BLOCKCHAIN

Şükrü ÇAKMAK
sukru@sukru.org

Blockchain Basics

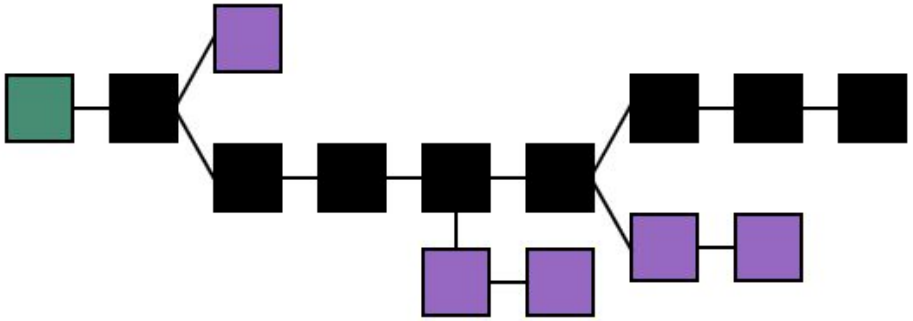
- Definition of Blockchain
- Centralized, Decentralized
- Distributed Ledger
- Cryptographic Hash
- History
- Blockchain Types
- Public vs Private

Definition of Blockchain

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).

Digitally protected, decentralized, distributed ledger.



Definition of Blockchain

Basic Terms

- ***Immutable***
- ***Append-Only***
- ***Ledger***
- ***Consensus***

Definition of Blockchain

Basic Terms

- ***Immutable***

  Cannot be changed, edited, or deleted. Permanent record.
- ***Append-Only***

  A system in which data can only be read or added. No deletes or edits are possible.
- ***Ledger***

  A log or historical record of events for a particular item.
- ***Consensus***

  The truth is assumed to be whatever the majority of participants believe it to be.

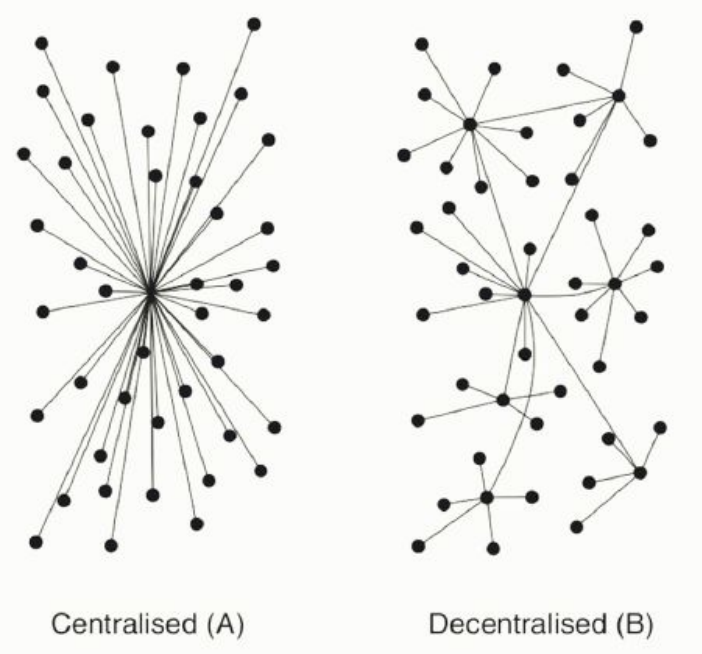
Definition of Blockchain

So, what is blockchain?

- An immutable, append-only ledger
- Multiple copies of this ledger are stored on nodes (computers, servers) across a network
- Nodes attempt to reach consensus on the contents of the ledger

Centralized vs Decentralized

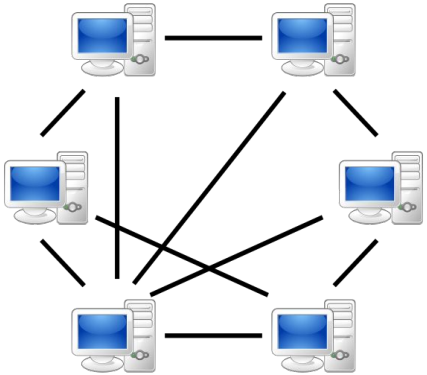
Centralized	Decentralized
Slow	Fast
Single Point of Failure	No Single Point of Failure
High Bandwidth Usage for Server	All Downloader and Uploaders



Distributed Ledger

A blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks.

Peer-to-peer (P2P) networking is distributed application architecture that partitions tasks between peers.



Cryptographic Hash

It is a mathematical ***algorithm*** that maps data of arbitrary size (often called the "message") to a bit string of a fixed size (the "hash value", "hash", or "message digest") and is a ***one-way function.***

The ***SHA-256 algorithm*** generates an almost-unique, fixed-size 256-bit (32-byte) hash. This is a one-way function, so the result cannot be decrypted back to the original value.

MD5? SHA-1? Bcrypt?

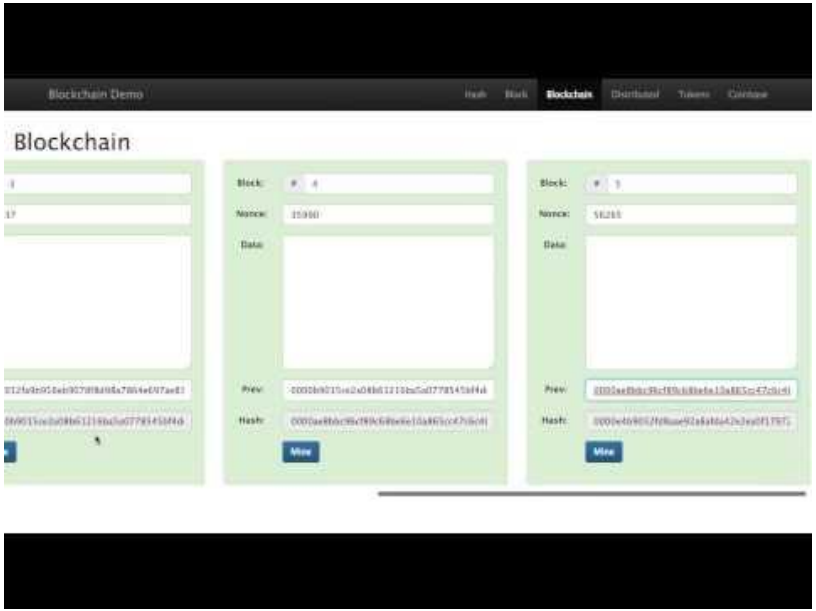
Cryptographic Hash

	Input				Output
One-way	Lorem		crypto-hash-func		1b7f8466f087c27f24e1c90017b829cd8208969018a0bbe7d9c452fa224bc6cc
Deterministic	Lorem		crypto-hash-func		1b7f8466f087c27f24e1c90017b829cd8208969018a0bbe7d9c452fa224bc6cc
Fixed size	Lorem ipsum dolor sit amet		crypto-hash-func		16aba5393ad72c0041f5600ad3c2c52ec437a2f0c7fc08fadfc3c0fe9641d7a3
Psuedo Random	Lorem ipsum dolor sit amer		crypto-hash-func		bf36444fc3fb5a04a578cb69b98b343c0384c505e2b956ddb54af3f83ec92f1c

Cryptographic Hash

```
public class SecureHashAlgorithm {

    public static void main(String[] args) throws Exception {
        String message = "Hello from Sukru";

        MessageDigest digest = MessageDigest.getInstance("SHA-256");
        byte[] encodedHash = digest.digest(message.getBytes());

        System.out.println("Encoded: "+ bytesToHex(encodedHash));
    }

    private static String bytesToHex(byte[] hash) {
        StringBuffer hexString = new StringBuffer();

        for (int i = 0; i < hash.length; i++) {
            String hex = Integer.toHexString(0xff & hash[i]);
            if(hex.length()==1) hexString.append('0');
            hexString.append(hex);
        }
        return hexString.toString();
    }
}
```

Visualisation



https://www.youtube.com/watch?v=_160oMzblY8

Who invented?

Blockchain was invented by a person (or group of people) using the name ***Satoshi Nakamoto*** in 2008 to serve as the public transaction ledger of the ***cryptocurrency bitcoin***.
https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. 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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin Block Mining

transaction:{from: sukru, to: ege, amount:100}
transaction:{from: ege, to: sukru, amount:58}
transaction:{from: sukru, to: yasar, amount:34}

choose a random nonce: *2083236893*

calculate the hash, starting with zero: *0000 0000 00*

https://www.blockchain.com/btc/block/00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Homework

Write your own mining demo!

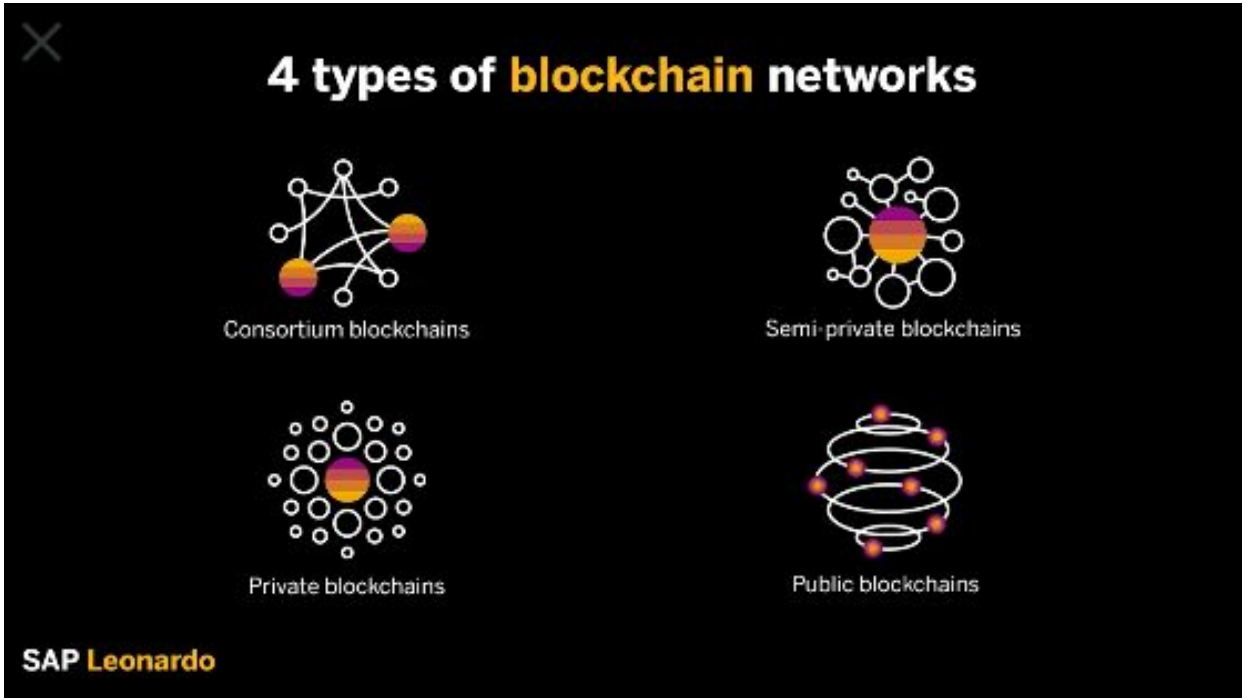
Blockchain Types

1. Public
2. Private
3. Consortium
4. Hybrid

Blockchain Types

1. Public **(Bitcoin, Ethereum, Litecoin etc.)**
2. Private **(Enterprise blockchains like Hyperledger)**
3. Consortium **(R3 Corda)**
4. Hybrid **(Dragonchain)**

Blockchain Types



1. Public

Advantages
Trustable
Secure
Open and Transparent

Disadvantages
Lower TPS
Scalability
High Energy Consumption

Bitcoin can process 7 transactions per second (TPS)
Ethereum 15 TPS

Visa 24.000 TPS

2. Private

Advantages
Speed
Scalability

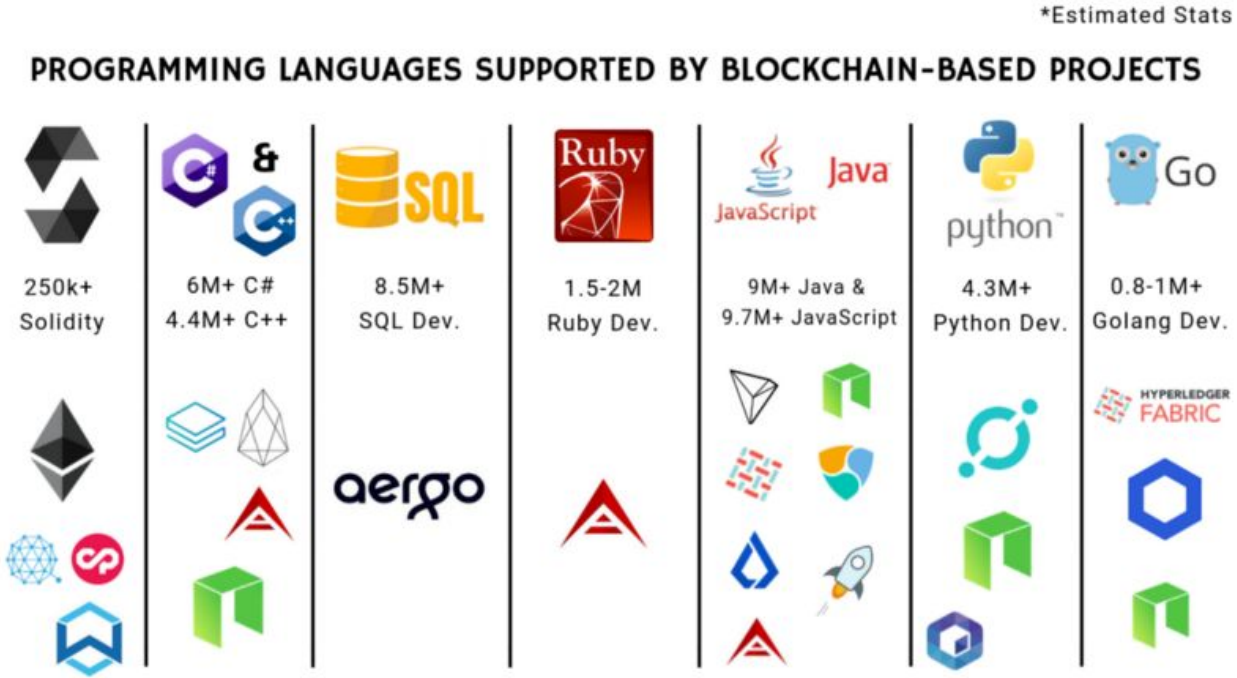
Disadvantages
Never Trust Building
Lower Security
Centralization

Identity and Access Management (IAM)

Public vs Private

	Public Blockchains	Private Blockchains
Access level	○ Anyone	○ Single organization
Participation	○ Permissionless ○ Anonymous	○ Permissioned ○ Identities are known
Security	○ Consensus mechanism ○ Proof of Work / Proof of Stake	○ Pre-approved participants ○ Voting / multi-party consensus
Performance	○ Slow transaction speed	○ Lighter blockchain ○ Fast transaction speed

Smart Contracts



https://www.freecodecamp.org/news/the-most-popular-programming-languages-used-in-blockchain-development-5133a0a207dc/

Key Concepts

Cryptographic Hash
Merkle Tree
Peer-to-peer
SHA-256
Block
Nonce
TPS
Mining
Public vs Private Blockchains

Please feel free to contact me if you need any further information

sukru@sukru.org