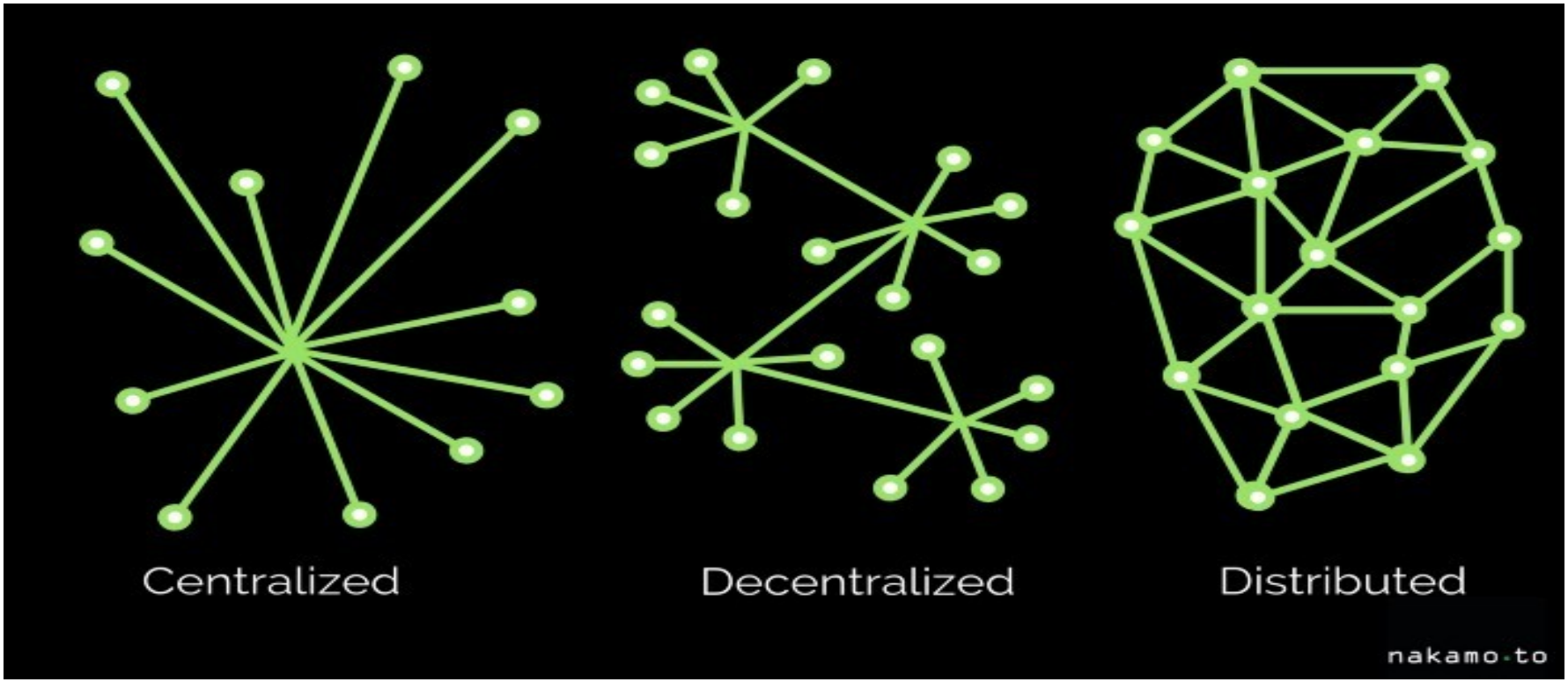
Blockchain Fundamentals Part 1

Definition, History, Consensus mechanisms

Blockchain and Bitcoin

- What is Blockchain?
- What is Bitcoin – what is the difference between those?
- What's the difference between technology and protocol?
- Bitcoin is also cryptocurrency
- Short abbreviation BTC or XBT (trading)

Types of Network by level of segregation



- Bitcoin’s blockchain protocol, is a decentralized system for exchanging digital value — but it’s also an example of distributed ledger technology.
- Bitcoin uses both Decentralized and Distributed network approach

Distributed ledger - DLT

- Ledger – Accounting book
- A distributed ledger (also called a shared ledger or distributed ledger technology or DLT) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions

Distributed ledger - DLT

- Please give example of Ledger Technology

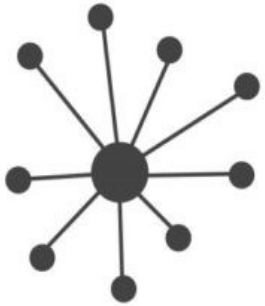
Robinson Crusoe Ledger

Yapese island

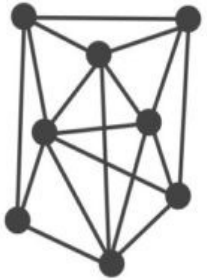
Comparing DLT and RDMS or Database

- What is the difference between DLT and standart Database?
- Database has CRUD operations
- **DLT supports “Append only” mode**
- **DLT is replicated on all nodes**

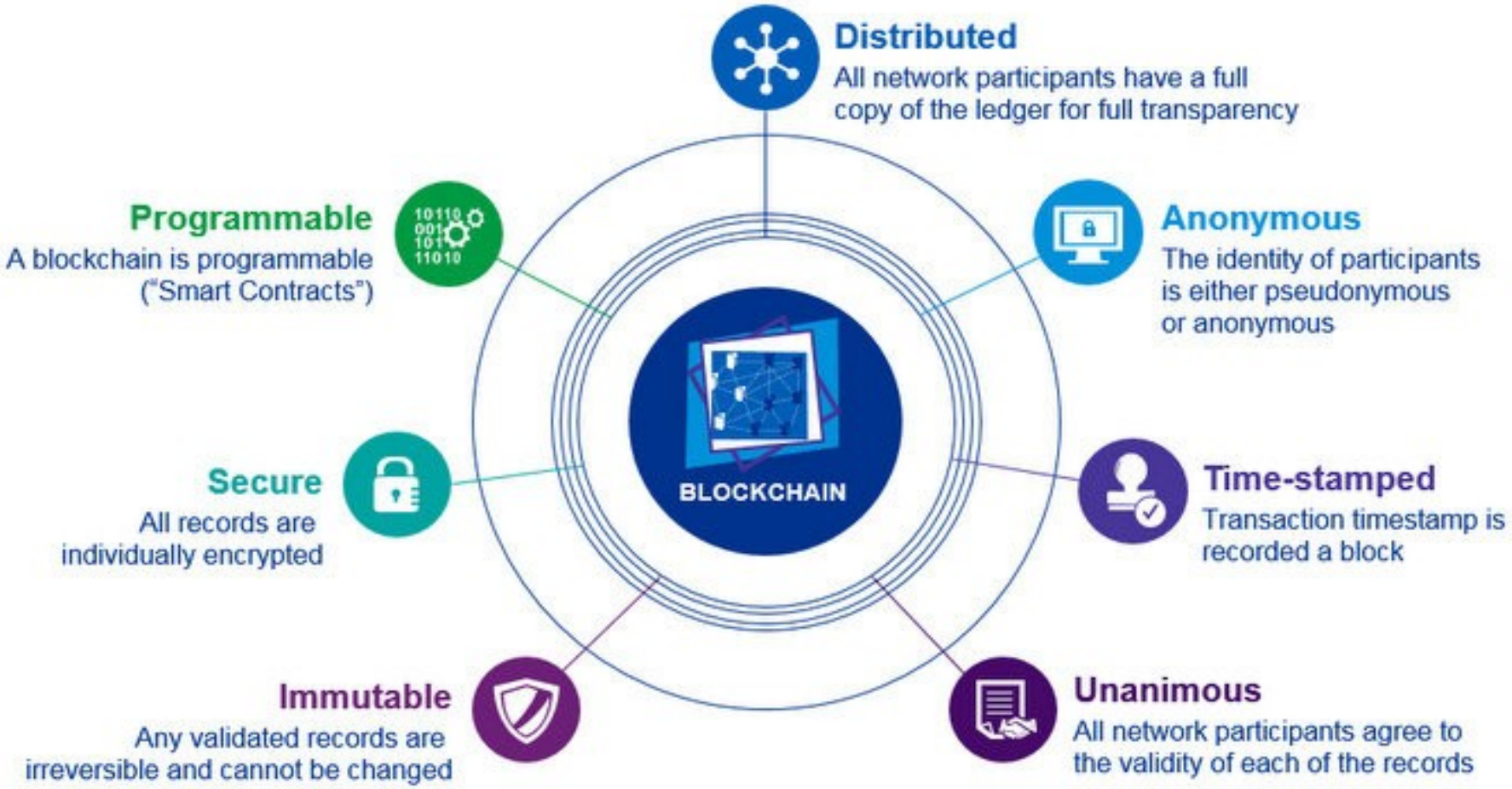
TRADITIONAL DATABASE



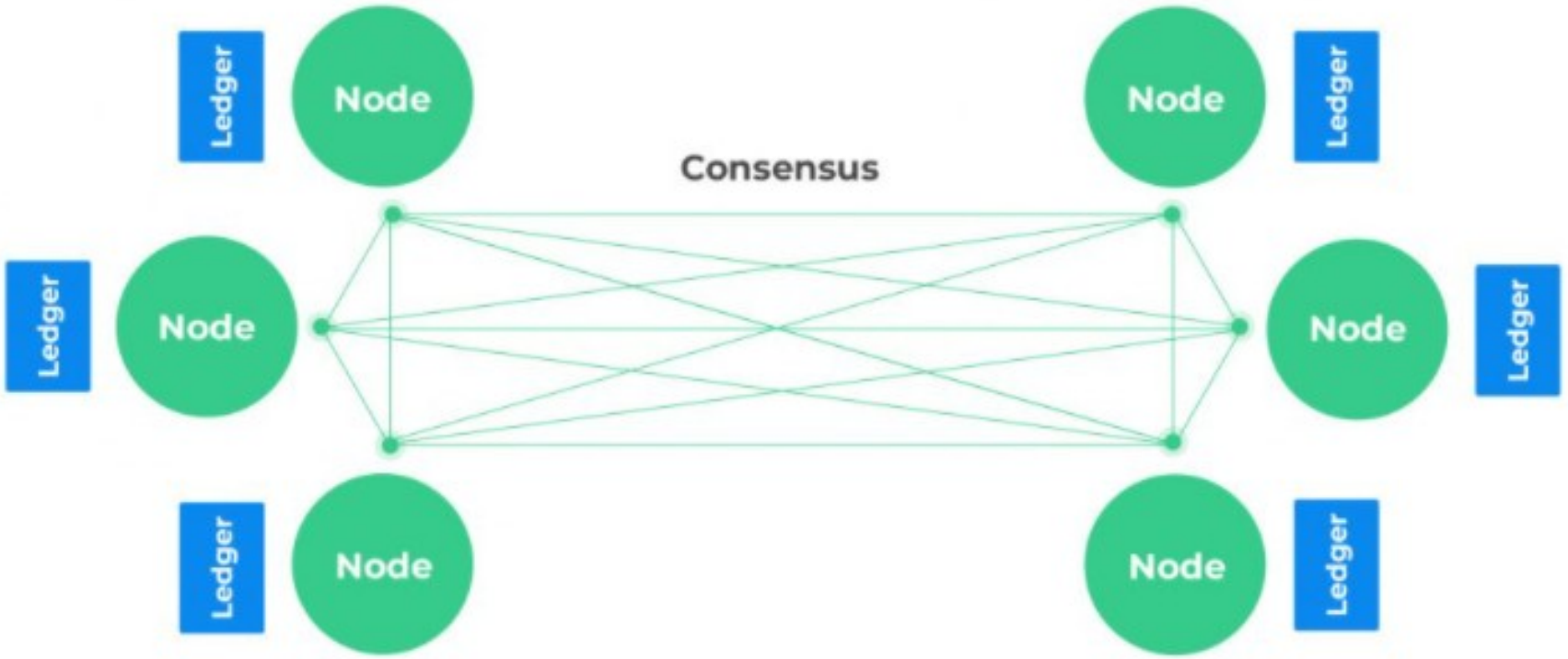
BLOCKCHAIN



Properties of Digital Ledger Technology (DLT)



Ledger technology



Blockchain definition

- A blockchain, originally block chain, is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree
- **It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way**

Blockchain definition

A blockhain is essentially a digitally-signed ledger. Each transaction on the blockchain is visible on the public ledger, and all entries are distributed across the network, requiring consensus about each transaction.

Blockchain and DLT

- What is the relation between DLT and Blockchain ?
  - Every Blockchain is / supports DLT, but not every DLT is blockchain

Bitcoin History

- When all started ?
  - First concept of Cryptocurrency is described in 1998 in Cyberpunk society (b-money and bit gold)
  - 2008 Satoshi Nakamoto releases BTC White paper
  - January 2009 the first block (Genesis block) is submitted
  - 2011 Based on BTC new Cryptocurrencies start to emerge

Genesis block

- First genesis block is release after 3rd of January because it contains information from “The Times” newspaper

Bitcoin Genesis Block

Raw Hex Version

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

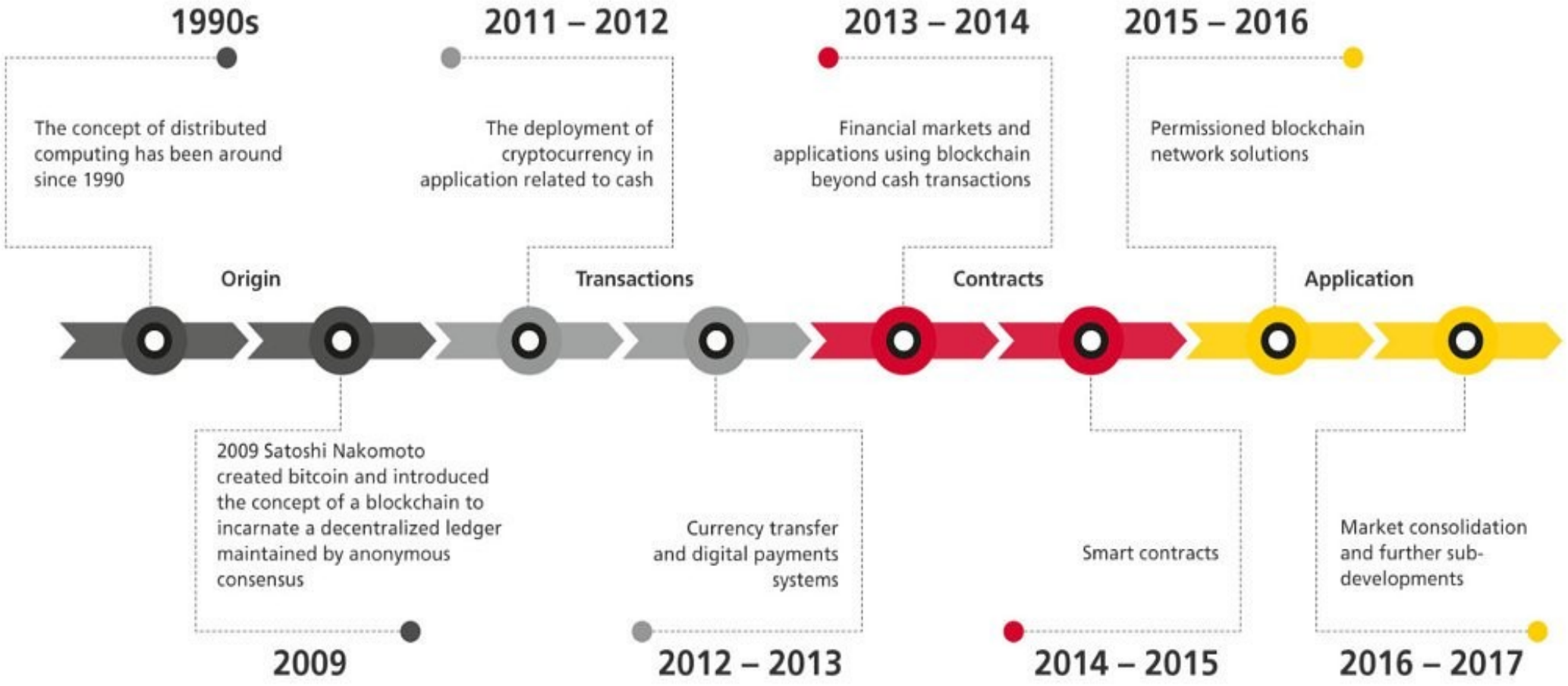
Bitcoin definition in Statoshi's vision

- BTC Whitepaper: https://bitcoin.org/bitcoin.pdf
- In Bitcoin WhitePaper: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

Bitcoin History

- Creator of BTC – Satoshi Nakamoto
- Who is Satoshi Nakamoto?
- Last posts from Nakamoto were from 2011
- https://satoshi.nakamotoinstitute.org/posts/

BLOCKCHAIN HISTORY



Fundamental values

- What are Blockchain and BTC fundamental values?
- Immutability
  - Immutable = Resistant to change
- Transparency
  - Transparent = Public, able to verify
- Decentralized
  - No single entity controls the Network

Fundamental values

- Privacy – how is that we have privacy with Bitcoin?
- Security
  - What secures the network?
  - What is Byzantine Fault Tolerance (BFT) ?

Byzantine Fault Tolerance(BFT) is the feature of a distributed network to reach consensus(agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information.

Consensus algorithm

- What is consensus algorithm ?

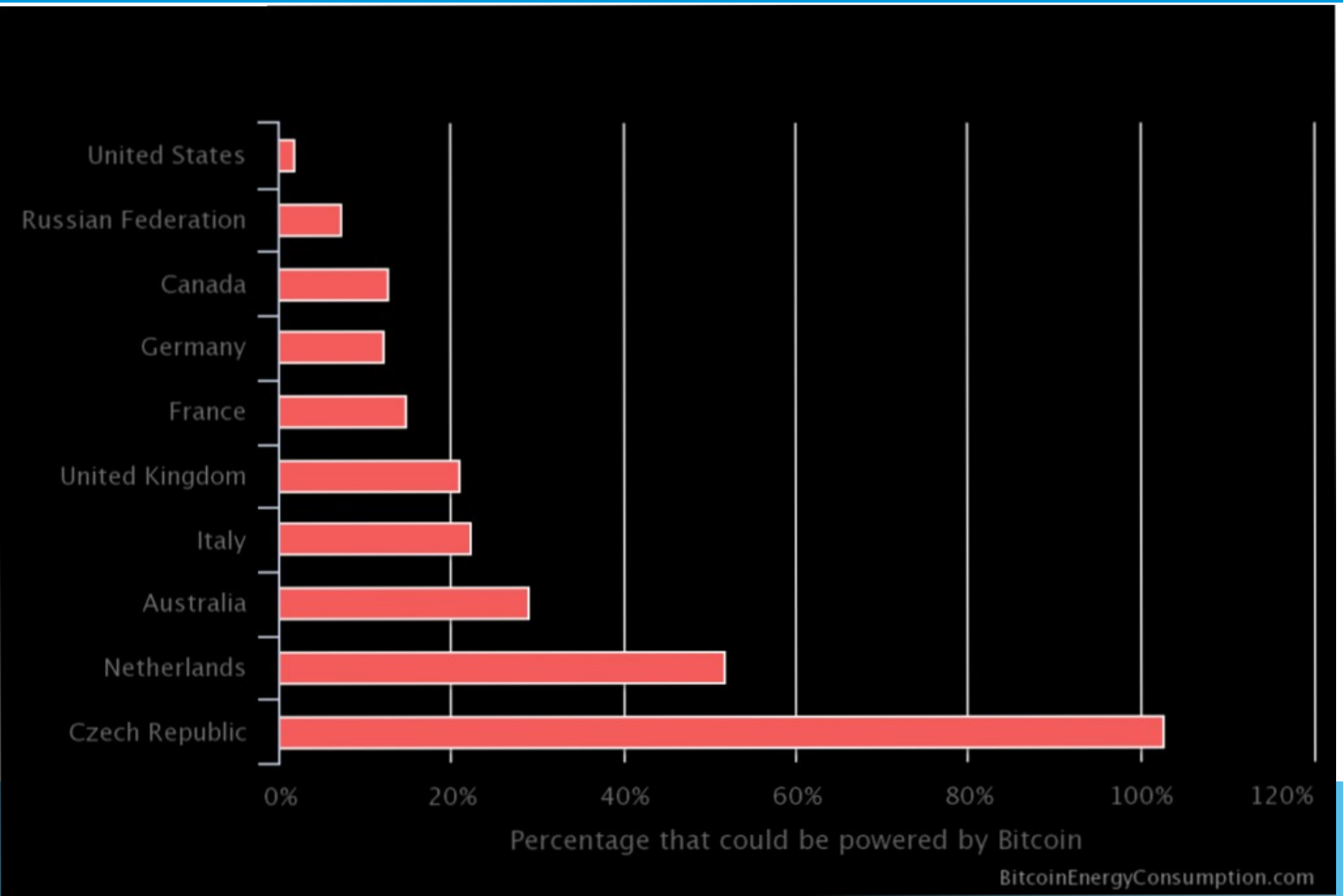
A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger.

Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

Bitcoin uses Proof of work (POW)

- Definition
- Proof of work describes a system that requires a not-insignificant but feasible amount of effort in order to validate next blockchain block
- Calculate the NONCE – number only used once.
- When rehashed, meets the difficulty level restrictions. The nonce is the number that blockchain miners are solving for. When the solution is found, the blockchain miners are offered cryptocurrency in exchange.
- Bitcoin uses SHA-256 hashing algorithm
- List of mining algorithms.
    - https://en.bitcoinwiki.org/wiki/Mining_algorithms

Electricity consumption related to countries



Pros and Cons of POW

- What are pros and cons of POW algorithms?
  What happens to miners with small computing power (hashrate) try to validate block in pair with participants with huge computing powers?

- **Pros -** Security Very hard to tamper and attack the network when hashrate is high
- **Cons** – huge energy consumption, not environmentally friendly
- online source:
- https://digiconomist.net/bitcoin-energy-consumption

Possible attacks of POW

- Can the network be attacked ?

Distributed Denial of Service

For this attack, hackers initiate multiple, fake requests. Consequently, they consume most or all of the network's processing resources. The obvious result? The network server crashes! When this happens, every other node in the network is cut off from the server.

51% Attack

Theoretically, if a node acquires 51% of the network's total mining power, it can bend the network according to its wishes. The attacker who controls a majority of the network can:

Validate fraudulent blocks beneficial to it.
Revert previously validated transactions.
Enforce double-spending.

Other problems of POW

- What other problems have the POW blockchains?

Double spending

Double-spending is the risk that a digital currency can be spent twice. It is a potential problem unique to digital currencies because digital information can be reproduced relatively easily by savvy individuals who understand the blockchain network and the computing power necessary to manipulate it.

How can double spending be stopped?

Using higher confirmation time! (cofirmation time is the time between two validated blocks)

Proof of stake

The Proof of Stake consensus algorithm was introduced back in 2011 on the Bitcointalk forum to solve the problems of the current most popular algorithm in use - Proof of Work. While they both share the same goal of reaching consensus in the blockchain, the process to reach the goal is quite different.

Different POS implementations takes different aspects of the validating nodes:

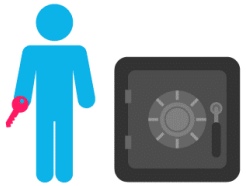
- Staking Age
- Randomization
- Node's wealth – the bigger the stake, the bigger chance is the node to be accepted as next validators

Consensus Mechanisms

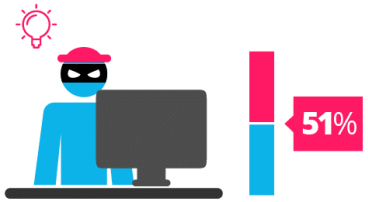
- Difference between
  - POW and POS

Proof of Work vs Proof of Stake

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

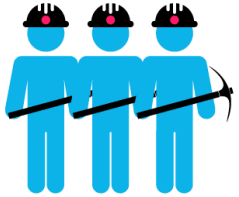


Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



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.

Sources

- Consensus
  - https://dzone.com/articles/the-proof-of-work-vs-proof-of-stake-an-in-depth-di
- Immutability
  - https://medium.com/the-bitcoin-times/immutability-5cfeb53cd6fb

- Useful blockchain links:
  - https://www.geeksforgeeks.org/blockchain-technology-introduction/
  - https://digiconomist.net/bitcoin-energy-consumption (PoW consumption)
  - https://theblockbox.io/examining-the-distinctions-between-distributed-ledger-technology-and-blockchain/

Questions ?

- Thank you for your attention!