openHPI Course: Blockchain – Revealing the Myth

Blockchain Alternatives

Prof. Dr. Christoph Meinel
Tatiana Gayvoronskaya
Hasso Plattner Institute
University of Potsdam, Germany

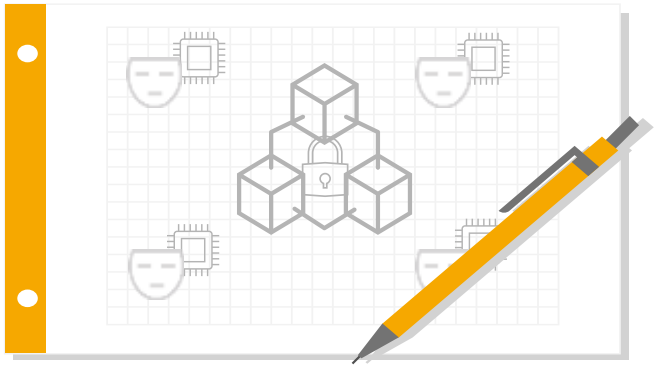
First Generation Blockchain Definition

You probably remember our blockchain definition. Let's take it up and see if it still works in the context of Blockchain 2.0

Blockchain technology provides a

- *permissionless peer-to-peer network*
- *using proof-of-work to record a public history of contents*
- *that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.*
- *This is done without any trusted third party and does not require trust between peers*

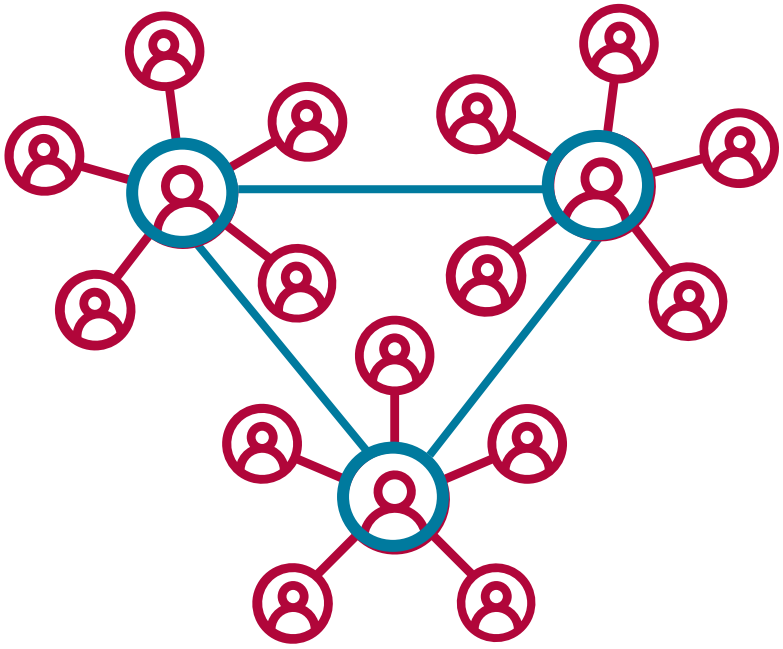
See also Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008



From Public Blockchains to More "Efficient" Systems

First generation blockchains such as Bitcoin were always **permissionless public blockchain**

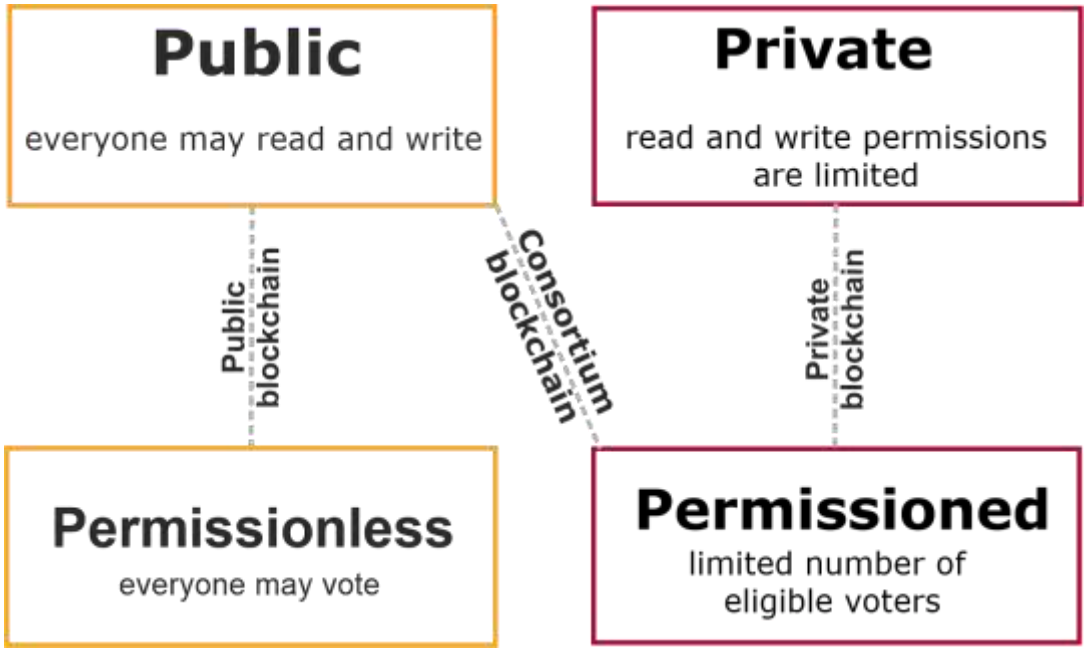
- Intention of restricting the terms of use is a way to make the system more efficient
- Decentralization of the system is in this way secondary



Private and Public Blockchains

It is about a combination of the **following restrictions**:

- **Read permission** – who can see the blockchain contents
- **Write permission** – who can create transactions
- **Consensus permission** – who can vote for the longest chain (attach blocks to the chain)



Private Blockchains

These restrictions mean that **users have to authenticate and authorize themselves** to use the system

- There is **no need in transparency** of content for all, e.g. transactions
- Voting on the next block can be done with **more efficient strategies than Proof-of-Work**
- This is because **miners or validators are known and limited**
- Risk: These preselected miners and validators can be **more easily manipulated by attackers**

Efficiency of Proof-of-Work

Why would we even consider to replace Proof-of-Work?

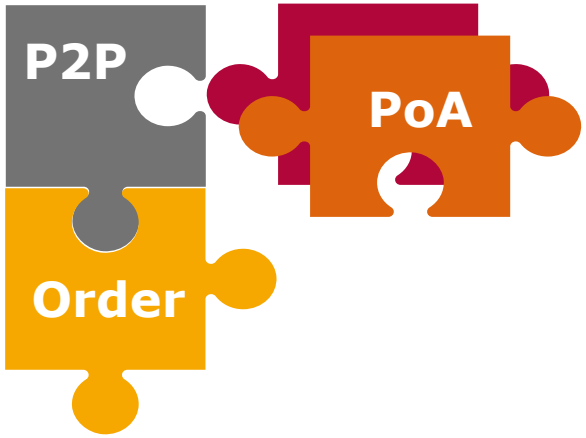
- Among the most widespread headlines is the energy consumption of the Bitcoin System
- **Annualized energy** consumption equivalent to **Chile**
- Carbon footprint of a **single transaction** equivalent to **725,148 VISA transactions**
- Price of Bitcoin influences energy spent on mining

https://digiconomist.net/bitcoin-energy-consumption/

Proof-of-Authority

An alternative to PoW for permissioned blockchains is called **Proof-of-Authority** (**PoA**) and is no longer based on the effort expended in solving a computational (electricity intensive) task

- A **limited group** of users can participate in the **consensus algorithm** for the creation of the next block
- Relies on the **trust in that group of nodes**
- Also called "**consortium blockchain**"
- The smaller group can simply do a **majority vote** as they are authenticated and authorized

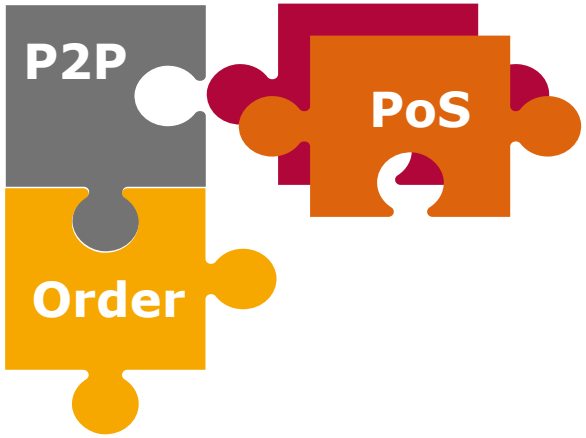


Risk Manipulation by the selected nodes

Proof-of-Stake

An alternative to PoW for public/unpermissioned blockchains is called **Proof-of-Stake** (**PoS**) relies on the "staking" of a **proportion of digital coins in a cryptocurrency**

- Users use their stakes to vote – who have the **n percent** of the digital coins, may create **n percent** of the blocks
- Miners are replaced by **validators**, which use the PoS algorithm and have the possibility to create a block



Is it Still Blockchain-based?

Many new **independent** blockchain networks with **adapted parameters** or **new functionalities** are created using Bitcoin or Ethereum source code

- Numerous technical concepts and projects, which **already existed before blockchain technology**, using the hype surrounding blockchain experience higher sales when **marketed under the blockchain** name
- The question arises as to which changes and adaptations would we say that **it is no longer blockchain-based**