BLOCKCHAIN TECHNOLOGY

Chapter 6 – Industry 4.0

Till Ptassek, Sina Hofbauer

https://www.youtube.com/watch?v=w_Q9Ska_DLw

What is Blockchain?

Definition

A blockchain is a database not located centrally on a single server, but distributed across thousands of computers (nodes).

Individual data records (blocks) are linked together using cryptographic processes — hence the name 'block-chain'.

Because no single entity controls the data, it is called a decentralized database.

Became widely known:

2008 – Satoshi Nakamoto
"Bitcoin: A Peer-to-Peer Electronic Cash System"

Core concept:

Peer-to-peer (P2P) network — each participant (Node) acts as a single peer with equal rights

No third parties required for financial transactions

…linked via cryptographic hash references

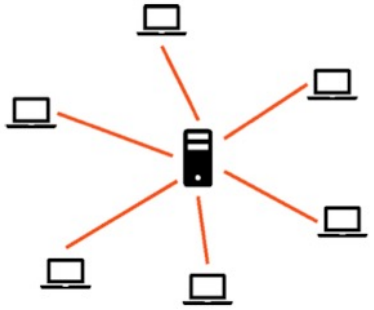
6.1 Distributed Ledger Technology (DLT)

DLT = a public, decentralized database ensuring all participants share read and write permissions

Centralized

Single central server controls all data.
All participants trust one central instance.

Example: Traditional banking system

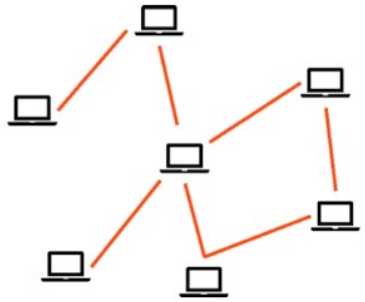


All connections go through center

Decentralized

Multiple hubs, each controls sub-nodes.
Reduced single point of failure.

Example: Internet (partial)

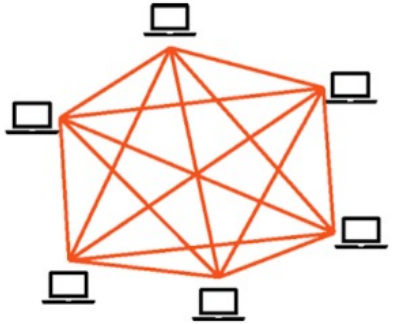


Several control points

Distributed

All nodes equal – no central control.
Each node stores a full copy of the data.

Example: Blockchain



Fully meshed – blockchain model

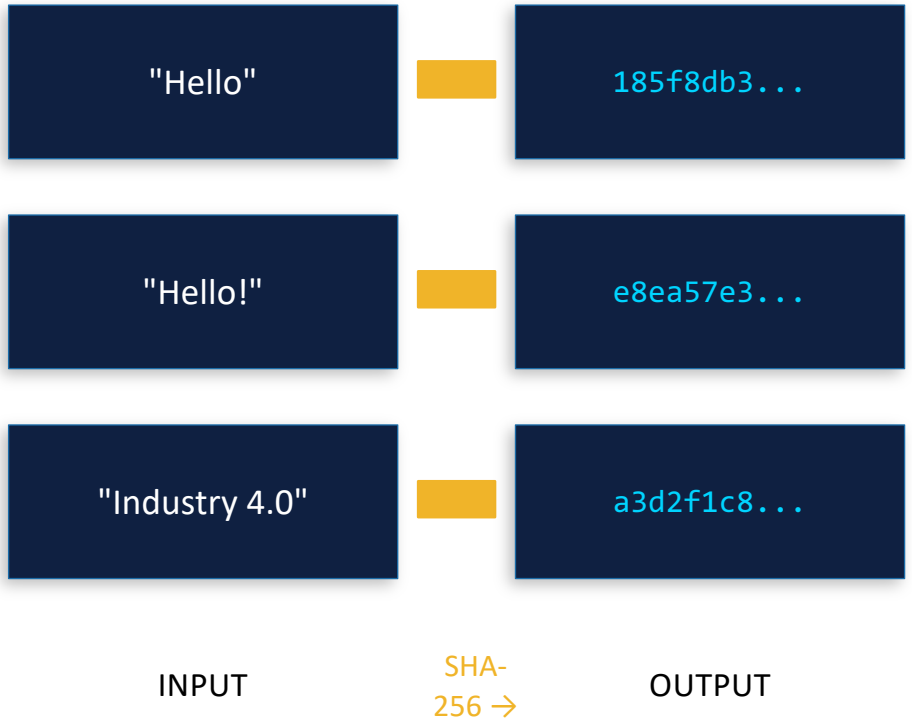
Key DLT Properties:

Chronological transaction records • Consensus mechanism validates new blocks • Redundant data storage across all nodes • Failure of one node does not affect others

6.2 Hash Values & Hash Functions

Hash	From Greek: to chop/scatter. Used for data storage and cryptology.
Hash Function	Maps any-length string → fixed-length hash value. Acts as a digital fingerprint.
Hash Value	Collision-resistant: no two different inputs produce the same hash output.
Hash Reference	Data stored elsewhere than the reference. Enables exact, change-sensitive linking.
SHA-256	Secure Hashing Algorithm used by Bitcoin. One-way function — cannot be reversed.

How SHA-256 Works



⚠ Even a tiny change in input completely changes the hash — this makes tampering immediately detectable!

6.3 Asymmetric Encryption & Digital Signatures

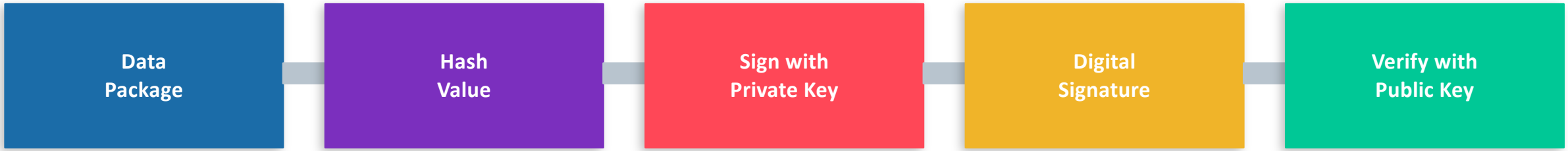
Public Key

- Shared openly with everyone
- Used to encrypt data for the key owner
- Used to verify digital signatures
- Authenticate the identity of the sender

Private Key

- Kept strictly secret by owner
- Used to decrypt data encrypted with public key
- Used to generate digital signatures
- Stored securely in a wallet (Bitcoin)

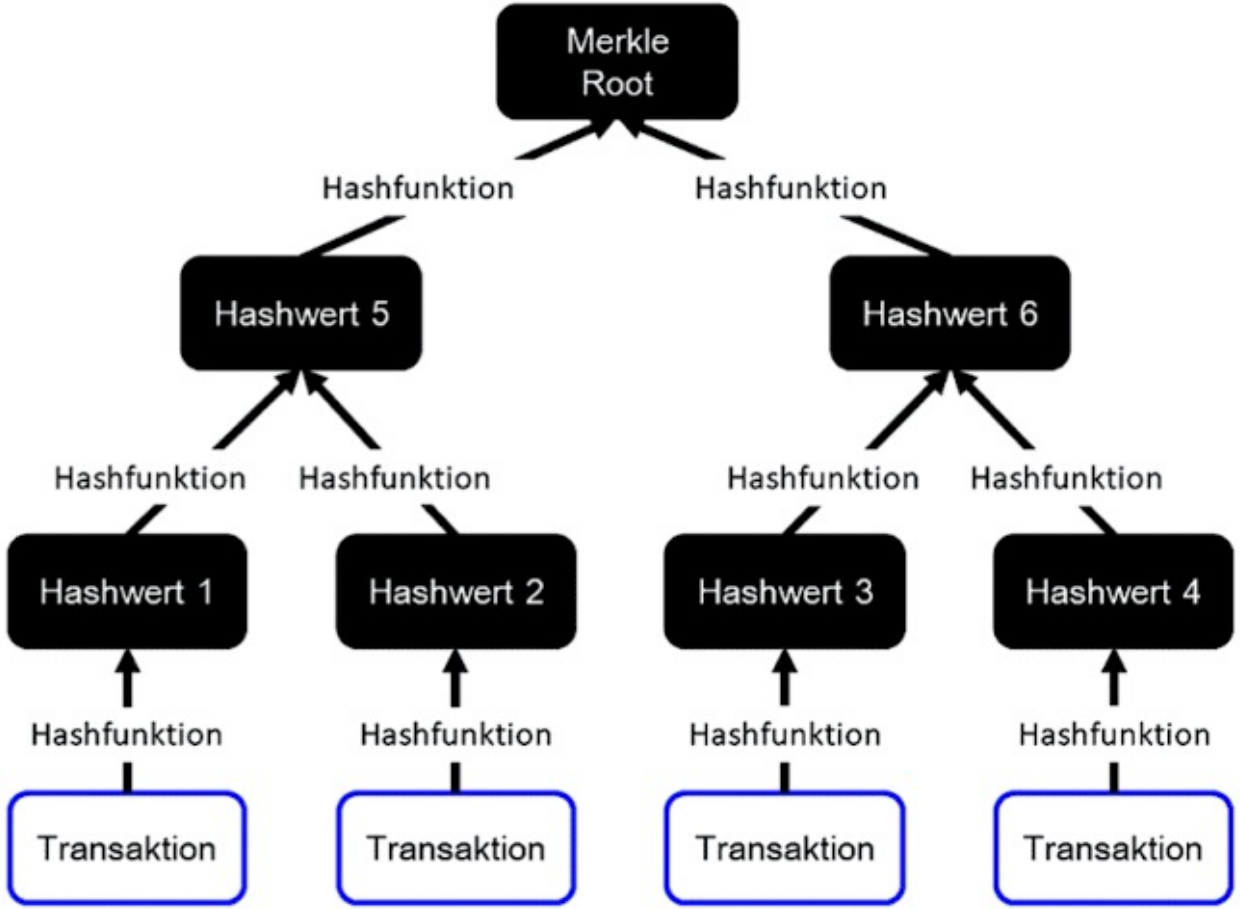
Digital Signature Process



If hash values match → message is authentic and unmodified ✓

6.4 Merkle Tree (Hash Tree)

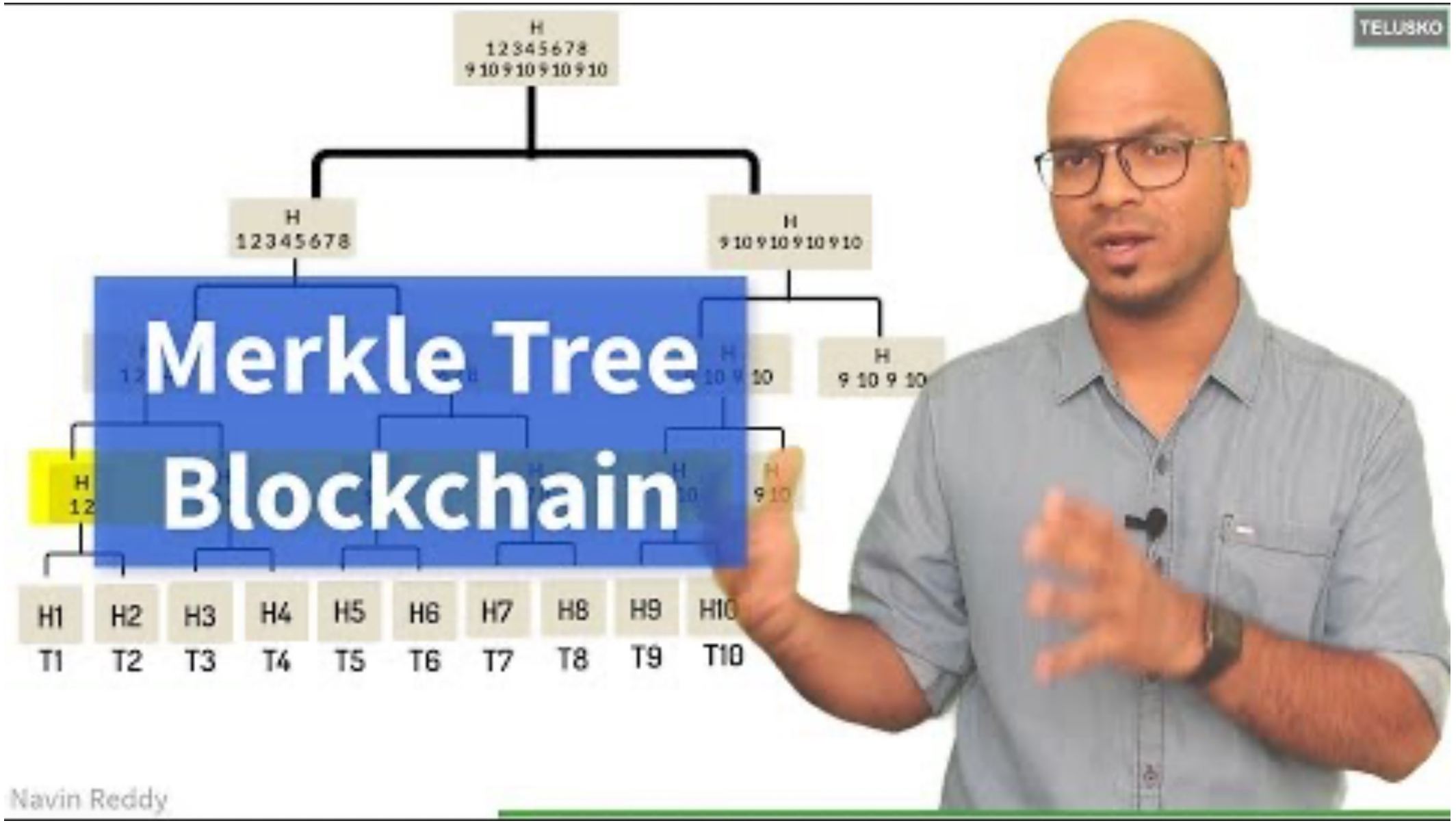
Goal: Express multiple transactions by a single root hash value



Key Properties

- Hash values are paired and combined until only one root hash remains
- Manipulations are immediately detected — any change cascades up to the root
- Enables efficient and secure verification of large transaction sets
- Used in Bitcoin and most major blockchains

6.4 Merkle Tree (Hash Tree)



https://www.youtube.com/watch?v=fB41w3JcR7U&list=WL&index=18

6.5 Consensus Mechanisms – Overview

Since no central authority controls the blockchain, all participants must agree on which blocks are valid — this is called consensus.

Why are consensus mechanisms needed?

Blockchains are open P2P networks — anyone can try to add or modify blocks. Without consensus, attackers could insert false transactions. Consensus ensures correctness with minimal time and effort.

⛏️ Proof of Work (PoW)

Miners compete to solve complex computational puzzles. The winner adds the next block and receives a reward.

Used by: Bitcoin, Ethereum (pre-2022)

✅ Very secure — attack requires >50% of total network compute power

⚠️ Extremely energy-intensive; costly hardware; scaling issues

 Proof of Stake (PoS)

Validators are selected based on their stake (value deposit). No mining competition.

Used by: Cardano, Algorand, Ethereum (post-2022)

✅ Energy-efficient; higher transaction throughput; no mining hardware

⚠️ Tendency toward centralization; wealthy participants favored

Proof of Work (PoW) – Deep Dive

1

New Transaction

A user initiates a transaction (e.g., sends Bitcoin)

2

Miners Compete

Network participants (miners) attempt to solve a complex task to find a random value

3

Hash Puzzle

Miners try billions of hash values until the result meets the target

4

Block Found!

Winning miner broadcasts the block to the network

5

Verification

Other nodes check the block hash for correctness

6

Reward

Miner receives a block reward (e.g., newly created Bitcoin)

🔒 **Security: Attacker must control >50% of total network hash power — practically impossible on large networks like Bitcoin**

Proof of Stake (PoS) – Deep Dive

How Proof of Stake Works

1. Validators lock up a share of their cryptocurrency as a stake (deposit)
2. Probability of being chosen to validate a block proportional to stake size
3. Selected validator proposes and signs the new block
4. Other validators confirm; validator earns transaction fees (no new coin creation)

PoW vs PoS

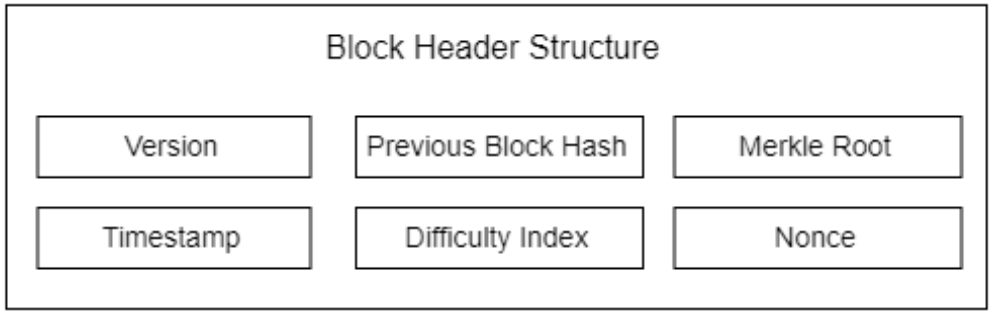
Feature	PoW	PoS
Role	Miners	Validators
Resource	Computing power	Stake (coins)
Reward	New coins	Transaction fees
Energy	Very high	Low
Throughput	Limited	Higher
Centralization risk	Mining pools	Wealthy stakers
Examples	Bitcoin	Ethereum, Cardano

Chaining of Blocks – Bitcoin Example

What is a Blockchain?

- Distributed ledger shared across a **peer-to-peer network**
- All participants store the **entire blockchain**
- First block = **Genesis Block** (starting point)

Block Structure:

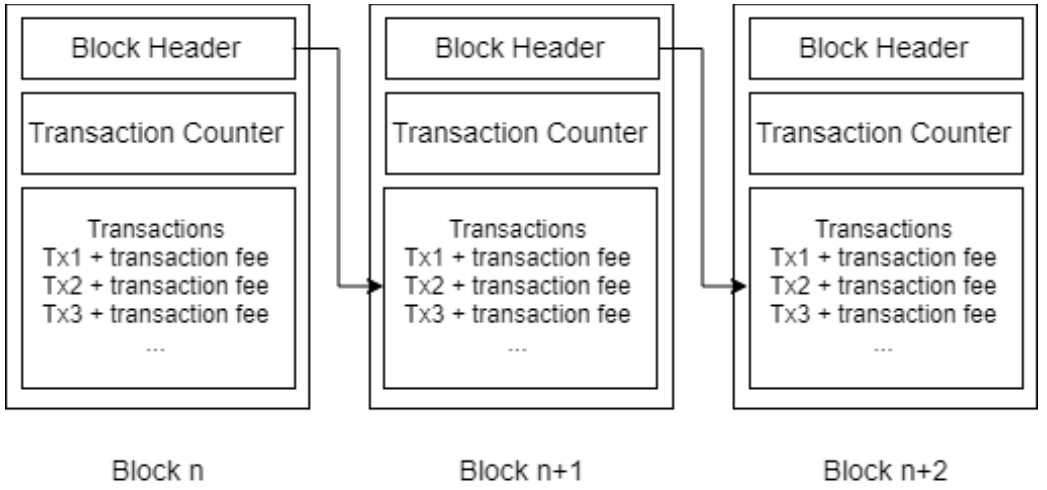


How Blocks are Chained?

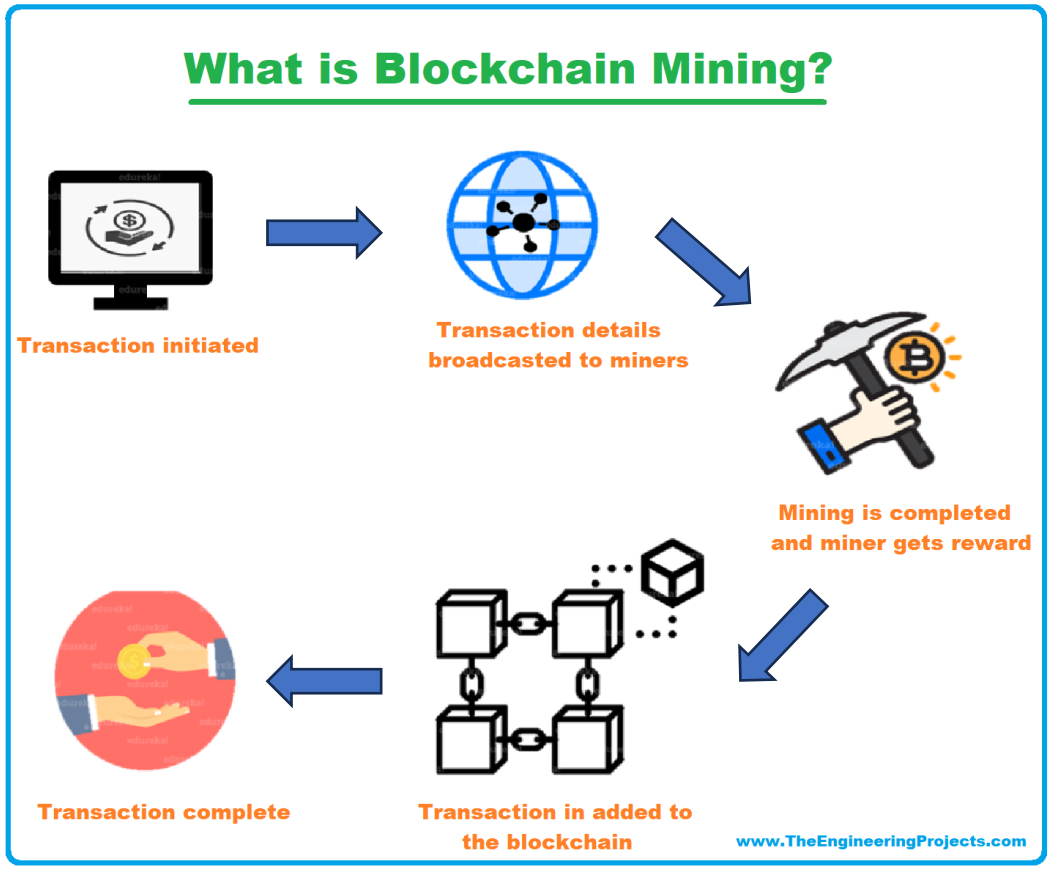
- Each block contains:
  - Hash of the **previous block**
  - **Timestamp** (creation time)

→ Forms a **chronological, secure chain**

→ Any change breaks the chain (**tamper-resistant**)



Chaining of Blocks – Bitcoin Example



- New block **every ~10 minutes**
- Miners solve **Proof-of-Work**
- Goal: find a **nonce** → hash with required leading zeros

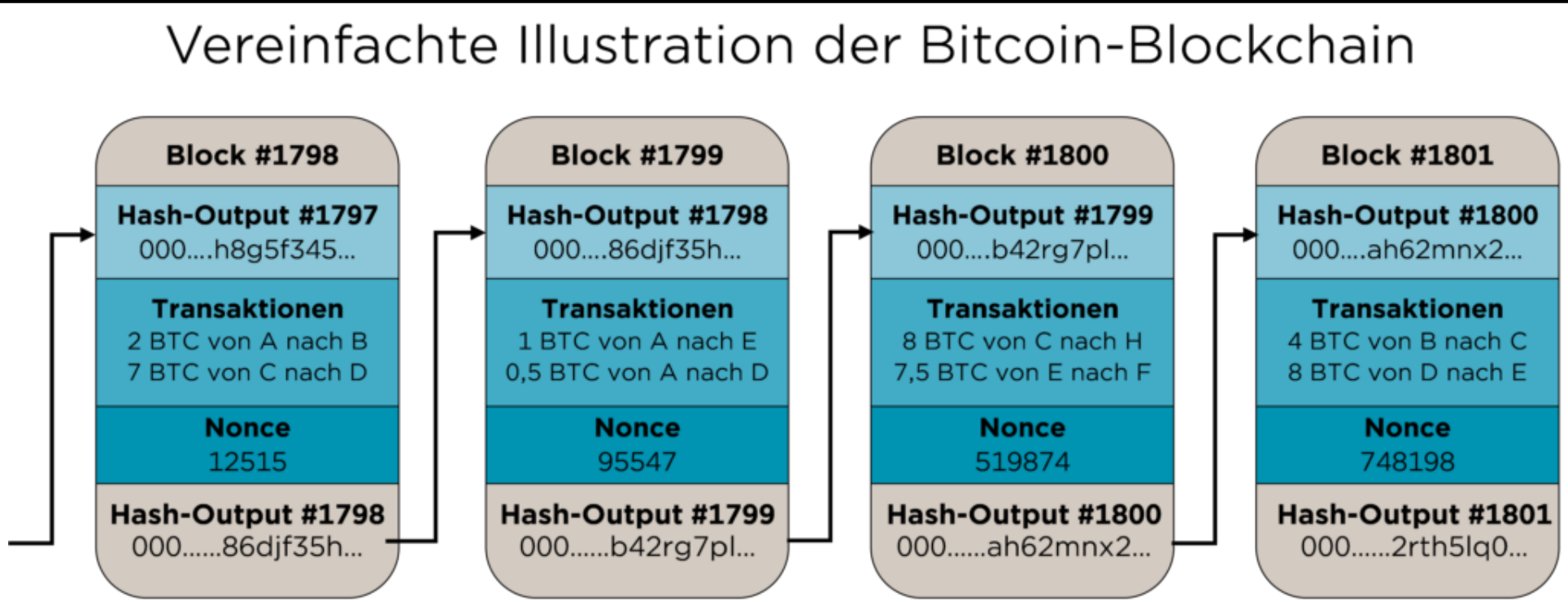
Dificulty Adjustment

- Controls how hard mining is
- Adjusted to keep block time **constant**
- Increases with more computing power

Nonce

- Nonce = “Number used once”
- A random number included in the block header
- Used in the mining process (Proof of Work)
- Miners repeatedly change the nonce
- Each change produces a different hash
- The nonce is the only value miners can freely adjust

Chaining of Blocks – Bitcoin Example



Quelle: Eigene Darstellung in Anlehnung an Deutsche Bundesbank, 2021

Blocks are securely linked via hashes

→ **Creates a transparent, immutable chain of data**

Autorisation Architecture

Blockchain Access Types

Public Blockchain:

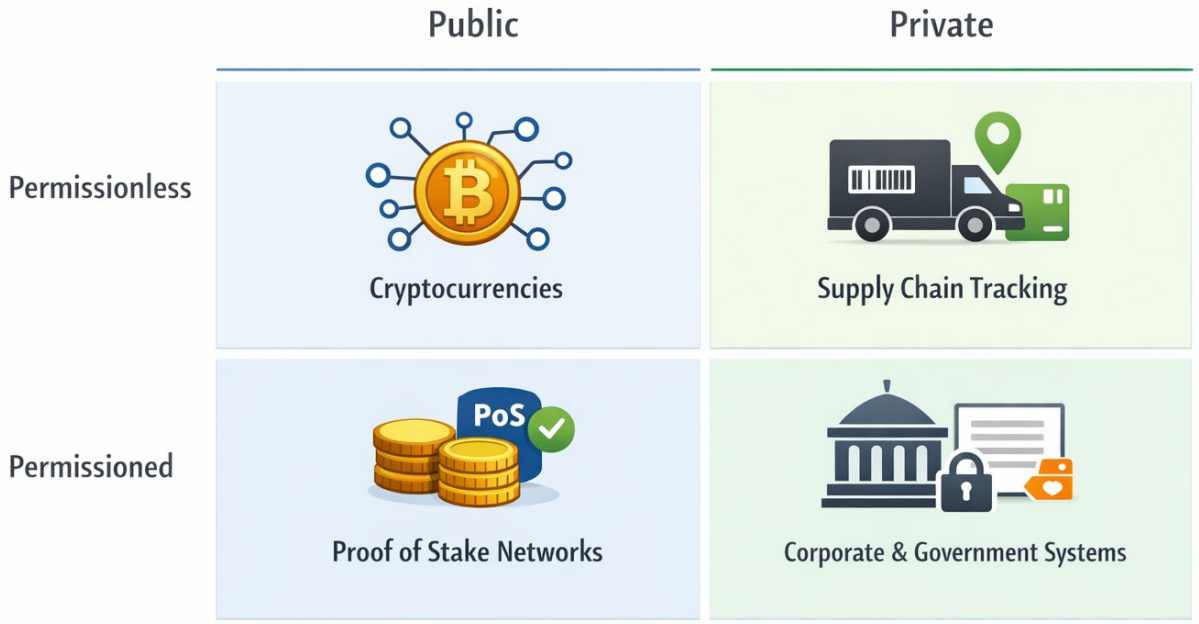
- Open to everyone
- Anyone can read, write, and validate transactions
- No access restrictions

VS

Private Blockchain:

- Restricted access
- Only authorized users can participate
- Used for internal or sensitive applications

Blockchain Use Cases



Field of Application

Logistics

- Blockchain unifies **transactions and related data**
- Provides a **shared, transparent system** for all participants
- Improves **trust, efficiency, and traceability**

Smart Identities

- Users control their **own digital identity (decentralized)**
- No need for central identity providers
- Use of **digital certificates** (e.g. age, address)
- Blockchain ensures:
  - **Authenticity and trust**
  - No direct exposure of personal data
- Applicable to:
  - People, machines, and companies
- Improves **efficiency in compliance & supply chains**

Smart Cities

- Cities become **digitally interconnected systems**
- Examples:
  - Intelligent traffic systems & adaptive speed limits
  - Automatic air quality monitoring
  - Smart energy grids & charging stations
- Blockchain enables **secure networking of city systems**

Smart Home

- Modern homes already include many smart home features
- Devices are connected and exchange data continuously
- Smart homes are vulnerable to cyberattacks
- Provides enhanced **security through decentralization**

Field of Application

E-Health

- Supports **digital health records & access control**
- Improves diagnosis and healthcare management
- Tackles **counterfeit drugs** problem
- Ensures:
  - **Transparent and secure supply chains**
  - Patient safety
- Alternative to centralized healthcare databases

Smart Contracts

- **Digital contracts stored as code**
- Automatically execute when conditions are met
- Example:
  - Flight delay → automatic compensation
- Benefits:
  - No intermediary needed
  - Faster and cheaper transactions
- High trust via blockchain consensus

Automotive

- Future mobility = **autonomous + connected systems**
- Enables **machine-to-machine (M2M) transactions**
- Example:
  - Car pays automatically for fuel or charging
- Use cases:
  - Car sharing
  - Parking & toll payments
- Vehicles can have their own **digital wallets**

Smart Grids

- Shift from centralized → **decentralized energy systems**
- Connects local **energy producers and consumers**
- Enables:
  - Direct energy trading
  - Faster and secure transactions
- Improves **efficiency and sustainability**

https://www.youtube.com/watch?v=znwOhOtm6go

When to Use Blockchain? – Decision Path

Q1 Is data distributed across a database? **YES →**

Q2 Are multiple actors involved in business processes? **YES →**

Q3 Is there information-based conflict potential? **YES →**

Q4 Are there different IT standards / guidelines? **YES →**

Q5 Must (old) data be stored / retrieved regularly? **YES →**

All YES → Blockchain has potential for strategic deployment!

Blockchain is NOT always the right solution!

Consider blockchain only when:

- Multiple actors share data
- Trust between parties is low
- Immutability is important
- No central authority is desired

Otherwise, a traditional database (e.g., ERP system) is often simpler, faster, and cheaper.

Opportunities and Risks of the Technology

Data availability
- The data is stored redundantly and distributed to the nodes using a peer-to-peer network.

Irreversibility of the data
- Data cannot be manipulated or deleted.

Decentralization
- A consensus process ensures the trust of the participants.

Data integrity
- Block chaining means that the data is logged in the time sequence in a traceable, comprehensible and secure manner.

Transparency
- Each network participant has access to the database and can view transactions.

Automation
- The programmability of transactions as well as the execution of a computer program (smart contracts) is possible.

High energy consumption
- The proof of work consensus mechanism requires high computational power, resulting in high energy consumption.

Scalability
- In a public blockchain, there is the challenge of scalability due to the large volume of data that must be exchanged between participants. Larger blocks enable higher transaction rates in the network, but increase the computational and communication overhead for the consensus mechanisms.

Legal Framework
- Blockchain can operate without borders of nations, the transaction participants can be located in different legal jurisdictions.

Irreversibility
- Specification or programming errors can have severe consequences, especially with smart contracts

Summary

Blockchain Potential

- Versatile technology with **wide range of applications**
- Can transform industries and society
- Examples:
  - Smart Contracts
  - Smart Cities & Smart Homes
  - Logistics & Supply Chains
- Energy & Mobility

Key Strengths

- Decentralization → no central authority
- Transparency & Trust
- Security & Immutability
- Automation through smart contracts

Challenges

- Scalability limitations
- Privacy & anonymity concerns
- Legal and regulatory uncertainties