Intro to Blockchain

Marisa Paryasto
25 Nov 2019

What is Blockchain

This fancy term blockchain actually means a block of data that has been recorded over a certain amount of time and is grouped and cryptographically linked to a previous set of data forming a chain of events.

What Does Blockchain Do

In short, blockchain creates a true peer-to-peer secure transaction.

Blockchain has two main jobs:

1. **Securing** your data (trust)
2. **Recording** virtually everything of value (history)

Why Blockchain

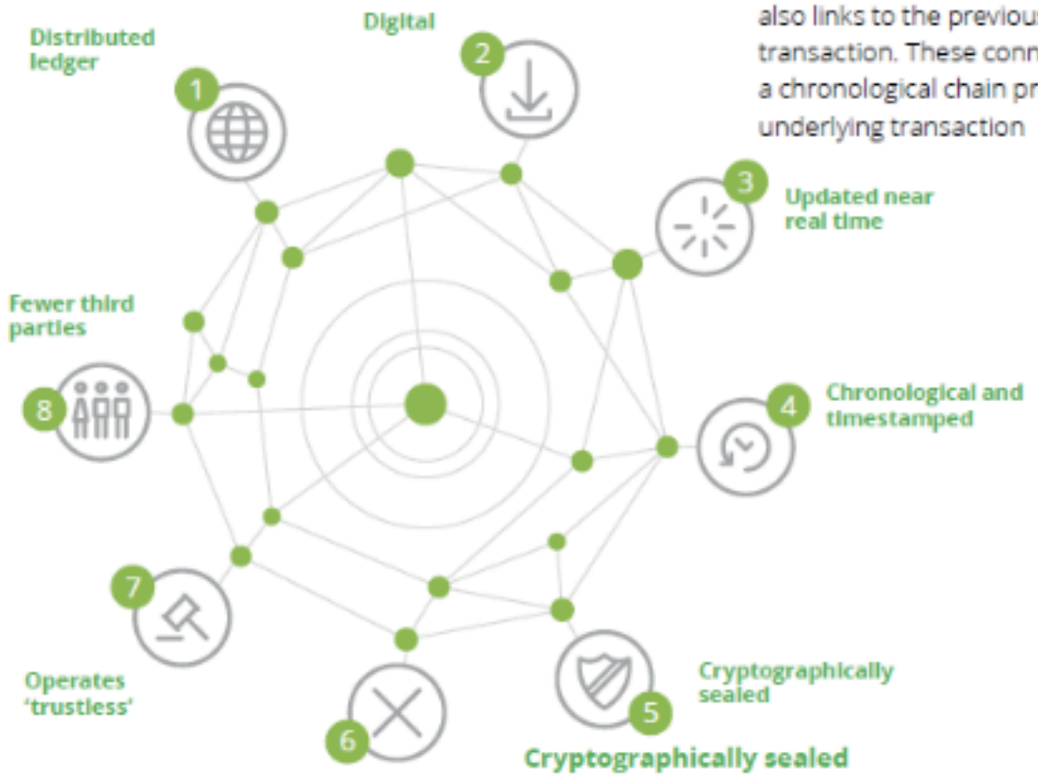
1. **Trust** — Blockchain helps in creating applications that are decentralized and collectively owned by multiple people. No body within this group has the power to change or delete previous transactions. Even if someone tries to do so, it will not be accepted by other stakeholders.
2. **Autonomy** — There is no single owner for Blockchain based applications. No one controls the blockchain, but everyone participates into its activities. This helps in creating solutions that cannot be manipulated or induce corruption.
3. **Integrity** — The state and transactions are secured cryptographically and cannot be modified easily.
4. **Intermediaries** — Blockchain based application can help remove the intermediaries from existing processes. Generally, there is a central body like Vehicle registration, licence issuing etc who acts as registrar for registering vehicles as well as issuing driver licences. Without Blockchain based systems, there is no central body and if a licence is issues or vehicle is registration after Blockchain mining process, that will remain a fact for epoch time-period without the need of any central authority vouching for it.

KEY CHARACTERISTICS OF THE BLOCKCHAIN

Digital
All the information on Blockchain is digitized, eliminating the need for manual documentation

Chronological and time-stamped
Blockchain, as the name suggests is a chain of blocks – each being a repository that stores information pertaining to a transaction and also links to the previous block in the same transaction. These connected blocks form a chronological chain providing a trail of the underlying transaction

Distributed ledger
Indistinguishable copies of all information are shared on the Blockchain. Participants independently validate information without a centralized authority. Even if one node fails, the remaining nodes continue to operate, ensuring no disruption



Consensus-based
A transaction on Blockchain can be executed only if all the parties on the network unanimously approve it. However, consensus based rules can be altered to suit various circumstances

Cryptographically sealed
Blocks created are cryptographically sealed in the chain. This means that it become impossible to delete, edit or copy already created blocks and put it on network, thereby creating true digital assets and ensuring a high level of robustness and trust. Furthermore, the decentralized storage in a Blockchain is known to be very failure-resistant. Even in the event of the failure of a large number of network participants, the Blockchain remains available, eliminating the single point of failure. Data stored in a Blockchain is immutable.

Explore more about this at : www.deloitte.com/convergence

101 Blockchains | KEY FEATURES OF BLOCKCHAIN TECHNOLOGY

01 CANNOT BE CORRUPTED

Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

02 DECENTRALIZED TECHNOLOGY

The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Instead, a group of nodes maintain the network making it decentralized.

03 ENHANCED SECURITY

As it eliminates the need for central authority, no one can just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.

04 DISTRIBUTED LEDGERS

The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.

05 CONSENSUS

Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

06 FASTER SETTLEMENT

Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

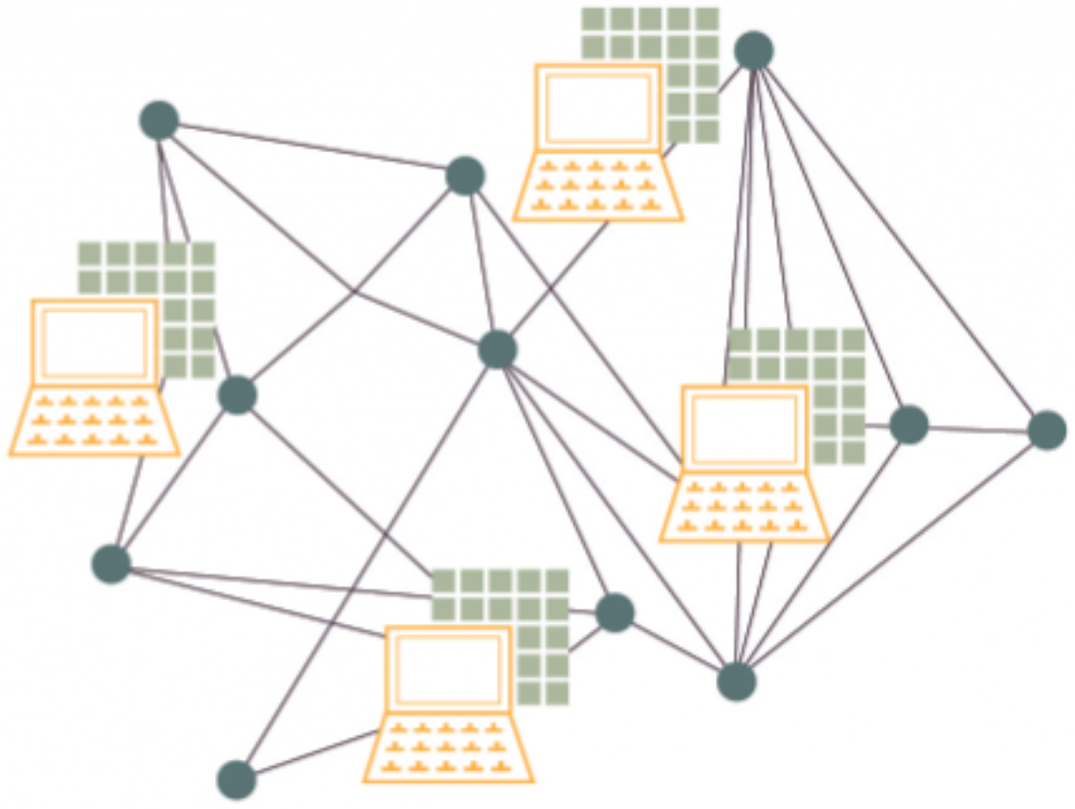
BLOCKCHAIN FEATURES

Created by 101blockchains.com

*https://101blockchains.com/introduction-to-blockchain-features/

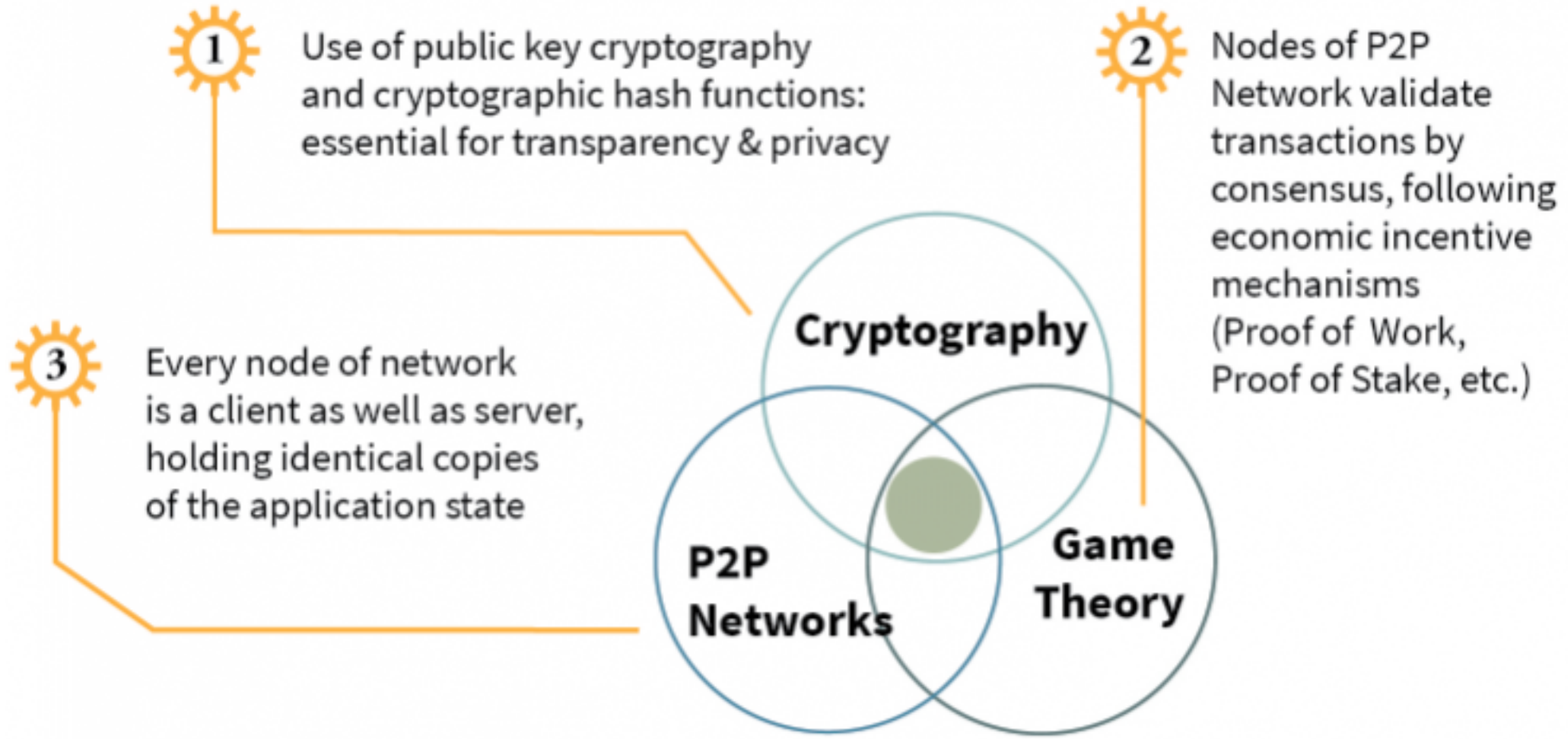
Like a spreadsheet in the sky

- Shared
- Public
- Ledger of transactions
- Anyone can inspect the transactions
- No single entity controls



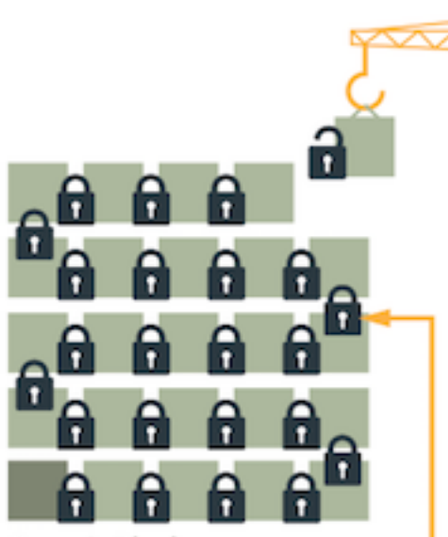
From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**

Behind the Blockchain Protocol



From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**

Why is it called Blockchain?



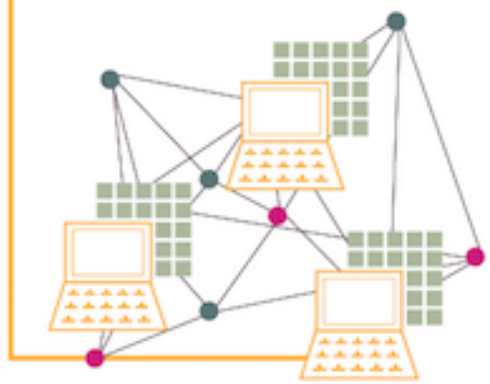
Genesis Block

The network stores all the information in cryptographically secured data pieces called blocks. The first block in a blockchain is called the Genesis Block. Each block has limited storage size. Blocks store a fingerprint (the hash) of the previous block, thus they are 'chained' together with cryptography.

3 Cryptography

2 Game Theory

Each new block of transaction get added to the blockchain by consensus of network validators at even time intervals. Validators are rewarded with a native token for validating transactions according to the rules through fault tolerant and attack resistant economic incentivisation mechanism.



1 P2P Network

Each full node on the network stores a copy of the entire blockchain (transaction history).

From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**

Why is a Blockchain tamper resistant?

Each network participant keeps a copy of the entire blockchain - the file where all past transactions are recorded. Consensus of network validators verifies new transactions. In the Bitcoin network transactions are validated by network miners who are ircentivised to verify transactions through PoW (Proof of Work).

If a malicious party makes unauthorized changes to his copy of the blockchain on one computer, other members of the network will refuse the transaction since that malicious version of the blockchain data will differ from the rest of network.

From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**

Blockchain Technology Stack

Ethereum and similar Blockchain

Smart Contracts

Relationship

Define behavioural rulesets for all participants of the smart contracts

Application

Record of Transaction (Ledger)

Assets

File (ledger) containing all information, tracking all assets since genesis block, which is stored on every (full) node of the network.

Consensus Rules

Governance

Encoded rulesets of all rights and obligations of all actors in the network: conditions under which transactions are created, sent and verified by the network, including economic incentive (token) & the creation/referencing of identities & addresses.

Nodes in the Network

Network

A network of all devices running the blockchain protocol and keeping records of transactions (ledger).

Blockchain

From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**