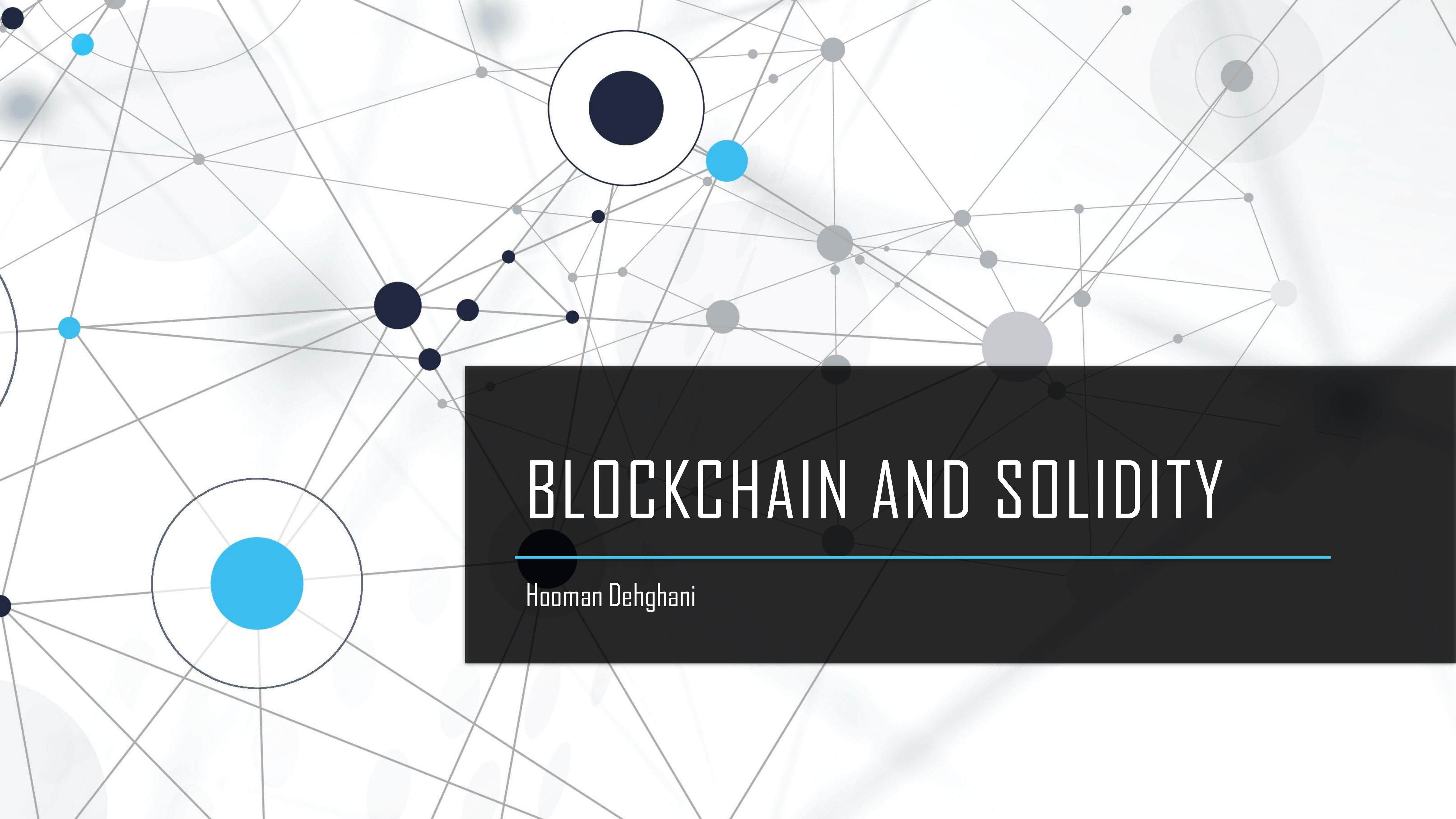


BLOCKCHAIN AND SOLIDITY

Hooman Dehghani

HOOMAN DEHGHANI | DMINDDEV01

- GitHub: https://github.com/DmindDev01
- Twitter: https://twitter.com/DmindDev01
- LinkedIn: https://www.linkedin.com/in/hooman-dehghani-27089117b
- Instagram: https://www.instagram.com/hooman.dehghani/
- Email: dminddev01@gmail.com

BLOCKCHAIN AND SOLIDITY COURSE

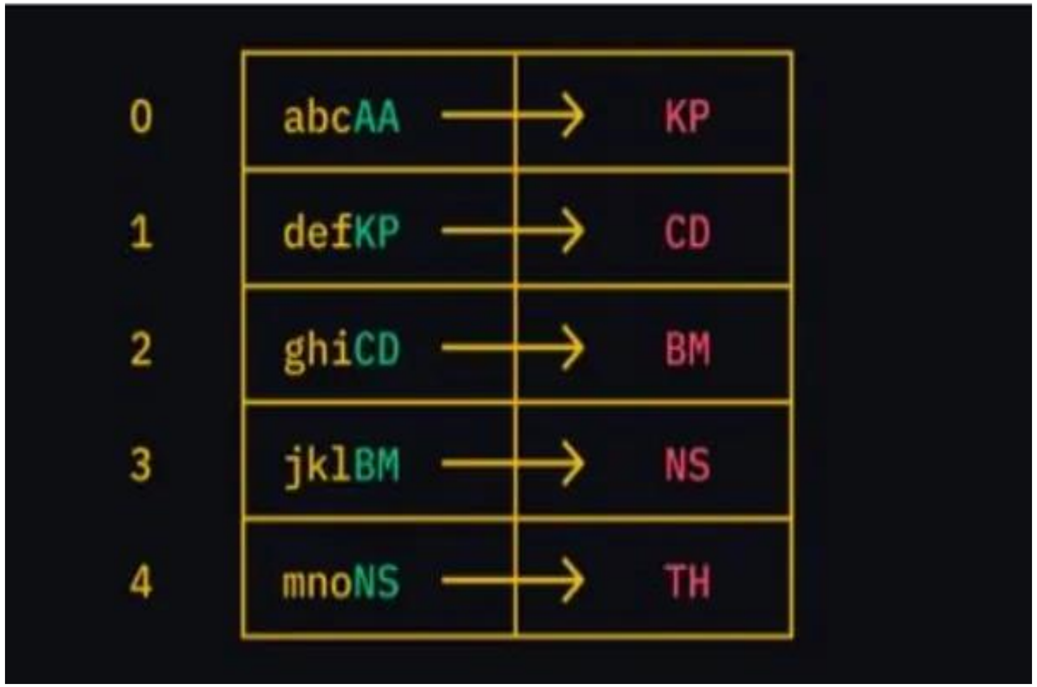
About this course:

- Our approach:
  - Part 1: Blockchain
  - Part 2: Solidity Programming

  - Course git: https://github.com/DmindDev01/SolidityCourse

WHAT IS BLOCKCHAIN?

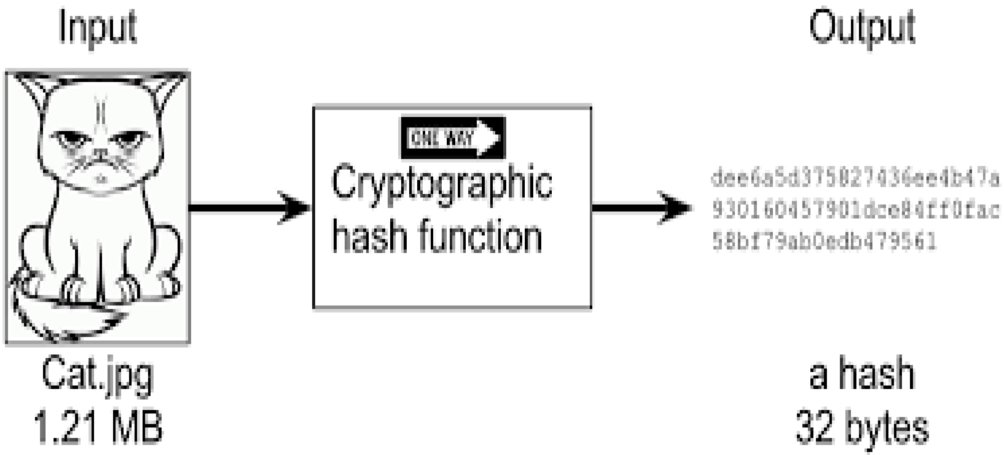
- Special type of Database
- There are some specified rules to INSERT into Blockchain
- No modification
- Data insert to this after generating Genesis Block

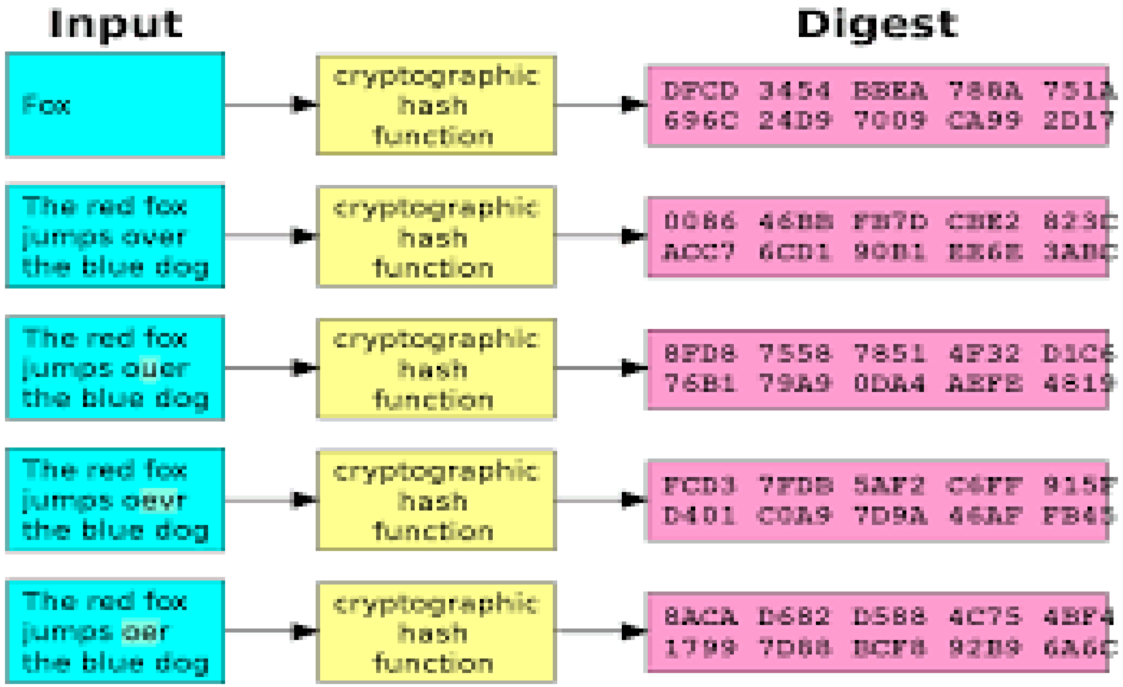


0	abcAA →	KP
1	defKP →	CD
2	ghiCD →	BM
3	jklBM →	NS
4	mnoNS →	TH

HASH FUNCTIONS IN BLOCKCHAIN

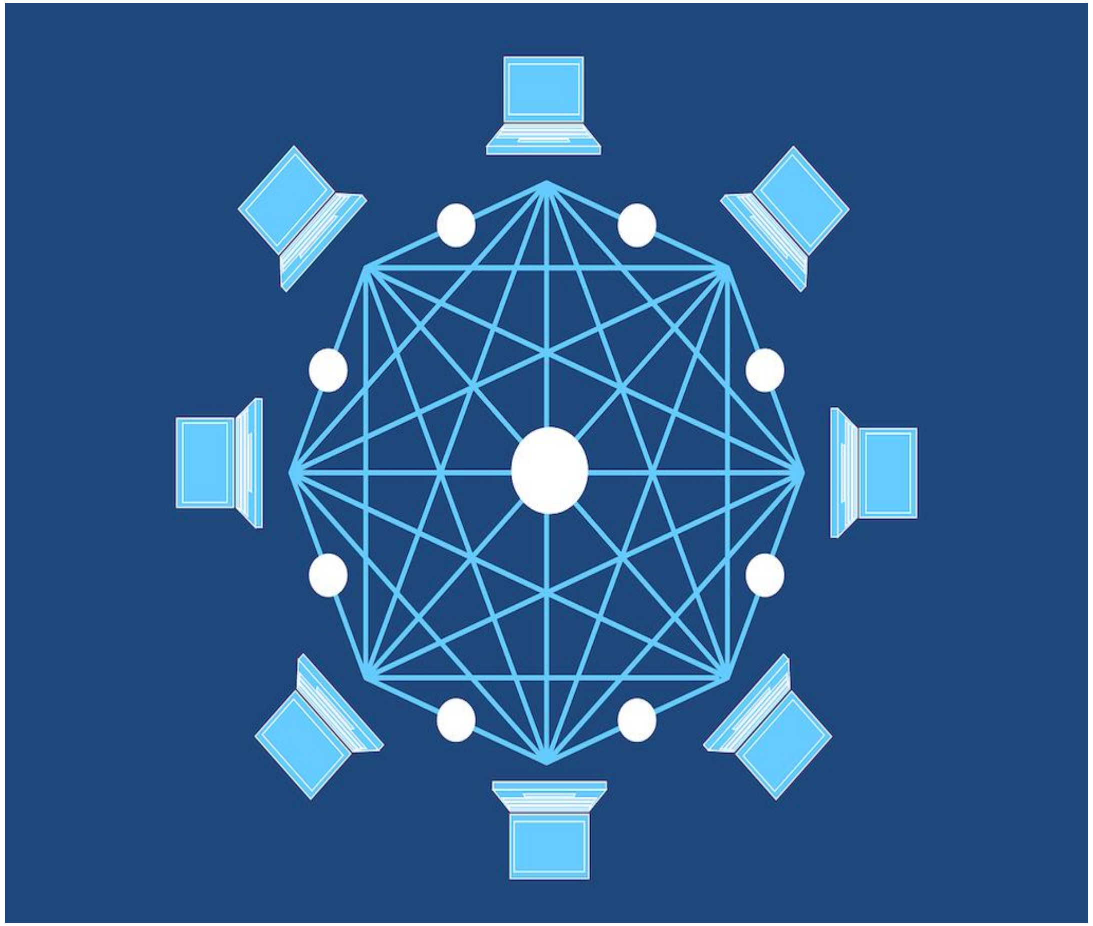
- Mapping data of arbitrary size to fixed-size values.
- The values returned by a hash function are called hash values.
- The values are usually used to index a fixed-size table called a hash table.
- What is collision?




Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

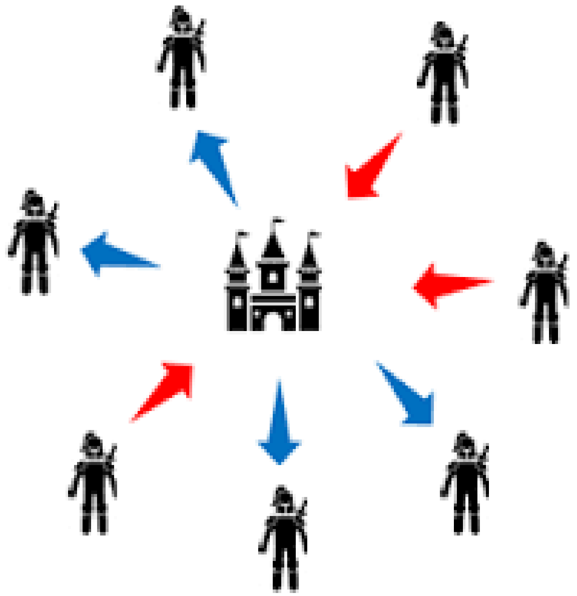
DECENTRALIZED

- Game Theory
- No one has to know or trust anyone else
- Who maintains the ledger of transactions?
- Who has authority over which transactions are valid?
- Who determines how the rules of the system change?
- Distributed Ledger
  - Database
  - Syncronized
  - Multiple participants



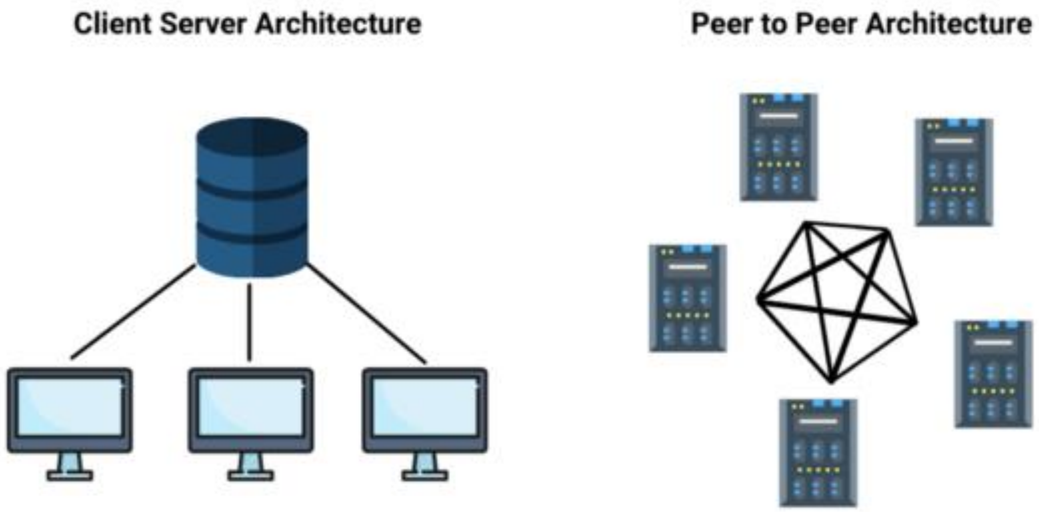
BYZANTINE GENERALS IN BLOCKCHAIN

- The term takes its name from an allegory , the "Byzantine generals problem", developed to describe a situation in which, in order to avoid catastrophic failure of the system, the system's actor must agree on a concerted strategy, but some of these actors are unreliable.
- Problem: Unreliable environment
- What we need here to avoid failure?



PEER TO PEER

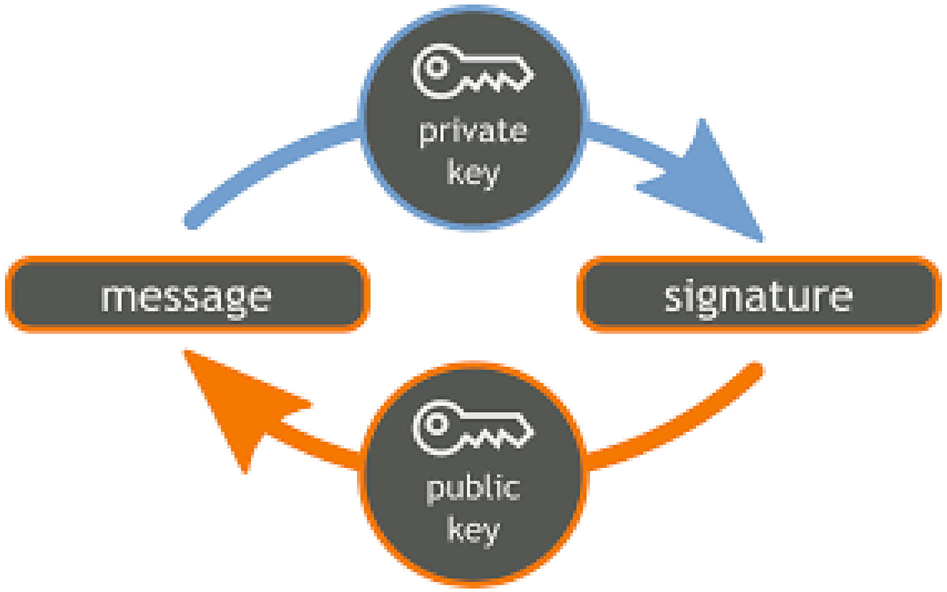
- Distributed application architecture
- Equally privileged
- This network is against Client-Server



SIGNATURES

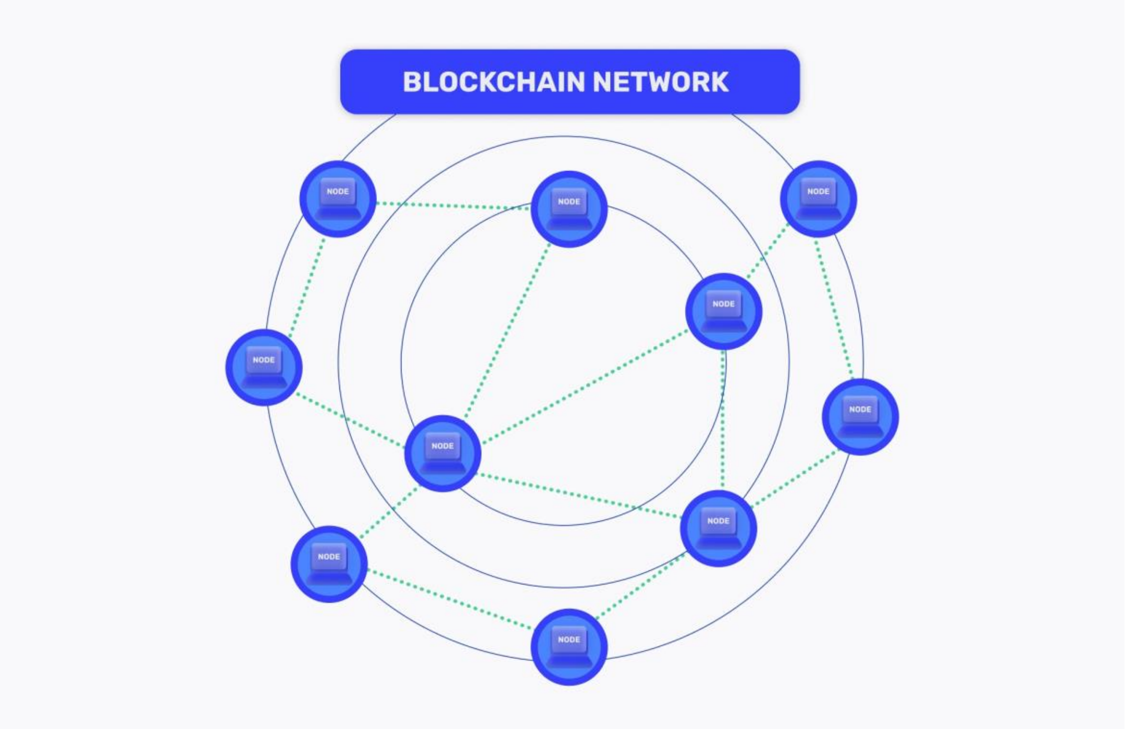
- One can sign and everyone can verify
- (SK,PK) = GenKey(size)
- Sig = (SK,Message)
- IsValid = (PK,Message,Sig)

- PK is your identity:
  - No need for username
  - No need for authority
  - Your address is the hash of your PK



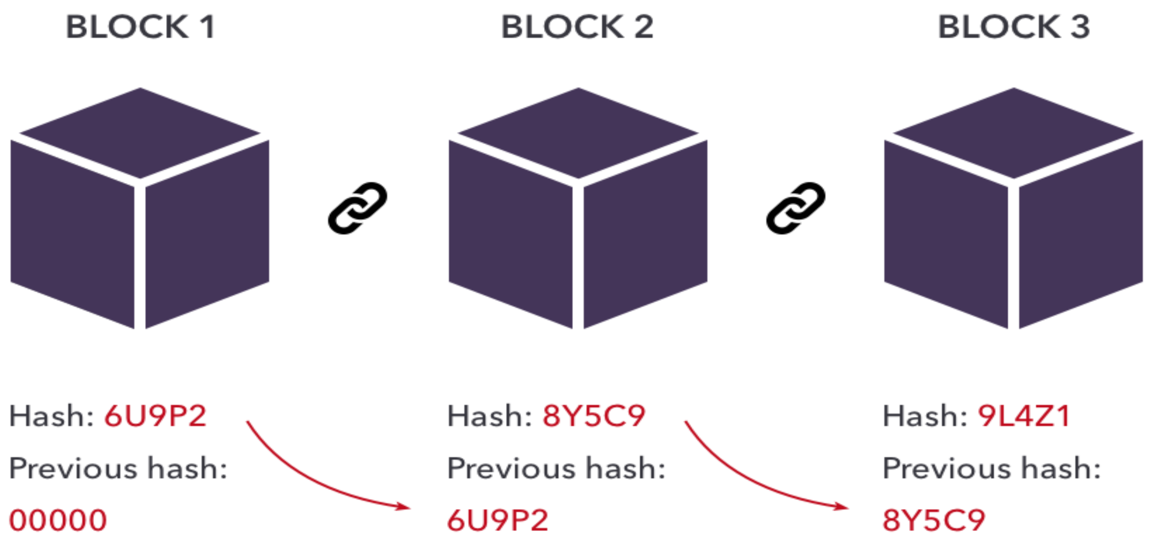
NODE

- In computer science, the term "node" simply means a device that plays a part in a larger network. In the context of crypto and blockchain, a node is one of the computers that run the blockchain's software to validate and store the complete history of transactions on the network.



BLOCK

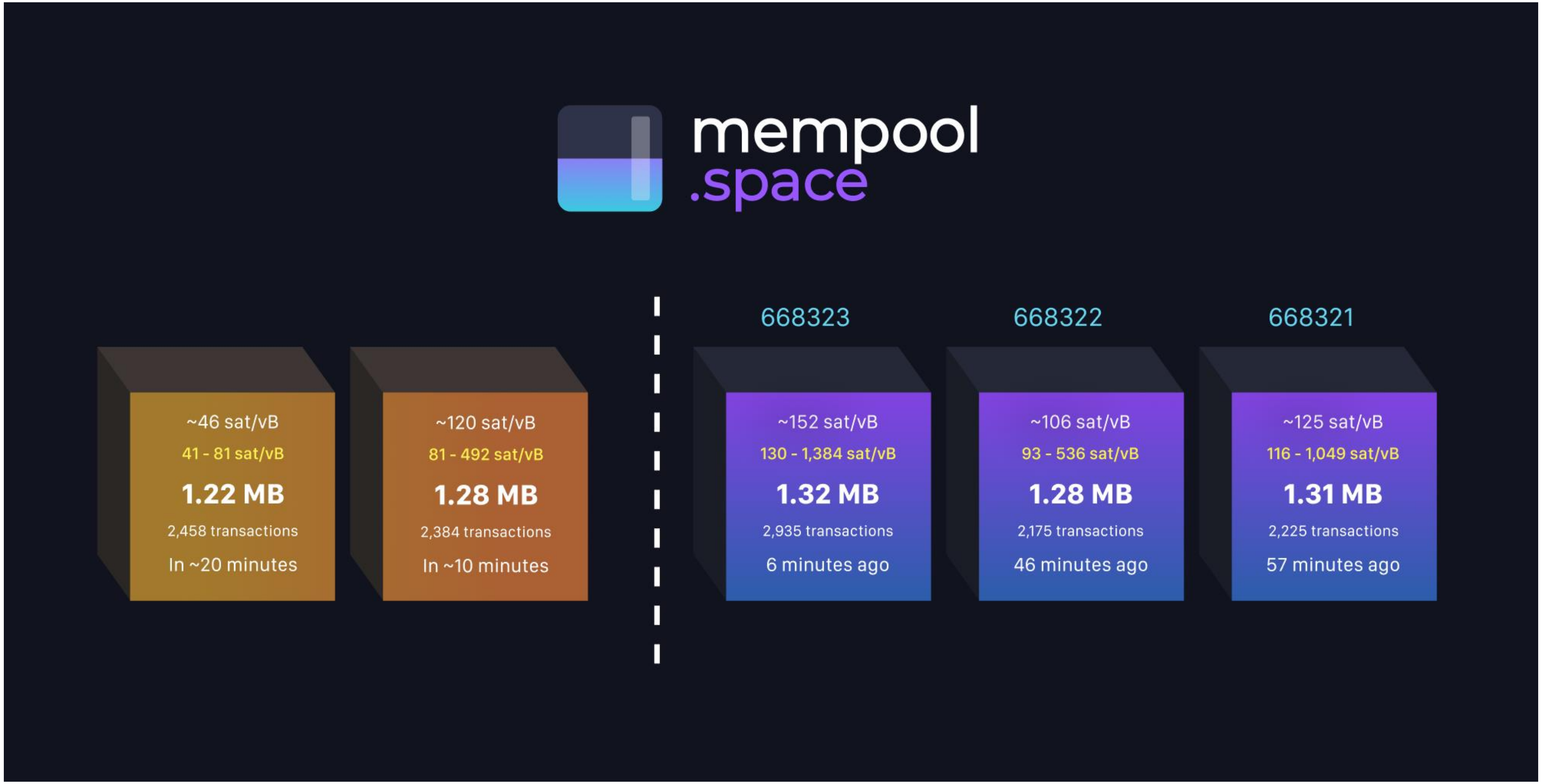
- TRX
- Timestamps
- Information is stored and encrypted
- Must be verified by a network
- Blocks are TRXs, timestamps, previous hash and have a hash
- Hash
  - Deteministic
  - One way



HOW BLOCKS ARE CREATED

- TRXs are added to the mempool
- When we have enough TRXs, it is called unconfirmed block
- We move to the next pool and will try to confirm the last block
- Announce our block and 51% should confirm (consensus)

- But what happens if someone tampers a block?
- What happens if he recalculates other hashes too?



mempool
.space

~46 sat/vB
41 - 81 sat/vB
1.22 MB
2,458 transactions
In ~20 minutes

~120 sat/vB
81 - 492 sat/vB
1.28 MB
2,384 transactions
In ~10 minutes

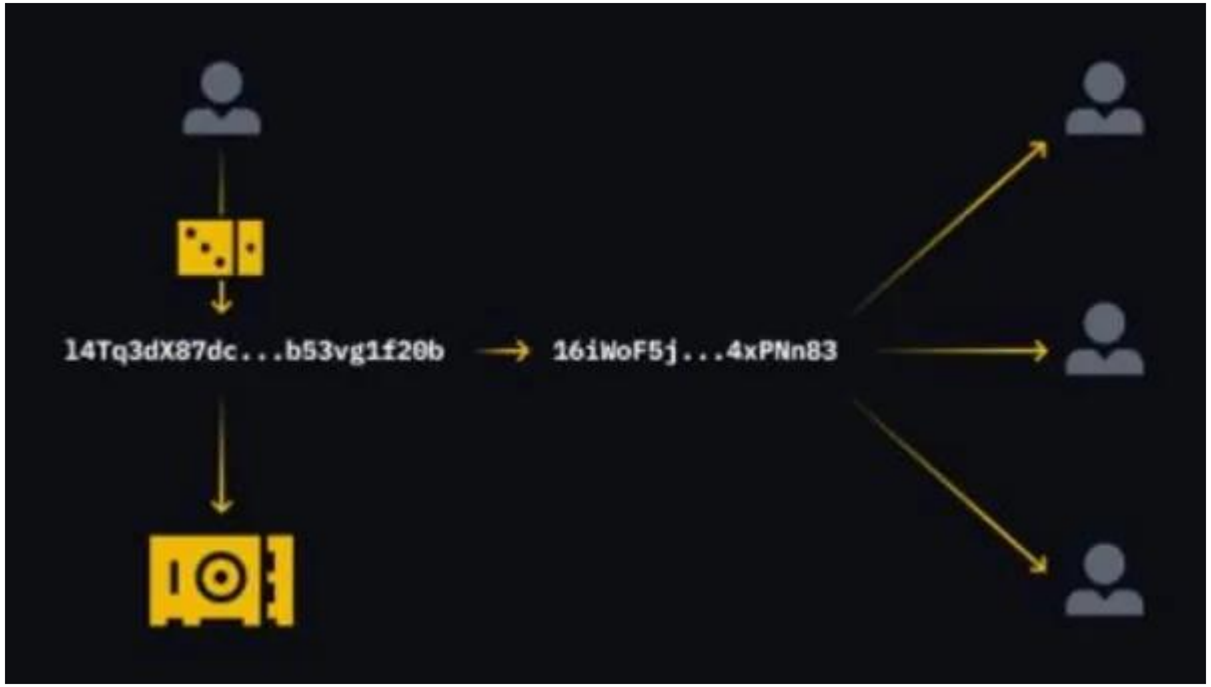
668323
~152 sat/vB
130 - 1,384 sat/vB
1.32 MB
2,935 transactions
6 minutes ago

668322
~106 sat/vB
93 - 536 sat/vB
1.28 MB
2,175 transactions
46 minutes ago

668321
~125 sat/vB
116 - 1,049 sat/vB
1.31 MB
2,225 transactions
57 minutes ago

OWNERSHIP IN BLOCKCHAIN

- Public Key Cryptography
- Asymmetric cryptography
- We have sensitive data.
- Private key
  - Encrypting
  - Decrypting
- Public Key
  - Encrypting



CONSENSUS

- Difficult or impossible in the presence of malicious; Byzantine Generals Problem
- But sometimes practice is better than theory especially in these two conditions:
    - We have incentives for good people
    - Random people will decide the next block
  - Anonymous consensus is even more difficult
    - Sybil attack
    - Random choice

IMPLICIT CONSENSUS

- In 5 steps

A. New transactions are broadcast to all nodes.

B. Each node collects new transactions into a block.

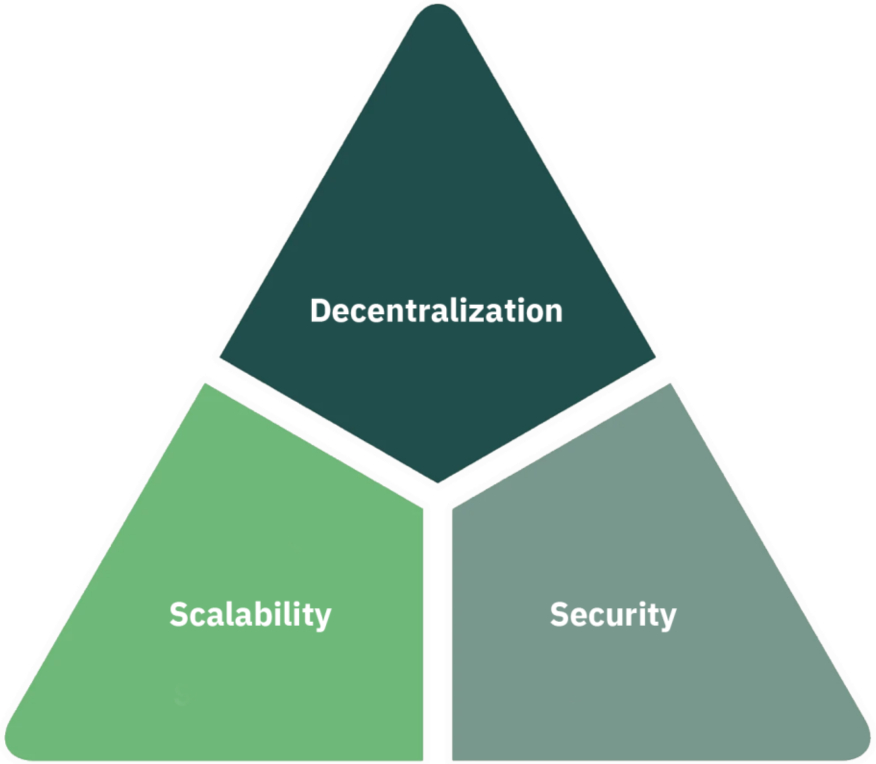
C. In each round, a *random* node gets to broadcast its block.

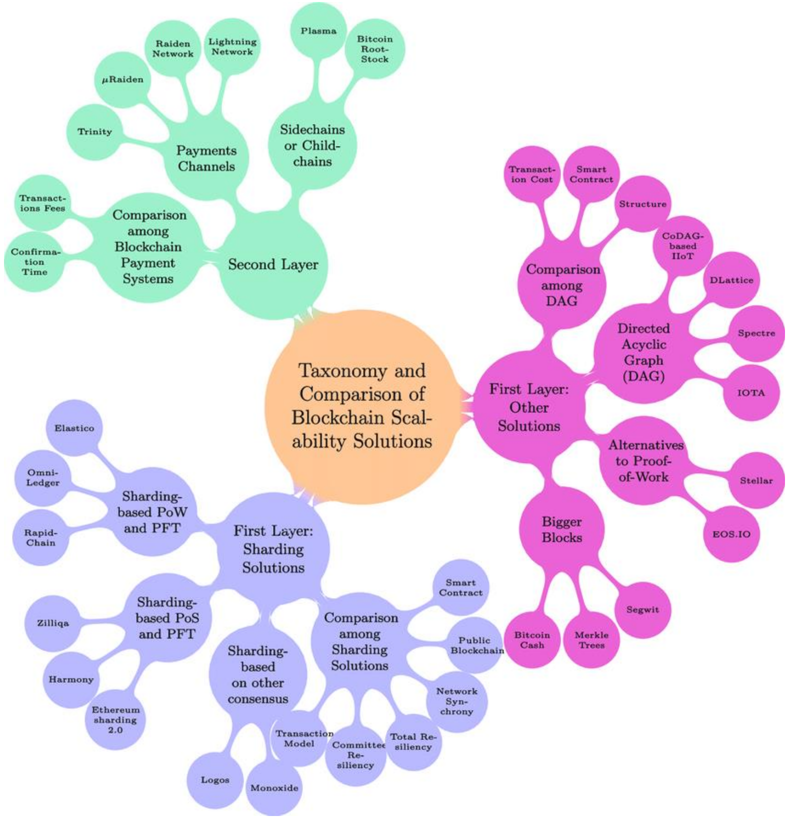
D. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures).

E. Nodes express their acceptance of the block by including its hash in the next block they create.

SCALABILITY

- Scalability of blockchain networks is the ability of that platform to support increasing load of transactions, as well as increasing the number of nodes in the network.





ADVANTAGES AND DISADVANTAGES

- The main advantages:
  - Decentralized network
  - Transparency
  - Trusty chain
  - Unalterable and indestructible technology
- The main disadvantages:
  - High energy dependence
  - The difficult process of integration and the implementation's high costs

MONEY HISTORY

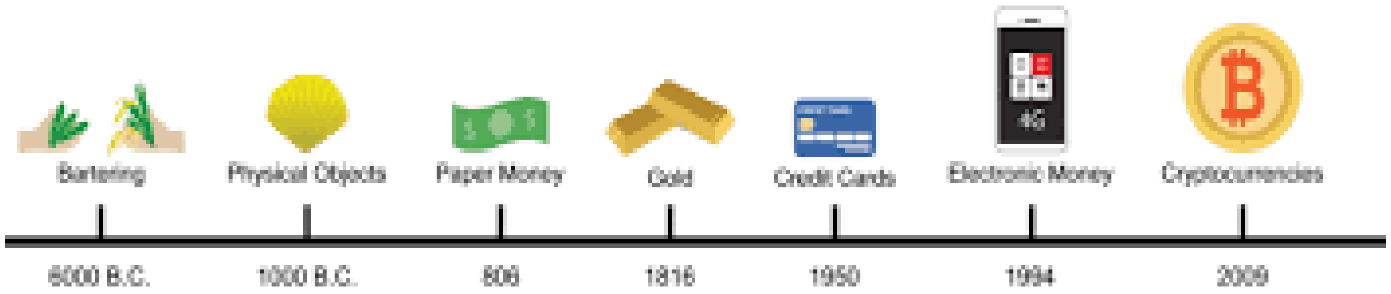
Need

- Exchange
- Value
- Coins
- Notes
- Bank notes
- Digital notes

Prehistory(b coin and others)

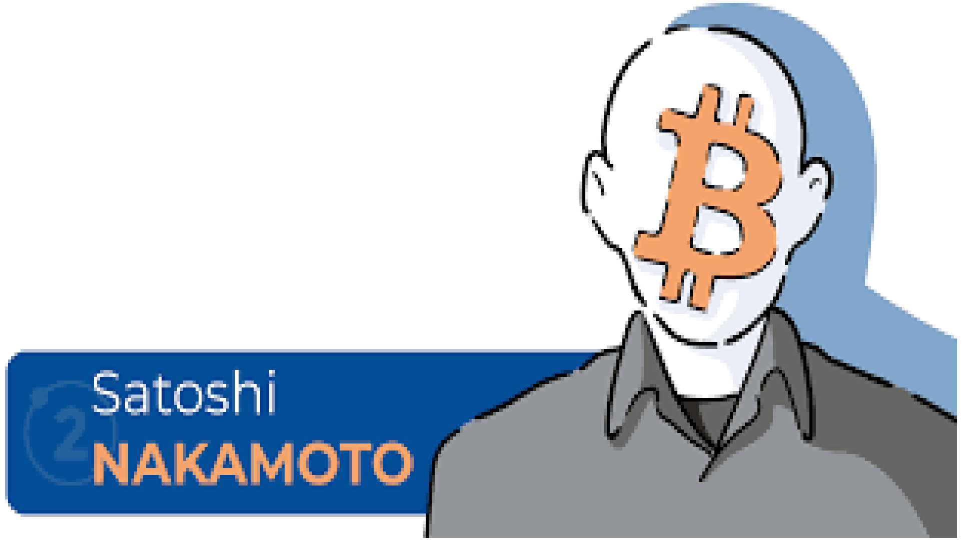
- Anonymity vs Double
- Spending vs centralized
- A lot of tries, but all failed.
- You had to give money to get money

Evolution of Money



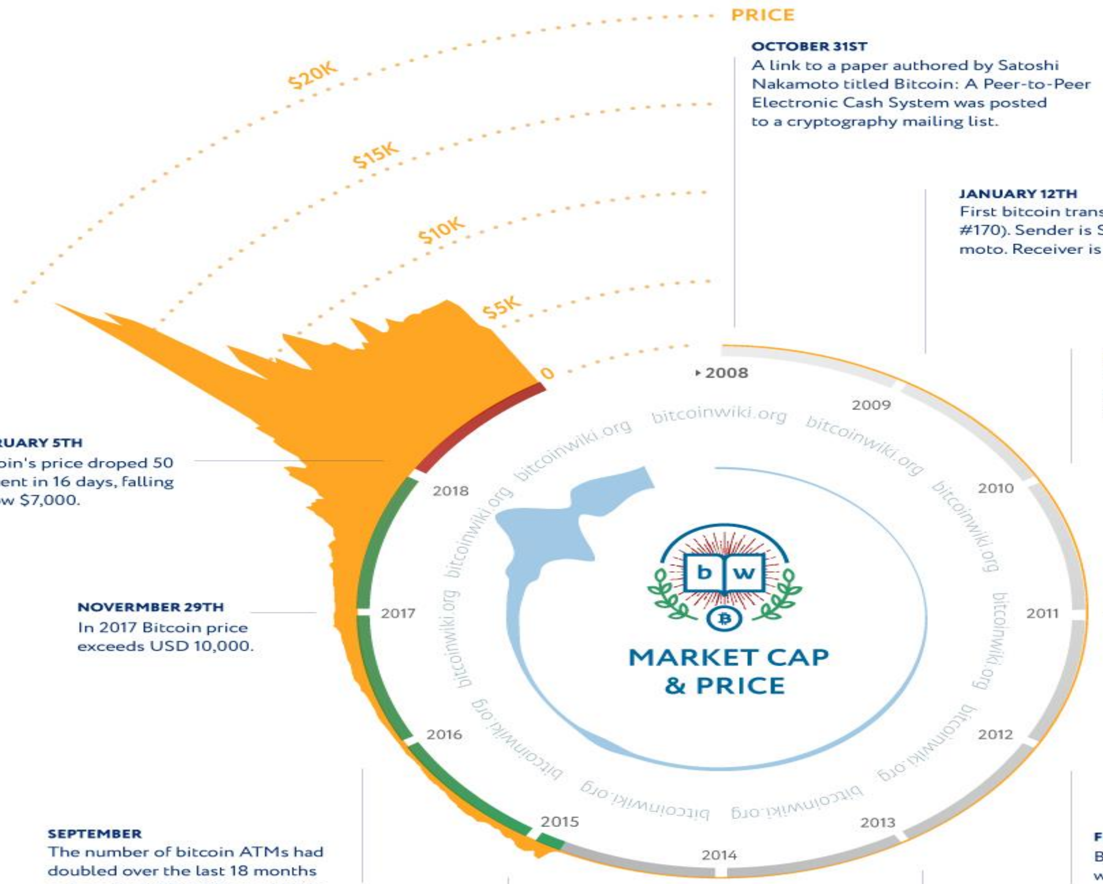
MONEY HISTORY

- Satoshi Nakamoto
  - True identity has not been verified or revealed.
  - Authored the Bitcoin whitepaper.
  - Designed first blockchain database.
- Why anonymous?
- 2008 till now



BITCOIN

- Decentralized
- To make value you need some scare
- Some programming and politics



OCTOBER 31ST
A link to a paper authored by Satoshi Nakamoto titled Bitcoin: A Peer-to-Peer Electronic Cash System was posted to a cryptography mailing list.

JANUARY 12TH
First bitcoin transaction, (block #170). Sender is Satoshi Nakamoto. Receiver is Hal Finney.

FEBRUARY 6TH
Bitcoin Market, the first official cryptocurrency stock exchange, is launched.

FEBRUARY 9TH
Bitcoin reaches parity with the US dollar (the exchange rate was one BTC to the USD).

FEBRUARY 27
Bitcoin magazine is launched with articles about bitcoin and cryptocurrency.

APRIL 1ST
Exchange rate of Bitcoin reaches 100 USD to 1 BTC

DECEMBER
Microsoft began to accept bitcoin to buy Xbox games and Windows software.

MARCH
Bitcoin startup 21 Inc. announced it had raised 116 million USD in venture funding, the largest amount for any digital currency-related companies.

SEPTEMBER
The number of bitcoin ATMs had doubled over the last 18 months and reached 771 ATMs worldwide.

NOVERMBER 29TH
In 2017 Bitcoin price exceeds USD 10,000.

FEBRUARY 5TH
Bitcoin's price droped 50 percent in 16 days, falling below $7,000.

Bitcoin historical price

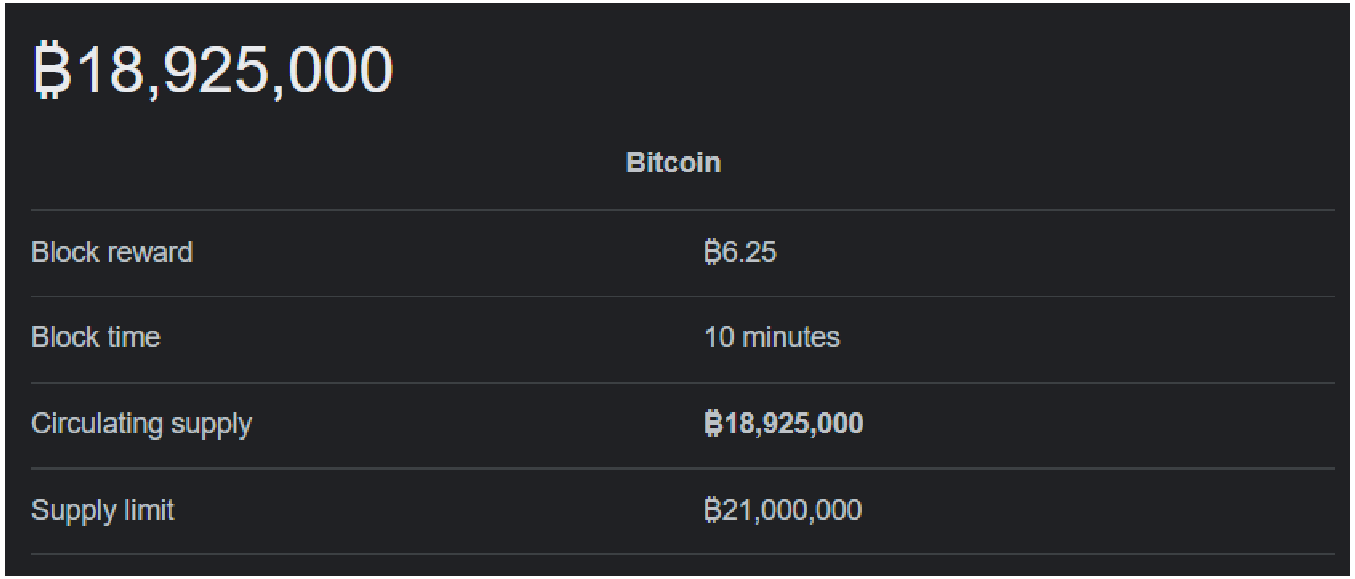
Bitcoin historical market cap

⬜ 🟩 🟥 Price rise/fall

BITCOIN MAIN ISSUE

- What is Bitcoin goal?
- Who made Bitcoin?
- Was Bitcoin created by the US National Security Agency? (ECDSA)
- What is Bitcoin's support?
- How is Bitcoin valued?
- No one is in power…
- The number of bitcoins is limited…
- Transactions are semi-anonymous…
- Transactions are irreversible…

BITCOIN CIRCULATING SUPPLY



₿18,925,000

	Bitcoin
Block reward	₿6.25
Block time	10 minutes
Circulating supply	**₿18,925,000**
Supply limit	₿21,000,000

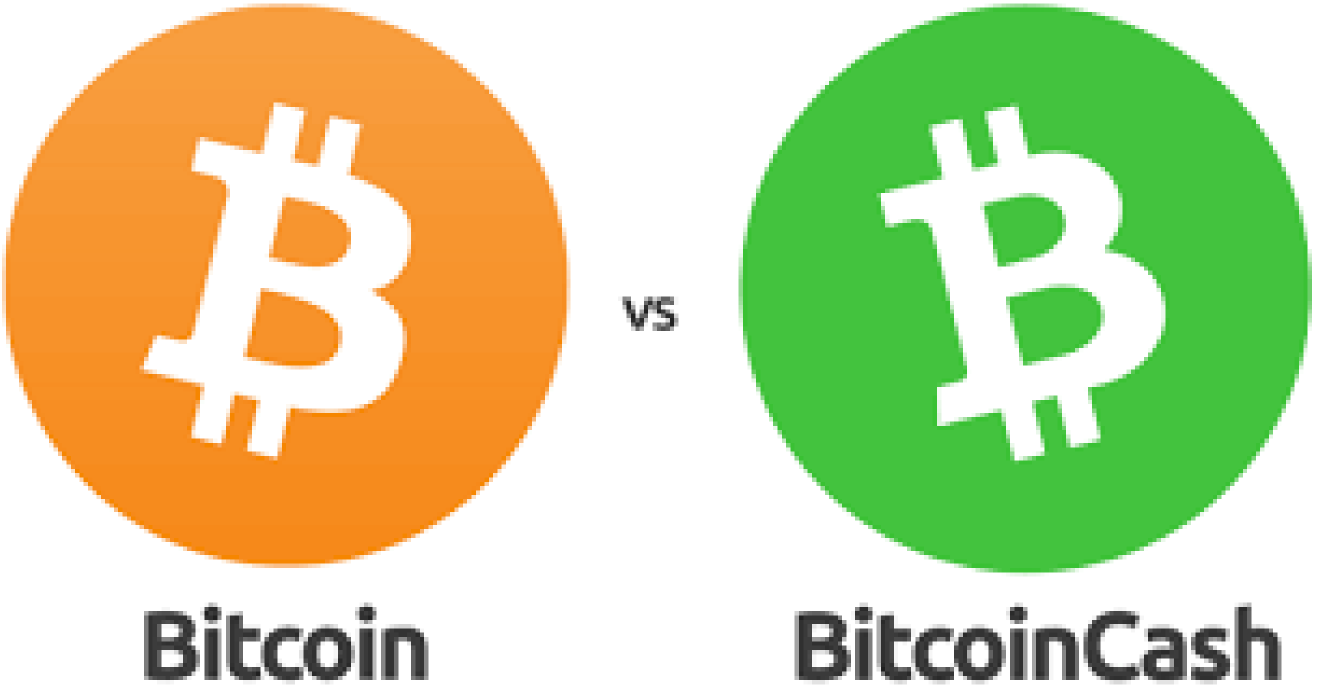
BITCOIN NETWORK

- Peer to Peer
- TCP and random topology
- Anyone can download the client and join; EQUAL
  - You will need a seed note
  - Others will start to forget you if you are not active for 3 hours
- Flood or Gossip protocol. You tell the people you know, they check and pass if checks are passed
  - Latency can lead to different mempool, but mining will decide the ties (race condition)
- Around 10K full chain nodes are 24/7 active

BITCOIN LIMITATION

- Created in 2009
- Each block is 1MB, each TRX is 250 bytes -> each block contain 4K TRX only
- One block every 10 minute -> 7 TPS! (VISA handles around 2K TPS and can handle 10K TPS peak)
- Cryptographic algorithm is ECDSA. Some believe this will be broken during bitcoins life span
- Solution? Soft and hard forks

BITCOIN FORK EXAMPLE



ETHEREUM

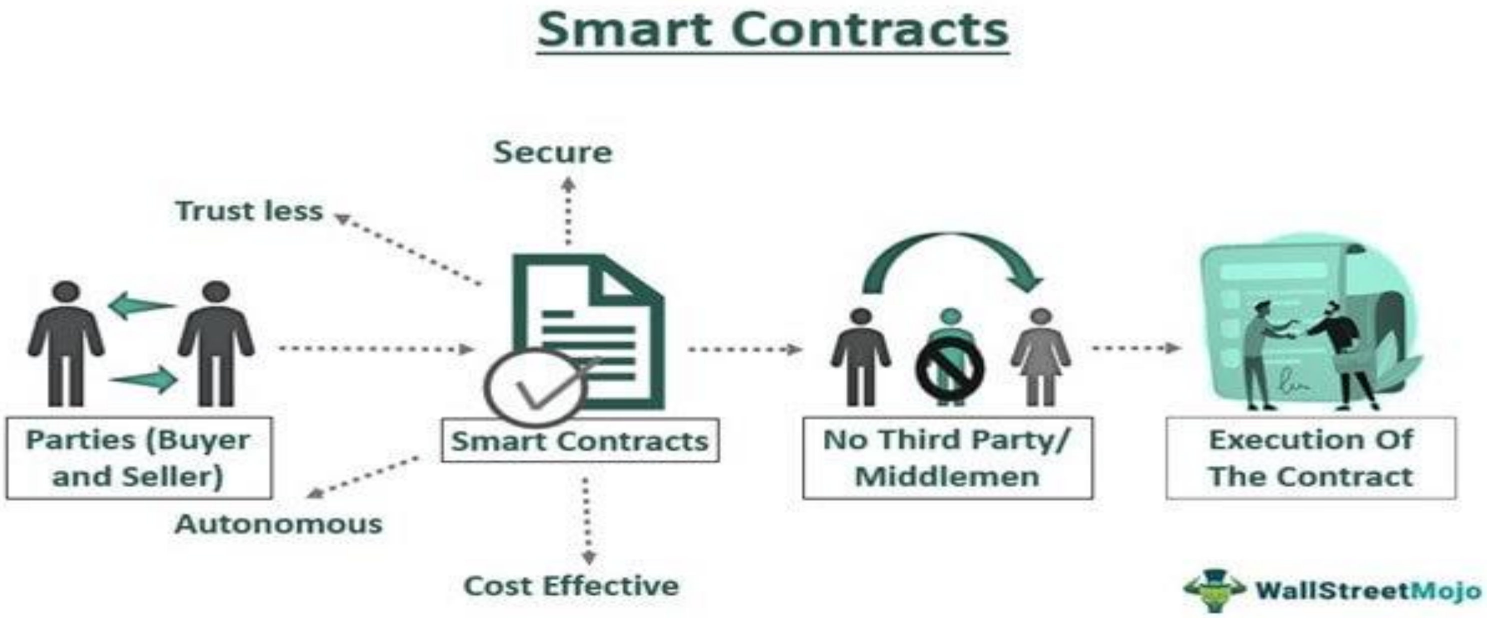
- Decentralized
- open-source blockchain with smart contract functionality
- Ether is the native cryptocurrency of the platform
- Ethereum was conceived in 2013 by programmer Vitalik Buterin
- Ether is second only to Bitcoin in market capitalization.

WHAT ARE THE FEATURES OF ETHEREUM?

- Financial services
- Privacy protection
- Removal of intermediaries
- Resistant to censorship
- Constant development

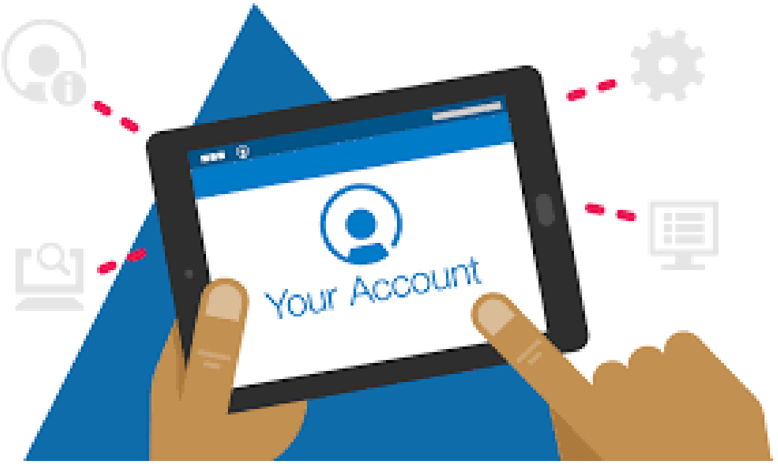
WHAT IS ETHEREUM SMART CONTRACT?

- Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.
- computer program or a transaction protocol
- Intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement

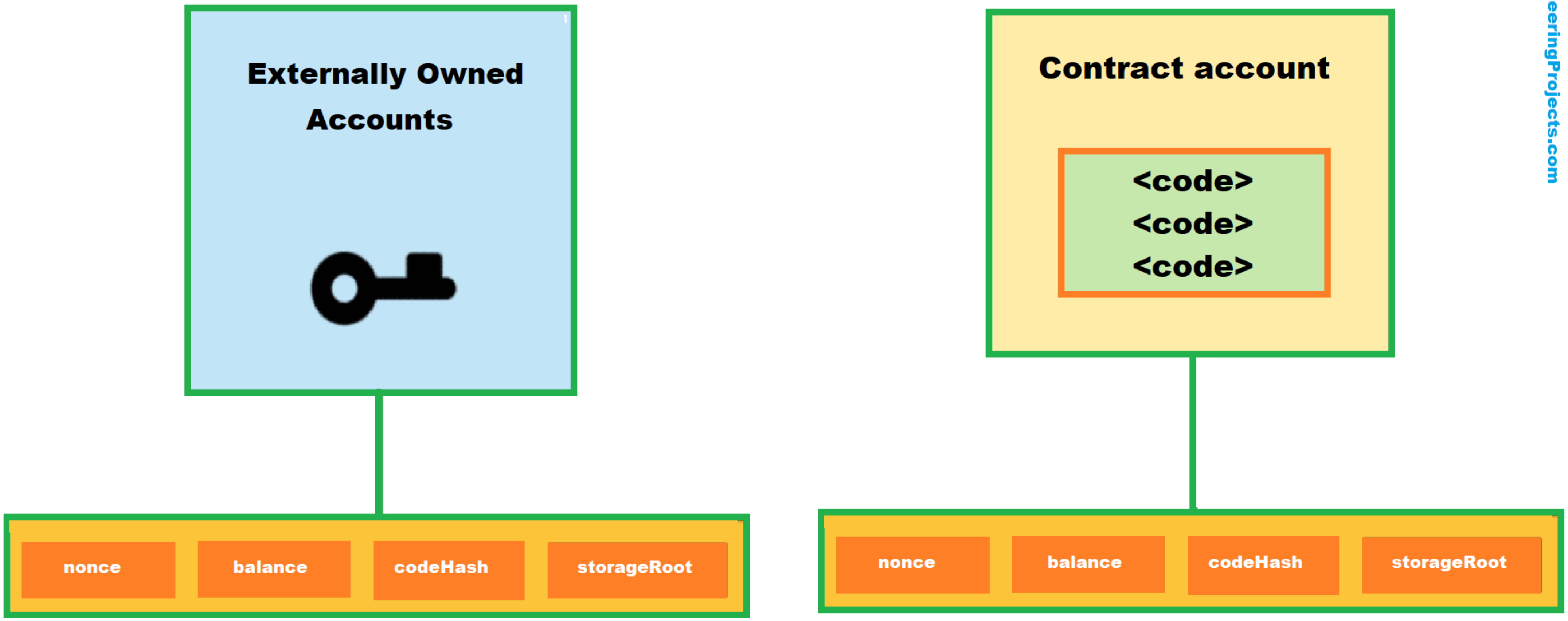


TYPES OF USER ACCOUNTS IN ETHEREUM?

- Externally Owned Account | EOA
- Smart Contract Account | SCA
- What are different?
- Features of Ethereum user accounts?



Externally Owned Account Vs Contract Account



Externally Owned Accounts

nonce

balance

codeHash

storageRoot

Contract account

<code>
<code>
<code>

nonce

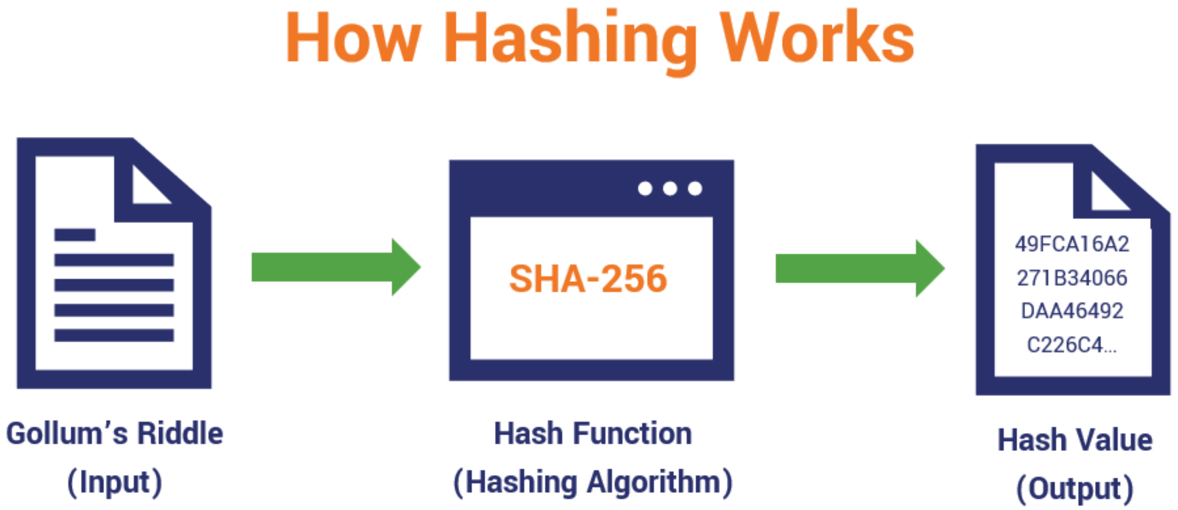
balance

codeHash

storageRoot

HOW DOES THE ETHEREUM BLOCKCHAIN WORK?

- Ethereum Proof of Work Consensus Algorithm
- Proof of Work | PoW
- Hash Functions (ETHash)
- Network Difficulty



How Hashing Works

SHA-256

49FCA16A2
271B34066
DAA46492
C226C4...

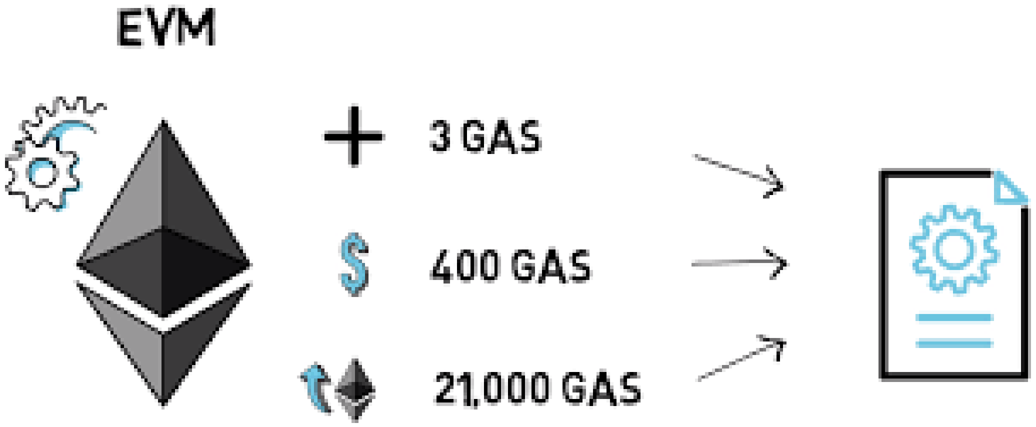
Gollum's Riddle
(Input)

Hash Function
(Hashing Algorithm)

Hash Value
(Output)

TRANSACTIONS IN ETHEREUM

- First type transaction
- The second type of transaction
- The third type of transaction
- What is the cost of Gas in Ethereum?
- What is Gwei in Ethereum?



BITCOIN AND ETHEREUM SOURCE

https://github.com/bitcoin

https://github.com/ethereum

MINING

- What is mining?
- Where did mining come from?
- How mining works?
- Who is Miner?
- Mining in the proof-of-work consensus algorithm

BITCOIN MINING

- What is the task? Finding a valid block, less than 2^68 nonces will work
- Difficulty changes every 2016 blocks
- Hardware (CPU (20M), GPU (200M), FPGA(1G), ASIC(14G))
- Energy consumption
  - Thermodynamic Limits (Landauer's principle: each bit $kT\ln 2$ joules)
  - Repurposing energy!
  - Electricity into cash

BITCOIN MINING HARDWARE

- Important factors in choosing a miner
  - Price
  - Hash Rate
  - The electricity consumption of all types of miners
- Popular Miners:
  - Bitmain
  - Canaan
  - Innosilicon
  - Cheetah Miner
  - MicroBT
  - Obelisk
  - Halong Mining
  - Alddin Miner

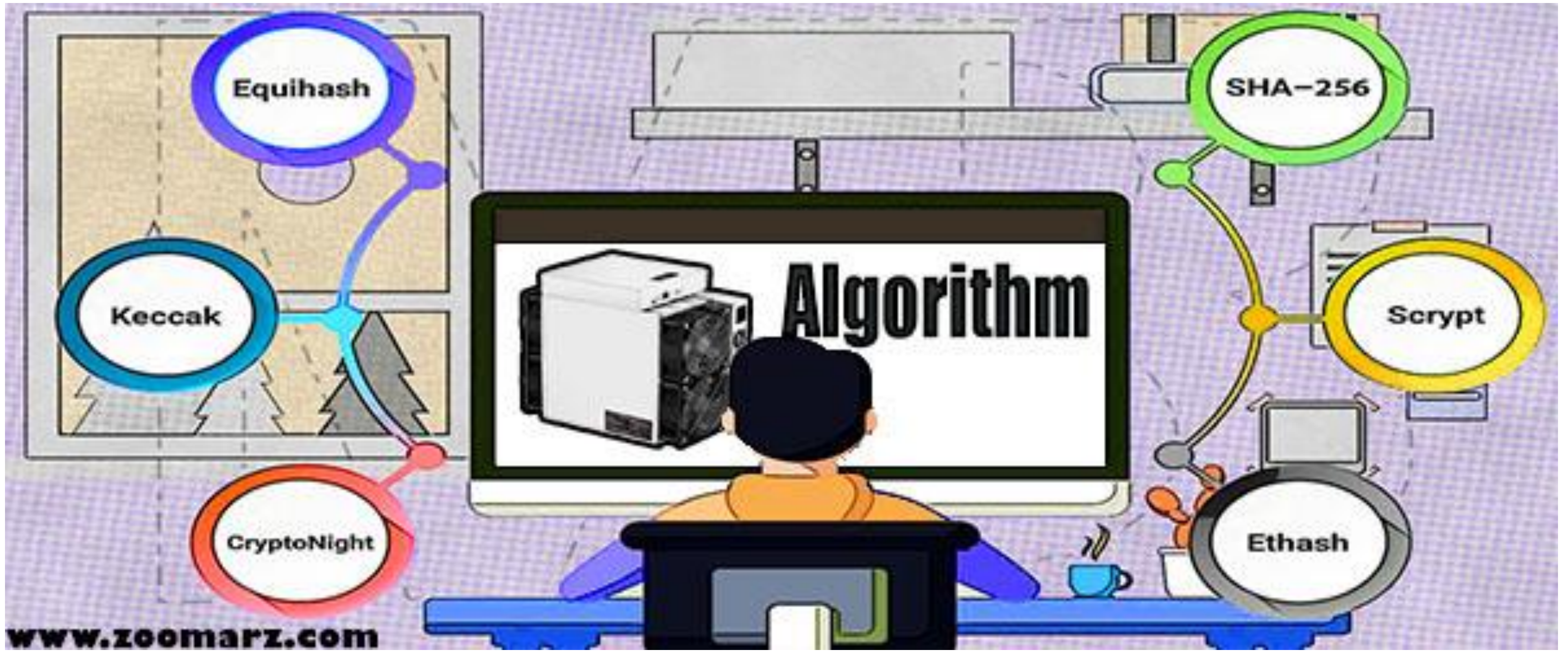
PROFIT CALCULATOR

How to estimate our mining profit?

https://arzdigital.com/calculate-profitability/#coin=BTC&hashrate=30.00*th/s&power=220&cost=90&poolfee=1&devname=aladdin-12-30t&algo=sha256

bitcoin

MINING ALGORITHMS



POOL

- What is a mining pool?
  - Syndicate idea
  - Anti cheat
  - 51% GHash
- Types of rewards in mining pools…
  - **PPS**
  - **Proportional**
  - **Score-Based**
  - **Pay Per Last N Share**
- Selection of mining pool…
  - Check your infrastructure
  - Know the pool payment methods well
  - Keep in mind the fees for each pool
  - Some pools impose restrictions on miners

Poolin

f2pool

MINING ATTACKS

- Forking Attack (Spending and then mining the previous block)
- Forking via Bribery (clever idea? Run a pool with loss of revenue, or give tips in blocks!)
- Block Withholding Attacks = Selfish Mining
- Blacklisting or Punitive Forking (announcing that you won't work on a chain if it contains blah blah)
- Feather Forking (just like punitive forking but just for a short period of time)
  Future? Moving toward mining based on TRX Fees

MINING SOURCE CODE

- https://github.com/topics/mining

ANONYMITY IN BITCOIN

- Anonymous = without name
- Anonymous vs pseudo-anonymous (reddit vs 4chan) vs unlikability
- In bitcoin, you don't have a real name but you have an address
- Side channels (big data)
- It is difficult to reach Unlikability because receiver sees the senders address
- Why anonymity is needed?
    - To reach the traditional privacy we had
    - To reach a new level of privacy
        - Salary, class fees, paying subcontractors will reveal business plans
        - It is difficult to exchange fiat with cryptocurrency, laundering is difficult

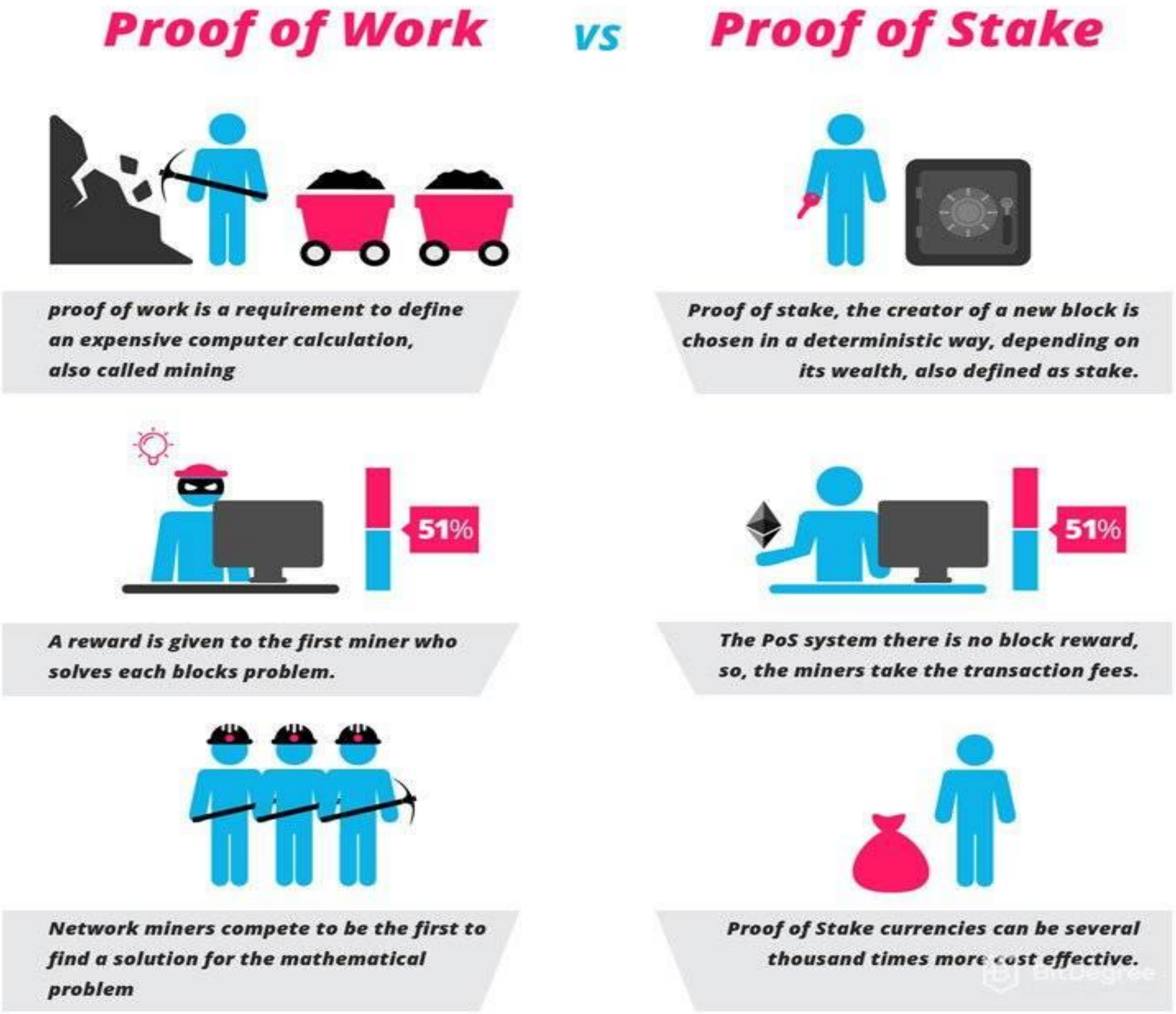
POW

- Proof of work is a software algorithm used by Bitcoin and other blockchains to ensure blocks are only regarded as valid if they require a certain amount of computational power to produce," says Amaury Sechet, founder of the cryptocurrency eCash.

- Proof of work is a form of cryptographic proof in which one party proves to others that a certain amount of a specific computational effort has been expended. Verifiers can subsequently confirm this expenditure with minimal effort on their part

POS

- Proof of Stake (PoS) is an algorithm employed by cryptocurrency protocols to reach consensus. In PoS blockchains, an individual or group is algorithmically chosen to verify transactions with computer hardware based on the tokens they have staked, or locked up, in the network as a form of collateral.



Proof of Work vs Proof of Stake

proof of work is a requirement to define an expensive computer calculation, also called mining

Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

A reward is given to the first miner who solves each blocks problem.

The PoS system there is no block reward, so, the miners take the transaction fees.

Network miners compete to be the first to find a solution for the mathematical problem

Proof of Stake currencies can be several thousand times more cost effective.

HOOMAN DEHGHANI | DMINDDEV01

- GitHub: https://github.com/DmindDev01
- Twitter: https://twitter.com/DmindDev01
- LinkedIn: https://www.linkedin.com/in/hooman-dehghani-27089117b
- Instagram: https://www.instagram.com/hooman.dehghani/
- Email: dminddev01@gmail.com

Thank You!