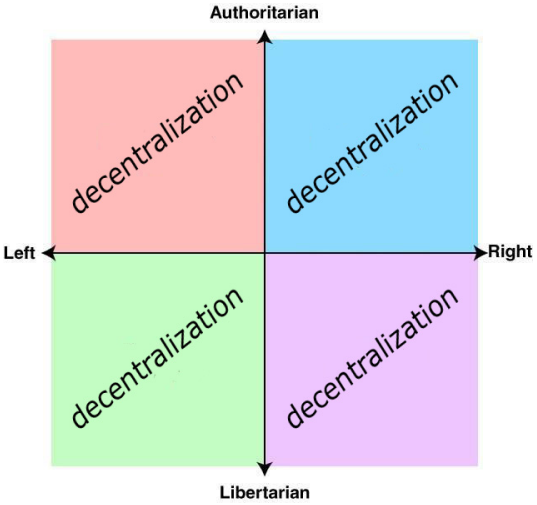
Use Cases II

- Digital voting
- Transparent Budgeting (anti-corruption)
- Digital IDs (passports, marriages...)
- Copyright management
- Proof of ownership of something
- Games
- Art
- Smart contracts (contracts remove intermediaries)

Use Cases III

- And also in cybersecurity!!
  - Decentralizing DNS
  - Decentralize device administration
  - Software verification

Use Cases IV

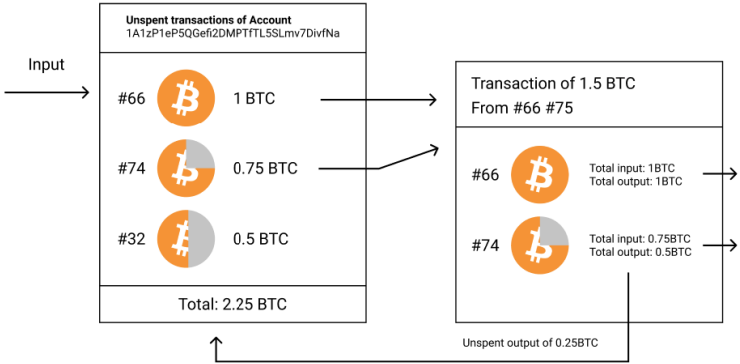

Authoritarian
decentralization
decentralization
Left
Right
decentralization
decentralization
Libertarian

Bitcoin I

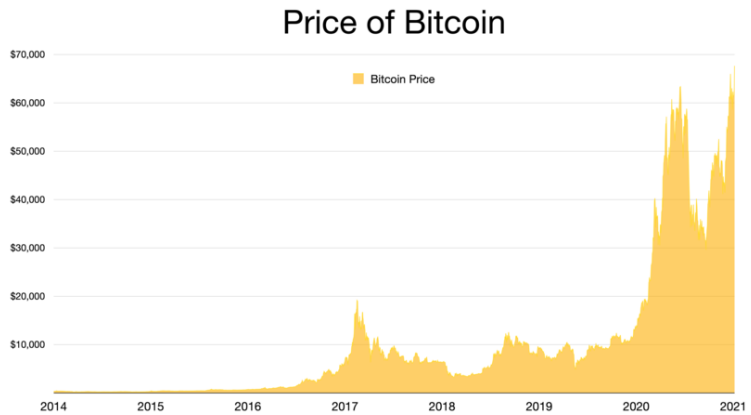
Bitcoin II

- A distributed, decentralized digital currency system
- Released by Satoshi Nakamoto 2008
- Nobody knows who is Satoshi Nakamoto
- The first cryptocurrency to appear in the market
- PoW as consensus algorithm
- Maximum of 21.000.000 BTC
- Today there are around 19.000.000 BTC (May 2022)
- UTXO model

Bitcoin III

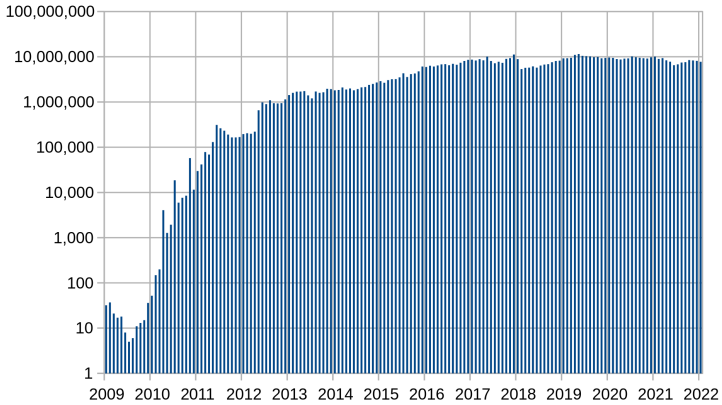

Input
Unspent transactions of Account
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
#66
1 BTC
#74
0.75 BTC
#32
0.5 BTC
Total: 2.25 BTC
Transaction of 1.5 BTC
From #66 #75
#66
Total input: 1BTC
Total output: 1BTC
#74
Total input: 0.75BTC
Total output: 0.5BTC
Unspent output of 0.25BTC

Bitcoin IV


Price of Bitcoin
Bitcoin Price
$70,000
$60,000
$50,000
$40,000
$30,000
$20,000
$10,000
2014
2015
2016
2017
2018
2019
2020
2021

Bitcoin V

Transactions



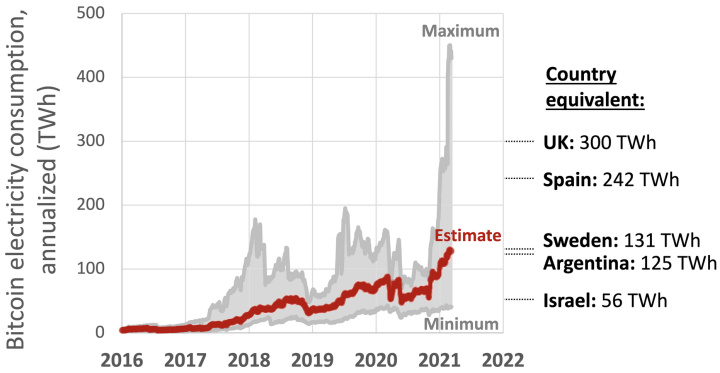
Bitcoin Strengths

- Deflationary: store of value as gold
- Decentralized: no banks in the middle of transactions
- Pseudonymous addresses: Bitcoin chain is public, but if you can link address-person you can deanonymize people
- "Low transfer fees": Low fees for sending a large amount of BTC
- Not your keys, not your bitcoins

Bitcoin Criticism I

- Economic concerns: Bubble, non regulated
- Illegal purposes taking advantage of pseudonymity
- Maximum of (more or less) 7 transactions per second
- Not your keys, not your bitcoins
- Energy consumption: see next picture

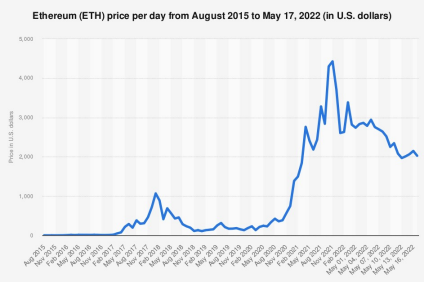
Bitcoin Criticism II



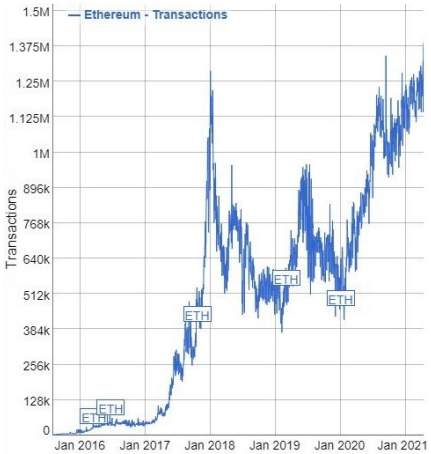
Ethereum I

- Ethereum is a technology that's home to digital money, global payments, and applications
- Released in 2015 by a group of researchers
- PoW as consensus algorithm but is migrating to PoS
- There is no maximum supply for Sthereum
- Wallet model
- Smart contracts

Ethereum II


Ethereum (ETH) price per day from August 2015 to May 17, 2022 (in U.S. dollars)
Price in U.S. dollars
5,000
4,000
3,000
2,000
1,000
0
Aug 2015
Nov 2015
Feb 2016
May 2016
Aug 2016
Nov 2016
Feb 2017
May 2017
Aug 2017
Nov 2017
Feb 2018
May 2018
Aug 2018
Nov 2018
Feb 2019
May 2019
Aug 2019
Nov 2019
Feb 2020
May 2020
Aug 2020
Nov 2020
Feb 2021
May 2021
Aug 2021
Nov 2021
Feb 21, 2022
May 24, 2022
May 26, 2022
May 28, 2022
May 30, 2022
May 16, 2022

Ethereum III



Ethereum Strength

- Decentralized: no banks in the middle of transactions
- Pseudonymous addresses: Ethereum (as bitcoin) is public, but if you can link address-person you can deanonymize people. But, ZKP...
- Smart Contracts: programs stored in the blockchain DApps (Decentralized Apps)
- Tokens: coins on top of ethereum to pay for services, governance, etc...

Ethereum Criticism

- Economic concerns: Bubble, non regulated
- Illegal purposes taking advantage of pseudonymity
- Slow: $\tilde{1}5$ transactions per second
- Energy consumption: less than bitcoin but considerably high

Discussion

- What do you think about BTC, ETH and cryptocurrencies?

The END!