

# Blockchain

## Transactions and Beyond

**M. Osmanovic**

Jönköping Uni.

March 7, 2024

GitHub: *mosmar99*

# Outline

- 1 Introduction
- 2 Functionality
  - How does the Blockchain work?
  - Block validation
- 3 PROs and CONs
  - The CONs of the Blockchain
  - The PROs of the Blockchain
- 4 The Future

# Introduction

- Blockchain =?= Bitcoin
- Satoshi Nakamoto: *"Bitcoin: A Peer-to-Peer Electronic Cash System"* (October 31, 2008)

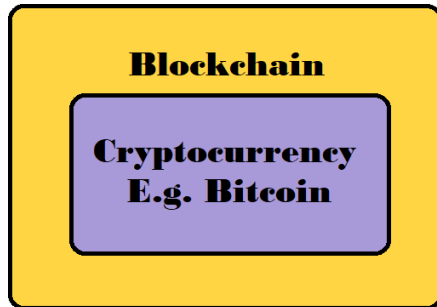


Figure 1: Source: M. Osmanovic



Figure 2: Source: Cointelegraph

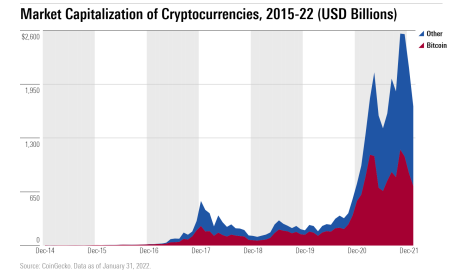


Figure 3: Source: Morningstar

*Question: Ledger..?*

What is a *ledger*?

# Cambridge Definition

Meaning of **ledger** in English



## ledger

**noun** [ C ]

UK /ˈledʒ.ə/ US /ˈledʒ.ə/

Add to word list

**a book in which things are regularly recorded, especially business activities and money received or paid**

Figure 4: Source: Cambridge Dictionary

# How does the Blockchain work?

## — The ledger details

- Blockchain vs. Cryptocurrencies (E.g: Bitcoin)
- Publicly Distributed Ledger: *chain of blocks*
- Hashing Algorithm used by Bitcoin: SHA256 - *novel hash functions computed with eight 32-bit and 64-bit words*

General Ledger				
Go Away Travel Services For Jan 1, 2022 - Dec 31, 2022				
Petty Cash (1000-1) Cash				
Transaction / Reference	Date / Note	Debit	Credit	
Payment 0000001	Jul 6, 2022 —	700.00		
Payment 0000002	Jul 6, 2022 —	500.00		
Net Movement		1,200.00 USD		

Figure 5: Source: FreshBooks

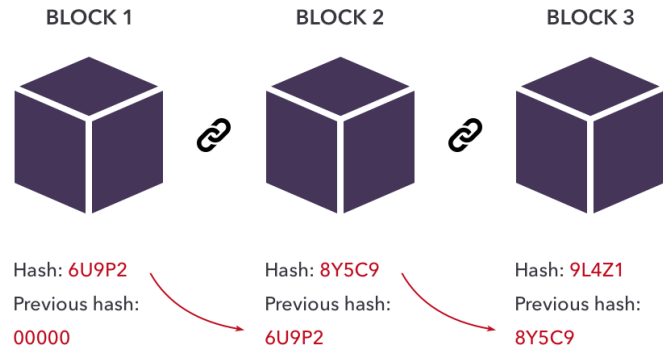


Figure 6: Source: Johnmiracle Ejikeme

# How does the Blockchain work?

— *Keys*

- **Every** user has a public **and** a private key.
- **Private Keys:** *An adress that everyone in the network knows of*  
(e-mail)
- **Public Keys:** *Unique Adress that only the user has knowledge of*  
(password)

# How does the Blockchain work?

— *Transaction: Phil and Jack*

- Send **data note** containing: *Sender* (Phil), *Receiver* (Jack), their *unique wallet addresses* and *amount* (say, 8 bitcoins)
- Data note is passed through a **hashing algorithm** and **digitally signed** using Phil's private key.
- **Signed data note is echoed to the world** using Jack's public key. This way, it can only be decrypted using Jack's private key.

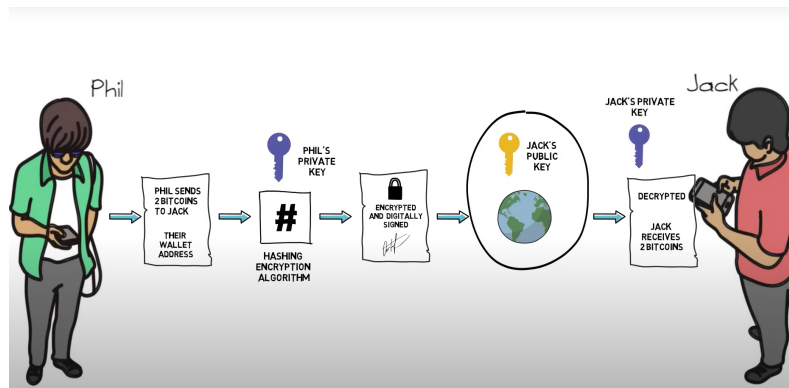


Figure 7: Source: Simplilearn



# Block validation

## — *Proof-of-Work*

- Transaction occur globally, are validated and added block by block.
- **Miners:** People who validate a block
- **Mining:** Adding a block to the blockchain
- In order for a miner to add a block to the blockchain, they have to solve a complex mathematical problem. Is rewarded with 6.25 bitcoins (about 4.3 million SEK: 6th of March, 2024)
- **Solving the mathematical problem** is called: **Proof of Work**



Figure 8: Source: Adobe Stock

# The CONs of the Blockchain

- **Scalability Challenges:**

- **Issue:** Blockchains may struggle to handle a large number of transactions quickly. Partly due to set timers and Proof-of-Work.

- **Energy Consumption:**

- **Issue:** Proof-of-Work (PoW) consensus mechanisms, as in Bitcoin, can be energy-intensive. Raises *environmental* concerns due to the substantial computational power required for mining.

- **Regulatory Uncertainty:**

- **Issue:** The regulatory environment for blockchain is uncertain due to inconsistent regulations. Disincentivizes widespread adoption.

# The PROs of the Blockchain

- **Immutability:** The blockchain is immune to counterfeiting, ensuring the *integrity of data*.
- **Security:** A hacker cannot alter blockchain data as *each user possesses* a copy of the ledger. Data within blocks is encrypted using complex algorithms.
- **Decentralization:** No central authority is required, reducing the risk of a single point of failure and enhancing resilience.
- **Transparency:** Public ledger visibility fosters trust among users and stakeholders.
- **Efficiency:** Blockchain streamlines processes, *reducing the need for intermediaries* and increasing transaction speed.
- **Global Accessibility:** Facilitates cross-border transactions without traditional banking systems.

# The Future

- **Interoperability and Standardization:**

- Increased focus on interoperability standards to facilitate seamless communication between diverse blockchain networks.

- **Evolution of Use Cases:**

- Continued exploration and expansion of blockchain applications beyond finance, impacting industries like healthcare, supply chain, and governance.

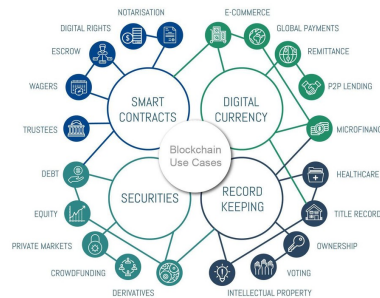


Figure 9: Source: Blockwiki

# The End