Distributed Ledger Technologies and Blockchain

A distributed system perspective

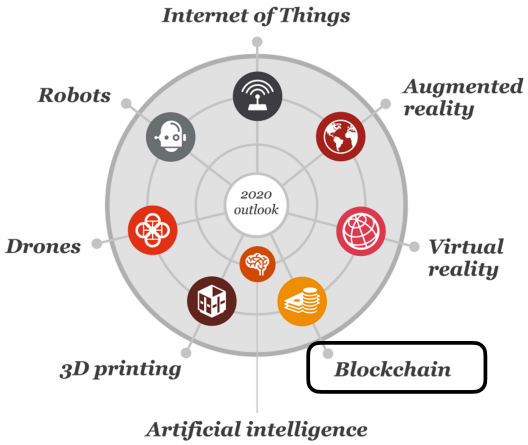
Claudio Bettini - Università degli Studi di Milano

Copyright

Claudio Bettini - Università degli Studi di Milano

Blockchain: a buzzword?

- Considered by market research among the "essential eight technologies"



#TechMegatrend

The DLT System Model

- A distributed system with
  - decentralised control
  - nodes run by different entities that do not trust each other and may even be malicious (Byzantine behavior)
  - a copy of data records (financial transactions, medical records, sensed data, …) is stored at each node
- A consensus problem:
  - Nodes need to agree on a history of data (e.g., a «ledger» with a history of financial transactions)

Blockchain: The story

- 2008: a whitepaper appears titled
  Bitcoin: A Peer to Peer Electronic Cash System
  The author is “Satoshi Nakamoto” (the true identity of the person or group is still unknown)

- 2009: opensource Bitcoin implementation and first client.

- 2012-2013: other DLT based cryptocurrencies are created.
  Ethereum is created to go beyond cryptocurrencies handling tokens and contracts

Blockchain beyond Bitcoin

Carrefour lancia la prima blockchain dedicata alla filiera del pollo

di **Filippo Piva**
SETTEMBRE 13, 2018

L'iniziativa, fino ad ora mai sperimentata nella Grande Distribuzione italiana, punta a migliorare la trasparenza offerta ai clienti, all'interno di un progetto orientato alle

Global Blockchain Technology in Healthcare Market to Approach USD 1415.59 Million By 2024

By Hiren Sam — On Apr 1, 2019

HOME › ESPERTI E ANALISTI › Blockchain e tokenizzazione per difendere e valorizzare il patrimonio artistico

Blockchain e tokenizzazione per difendere e valorizzare il patrimonio artistico

7 Aprile 2019 Giovanni Perani Esperti e Analisti, Media & Entertainment, Smart Contract

PA 4.0: il Comune di Bari avvia con SIA il primo progetto blockchain

7 Febbraio 2019 Claudia Costa

Prima sperimentazione nell'ambito della Pubblica Amministrazione per certificare l'autenticità e il rilascio di polizze fideiussorie attraverso l'utilizzo di smart contract [...]

BITGUILD
BLOCKCHAIN GAMING PLATFORM

Blockchain for gaming

	Traditional Games	Blockchain Games
True ownership	Virtual assets are held in the game company server.	Virtual assets are held in the player's digital wallet.
Cooperative global gameplay	Split into regions and servers.	Cooperative global gameplay.
In-game items trading	Trading on third-party websites. Players exposed to frauds and uncertainty.	Trading directly with each other through the use of smart-contract.
Microtransactions	Players must recharge a minimum amount of real money.	Perform directly microtransactions.
Cross-game compatibility	When a player quits the game, he loses each character and every virtual item.	Virtual assets can be transferred between different games.
Frauds	Easy refunds regardless of whether they are faulty.	Transparent and permanent transactions.

https://cryptopotato.com/bitguild-ico-evaluation/

Data in Blockchain

- A blockchain is a ledger of *transactions*
- A transaction is a data record
  - Example of a bitcoin transaction: *Alice transfers 0.15 BTC to Bob*

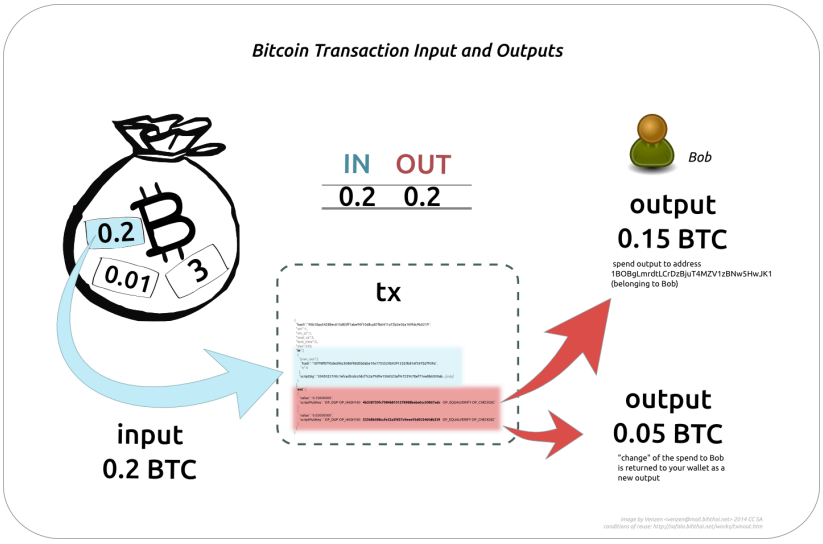


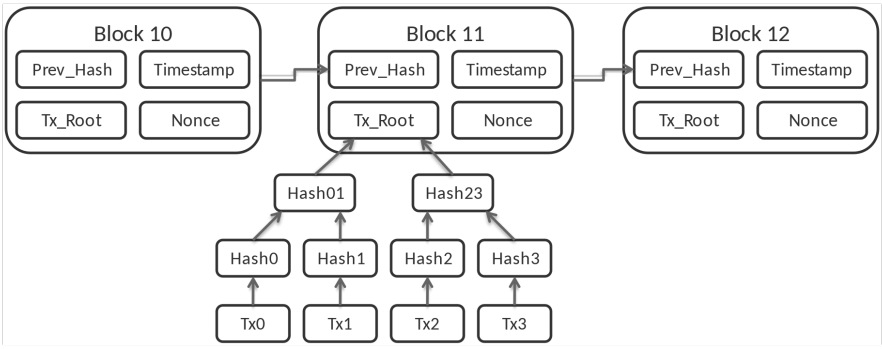
Image by Venzen venzen@mail.bihthai.net 2014 CC SA

The Blockchain approach

- Each transaction is digitally signed (with private key of the sender) and propagated to all participating nodes
- When a node receives a transaction, it validates it (according to some network-wide rule).
  - For example in a financial transaction it is possible to check if the sender actually has the money that is spending)
- Validated transactions are still considered “pending” as they are not yet part of the chain

The Blockchain approach

- In a blockchain, transactions are grouped in timestamped blocks and the whole history is stored at each node as a chain of blocks



Problems

Since there is unpredictable latency, imprecise clock synchronization, and faulty (malevolent) nodes:

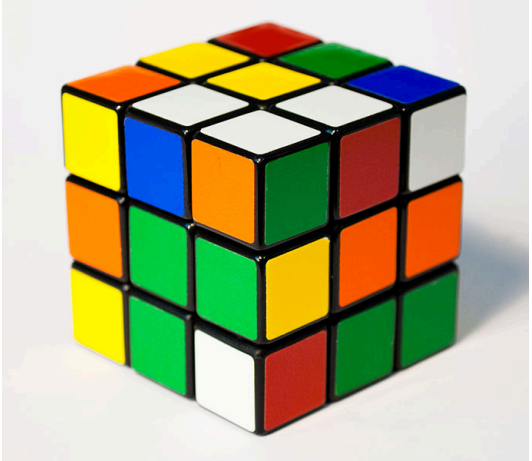
- The order of arrival of transactions may be different at different nodes
- Some transactions may be contradicting each other (e.g., double spending in bitcoin)
- Different nodes may build different blocks
- Different nodes may end up with different chains (*no consensus*)

Consensus in blockchain

- The challenge is for the nodes to have a **consensus on the blocks and on the sequence of blocks** (each node should eventually have the same copy of the chain)
- Main idea:
  - compute the hash of each transaction, and of a block
  - compute the hash of a block including the hash of the previous block in the chain
  - include a trick to make the computation of the block hash expensive but very easy to verify
  - make the nodes compete on this computation with a reward, and have the winner propagate its computed block to the others (it is like “electing” a node to impose its block)

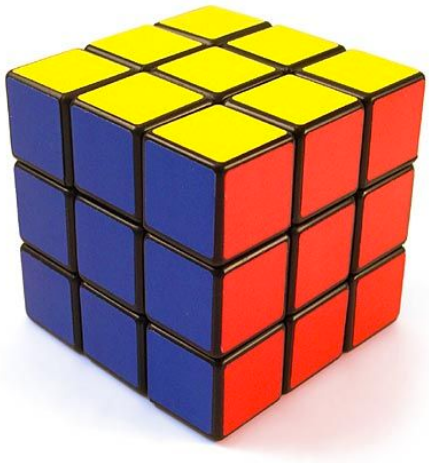
Every Ware Lab

Difficult problems



Every Ware Lab

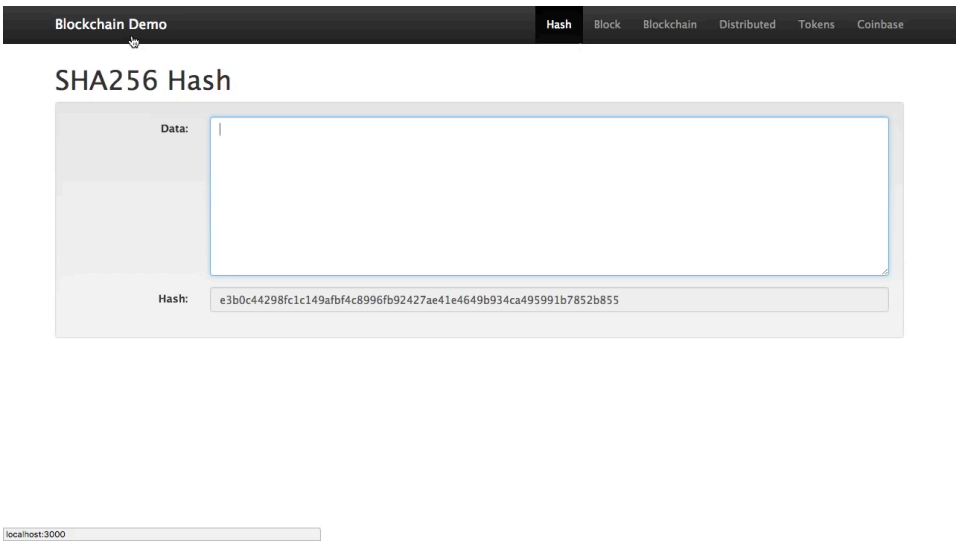
Easy to verify if solved



Hashing

- A cryptographic hash function *f* (e.g. SHA-256)
  - *f(A)* has fixed length (e.g., 256-bits independently of *A*'s length)
  - collision resistant (if A ≠ B then *f(A)* ≠ *f(B)*)
  - very difficult to find *A* from *f(A)*
  - quick computation of *f(A)* —> easy to verify given A and B if B= *f(A)*

Hashing



https://andersbrownworth.com/blockchain/

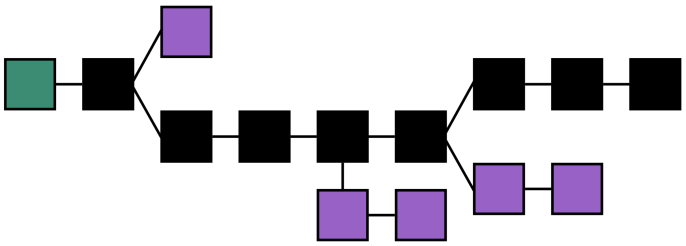
YouTube video by Anders Brownworth https://youtu.be/_160oMzblY8

Blockchain PoW algorithm

- The algorithm used for consensus is called Proof-Of-Work (POW)
- *Verifying* a block requires solving a computational puzzle while computing its hash
- A *miner* node needs to find a number (a nonce included in the block data) such that the hash of the block has a particular property
- Solving the puzzle requires a brute force approach (it is designed to take a certain amount of time that makes it unlikely that two miners solve their puzzle at the same time)
- A reward is given to *miners* that win.

Blockchain PoW algorithm

- A verified block is sent to all nodes
- When a node receives a block, it checks the puzzle solution and then adds it to its local copy of the chain (linked to the one whose hash is in the block).



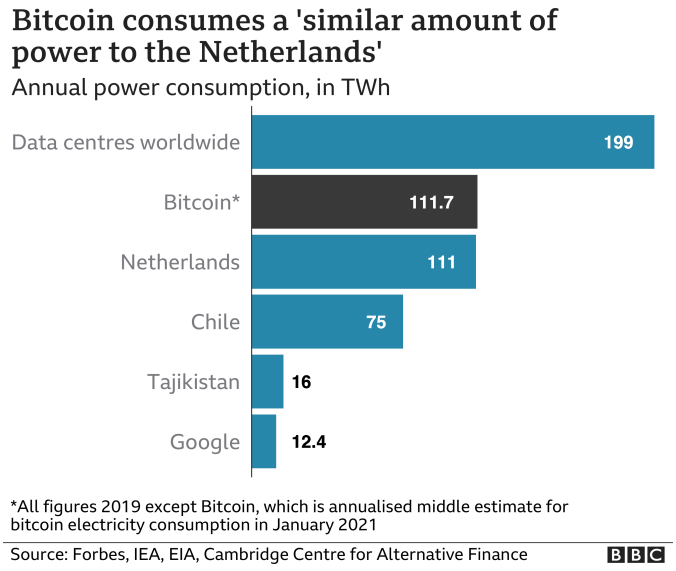
Claudio Bettini - Università degli Studi di Milano

Blockchain properties

- Assuming *most* nodes are working on the same chain, the one growing fastest will be the longest and most trustworthy
- In order for a malicious node to change a transaction in an intermediate block, it has to re-compute all the subsequent block hashes and prevail over other nodes in the network
- Blockchain is safe as long as more than 50% of the work being put in by miners is honest.

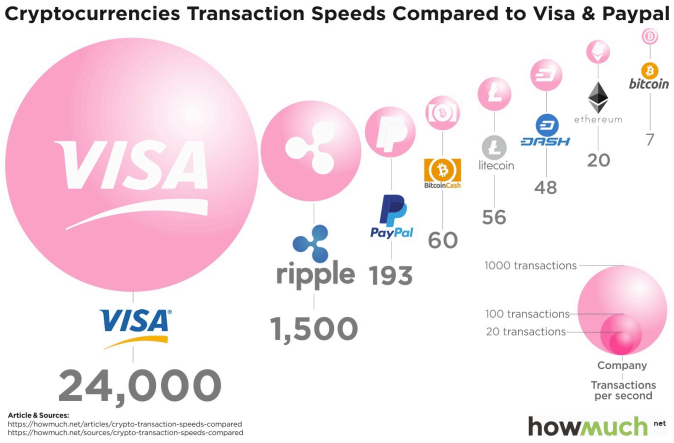
Major PoW limitations

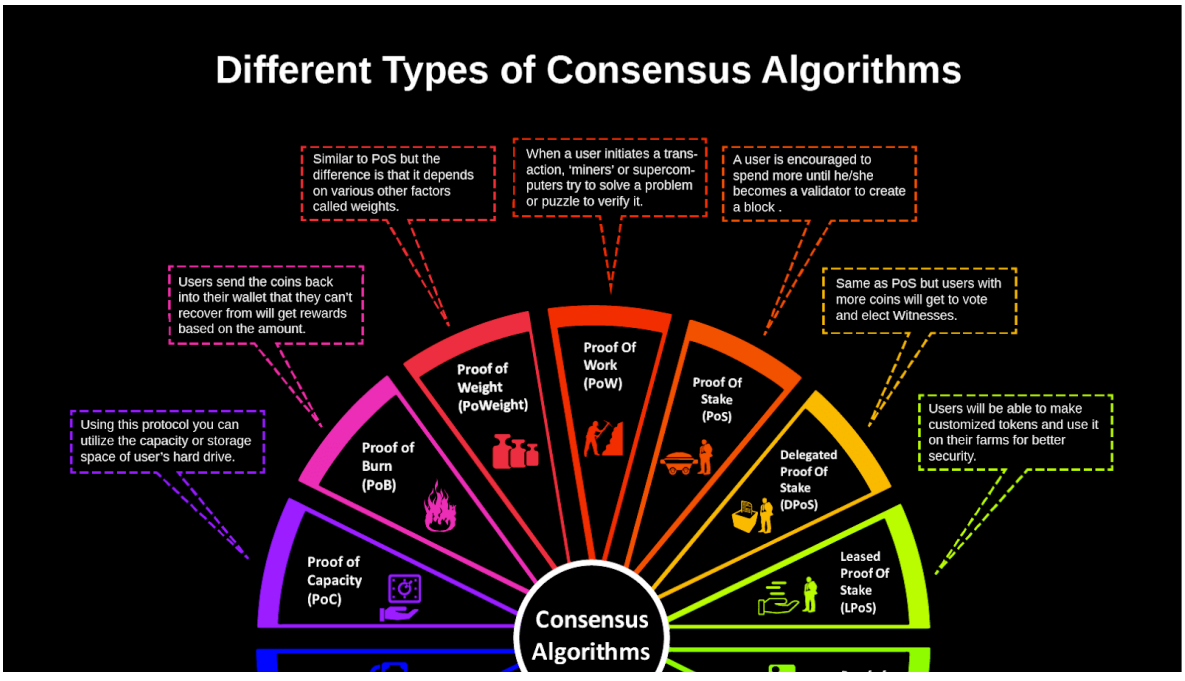
- Computing power consumption (electricity) and hardware cost (estimated $1 billion per day)

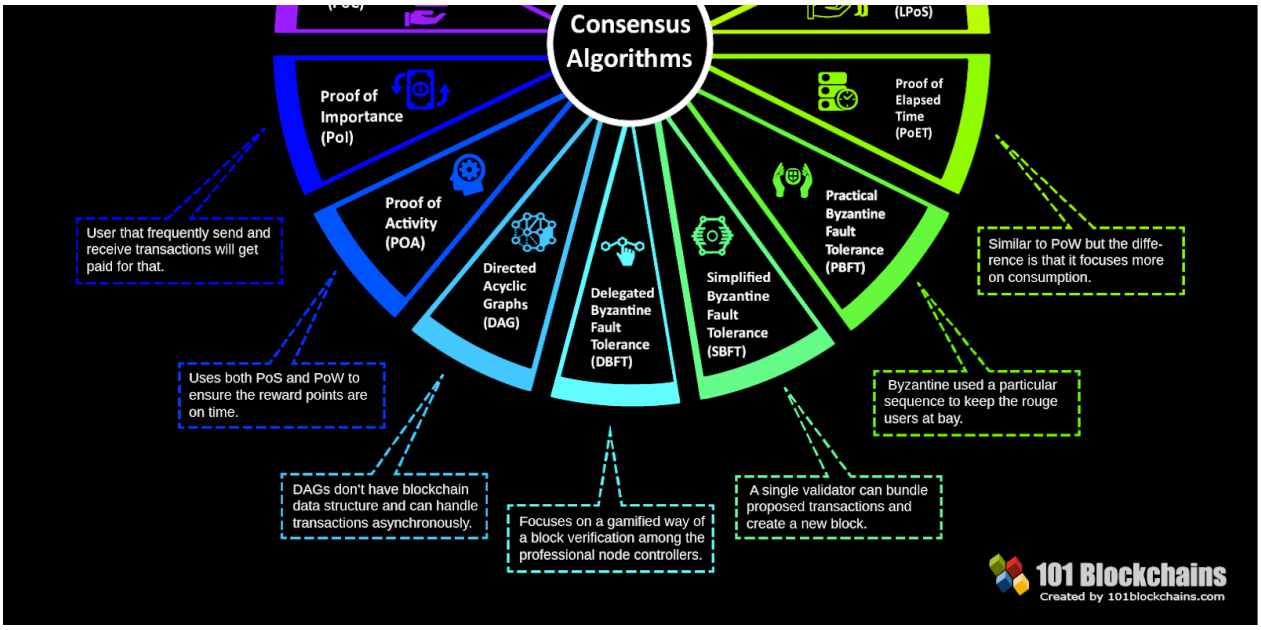


Major PoW limitations

- Limited number of transactions/sec

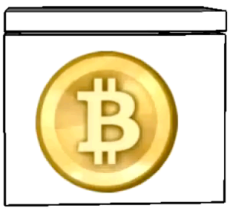






The Bitcoin DLT example

How does Bitcoin work?

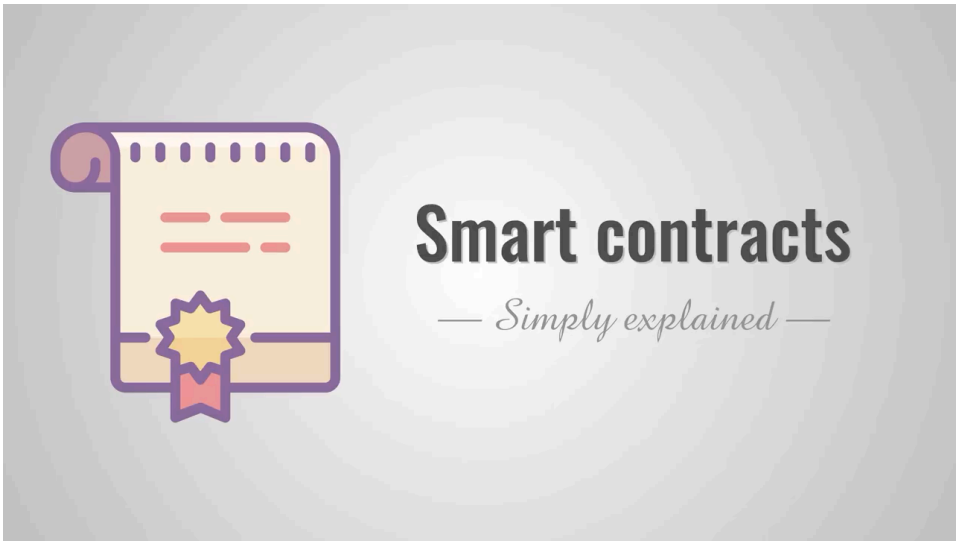


YouTube video by curiosinventor.com https://www.youtube.com/watch?v=Lx9zgZCMqXE

Smart contracts

- Beyond BitCoin: The Blockchain is useful to store more than financial transactions. *Ethereum* was specifically designed for smart contracts and more.
- Smart contract: A piece of software code defining a self-executing “contract”. While originally proposed as digital version of a legal contract it can be a general software program.
- It is usually stored on the Blockchain (becoming “immutable”).
- Each node can verify if the conditions of the contract are satisfied and perform the consequent actions (the output is “distributively validated”). In the end all nodes should agree on the resulting “state”.
- Application example : a crowdfunding platform without any central authority.

Smart contracts



YouTube video by SimplyExplained https://youtu.be/ZE2HxTmxfrI

Bitcoin and Ethereum are *permissionless*

- Decentralised DL that tracks all transactions
- No trusted third party
- Unconditioned access to the ledger
- Transactions validation and new “coins” generation by miners
- Pseudo-anonymity of participants
- Immutable transactions

Permissioned DLT

- Decentralised DL that tracks all transactions
- One or more trusted third parties
- Conditioned access to the ledger
- Transactions validation and new “coins” generation by miners
- Known identity of participants
- Immutable transactions

Hyperledger Fabric

- Hyperledger (2015). Consortium of industries to develop open-source blockchain technology for business, hosted by the Linux Foundation
- Fabric (2017) is one of the subprojects (original work by IBM)
  - permissioned DLT
  - modular architecture adapting to different requirements: private transactions, confidential contracts, different consensus protocols
  - distributed apps (contracts) in general-purpose programming languages
  - no dependency on a native cryptocurrency

Homework

- Look at the original Bitcoin paper by Satoshi Nakamoto (in course material)
- Read about DS and Blockchain
  - https://eng.paxos.com/why-arent-distributed-systems-engineers-working-on-blockchain-technology
- Learn more about Ethereum: read 2013 white paper by Vitalik Buterin (in course material)
- Read about the move of Ethereum to PoS https://www.technologyreview.com/2022/03/04/1046636/ethereum-blockchain-proof-of-stake/
- Watch a video about Hyperledger Fabric (https://youtu.be/k4KKrQOV6SE)