IT-SICHERHEIT UND DATENSCHUTZ

KAPITEL 10 - BLOCKCHAIN

buchmann@hft-leipzig.de

LERNZIEL UND AUFBAU DIESES KAPITELS

- Inhalte dieses Kapitels
  - Abgrenzung des Blockchain-Begriffs
  - Integritätssicherung in einem verteilten System
  - Umsetzung eines pseudonymen, dezentralen „write once read many“-Speichers
  - Anreizverfahren für das ehrliche Einbringen eigener Ressourcen

- Lernziele
  - Sie können erklären, wie die Blockchain-Datenstruktur aufgebaut ist und wie die Kommunikation innerhalb einer Blockchain abläuft.
  - Sie können erläutern, auf welche Weise die Blockchain dezentral den gültigen Systemzustand feststellt und wie die Integritätssicherung funktioniert.

Dieses Kapitel orientiert sich an [2].

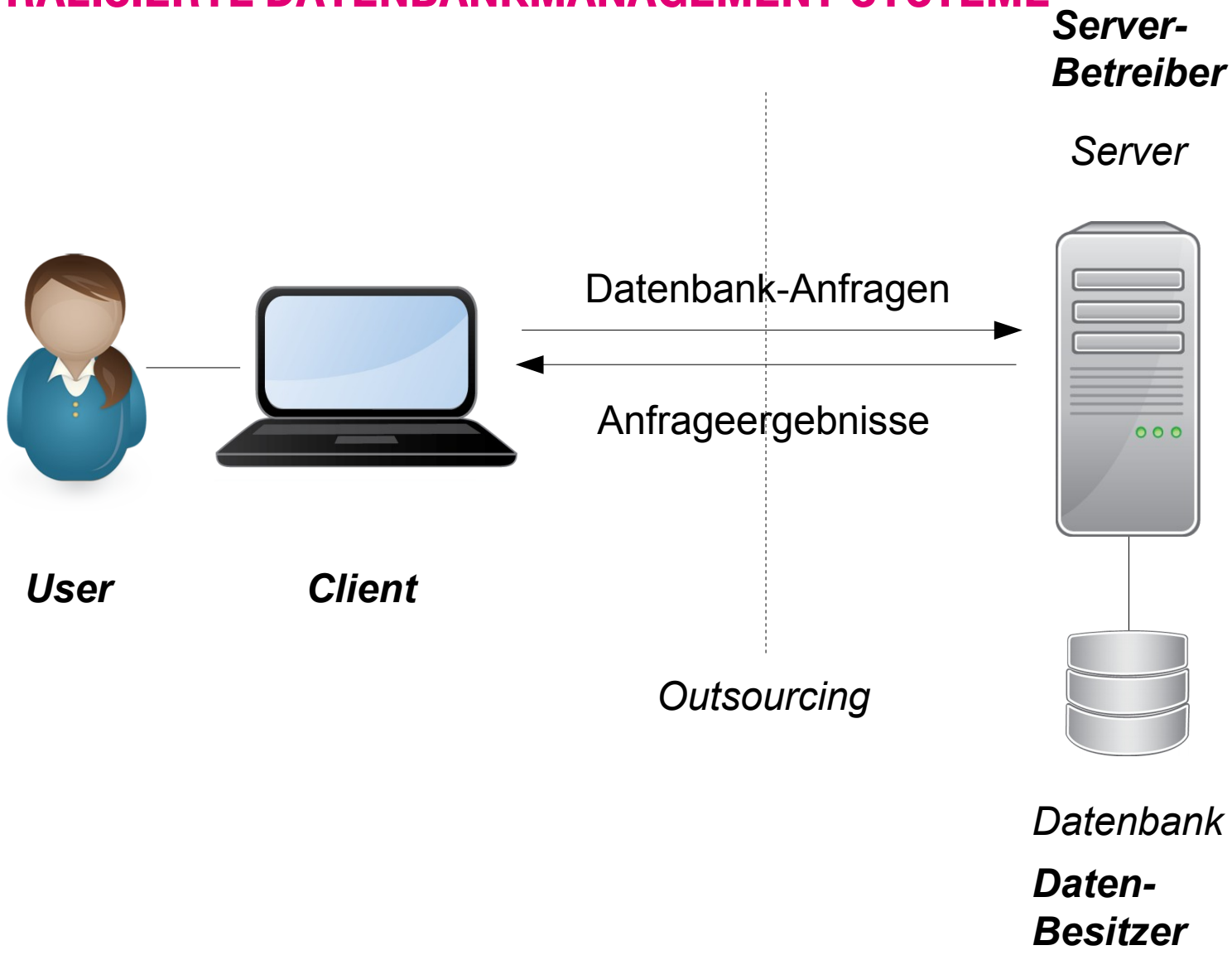
ZIELE DER IT-SICHERHEIT

- „Security triad“
  - **Vertraulichkeit**: Asset ist nur Autorisierten zugänglich
  - **Integrität:** Asset kann nur von Autorisierten modifiziert werden
  - **Verfügbarkeit**: Asset kann von Autorisierten genutzt werden

- ISO 7498-2 fügt hinzu
  - **Authentisierung**: Identität eines Senders wird überwacht
  - **Nichtabstreitbarkeit**: Sender kann nicht abstreiten, das eine Nachricht von ihm kam
- US Department of Defense fügt hinzu
  - **Auditierbarkeit**: Alle Aktionen mit dem Asset sind nachvollziehbar

MOTIVATION

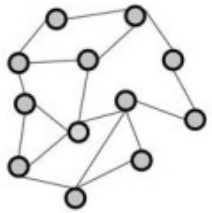
ZENTRALISIERTE DATENBANKMANAGEMENT-SYSTEME



HERAUSFORDERUNGEN

- Zentralisiertes System
  (Auch die Cloud ist zentralisiert, alles aus einer Hand)
  - Single Point of Failure
    - Verfügbarkeit, Intergritätssicherung etc. hängt von einer einzigen Stelle ab
    - Wie herausfinden, ob der Server-Betreiber bei der Sicherheit spart?
    - Was passiert, wenn der zentrale Server angegriffen wird?
  - Server-Betreiber darf alles
    - Nur Verträge und Vertrauen schützen den Datenbesitzer davor, dass der Server-Betreiber die Daten manipuliert
  - Umgang mit wechselnden Lasten
    - Server-Betreiber muss Vorkehrungen treffen, dass Server auch einen überraschenden Ansturm an Transaktionen bedienen kann
    - Wieviel Reservekapazität vorhalten?

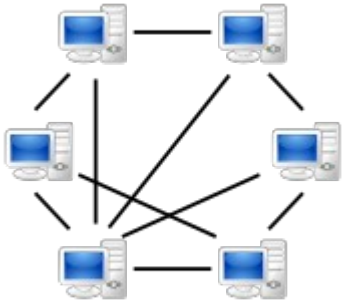
„ECHTE“ DEZENTRALE SYSTEME SIND NICHT SO EINFACH



- Vorteile dezentralisierter Systeme
  - Können durch Hinzufügen weiterer Rechnerknoten mit der Last mitwachsen, hohe Leistung zum günstigen Preis
  - Verfügbarkeit des Systems, unwahrscheinlich dass alle Rechnerknoten gleichzeitig ausfallen

- Nachteile dezentralisierter Systeme
  - Abstimmungsaufwand zwischen den Rechnerknoten
  - Abhängigkeit von umfassender Netzwerk-Verfügbarkeit
  - Höhere Komplexität bei Entwicklung, Wartung, Administration von Anwendungen
  - Integrität und Vertraulichkeit problematisch, z.B. Kommunikation über unsichere Verbindungen, Rechnerknoten unter der Kontrolle von Dritten
  - Verfügbarkeit der Daten aufwendig, wenn Knoten ausfallen dürfen

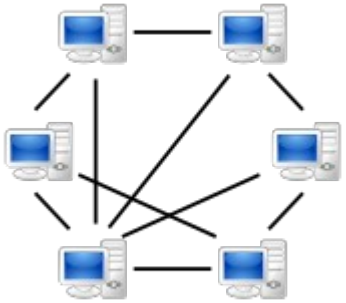
VERTEILTE PEER-TO-PEER-SYSTEME



- Spezialfall dezentralisierter Systeme

- Typische Eigenschaften eines Peer-to-Peer-Systems:
  - Alle Teilnehmer (Peers) sind unabhängig und gleichberechtigt
    - können (müssen aber nicht) jede Aufgabe im System übernehmen
    - können (müssen aber nicht) mit jedem anderen Knoten kommunizieren
  - Jeder Teilnehmer bringt soviele Ressourcen ein, wie er verbraucht
    - Rechenleistung, Speicher, Netzwerkbandbreite
  - System skaliert (möglichst) linear
    - keine obere Grenze für die Zahl der Teilnehmer
      (In vielen verteilten Architekturen nimmt ab einer bestimmten Größe der Verwaltungsoverhead so stark zu, dass das Hinzufügen neuer Teilnehmer mehr Ressourcen kostet, als der Teilnehmer mitbringt)
  - Selbstorganisierendes System ohne zentralen Koordinator
    - Teilnehmer dürfen jederzeit ein- und austreten, ausfallen, etc.

HERAUSFORDERUNGEN FÜR PEER-TO-PEER SYS.



- Herausforderung Vertrauen:
  - Viele (eigenständige) Knoten müssen sich im Sinne des Systems korrekt verhalten
    - Daten speichern, Nachrichten unmanipuliert weiterleiten, etc.
  - Nur dann hohe Verfügbarkeit, wenn die Knoten nicht nur Ressourcen konsumieren, sondern auch ihre eigenen Ressourcen bereitstellen
    - „Freeloader“-Phänomen bekannt aus Napster, Gnutella…

  Anm.: Dieses Problem besteht im Business-Umfeld nicht

- Aufgaben für die Integritätssicherung:

  1) Technische Fehler
    - Ausfall von Knoten, Ausfall der Netzwerkverbindung, Knoten treten aus ohne sich vorher von ihren Peers abzumelden

  2) Unredliche Knoten
    - Nachrichten manipulieren, Daten manipulieren, Angriffe auf die Verfügbarkeit des Systems und der Daten, Ausspähen von Daten und Teilnehmern

AUSGANGSPUNKT BLOCKCHAIN

- Architektur eines Peer-to-Peer-Systems
  - Offenheit, Skalierbarkeit, Perfomanz, Kosten, Verfügbarkeit des Systems, etc. pp.
- Verfügbarkeit der Daten
  - Verteile Daten über möglichst viele Knoten

Das ist das Neue an Blockchain

- Verfügbarkeit der Services
  - Korrekte Teilnahme im Sinne des Systems wird belohnt durch einen verteilten ökonomischen Anreiz-Mechanismus (Bitcoins, Ether)
- Integritätssicherung
  - Blockchain sorgt dafür, dass Fälschungen/Manipulationen mehr Rechenleistung benötigen als ein Knoten aufbringen kann
  - Majority Vote zur Bestimmung der gültigen Kopie

WAS BEZEICHNET „BLOCKCHAIN“?

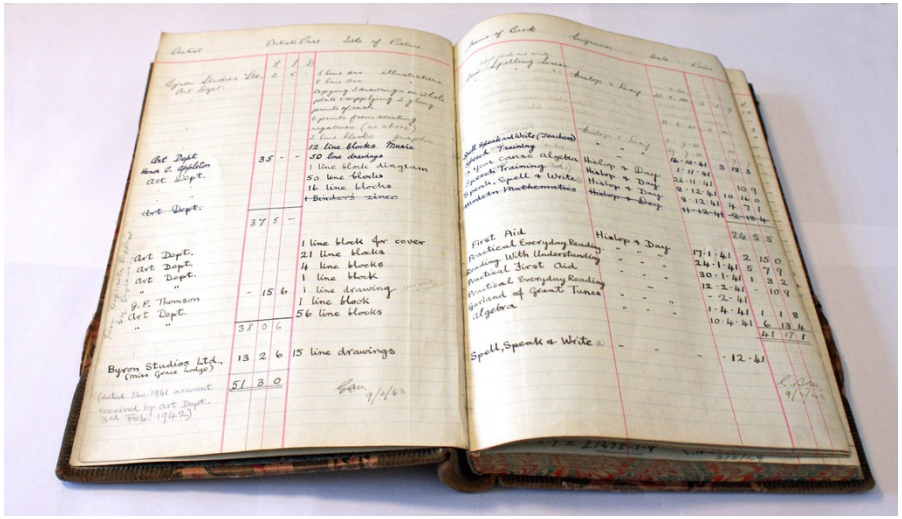
- Eine Datenstruktur
  - Miteinander verkettete Datenblöcke, bei denen der letzte den aktuellen Systemzustand beschreibt, die davor die Systemhistorie
- Einen Algorithmus
  - Verfahren zur Integritätssicherung in einem Peer-to-Peer-System ohne zentralen Koordinator
- Eine Familie von IT-Produkten
  - Ethereum, Bitcoin, Quorum, Hyperledger, …
- Einen Gattungsbegriff
  - Vollständig verteilte Peer-to-Peer-Systeme mit Integritätssicherung auf der Basis von Blockchain-Ledgers

BESTANDTEILE DER BLOCKCHAIN-TECHNOLOGIE

ACCOUNTS

- Jeder Nutzer darf beliebig viele Accounts anlegen
  - Existenz öffentlich bekannt
  - Jeder darf Transaktionen mit dem Account durchführen (d.h., den Besitz von digitalen Objekten an den Account übertragen)
- **Transaktionshistorie** in Blockchain **definiert Account-Zustand**
  - es gibt kein Nutzerkonto mit einem festen Inhalt!
- **Authentifizierung** über Challenge-Response **mit Public Key**
  - Ein Node verschlüsselt zufälligen Klartext mit Public Key eines Accounts
  - Nur Besitzer des Private Keys kann das Chiffrat wieder entschlüsseln
  - Antwort mit Klartext: Identität des Account-Inhabers bewiesen *(z.B. Übertragung vom Account des Nutzers autorisiert)*

LEDGER („KONTOBUCH“)



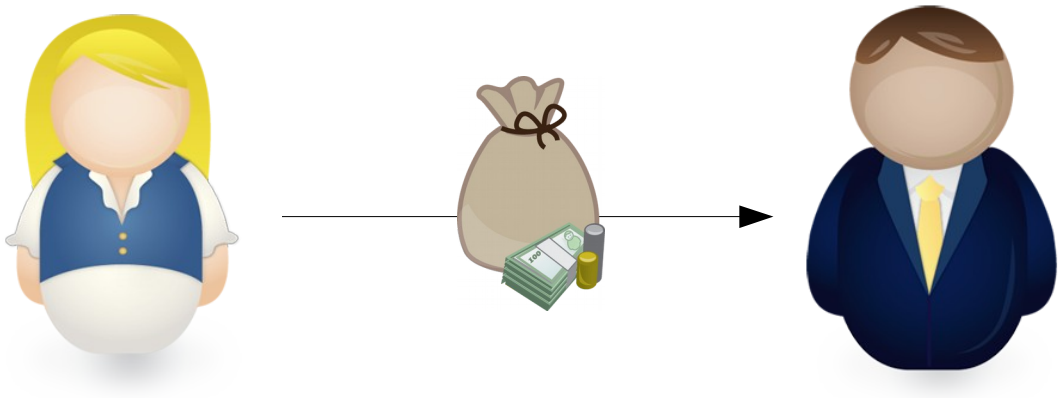
- Verteilte Liste von Transaktionen
  - Organisiert als Blockchain, d.h., Aneinanderreihung von Blöcken, die jeweils mehrere Transaktionen speichern
  - Eine Blockchain speichert ein Ledger
  - Ledger enthält Informationen über die Transaktionen, die digitale Güter von einem Account zu einem anderen übertragen

- Wie bei einem Kontobuch nur neue Transaktionen hinzufügen
  - Einmal geschriebene Transaktionen sind für alle Zeiten festgesetzt
  - Vgl. Datenbanksysteme: Hier stehen die Transaktionen in einem Log, das nicht vor Manipulationen geschützt ist

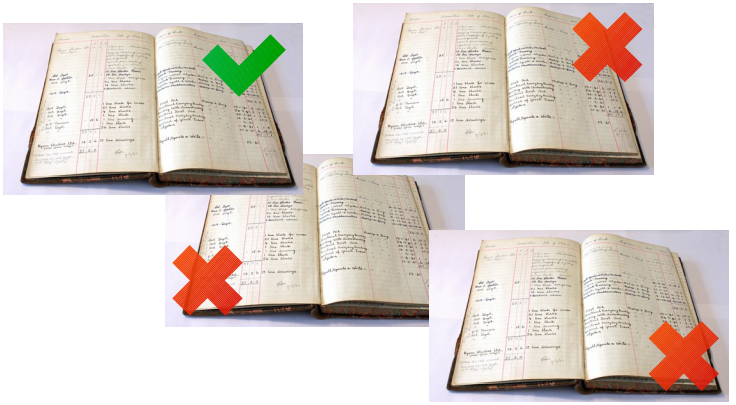
TRANSAKTIONEN

- Abhängig davon, was man mit der Blockchain machen möchte
  - Je nach Implementierung alles, von Smart Contract-Informationen über Bitcoin-Überweisungen bis zum Aktivieren eines Lichtschalters im IoT

- Bitcoin, Ethereum
  - Quell-Account, Bitcoin/Ether-Betrag, Ziel-Account
  - *Anm.: Es gibt IMMER offene Transaktionen (Festschreiben der beim letzten Block erarbeiteten Bitcoins, Ethers)*



VERTEILTER INTEGRITÄTSBEWEIS



- Für jeden Teilnehmer nachvollziehbarer Beweis, dass er im Besitz einer korrekten, aktuellen Kopie des Ledgers ist

Mittlerweile drei große Varianten:

- **Proof of Work**
  - Festschreiben einer Transaktion erfordert Lösen eines ein Hash-Puzzles
    → Rechenleistung vieler Teilnehmer, *energieintensiv aber sehr sicher*
- **Proof of Stake**
  - Festschreiben einer Transaktion über verteilten Konsens-Algorithmus
    → Teilnehmerauswahl bestätigt Korrektheit, *energieeffizient*
- **Proof of Authority**
  - Festschreiben einer Transaktion über verteilten Konsens-Algorithmus
    → Teilnehmer mit hoher Reputation bestätigen Korrektheit, *schnell*

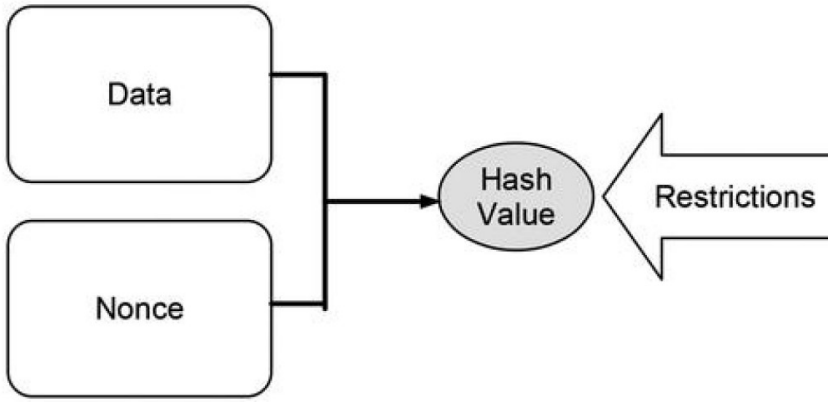
HASH-FUNKTIONEN

- Hash: **unumkehrbare** kryptographische Prüfsumme
  - Wenn sich ein Bit im Input ändert, ändern sich bei guten Hash-Verfahren 50% der Bits in der Prüfsumme
  - Aus der Prüfsumme lässt sich nicht auf den Originaltext zurückschließen
- Beispiel (https://hashgenerator.de)

PROOF OF WORK

Hash-Puzzle liefert Nachweis, dass eine Arbeit geleistet wurde

- Gegeben:
  - Ein zu hashender Text („Challenge“), z.B.: „Hello World!“
  - Eine Beschränkung („Restriction“), die eine Hash-Prüfsumme erfüllen muss, z.B.: Prüfsumme muss mit dem Buchstaben „A“ beginnen
- Gesucht:
  - Eine bestimmte Zeichenfolge („Nonce“), für die gilt:
    der Hashwert von (Challenge + Nonce) erfüllt die Restriction



BEISPIEL HASH-PUZZLE

- Gehasht wird „Hello World!“
- Restriction: Hash soll mit „000“ beginnen
- Nach dem ausprobieren von 615 verschiedenen Nonces ergibt sich ein Hash-Wert, der die Restriction erfüllt

Nonce	Text to Be Hashed	Output
0	Hello World! 0	4EE4B774
1	Hello World! 1	3345B9A3
2	Hello World! 2	72040842
3	Hello World! 3	02307D5F
	…	
613	Hello World! 613	E861901E
614	Hello World! 614	**00068A3C**

- **Difficulty Level**: Die Länge der Restriction
  - kürzere Restrictions sind offensichtlich leichter zu erfüllen
  - Beispiel Bitcoin: Difficulty Level zur Laufzeit so bestimmt, dass das Ausprobieren des richtigen Nonces im Schnitt 10 Minuten dauert, wenn alle gerade aktiven Miner eines Ledgers gemeinsam suchen

MINER

- Rechnerknoten, die *gemeinsam* durch das Lösen von Hash-Puzzles Transaktionen in der Blockchain festschreiben
  - Erhalten als Gegenleistung bei Bitcoin *Bitcoins* und bei Ethereum *Ether*

- Heute üblich
  - Mining auf Grafikkarten
  - Mining auf Spezialhardware
  - Mining durch infizieren von fremden Rechnern mit Mining-Trojanern ;-)

LOHNT SICH DAS?

Rechenbeispiel vom 06.03.2020

- Optimierte Spezialhardware (Antminer S17+)
  - Hash Rate 67TH/s
  - Verbrauch 2680W
  - Anschaffungskosten 2150 EUR (zzgl. Versand)
- Energiekosten
  - 30ct/kWh
- Bitcoins
  - Difficulty Factor 15466098935555
  - Wechselkurs Bitcoins/EUR 8.072,75

- (geschürfte Bitcoins – Energiekosten) pro Tag: -10,53 EUR

https://99bitcoins.com/bitcoin-mining/calculator/
https://www.protact.net/de/bitcoin-miner/76/bitcoin-miner-bitmain-antminer-s17-mit-67-th/s

PROOF OF STAKE

- Für Blockchains im Business-Umfeld (Hyperledger, Quorum) ist das Minen von Hash-Puzzles Energieverschwendung
  - *vertrauenswürdigere Teilnehmer*, kein Beweis durch Arbeit nötig

- Allgemeine Funktionsweise
  - Jeder Teilnehmer verfügt über Coins
  - Zufallsauswahl von Teilnehmern als **Validatoren**
    - Teilnehmer bieten Coins als **Stakes** für das Validieren einer Transaktion
    - Teilnehmer mit mehr Stakes werden wahrscheinlicher als Validator gewählt
  - Quorum über alle Validatoren bestätigt Korrektheit einer Transaktion
    - Validator arbeitet korrekt: erhält Coins als **Belohnung**
    - Validator arbeitet nicht korrekt: Stake wird als **Strafe** einbehalten, Coins weg

  → Practical Byzantine Fault Tolerance (PBFT)-Algorithmus

PROOF OF AUTHORITY

- Für Blockchains im Business-Umfeld ist das Berechnen von Coins Zeitverschwendung
  - Geschlossenes System, Teilnehmer können *zentral verifiziert* werden

- Allgemeine Funktionsweise
  - Eine beschränkte Anzahl von Teilnehmern wird **vorab verifiziert**
    - Datenbank der verifizierten Teilnehmer wird veröffentlicht
  - Zufallsauswahl von *verifizierten* Teilnehmern als **Validatoren**
    - Für jeden neuen Block eine neue **Zufallsauswahl**
  - Quorum über alle Validatoren bestätigt Korrektheit einer Transaktion
    - Validator arbeitet korrekt: Reputation bleibt erhalten
    - Validator arbeitet nicht korrekt: Wenn das öfter passiert, wird Validator aus Datenbank der verifizierten Teilnehmer entfernt

- Sehr schnelles Verfahren

INTEGRITÄTSSICHERUNG DURCH BLOCKCHAIN

WAS BEDEUTET INTEGRITÄT IN DER BLOCKCHAIN?

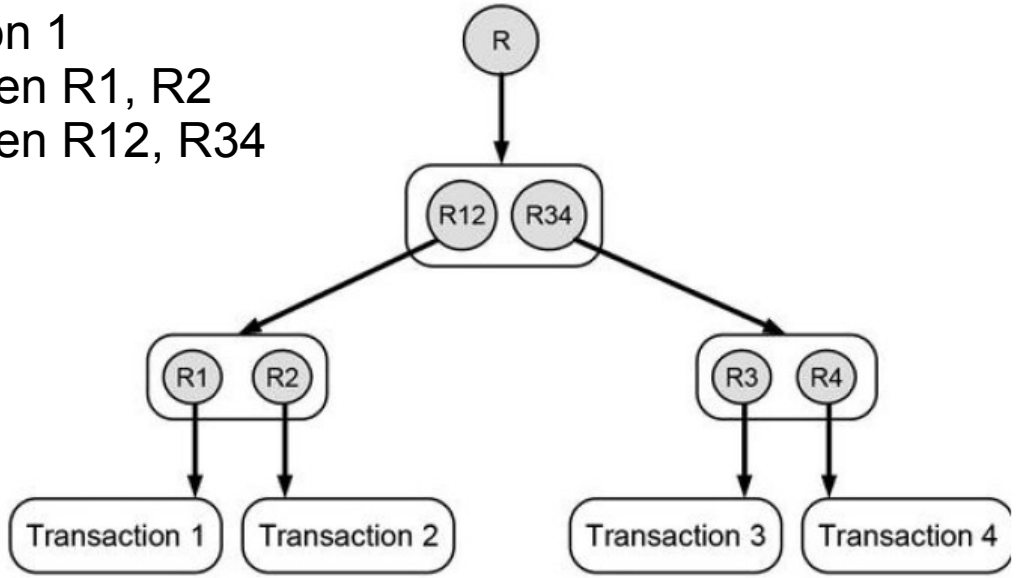
- vgl. Integrität in Datenbanken
  - **referentielle Integrität**
    Fremdschlüssel müssen auf existierende Tupel verweisen
  - **statische Integritätsbedingungen**
    Wertebereichsgrenzen, Unique-Eigenschaften, NOT-Null-Eigenschaften
  - **semantische Integritätsbedingungen**
    anwendungsabhängig, z.B.: Gehalt darf bei einem Update nur größer werden, Termine niemals kleiner als aktuelles Datum, etc.

- Integrität in der Blockchain: Integritätsbedingungen für die Blöcke
  - **statische Integrität**: protokollgerecht ausgefüllte Datenfelder, Nonce ist eine gültige Lösung für Challenge + Restriction, Account ist nicht Null...
  - **semantische Integrität**: kein Double Spending (digitale Objekte aus einer Transaktion können nur einem Teilnehmer gehören), Zeitstempel jünger als der vom Vorgängerblock, etc.

DIE TRANSAKTIONSDATEN

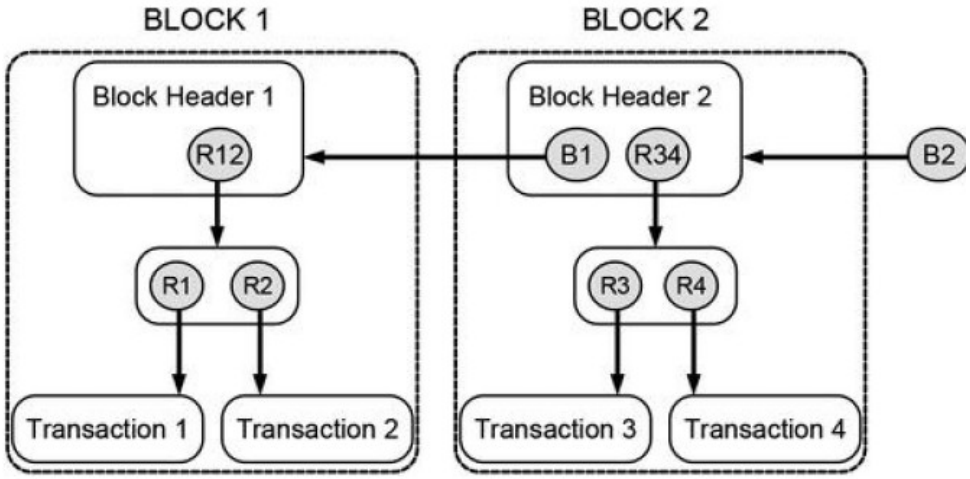
- Organisiert als sog. Merkle-Tree (Hash-Baum)
  - Verweis auf eine Seite mit Transaktionsdaten über die Hash-Prüfsumme der Wurzel („R“)

- Im Bild rechts:
  - R1: Hash von Transaktion 1
  - R12: Hash der Prüfsummen R1, R2
  - R: Hash der Prüfsummen R12, R34



DIE BLOCKCHAIN (1/2)

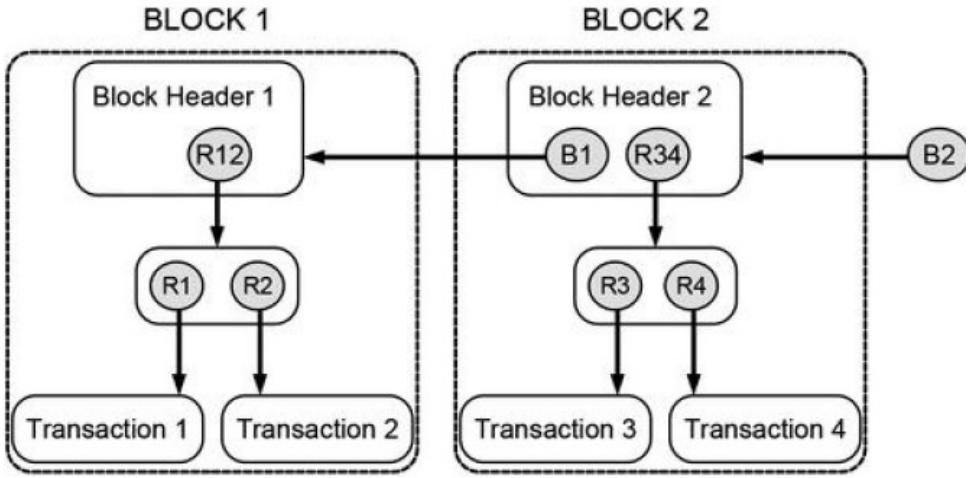
- Verkettete Liste von Datenblöcken



- Jeder Datenblock enthält (vereinfacht)
  - Einen Block-Header
  - Hash-Prüfsumme des vorangegangenen Blocks
  - Transaktionsdaten (verwaltet als Merkle-Tree, auf den mit der Hash-Prüfsumme der Wurzel verwiesen wird)
  - Die eigene Hash-Prüfsumme incl. Nonce

DIE BLOCKCHAIN (2/2)

- Reihenfolge der Blöcke
  - Sichergestellt durch Verlinkung
- Integrität der Blöcke
  - Sichergestellt durch Hash-Prüfsumme

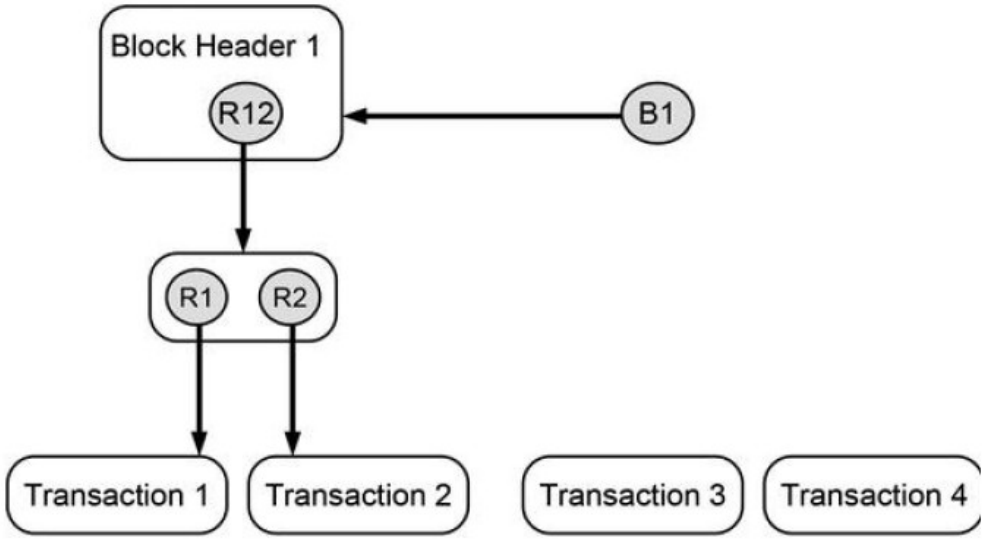


- Integrität der Transaktionshistorie
  - Sichergestellt, indem jeder Block eine Hash-Prüfsumme des vorangegangenen Blocks mit hasht

- *Wie funktioniert das Einfügen?*

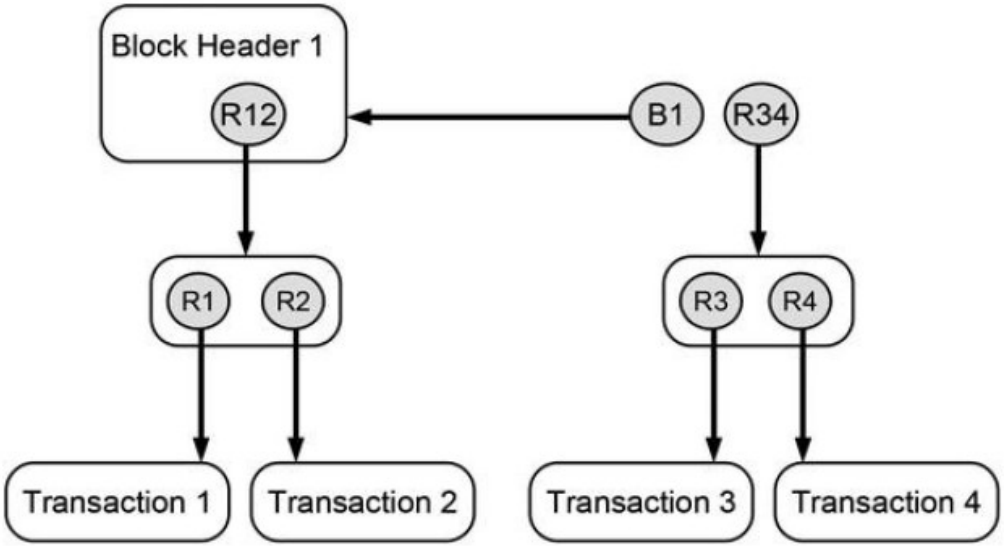
BLOCK HINZUFÜGEN

- Ausgangspunkt
  - Es existiert Block 1 mit Hash-Prüfsumme B1
  - Zwei neue Transaktionen 3, 4 sollen hinzugefügt werden



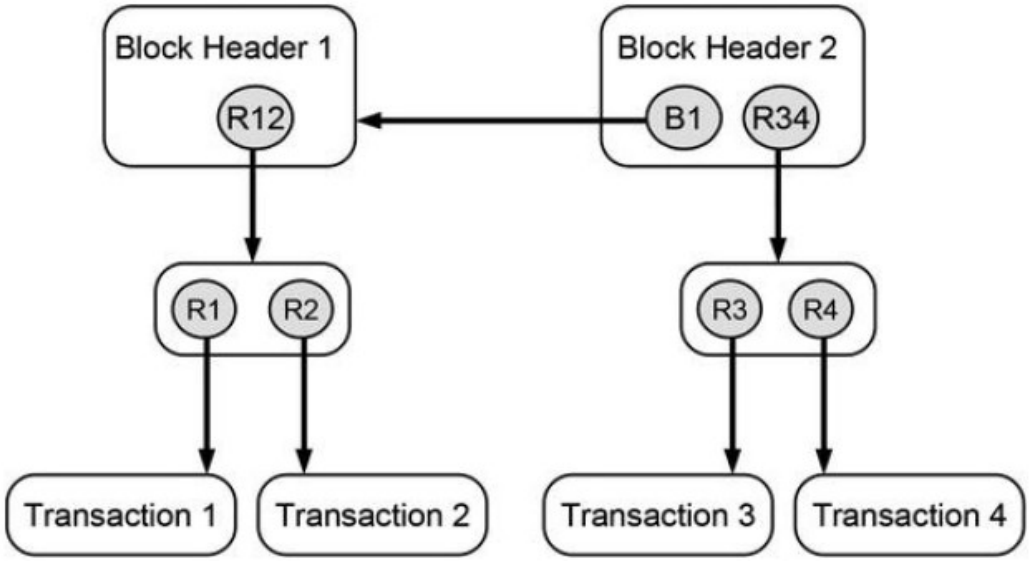
BLOCK HINZUFÜGEN

- Schritt 1: Merkle-Tree der neuen Transaktionen aufbauen
  - Hash-Prüfsummen für die Transaktionen berechnen (R3, R4)
  - Hash-Prüfsumme für die eben bestimmten Prüfsummen berechnen (R34)



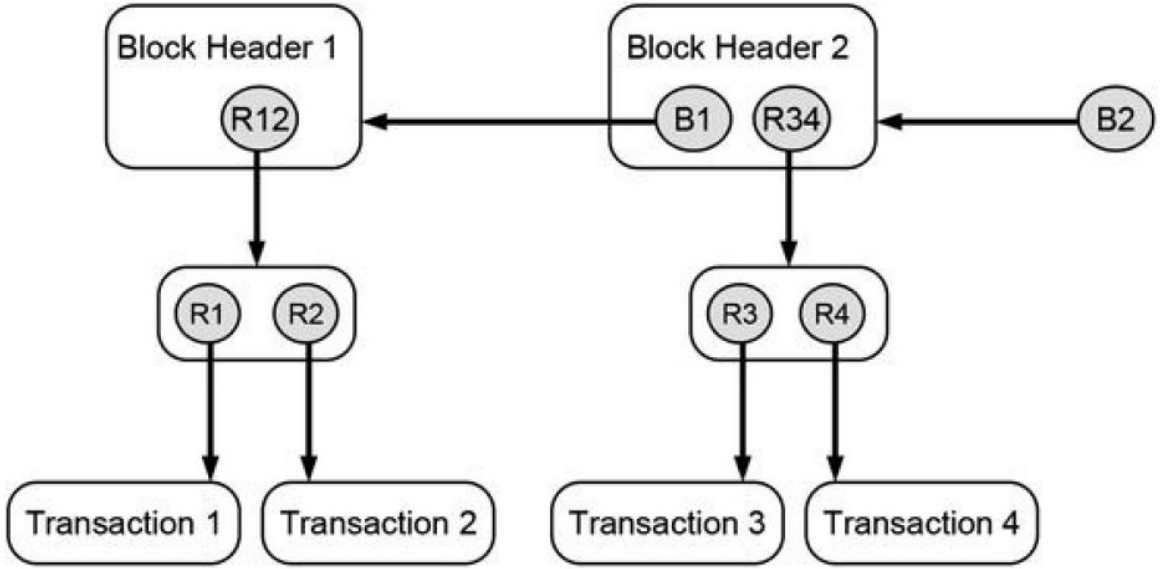
BLOCK HINZUFÜGEN

- Schritt 2: Block-Header bestimmen
  - Header enthält Wurzel des Merkle-Trees (R34) sowie Prüfsumme B1 des vorangegangenen Blocks



BLOCK HINZUFÜGEN

- Schritt 3: Neue Hash-Prüfsumme für Block 2 bestimmen
  - Dies ist bei Blockchain, Ethereum der Mining-Prozess, bei dem ein Hash-Puzzle gemeinsam von vielen Knoten als Proof-of-Work gelöst werden muss → *aufwendig und teuer*

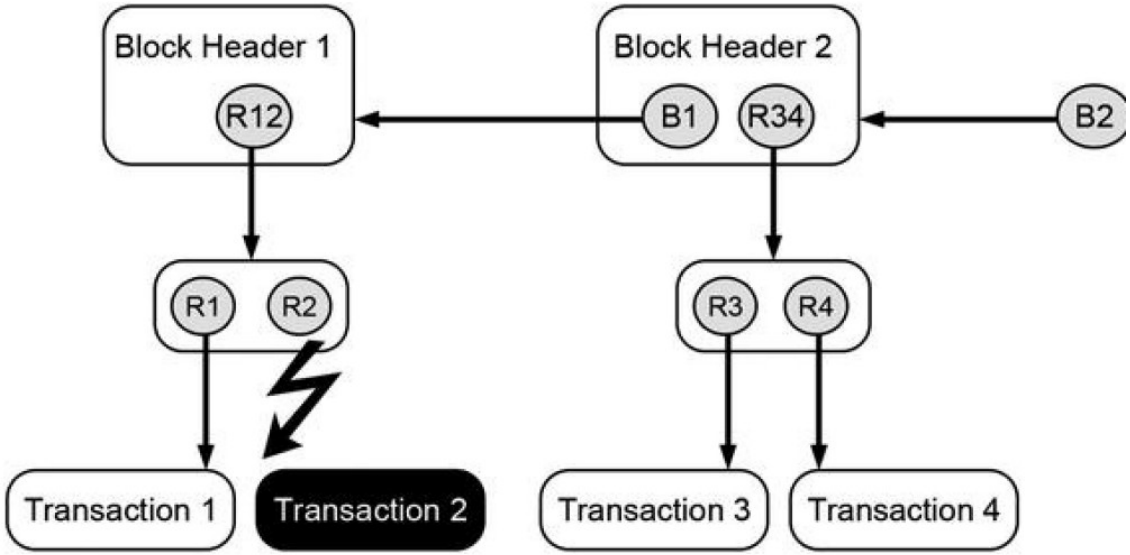


INTEGRITÄT DER BLOCKCHAIN

- Angreifer (böswilliger Knoten) könnte folgendes versuchen:
  1) Manipulation der Transaktionsdaten
  2) Manipulation der Referenzen im Merkle-Tree
  3) Ersetzen von Transaktionen
  4) Manipulationen der Wurzel des Merkle-Trees (Link zum Block)
  5) Manipulation der Reihenfolge der Blöcke

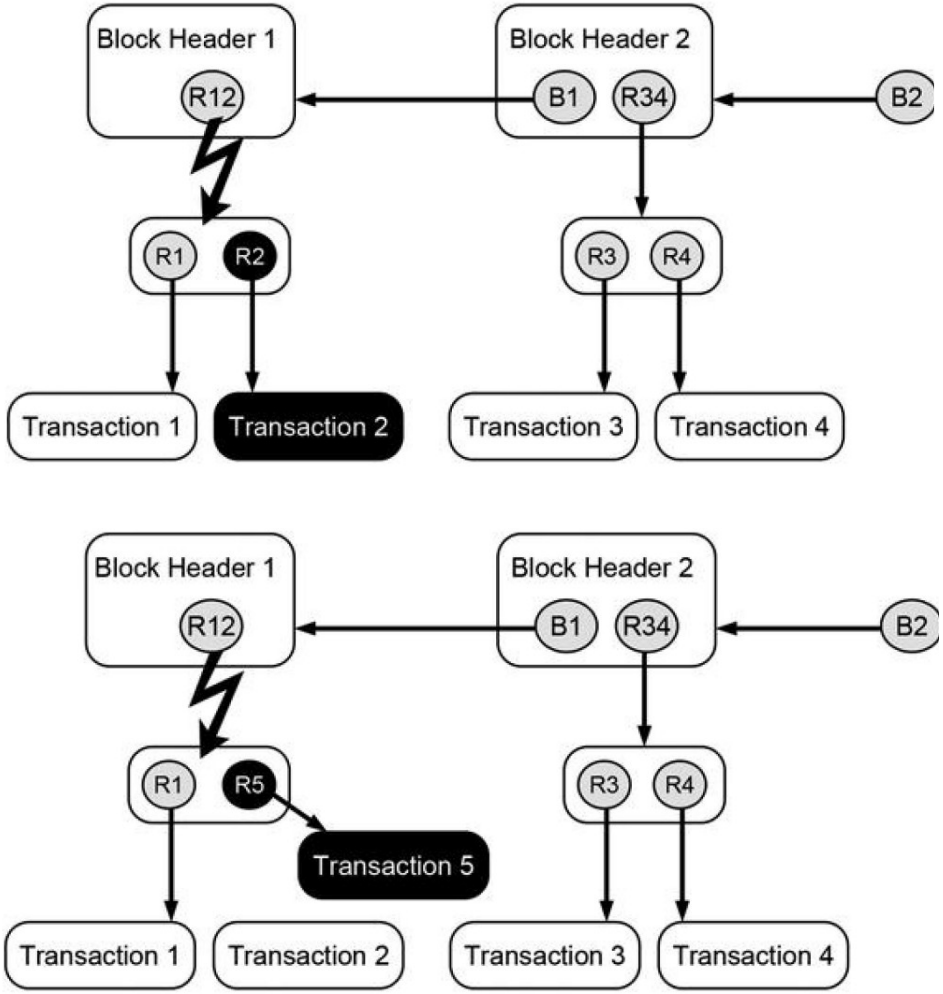
MANIPULATION VON TRANSAKTIONSDATEN

- Prüfsumme R2 stimmt nicht mehr,
  also stimmt auch Prüfsumme R12 nicht mehr,
  dann ist Prüfsumme B1 ebenfalls inkorrekt
  → *lässt sich erkennen*, manipulierte Kopie der Blockchain
  wird von den anderen Teilnehmern verworfen



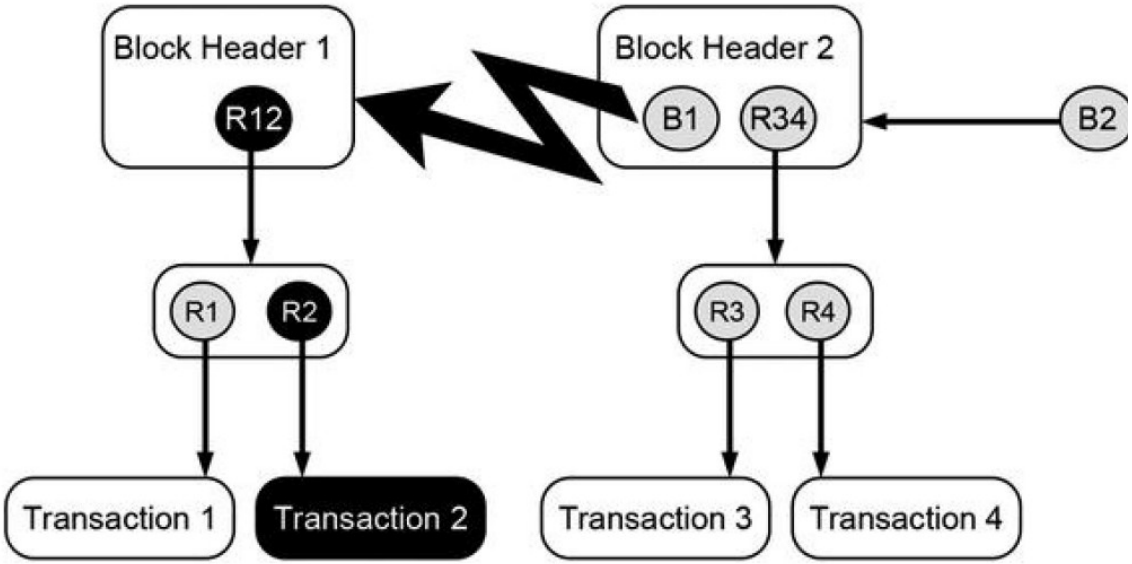
MANIPULATION VON REFERENZEN IM MERKLE-TREE ODER AUSTAUSCHEN EINER TRANSAKTION

- Prüfsumme R12 ist nicht mehr korrekt, dann ist Prüfsumme B1 ebenfalls inkorrekt
  → *lässt sich erkennen*



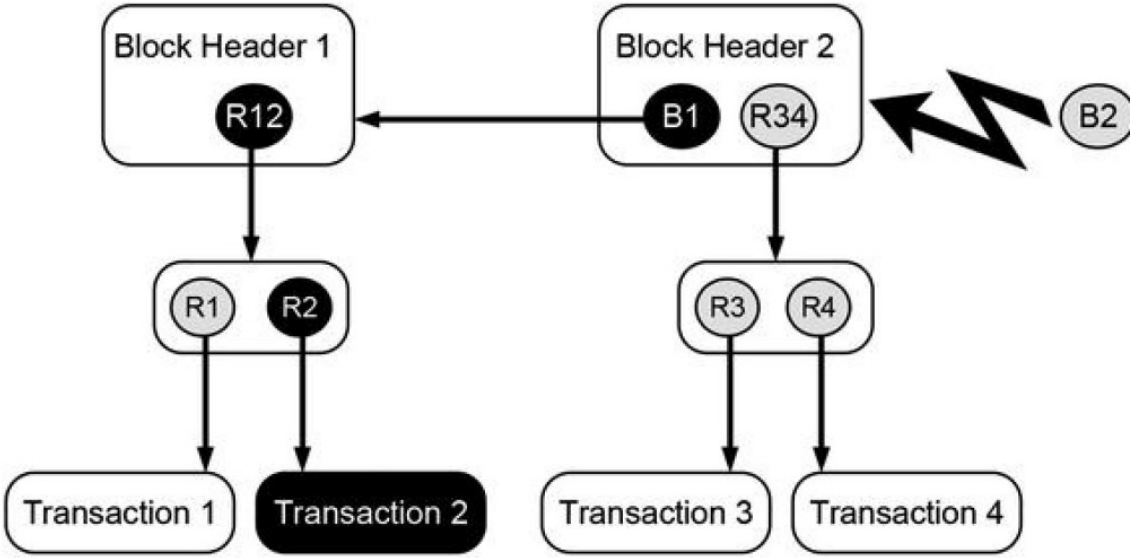
MANIPULATIN DER WURZEL DES MERKLE-TREES

- Da der Block-Header jeweils eine Prüfsumme (B1) des vorangegangenen Blocks enthält, zerstört diese Manipulation die Transaktionshistorie
  → *lässt sich erkennen*



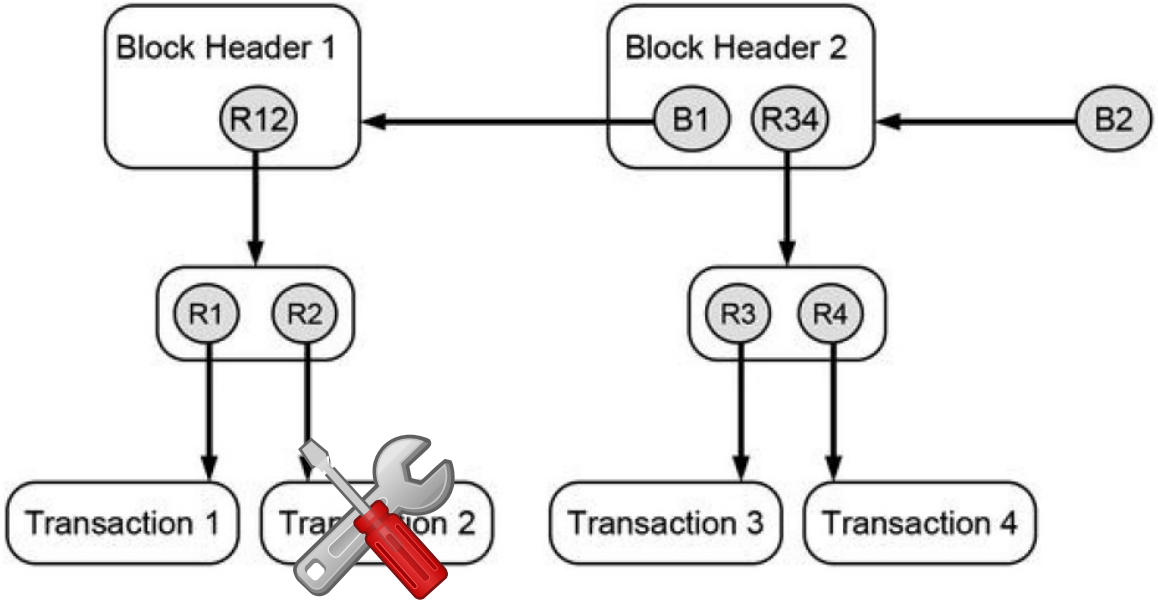
MANIPULATION DER BLOCK-ABFOLGE

- Änderungen innerhalb einer Blockchain verhindert die Prüfsumme
  → *lässt sich erkennen*
- Einschleusen eines neuen Headers (B2) mit gefälschter Blockchain möglich, wenn man 51% aller Knoten überzeugt, dass die gefälschte Blockchain die gültige ist
  → *unwahrscheinlich für große Netze*



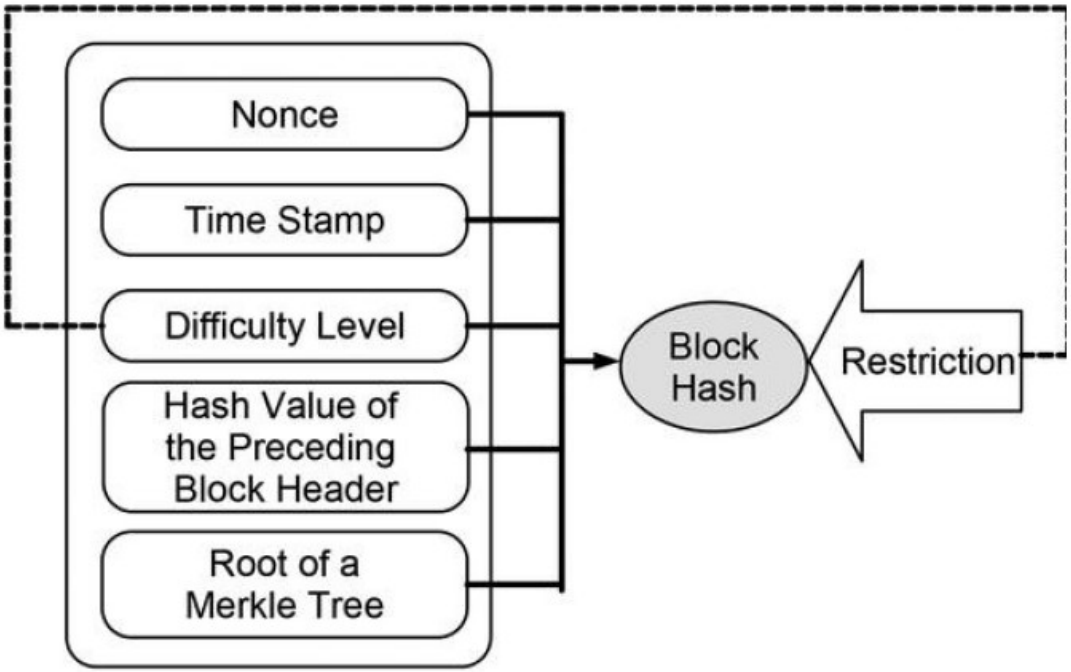
FRAGE AN SIE

- Angenommen, ein Angreifer möchte Transaktion 2 manipulieren.
- Was hält den Angreifer davon ab, einfach die Prüfsummen R2, R12, B1 und B2 neu zu berechnen und zu behaupten, seine Kopie der Blockchain ist der gültige Ledger?



MINING EINES NEUEN BLOCKS

- Hole die Wurzel des Merkle-Trees, den Hash des Vorgängerblocks und einen Zeitstempel
- Bestimme den Difficulty Level aus der Zahl der aktiven Miner
- Alle Miner gemeinsam lösen das Hash-Puzzle (suchen den richtigen Nonce durch ausprobieren)
- Füge den Nonce zum Block hinzu, Hash ist nun Referenz auf diesen Block



VALIDIERUNG EINES BLOCKS

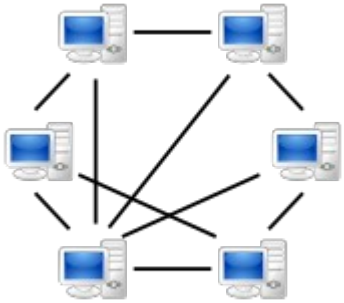
- Jeder Block-Header
  - korrekte Hash-Referenz auf den Vorgängerblock
  - korrekte Hash-Referenz als Wurzel des Merkle-Trees
  - enthält einen Nonce
  - enthält Difficulty Level/Restriction, der zum eigenen Hash/Nonce passt
  - Timestamp ist neuer als der vom Vorgängerblock

https://blockchain.info/de

← Diese Anzeige läuft rückwärts, wenn Blöcke verworfen werden

DEZENTRALE VERWALTUNG DER BLOCKCHAIN

PEER-TO-PEER SYSTEMARCHITEKTUR



- Jeder Node kann gleichberechtigt an der Blockchain teilnehmen

- Drei zentrale Aufgaben
  - Bestimmtung des gültigen Heads eines Ledgers, Validierung von Blöcken
  - „Minen“ von neuen Blöcken
  - Kommunikation mit den Peers, Weiterleiten von neuen Blöcken

MINEN VON NEUEN BLÖCKEN

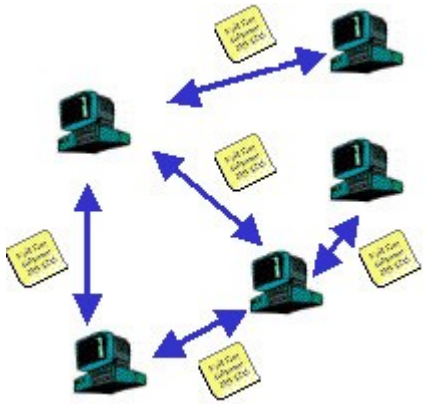
- Mining ist eine kollektive Aufgabe
  - Kein einzelner Node darf in der Lage sein, allein gültige Hash-Nonce-Kombinationen zu erzeugen!

- *Warum sollten sehr viele Nodes gemeinsam Hash-Puzzles korrekt lösen, damit irgendwer seine Transaktion festschreiben kann?*
  - **Belohnung** („Reward“)
    - Bitcoins oder Ether als Bezahlung für die geleistete Rechenarbeit beim einreichen eines gültigen Blocks
  - **Bestrafung** („Punishment“)
    - Aberkennen der Belohnung für Blöcke, die nicht validiert wurden

    (mehr dazu im Folgenden)

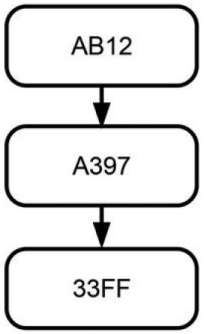
KOMMUNIKATION MIT DEN PEERS

- Gossip-Protokoll (to gossip = „tratschen“)
  - Jeder Peer leitet neue Blöcke und neue Transaktionsdaten an alle seine Kontakte weiter
  - Nachrichten, die ein Peer bereits von anderen erfahren hat, werden anhand des Zeitstempels als Duplikat erkannt und verworfen
  - Peers, die sich neu anmelden oder eine Zeitlang offline waren erhalten eine vollständige Kopie der Blockchain

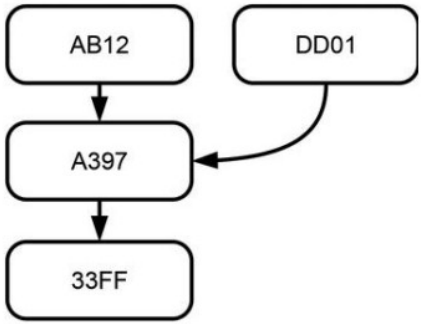


- Schnell und einfach, aber keine Garantie,
  - dass Blöcke bei jedem Peer in der gleichen Reihenfolge ankommen
  - dass Nachrichten ohne Verzögerung jeden Peer erreichen
  - dass Nachrichten überhaupt bei allen Peers ankommen

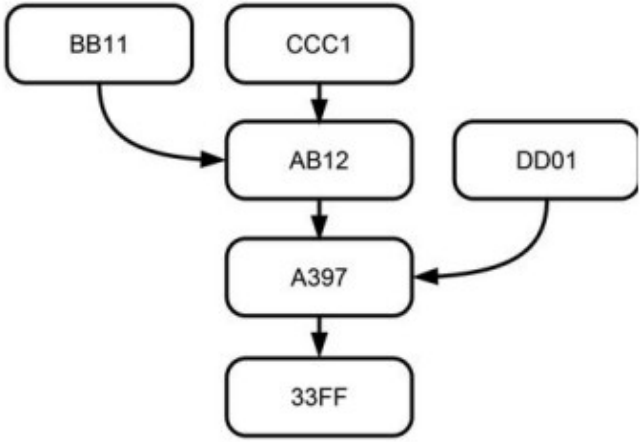
TYPISCHE FÄLLE



1. Blockchain nach dem Hinzufügen von drei Blöcken



2. Nachricht über Block AB12 verzögert, andere Nodes haben bereits Block DD01 erstellt

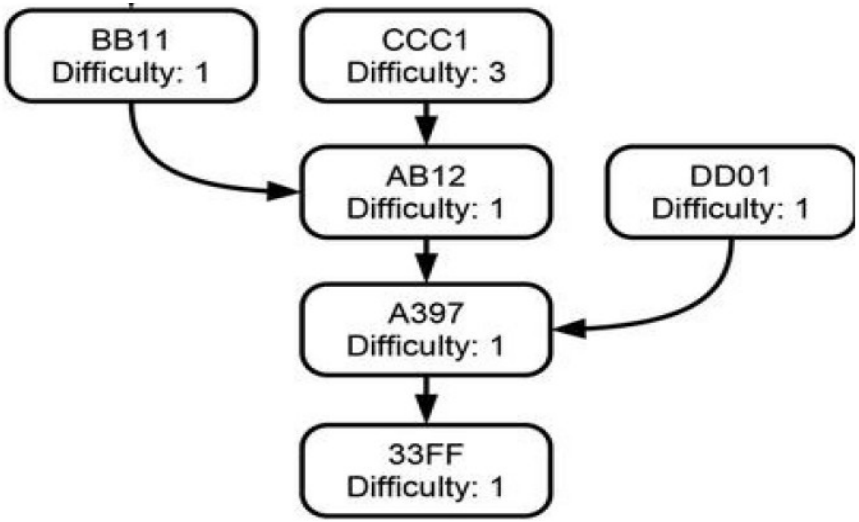


3. Zwei unabhängige Gruppen von Nodes haben zur gleichen Zeit zwei unterschiedliche Nachfolger für AB12 erstellt

Welches ist der gültige Head der Blockchain?

ZWEI KRITERIEN ZUR BESTIMMUNG DES HEADS

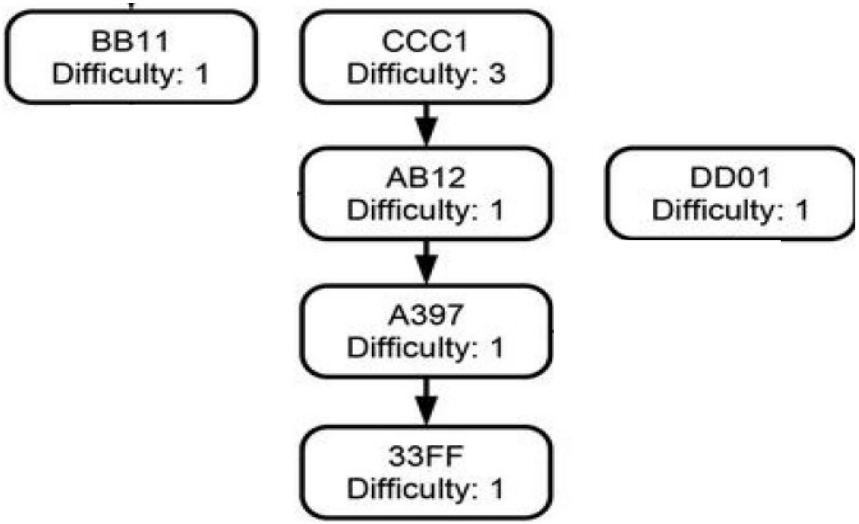
- **Longest Chain**
  - Die Kette mit der größten Länge gewinnt
  - Im Beispiel verliert DD01→A391→33FF
- **Heaviest Chain**
  - Die Kette, deren Summe der Difficulty Levels am größten ist, gewinnt
  - Im Beispiel ist das CC1→AB12→A397→33FF



KONSEQUENZEN

- Es entstehen verwaiste Blöcke
  - für die den Erstellern die Belohnung (Bitcoins) wieder entzogen wird

- Integrität durch Majority-Vote
  - BB11 und CCC1 gleichzeitig abgeschlossen, aber CCC1 hatte schwierigeres Puzzle
    → Nachweis dafür, dass Mehrheit für CC1!



- **Ökonomische Anreize**
  1) Zur Mehrheit zu gehören, die die Bitcoin-Belohnung erwirbt
  2) Zu den Knoten zu gehören, die am schnellsten einen neuen Block einreichen und damit gewählt werden
  3) Keine ungültigen Blöcke oder Blöcke mit niedriger Difficulty einzureichen

ERGEBNIS: JEDER KNOTEN KENNT ZWEI ZUSTÄNDE

1) Validieren von neuen Blöcken
   - So schnell wie möglich, um nicht ein Hash-Puzzle für einen veralteten oder ungültigen Block zu erstellen

2) Erstellen eines neuen Blocks
   - Ebenfalls so schnell wie möglich, damit niemand anderes einen neueren Block mit höherer Difficulty einreicht

   - *Anm.: Durch das Belohnungssystem gibt es immer neue Transaktionen im Pool, die erworbene Coins festschreiben müssen. Es gibt keinen Idle-Zustand, in dem die Blockchain nichts zu tun hat.*
   - *Anm. zur Anm.: Gilt nur für Bitcoin, Ethereum. Blockchains im Business-Umfeld binden Integrität nicht an die aufgewendete elektrische Energie, sondern verwenden einen Proof of Stake-Algorithmus*

DISKUSSION

GEGENÜBERSTELLUNG VON ANFORDERUNGEN UND LÖSUNGEN

- Beschreibung des Besitzes von digitalen Gütern
- Integritätssicherung
- Verteilung des Ledgers
- Hinzufügen von Transaktionen
- Kollektive Entscheidung, welcher Ledger der gültige ist

- Historie der Transaktionen im Ledger
- Prüfsummen mit Hash-Puzzle, dadurch unveränderliche Historie
- Forwarding im P2P-Netz
- Blockchain-Algorithmus, kollektives Mining der Nonces
- Longest Chain, Heaviest Chain zur verteilten Konsensfindung

51%-ANGRIFF

- Ein 51%-Angriff ist ein Versuch, die Mehrheit beim Voting-Prozess für einen gültigen Blockchain-Head zu stellen
  - Ziel
    - Über Heaviest-Chain Regel den Wahlausgang bestimmen
  - Nötige Ressourcen/Fähigkeiten
    - Mehr Rechenleistung unter Kontrolle als alle anderen Knoten zusammen
    - Störung der Kommunikation, Angriffe auf andere Knoten, etc.

- Lässt sich prinzipiell nicht verhindern, aber...
  - Betrifft nur die neuesten Blöcke, da der Angreifer sonst eine lange Kette aller Hash-Puzzles gelöst haben müsste, bevor alle anderen Knoten einen neuen Block erstellt haben
  - Wird schwerer, je mehr Teilnehmer an der Blockchain beteiligt sind

GRENZEN DER BLOCKCHAIN (1/3)

- Keine Privatheit
  - Komplette Transaktionshistorie ist jedem Node bekannt
  - Wer weiß, wem ein öffentlicher Schlüssel gehört, kann dessen komplette Transaktionshistorie einsehen
  - Unverzichtbar für die Validierung, also auch nicht „mal rasch“ änderbar
  - Mögliche Lösungen
    - Transaktionsdaten verschlüsseln, Verhindern von „Double Spending“ durch Secure Multiparty Computation-Techniken
    - Nutzung mehrerer Accounts
      (alles nicht wirklich überzeugend)

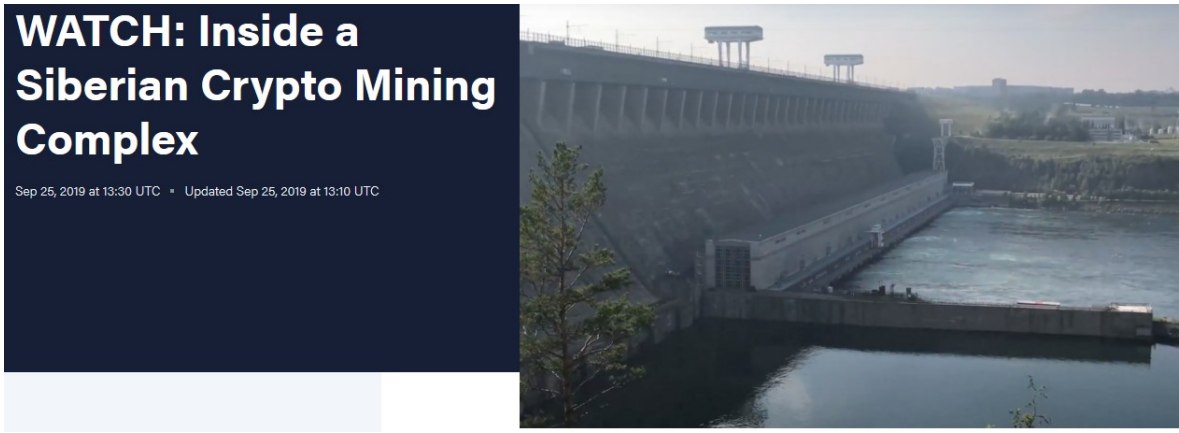
- Sicherheitsmodell ohne 2-Faktor-Authentifizierung
  - Identität ausschließlich über Public/Private Key
  - Wenn der private Key eines Accounts verlorenging oder öffentlich bekannt wurde, ist der Account verloren

GRENZEN DER BLOCKCHAIN (2/3)

- Skalierbarkeit
  - Blockchain ist append-only, wächst mit jeder Transaktion
  - Das Lösen von Hash-Puzzles ist notwendigerweise langsam
  - Mögliche Lösungen
    - Protokollerweiterung: Abschneiden der Blockchain, Neustart mit einem Ledger-Stand, zu dem alle Knoten zustimmen
    - Anstelle von Proof-of-Work in Form von Hash-Puzzles andere Verfahren zur Konsensbildung, PBFT-Algorithmus
      (*Anm.: funktioniert nur in kontrollierten Umgebungen*)
- Hohe Kosten
  - Enormer Energieverbrauch für das Minen von neuen Blöcken (Stand 2019: Bitcoin allein braucht ca. 46 TWh/Jahr, entspricht 22 Mio. t CO2)
  - Gleiches Problem wie bei Skalierbarkeit

GRENZEN DER BLOCKCHAIN (3/3)

- Versteckte Zentralität
  - Bitcoin-Mining findet zentral statt wo die Energie billig ist
  - Teilnahme unattraktiv für Personen mit Standardhardware



  - Widerspricht der Integritätssicherung per Mehrheitsentscheid
- Unflexibel
  - Komplexes Ökosystem aus Signaturverfahren, Protokollen, Hash-Funktionen etc. darf sich über Lebenszeit der Blockchain nicht ändern
- Kritische Minimalgröße
  - In kleinen Systemen ist die Mehrheit ebenfalls relativ klein
  - Finanzstarker Angreifer kann 51%-Angriffe fahren

The Register®
Biting the hand that feeds IT

Emergent Tech

Blockchain study finds 0.00% success rate and vendors don't call back when asked for evidence

Where is your distributed ledger technology now?

By Andrew Orlowski 30 Nov 2018 at 11:56 60 SHARE ▼

Though Blockchain has been touted as the answer to everything, a study of 43 solutions advanced in the international development sector has

ZUSAMMENFASSUNG

ZUSAMMENFASSUNG

- Blockchain ist ein Ansatz zur Integritätssicherung in einem dezentralen System aus nicht vertrauenswürdigen Knoten
  - Ökonomische Anreize zur ehrlichen Teilnahme und zum Einbringen möglichst vieler eigener Ressourcen
  - Abstimmungsverfahren zur Identifikation des korrekten Systemzustands
  - Unveränderliche Transaktionshistorie zur Integritätssicherung

- Einige (schwerwiegende!) Einschränkungen
  - Privatheit
  - Skalierbarkeit/Energieverbrauch
  - Unflexibel, problematisches Sicherheitsmodell

MÖGLICHE PRÜFUNGSFRAGEN

- Wie wird ein neuer Block zur Blockchain hinzugefügt?
- Wie funktionieren Hash-Puzzles? Welche Bedeutung haben sie für die Integritätssicherung in Blockchains?
- Erklären Sie, wieso es für die Integrität der Blockchain problematisch ist, wenn große Mining-Farmen ihre Ressourcen in den Mining-Prozess einbringen.
- Welche Bedeutung hat der Difficulty Level für die Identifikation des gültigen Ledgers?
- Welche Gründe gibt es dafür, dass Transaktionen manchmal zurückgezogen werden, obwohl alle Miner korrekt gearbeitet haben?

LITERATUR

[1] BASHIR, Imran. *Mastering Blockchain*. Packt Publishing Ltd, 2017.

[2] DRESCHER, Daniel. *Blockchain Basics*. Apress, 2017.