



Department of Software Engineering and Management Information Technology
Faculty of Computer Science and Software Engineering

Foundations of Blockchain Technology and its Applications



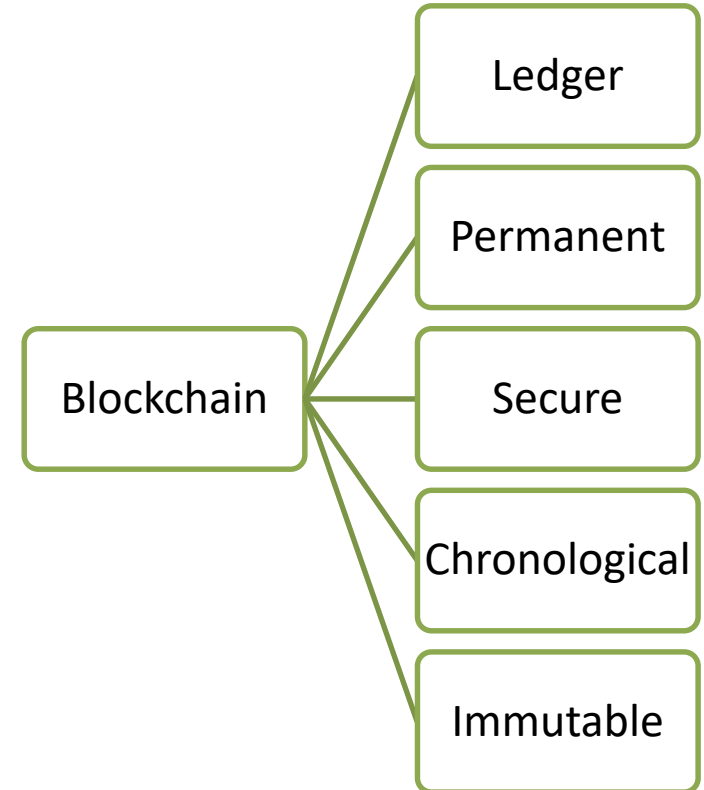
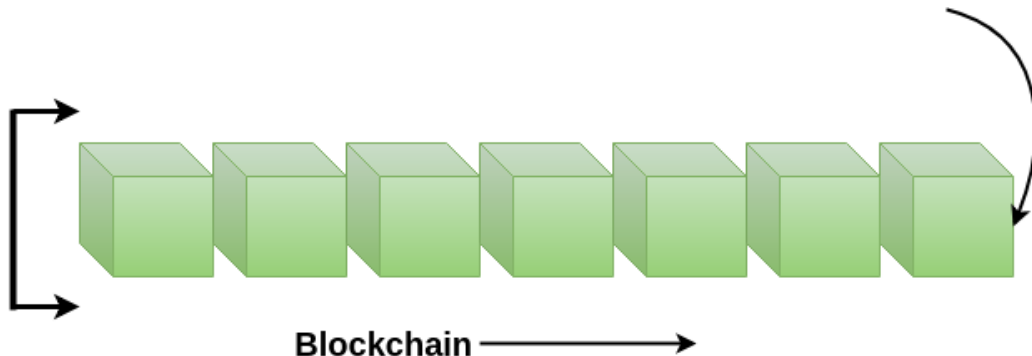
Andrii Kopp, Ph.D.



Dmytro Orlovskyi, Ph.D.

What is a Blockchain?

- “A blockchain is a constantly growing ledger which keeps a permanent record of all the transactions that have taken place in a secure, chronological, and immutable way.”





Blockchain Pillars

Ledger

- A file that is constantly growing

Permanent

- Once the data goes inside a blockchain, it is stored permanently in the ledger

Secure

- An advanced cryptography is used to lock the information inside the blockchain

Chronological

- Every information unit can be added only after the previous one

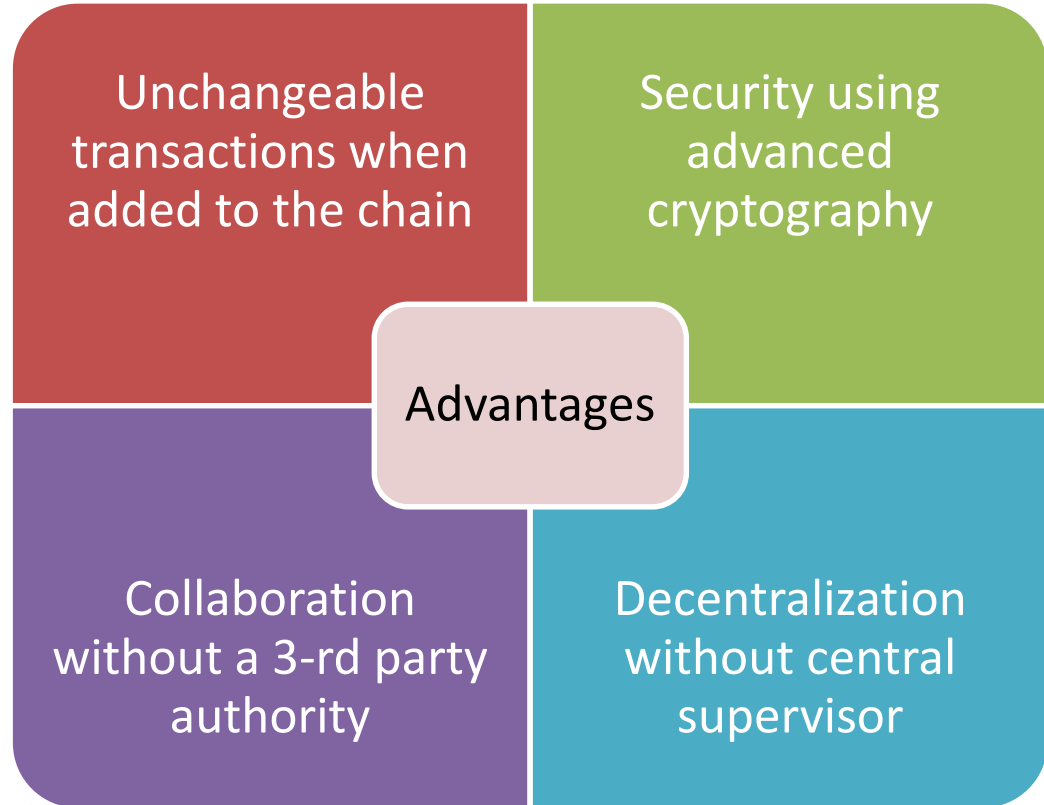
Immutable

- As the data is added to the blockchain, it can never be changed









When use the Blockchain?

- The primary use of the Blockchain is as a distributed ledger for transactions of cryptocurrencies (e.g. Bitcoin, Ethereum, Dogecoin, Litecoin, Tether etc.)
- Shows promising results if used in Banking, Manufacturing, Healthcare, Energy, Automotive, Government, Education, Retail, Insurance, Transportation etc.



When use the Blockchain?

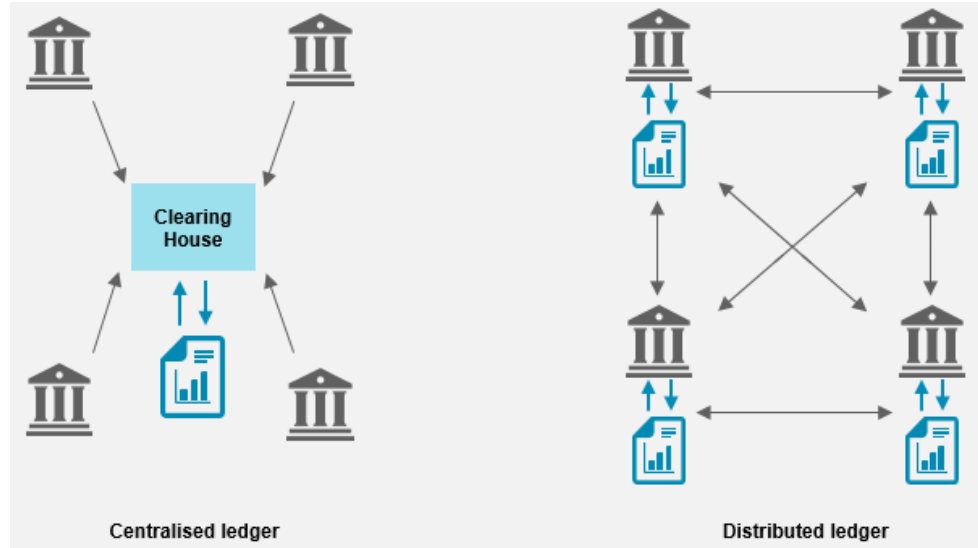
 <p>Supply Chain and Logistics</p> <p>End-to-end monitoring of supply chain processes</p>	 <p>Real Estate</p> <p>Secure and faster real estate transactions</p>	 <p>Healthcare</p> <p>National adoption of health information exchange systems</p>
 <p>Energy</p> <p>Distributed energy network transactions</p>	 <p>Insurance</p> <p>Enhanced underwriting and claims processes</p>	 <p>Retail</p> <p>Efficient validation of authenticity and purchase process</p>





Distributed Ledger

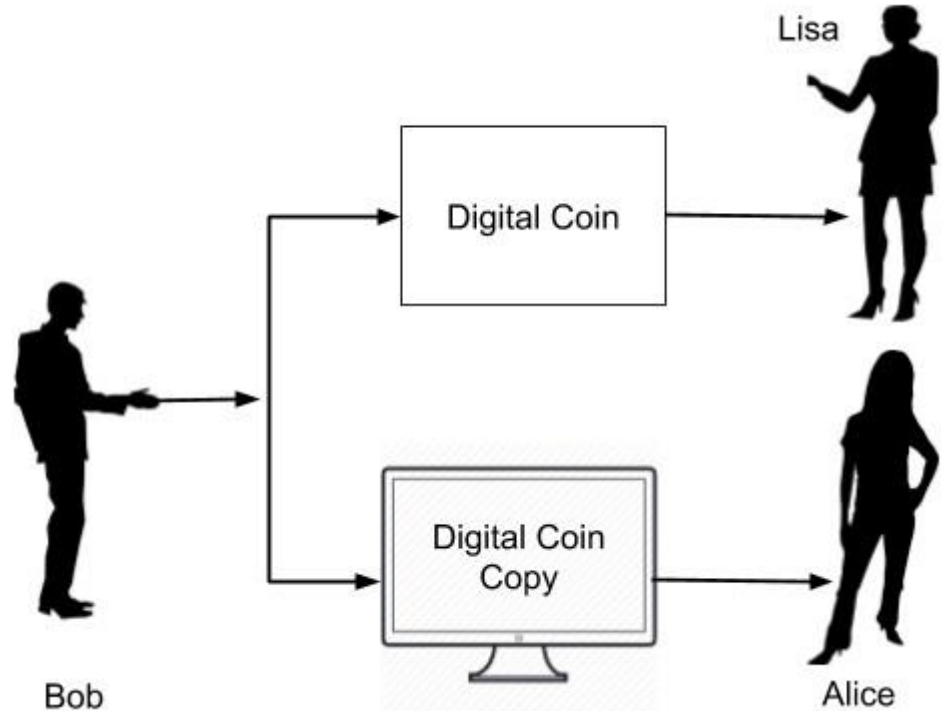
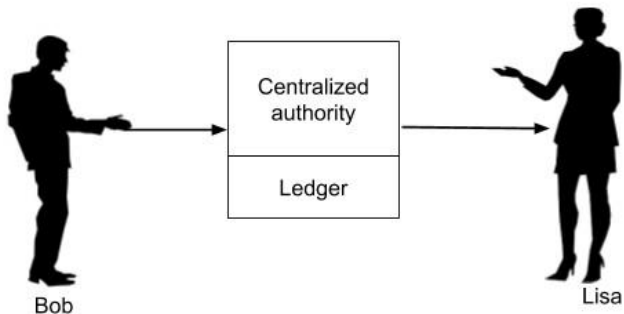
- “Ledger is a book in which items are regularly recorded, esp. business activities and money received or paid” (Cambridge dictionary)
- Blockchain is a Distributed Ledger, since it is shared, replicated, and synchronized among the members of a peer-to-peer (P2P) network
- It records the transactions such as the exchange of assets or data, among the participants in the network



- Data copied to all participants in seconds
- Each participant constructs the new transaction, and then participants vote by consensus algorithm on which copy is correct

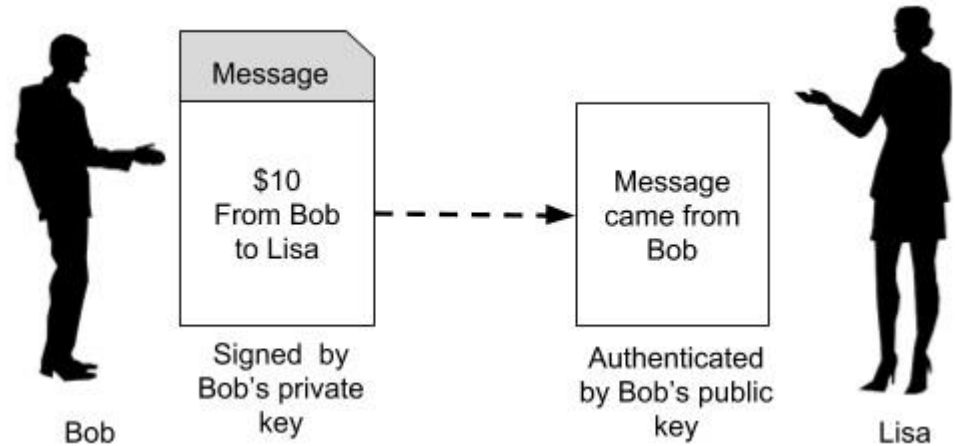
Double-Spending Problem

- As the format for money exchange is in the digital format, it is essentially a binary physical file stored somewhere on Bob's device. After Bob gives this file (digital money) to Lisa, he can also give a copy of the file to Alice.



Public Key Cryptography

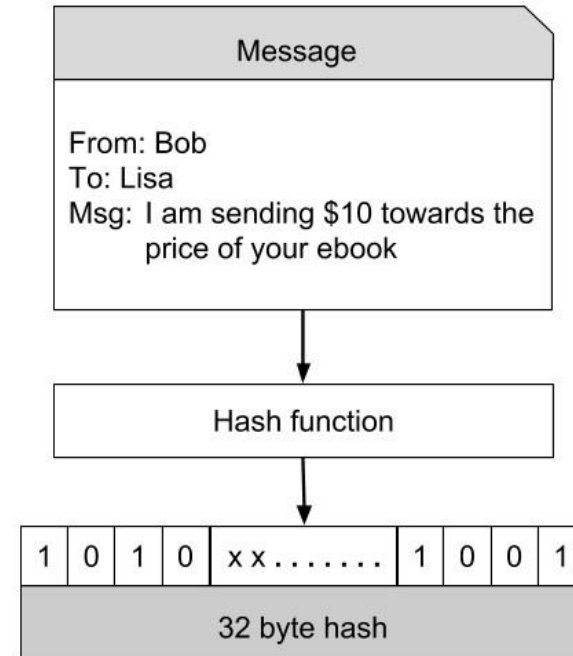
- When Bob wants to send some money to Lisa, he has to create a private/public key of its own (asymmetric cryptography)
- When Bob sending \$10 to Lisa he creates a message containing his public key, Lisa's public key, and the amount
- Authenticity (that Bob indeed sent his money) is achieved when Bob signed the message with his private key
- Identity could be checked by using sender's public key and a signature verification algorithm





Hashing

- Hashing and hashing functions are the underlying technology of Public Key Cryptography
- Hashing function maps the data of any arbitrary size to data of fixed size (e.g. Bitcoin and other cryptocurrencies use SHA-256 to produce 256-bit/32-byte "footprints" of any data put under hashing)
- Obtained hash value remains unique for the given message, so when the message is changed, the hash changes as well



- Hash functions are one-way, this means you can not reverse the hash to original message



Department of Software Engineering and Management Information Technology

Faculty of Computer Science and Software Engineering



12345678



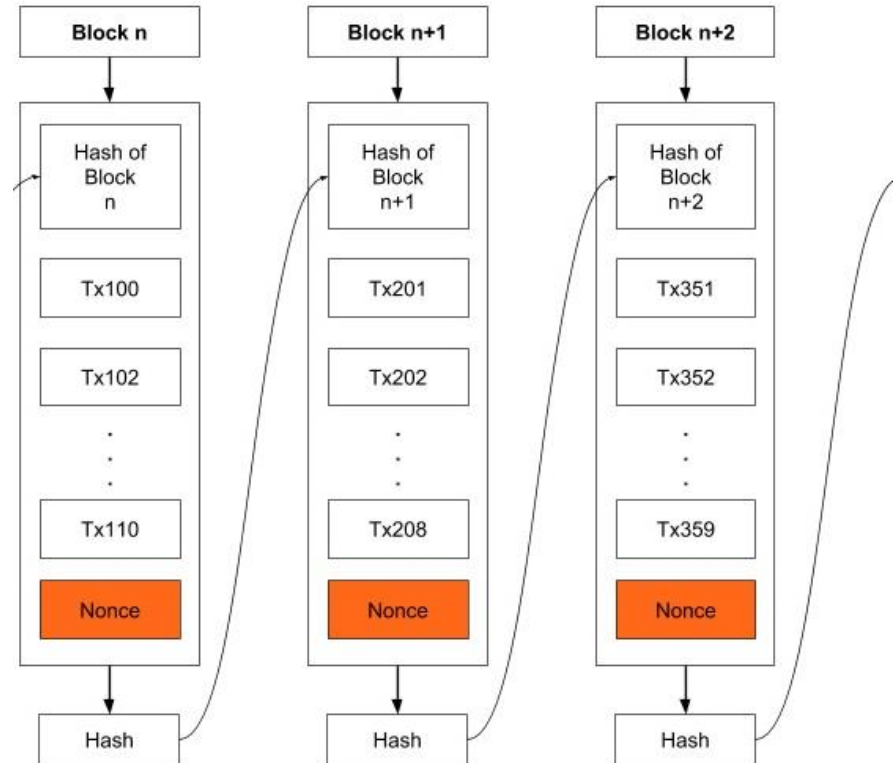
SHA-256(12345678)

ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f



Chain of Blocks

- Blocks are chained together to form what is known as a Distributed Ledger
- Each block in the chain contains necessary data (e.g. transactions in cryptocurrency blockchains)
- When creating the block, a miner or voter picks up the hash of the last block in the chain, combines it with its own block data and creates a hash for the newly created block
- Thus, the blockchain keeps on growing as more and more blocks are added





Block 0

Timestamp: Thu Jun 24 2021 15:51:12

Data: Genesis block.

Parent hash: 0

Hash: bf7ab8d60922475157b48de9893a3c554838ec0d9eb3bc99311ef4c88ae3b230

Nonce: 0

Mined by: 0



Block 1

Timestamp: Thu Jun 24 2021 15:54:32

Data: Some block data.

Parent hash: bf7ab8d60922475157b48de9893a3c554838ec0d9eb3bc99311ef4c88ae3b230

Hash: 000e8dbf1388267e9a0f44f1078a1e7d0de7e8fe120d953cdc1ec8206baad10c

Nonce: 1763

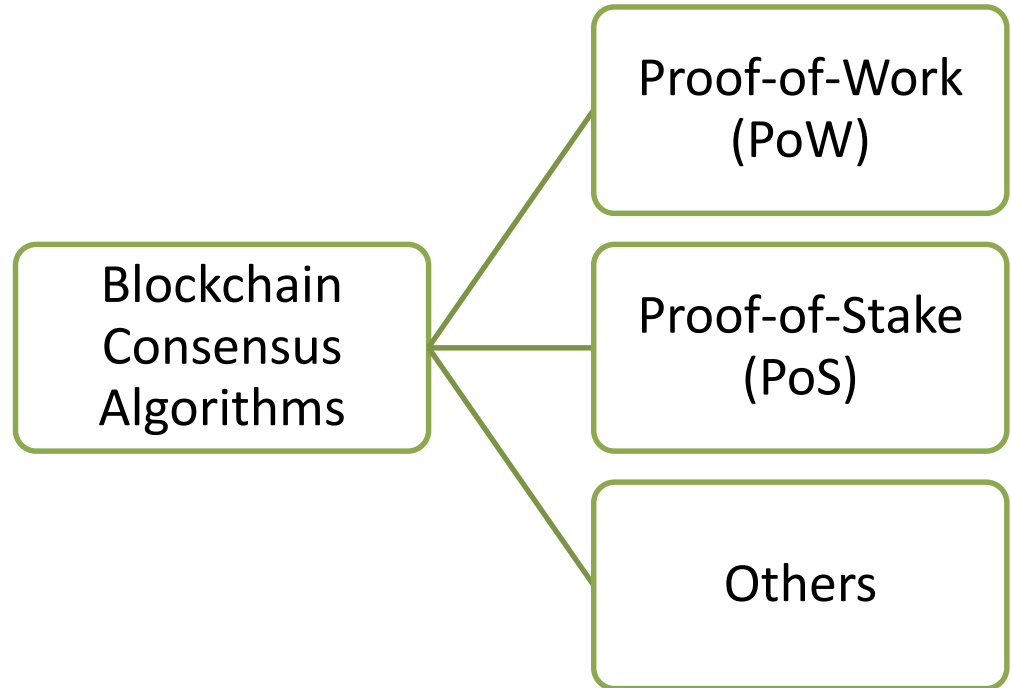
Mined by: ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f





Consensus Algorithms

- Consensus algorithms are used to reach consensus between the nodes (i.e. participants of the blockchain network) on how new blocks are created and added to the blockchain
- Two most popular consensus algorithms are Proof-of-Work (also known as Nakamoto consensus originally used in Bitcoin network) and Proof-of-Stake (energy efficient replace of the Proof-of-Work by voting instead of mining)



Proof-of-Work Consensus

- It is the original consensus algorithm proposed for the blockchain
- All network participants need to agree on the probability of some value (called "nonce") to be correct
- Participants are called "miners" who compete against each other to generate the new block and get rewarded with a certain amount of cryptocurrency

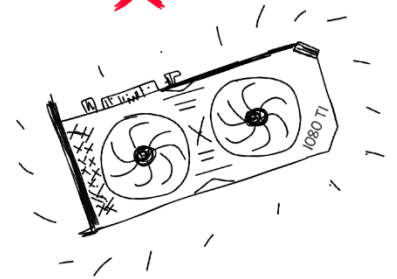
NONCE = 22811 -> HASH: AF59CCAIA3EF5DC66B08... ❌

NONCE = 15887893 -> HASH: E62B2C97D079BE77... ❌

◦ ◦ ◦ ENDLESS TIME LATER ◦ ◦ ◦

NONCE = 5423534123612344563... ->
HASH: 000000000010139AD76... ✓

STARTING WITH TEN ZEROS!





Block 0

Timestamp: Thu Jun 24 2021 15:51:12

Data: Genesis block.

Parent hash: 0

Hash: bf7ab8d60922475157b48de9893a3c554838ec0d9eb3bc99311ef4c88ae3b230

Nonce: 0

Mined by: 0



Block 1

Timestamp: Thu Jun 24 2021 15:54:32

Data: Some block data.

Parent hash: bf7ab8d60922475157b48de9893a3c554838ec0d9eb3bc99311ef4c88ae3b230

Hash: 000e8dbf1388267e9a0f44f1078a1e7d0de7e8fe120d953cdc1ec8206baad10c

Nonce: 1763

Mined by: ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f





Block 1

Timestamp: Thu Jun 24 2021 15:54:32

Data: Some block data.

Parent hash: bf7ab8d60922475157b48de9893a3c554838ec0d9eb3bc99311ef4c88ae3b230

Hash: 000e8dbf1388267e9a0f44f1078a1e7d0de7e8fe120d953cdc1ec8206baad10c

Nonce: 1763

Mined by: ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f



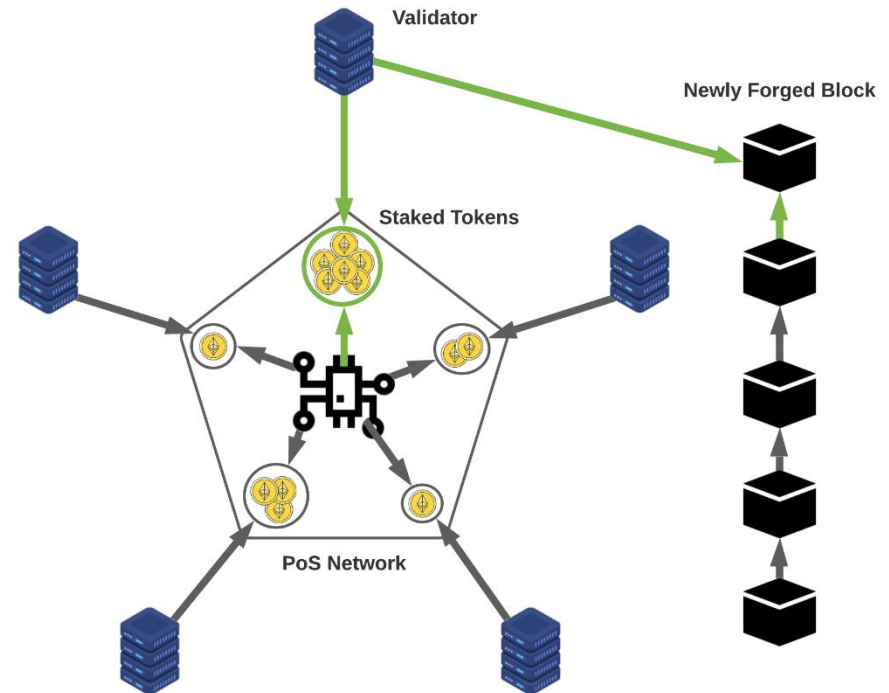
000e8dbf1388267e9a0f44f1078a1e7d0de7e8fe120d953cdc1ec8206baad10c

difficulty is set to secure the
blockchain
(currently difficulty = 3)

The thing is that only nonce = 1763 will give the
hash of this block (with all of its properties) that will
satisfy the difficulty of the blockchain

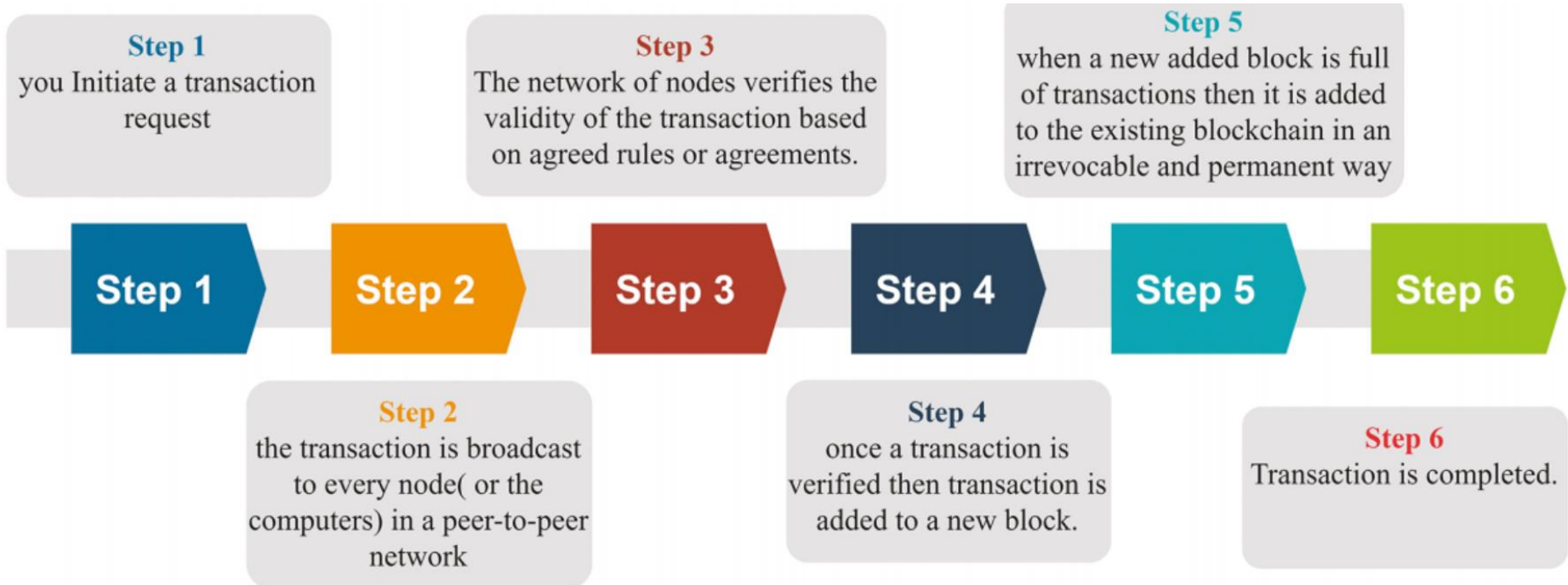
Proof-of-Stake Consensus

- In compare to PoW, this algorithm does not require waste of energy and computational power
- Participants are called "voters" or "validators" (not "miners"), since they deposit some amount of crypto-coins as the stake in the network
- The higher stake is, the higher is the probability of the participant to be selected to generate the new block and get rewarded similarly to PoW



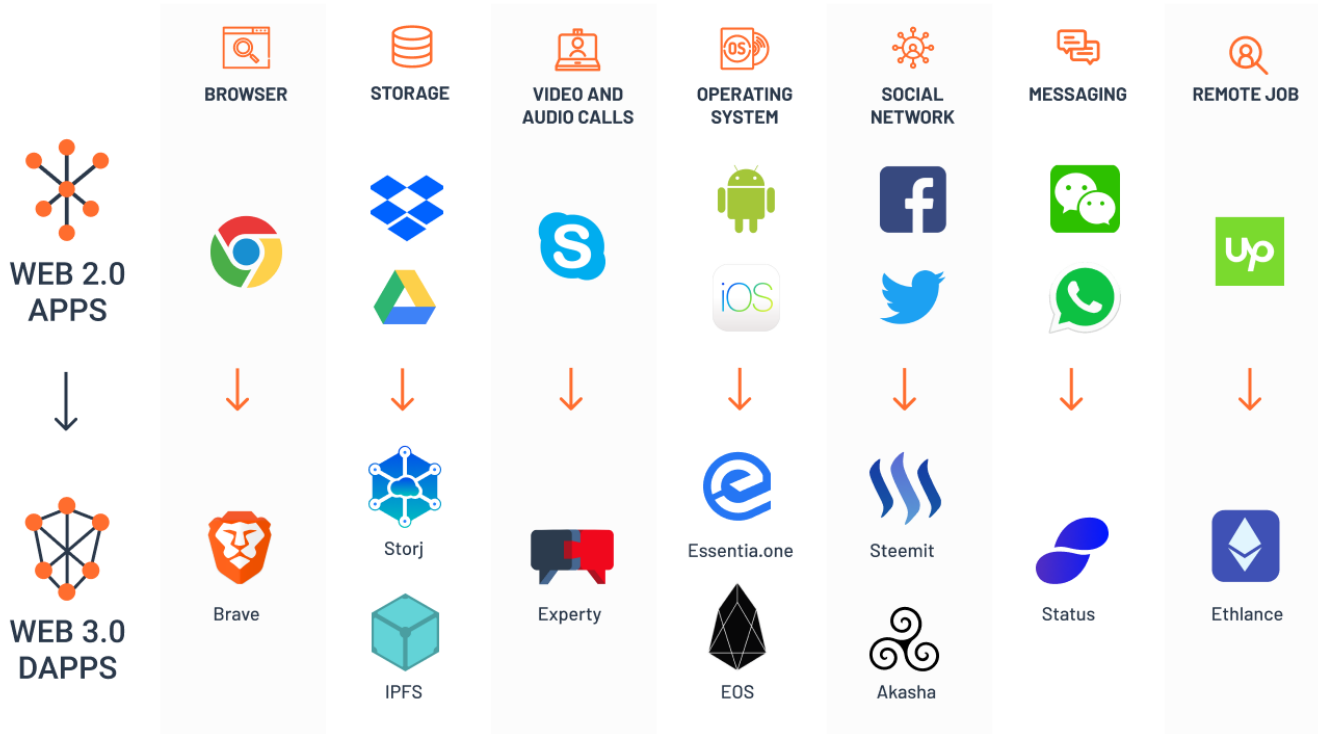


Working of Blockchain





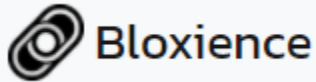
Decentralized Applications are the Future Internet





Dummy Blockchain for Education Purposes

- It is the education-oriented dummy JavaScript-based implementation of the Blockchain ledger with the PoW consensus, mining simulation, and validation
- It is named as “**Bloxience**” by combining two words “Blockchain” and “Science” to give the academic meaning to the application



It is now available for free online at this link:

<https://cloudfreebpmnquality.herokuapp.com/bloxience/>



Homepage

Bloxience Home

Bloxience — Dummy JavaScript Blockchain Sandbox for Education

Education-oriented dummy JavaScript-based implementation of the Blockchain ledger with the Proof-of-Work (PoW) consensus, mining simulation, and validation.

New block

Private key

Your private key to sign the message.

Block data

Any text data that you want to store on the blockchain.

[Mine block](#) [Validate blockchain](#)

Blockchain

```
Block: 0
Timestamp: Thu Jun 24 2021 16:10:05 GMT+0300 (Eastern European Summer Time)
Data: Genesis block.
Parent hash: 0
Hash: ac1b92c772a88247c4175c87d5967df56c5e74b1bfdbf81bb26a1ff69fa9d07e
Nonce: 0
Mined by: @
Alter block data
```

New block adding form

Blocks displayed



Mining new block

New block

Private key

.....

Your private key to sign the message.

Block data

New block data.

Any text data that you want to store on the blockchain.

Mine block

Validate blockchain

Enter the private key (i.e. your secret password)

Enter any text data you want to keep on the blockchain

Press the "Mine block button"



Altering block data

Blockchain

Block: 1
Timestamp: Thu Jun 24 2021 16:18:34 GMT+O300 (Eastern European Summer Time)
Data: **New block data.**
Parent hash: ac1b92c772a88247c4175c87d5967df56c5e74b1bfdbf81bb26a1ff69fa9d07e
Hash: 000cba6e57e4786ab6e5ab0856606481c96d1e159cfd99dd2503352984319871
Nonce: 234
Mined by: **ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f**
Alter block data

Block: 0
Timestamp: Thu Jun 24 2021 16:10:05 GMT+O300 (Eastern European Summer Time)
Data: **Genesis block.**
Parent hash: 0
Hash: ac1b92c772a88247c4175c87d5967df56c5e74b1bfdbf81bb26a1ff69fa9d07e
Nonce: 0
Mined by: **0**
Alter block data

Simulate the block altering attempt

Latest block is displayed at top



Blockchain validation

Blockchain

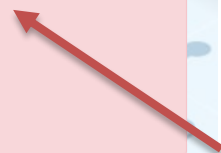
Block: 1
Timestamp: Thu Jun 24 2021 16:18:34 GMT+0300 (Eastern European Summer Time)
Data: **New block data. Altered at 1624540880973 ms.**
Parent hash: ac1b92c772a88247c4175c87d5967df56c5e74b1bfdbf81bb26a1ff69fa9d07e
Hash: 000cba6e57e4786ab6e5ab0856606481c96d1e159cfd99dd2503352984319871
Nonce: 234
Mined by: **ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f**

Alter block data

Block: 0
Timestamp: Thu Jun 24 2021 16:10:05 GMT+0300 (Eastern European Summer Time)
Data: **Genesis block.**
Parent hash: 0
Hash: ac1b92c772a88247c4175c87d5967df56c5e74b1bfdbf81bb26a1ff69fa9d07e
Nonce: 0
Mined by: **0**

Alter block data

Rejected blocks that were tampered are shown in red





Reach Us

Andrii Kopp

kopp93@gmail.com

Dmytro Orlovskiy

orlovskiy.dm@gmail.com

Website:

<https://freebpmnquality.github.io/>

Knowledge base (papers, slides, videos):

<https://freebpmnquality.github.io/kbase.html>

Twitter:

<https://twitter.com/freebpmnquality>, @freebpmnquality

Facebook:

<https://www.facebook.com/andriikopp/>



**Department of Software Engineering and Management Information Technology
Faculty of Computer Science and Software Engineering**

**THANK YOU FOR YOUR ATTENTION!
ANY QUESTIONS?**