Humanisten Leer
18.12.2024

Blockchain Überblick

Grundlegende Technologien

Hash-Funktionen bzw. kryptografische Hash-Funktionen

kryptografische Puzzles

Hash-Bäume (Merkel Tree)

digitale Signaturen für Nachrichten

Hash Funktionen

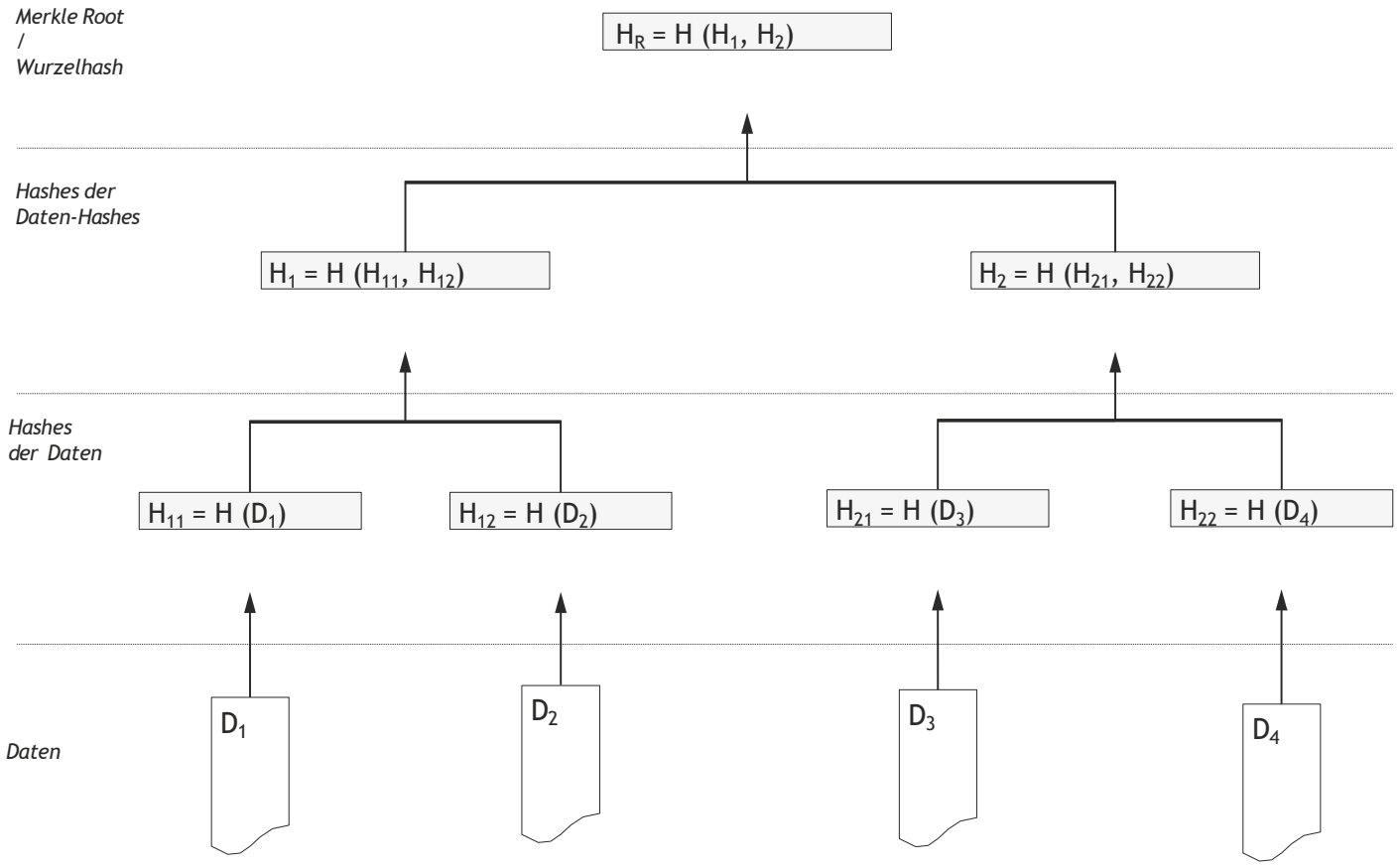
mathematische Funktionen, die dazu dienen, eine Menge von Informationen beliebiger Größe als Eingabemenge auf einen vorab definierten Bereich fixer Größe, den Zielbereich, abzubilden

Ändert sich auch nur ein geringer Teil des Eingabewertes, soll die Hash-Funktion einen gänzlich anderen Zielwert liefern. Aus dem Zielwert soll zudem nicht auf den Eingabewert geschlossen werden können und die Berechnung der Hash-Funktion soll rasch erfolgen.

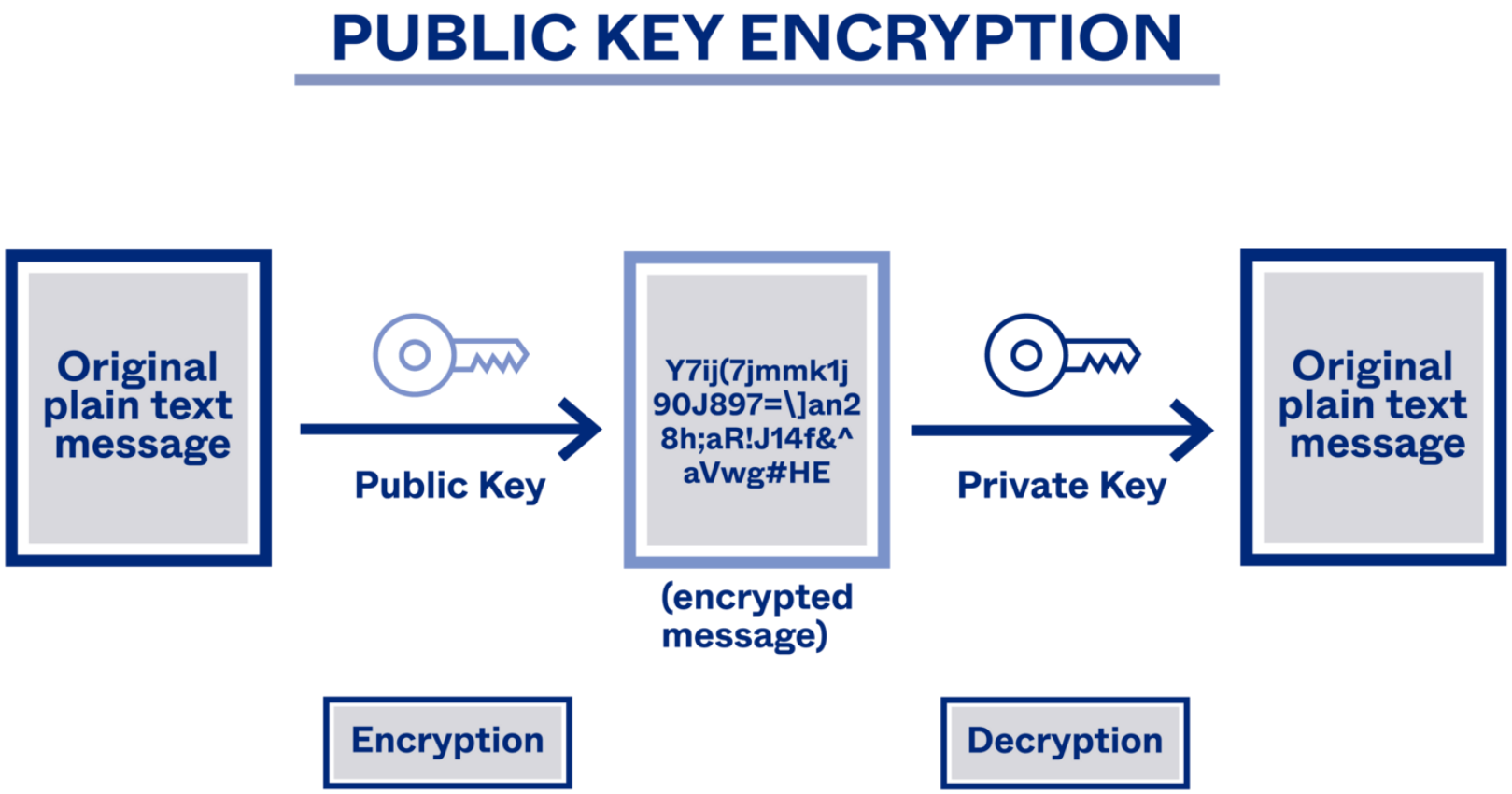
Ziel ist Unversehrtheit des Eingabewertes sicherstellen

Aktuell verwendet SHA-256

Merkel Tree

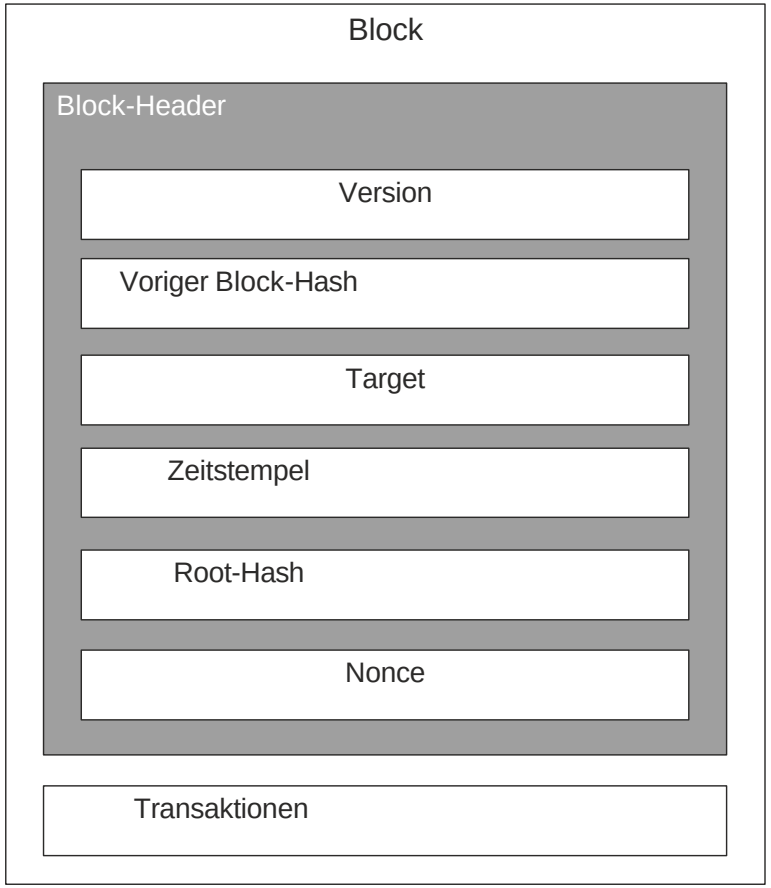

Merkle Root / Wurzelhash
$H_R = H(H_1, H_2)$
Hashes der Daten-Hashes
$H_1 = H(H_{11}, H_{12})$
$H_2 = H(H_{21}, H_{22})$
Hashes der Daten
$H_{11} = H(D_1)$
$H_{12} = H(D_2)$
$H_{21} = H(D_3)$
$H_{22} = H(D_4)$
Daten
D_1
D_2
D_3
D_4

Signaturen

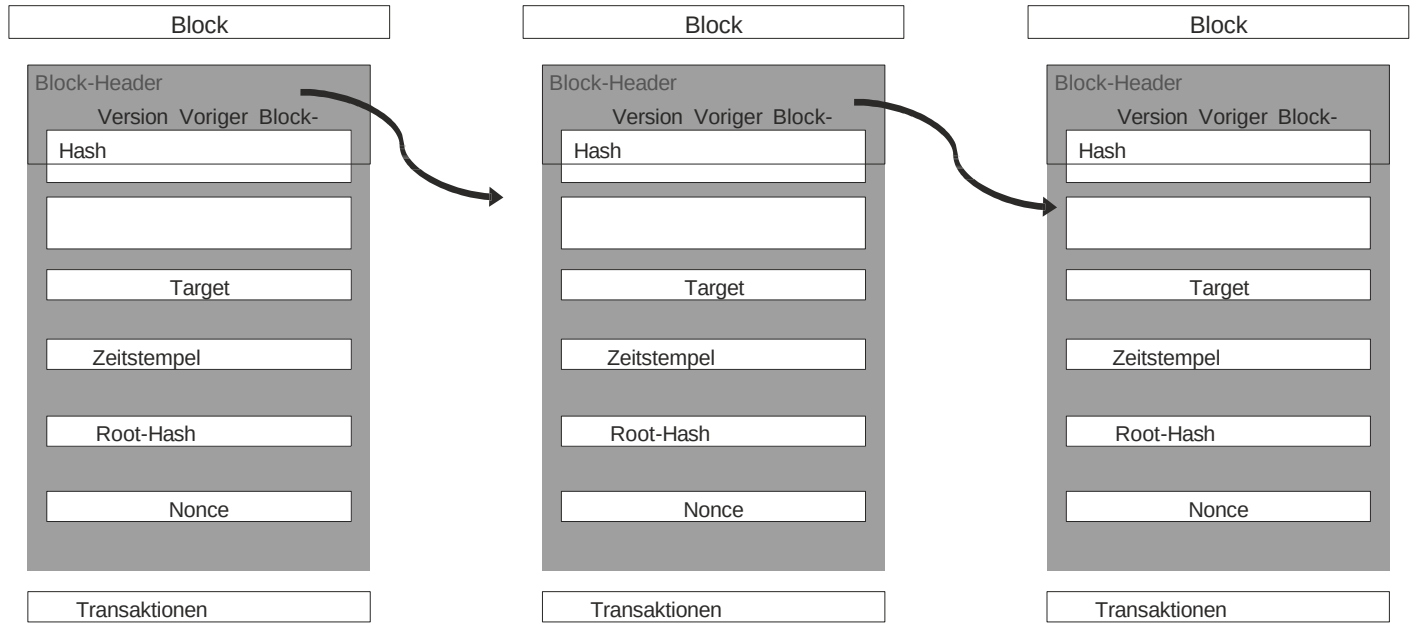

PUBLIC KEY ENCRYPTION
Original plain text message
Public Key
Y7ij(7jmmk1j 90J897=\]an2 8h;aR!J14f&^ aVwg#HE
(encrypted message)
Private Key
Original plain text message
Encryption
Decryption

Datenstruktur eines Blocks

- Datenstruktur der DB in der Blockchain
- Target→ Schwierigkeit des math. Rätsels → Mining
- Root Hash → Merkel Baum
- Nonce → Zähler
- Jeder Block kann eine oder mehrere Transaktionen beinhalten

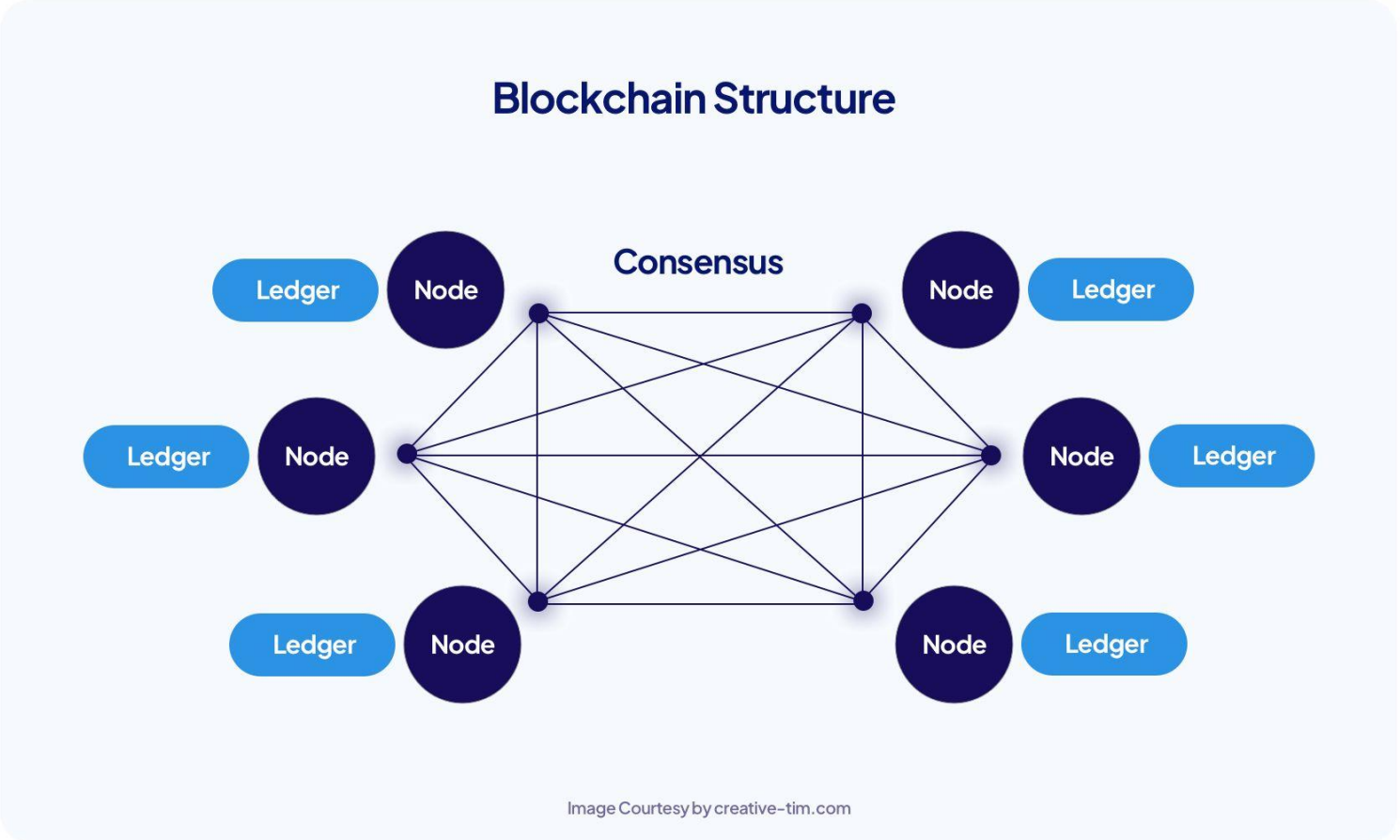


Blockchain – Verkettung

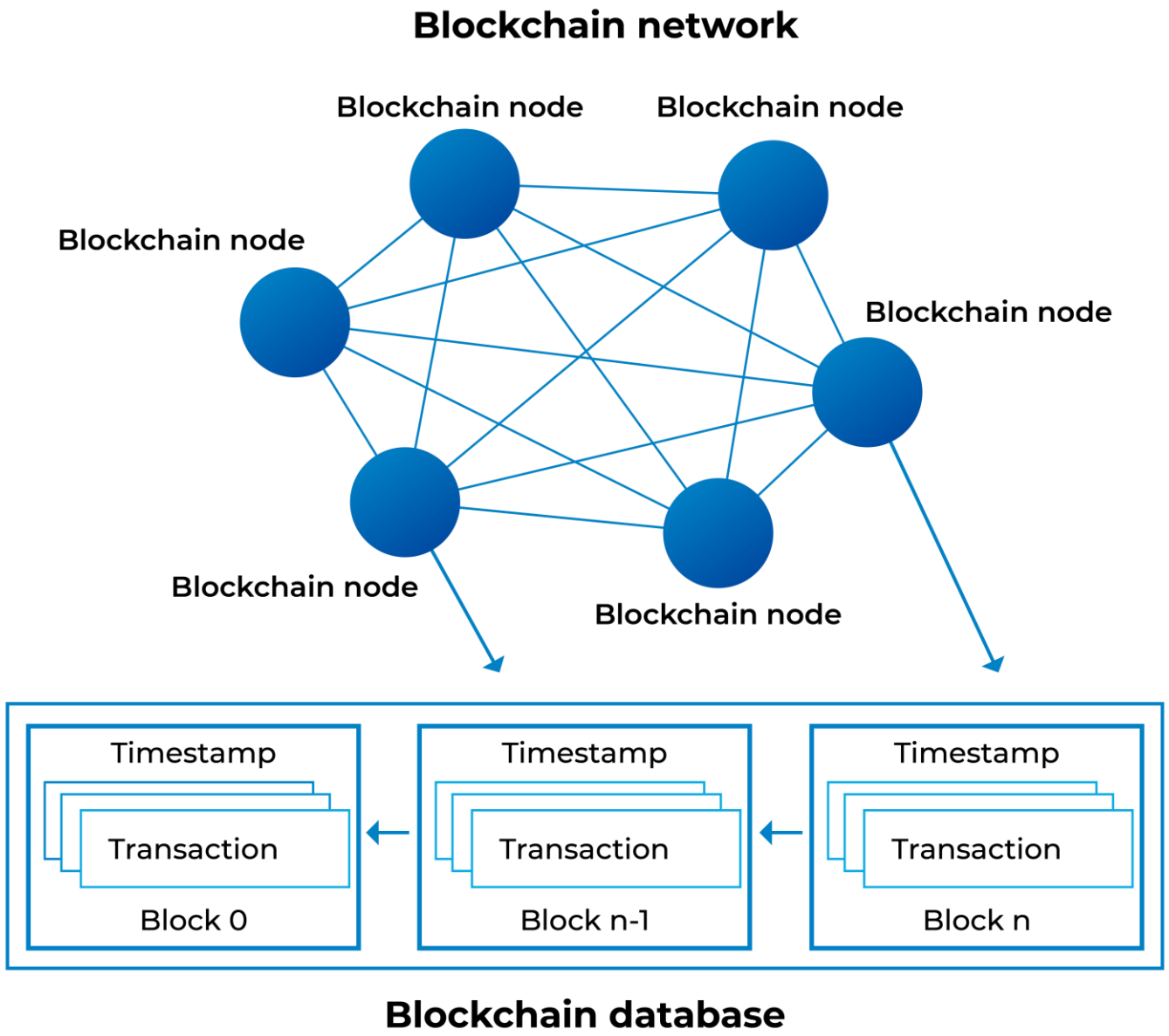


Blockchain Wachstum

BC Netzwerk


Blockchain Structure
Consensus
Ledger
Node
Ledger
Node
Ledger
Node
Ledger
Node
Ledger
Node
Ledger
Node
Image Courtesy by creative-tim.com

BC
Blöcke


Blockchain network
Blockchain node
Blockchain node
Blockchain node
Blockchain node
Blockchain node
Blockchain node
Timestamp
Transaction
Block 0
Timestamp
Transaction
Block n-1
Timestamp
Transaction
Block n
Blockchain database

Einschätzung

- Vorteile
- Nachteile
- Typische Anwendungen
- Beispiel

Vorteile

- **Decentralization**: Transaktionen benötigen keine Vertrauensinstanz (Bank, Noter, staatl. Stellen et.)
- **Transparency**: Jeder Teilnehmer kann die komplette Historie einsehen.
- **Security**: Momentan noch praktisch nicht zu entschlüsseln.
- **Immutability**: Einmal erfasst sind Änderungen nciht mehr möglich.
- **Consensus Mechanism**: transaktionen werden über einen Konsensalgorithmus validiert: Integrität ohne Kontrolle.
- **Smart Contracts**: Automatisierung von Verträgen, selbstständig ausführbar.
- **Traceability**: Jede Transaction ist überprüfbar.

Nachteile

- Energieverbrauch durch Mining
- Quantum Computing kann in naher Zukunft Verschlüsselung knacken

Typische Anwendungsgebiete

- Werttransfer (Fin, Banking, Diamantenhandel)
- Datenintegrität bei offiziellen Dokumenten (Notarfunktion)
- Gerätesicherheit bei IoT
- Lieferketten
- Energiemanagement
- Medizin
- Identitätsmanagement
- Vertragsmanagement (Automatisierung)
- Kombination mit Ki-gestützen Anwendungen

Beispiel – öffentlicher Dienst