Themen zur Computersicherheit

Bitcoins

PD Dr. Reinhard Bündgen
buendgen@de.ibm.com

Was sind Bitcoins?

- Digitale Währung / Digitales Geld
- ohne verantwortliche Instanz (Staat, Banken)
- basiert auf Kryptographie und einem verteiltem Protokoll
- 2008 in White Paper „Bitcoin: A Peer-to-Peer Electronic Cash System“ von Satoshi Nakamoto (Pseudonym) beschrieben
- Maximale Geldmenge: 21 M BTCs (2041)
- kleinste Einheit 10^{-8} BTC = 1 Satoshi

Herausforderungen an Digitale Währungen

- Wert: wer versichert, dass man für Bitcoins Waren einkaufen kann?
- Autorisierung einer Zahlung: Wie wird sicher gestellt, dass nur der Besitzer von Bitcoins diese ausgibt
- Fairness: Wie wird sicher gestellt, dass dasselbe Geld nicht mehrfach ausgegeben wird?
- Wie wird die Reihenfolgen von Transaktionen festgelegt?
- Reklamationen: Wie kann ich fehlerhafte Buchungen reklamieren?
- Anonymität: Können die Teilnehmer von Transaktionen geheim bleiben?
- Anreiz: Welche Motivation unterliegt dem Betrieb der Bitcoin Infrastruktur?

Herausforderungen an Digitale Währungen Kurzantworten

- Wert: wer versichert, dass man für Bitcoins Waren einkaufen kann?
  - niemand, alleine das Vertrauen, dass jemand Bitcoins als Zahlungsmittel akzeptiert
- Autorisierung einer Zahlung: Wie wird sicher gestellt, dass nur der Besitzer von Bitcoins diese ausgibt
  - digitale Signaturen
- Fairness: Wie wird sicher gestellt, dass dasselbe Geld nicht mehrfach ausgegeben wird?
  - Blockchain-Konsenzverfahren (Majorität der Arbeitsleistung)
- Wie wird die Reihenfolgen von Transaktionen festgelegt?
  - Blockchain-Konsenzverfahren (Majorität der Arbeitsleistung)
- Reklamationen: Wie kann ich fehlerhafte Buchungen reklamieren?
  - gar nicht, es gibt keine (zentrale) Beschwerdeinstanz, Checksummen sollen helfen Fehler zu vermeiden
- Anonymität: Können die Teilnehmer von Transaktionen geheim bleiben?
  - das System ist nicht anonym, es werden Pseudonyme unterstützt
- Anreiz: Welche Motivation unterliegt dem Betrieb der Bitcoin Infrastruktur?
  - Mining und Transaktionsgebühren

Transaktionen & Journal (Ledger)

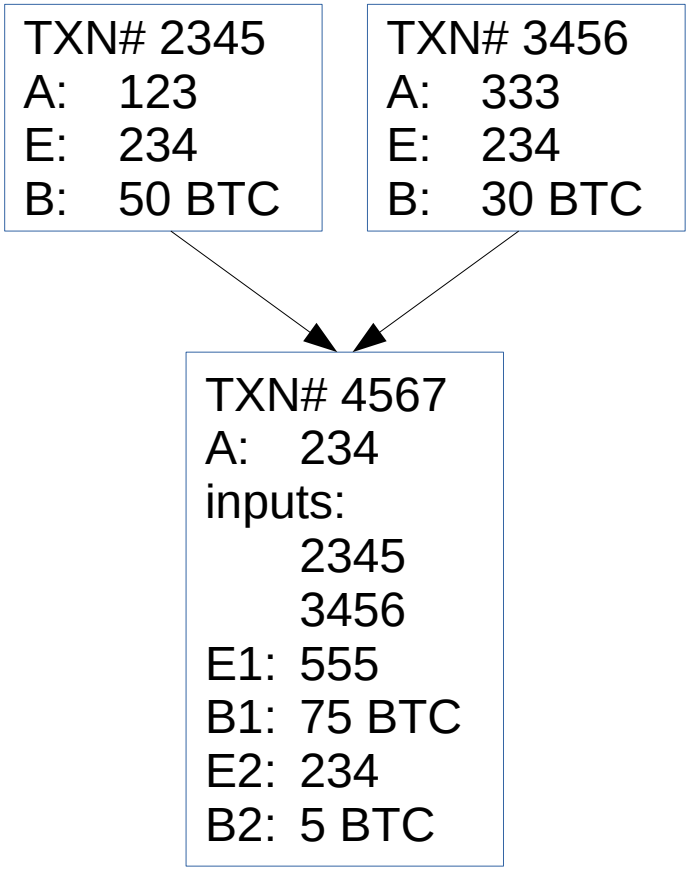
- Journal / Kontenbuch
  - engl. ledger
  - beschreibt Kontostände aller Teilnehmer
- Transaktion:
  - Überweisung von Bitcoinbeträgen an ein oder mehrere Empfänger
  - ändert Kontostände von Überweiser und Empfänger

Teilnemer	Kto-Stand
239472937	100
327497233	2000,3
327492374	0,05
234934990	1234

Überweisung
TXN# 1234
Auftraggeber: 879739742
Empfänger1: 98748927
Betrag1: 100 BTC
Empfänger2: 23794534
Betrag2: 0,1 BTC
Unterschrift

Darstellung von Journal und Transaktionen

- Transaktion
  - verbraucht (spends) ein oder mehrere ganze Überweisungen an Auftraggeber
  - Restbeträge kann Auftraggeber an sich zurück überweisen
- Journal:
  - Kette aller getätigten Transaktionen (zeitl. geordnet)
  - Kontostände müssen nachgerechnet werden
  - enthält Index nicht-verbrauchter Transaktionen



Absicherung von Transaktionsketten

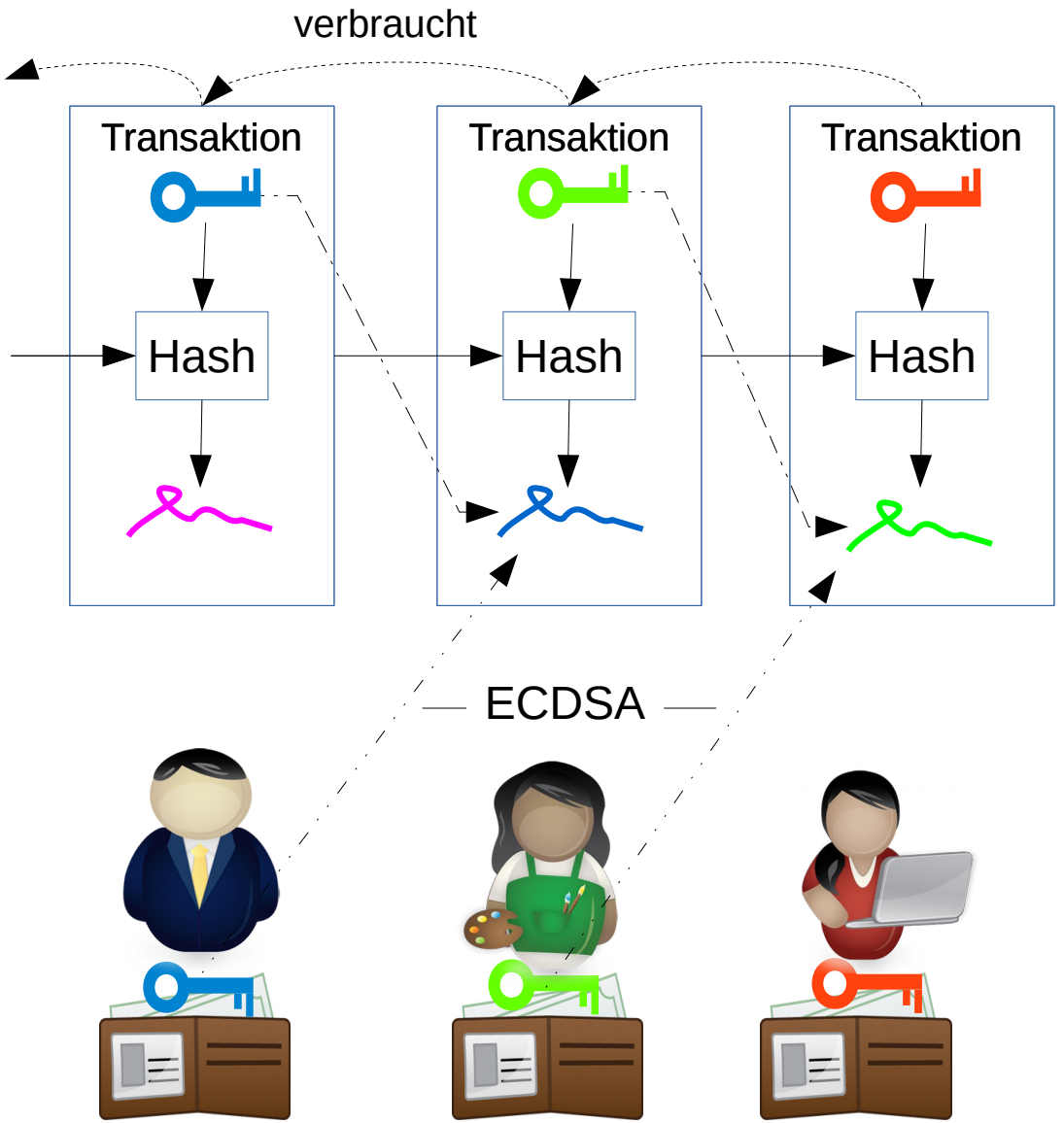
- Jeder Nutzer hat einen privaten Schlüssel
- öffentliche Schlüssel bezeichnen Empfänger
- TXN enthält Hash der verbrauchten Eingabe-TXN und des (öffentlichen Schlüssels des) Empfängers
- Auftraggeber unterschreibt Hash in TXN mit seinem privaten Schlüssel und bestätigt damit die Eingabe-TXN als verbraucht
- die Unterschrift einer TXN kann mit Hilfe verbrauchter TXN verifiziert werden

Absicherungen

- Nur Empfänger einer TXN kann diese verbrauchen
- TXN kann von keinem dritten geändert werden

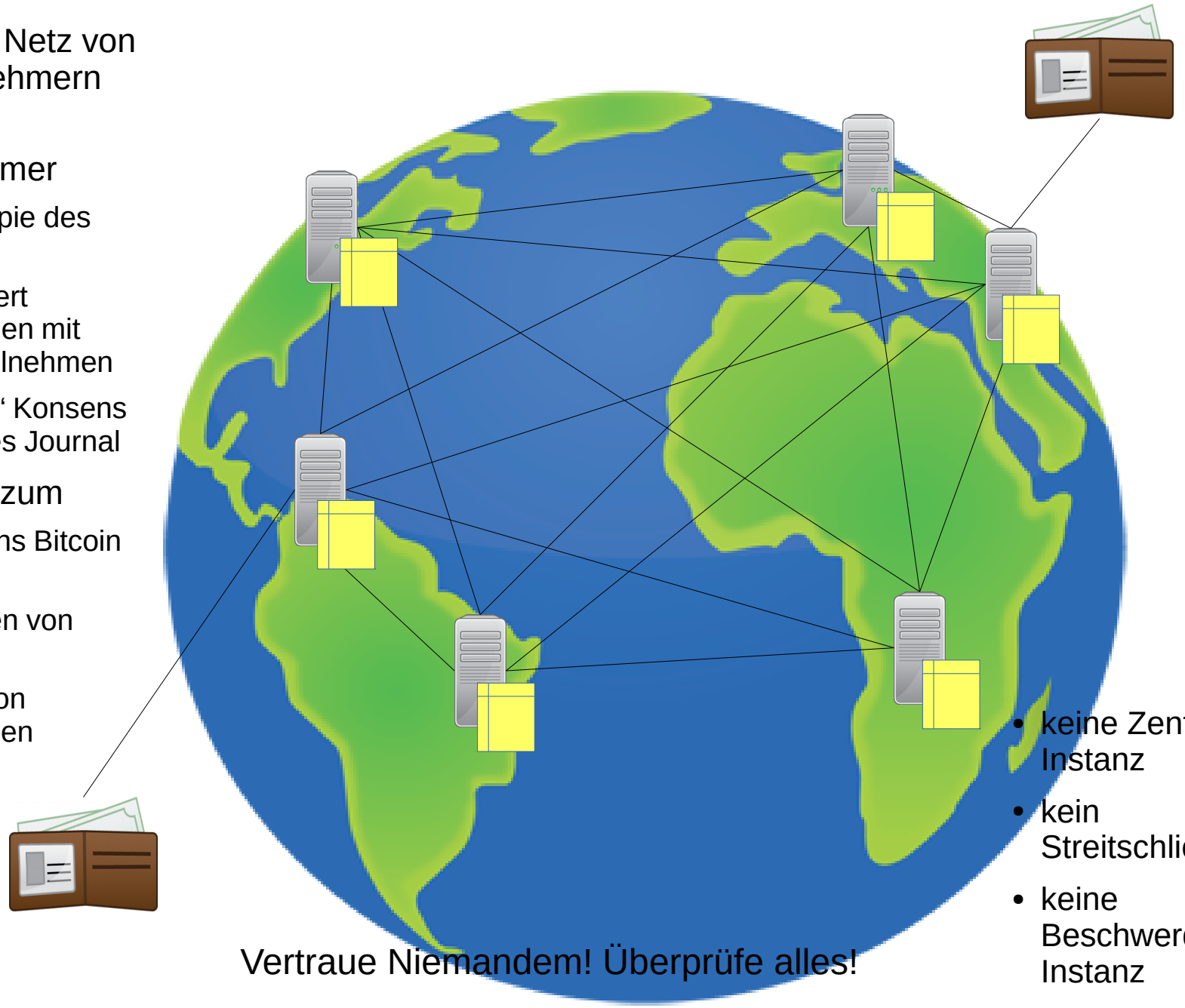
Offen

- Wie kann vermieden werden, dass eine TXN mehrfach verbraucht wird (z.B kopiert wird)?



Bitcointnetz

- peer-to-peer Netz von Bitcoin Teilnehmern (nodes)
- jeder Teilnehmer
  - hat eine Kopie des Journals
  - Kommuniziert Transaktionen mit anderen Teilnehmen
  - „verhandelt“ Konsens über gültiges Journal
- Wallets: SW zum
  - einwählen ins Bitcoin Netz
  - aufbewahren von Bitcoins
  - anstoßen von Transaktionen

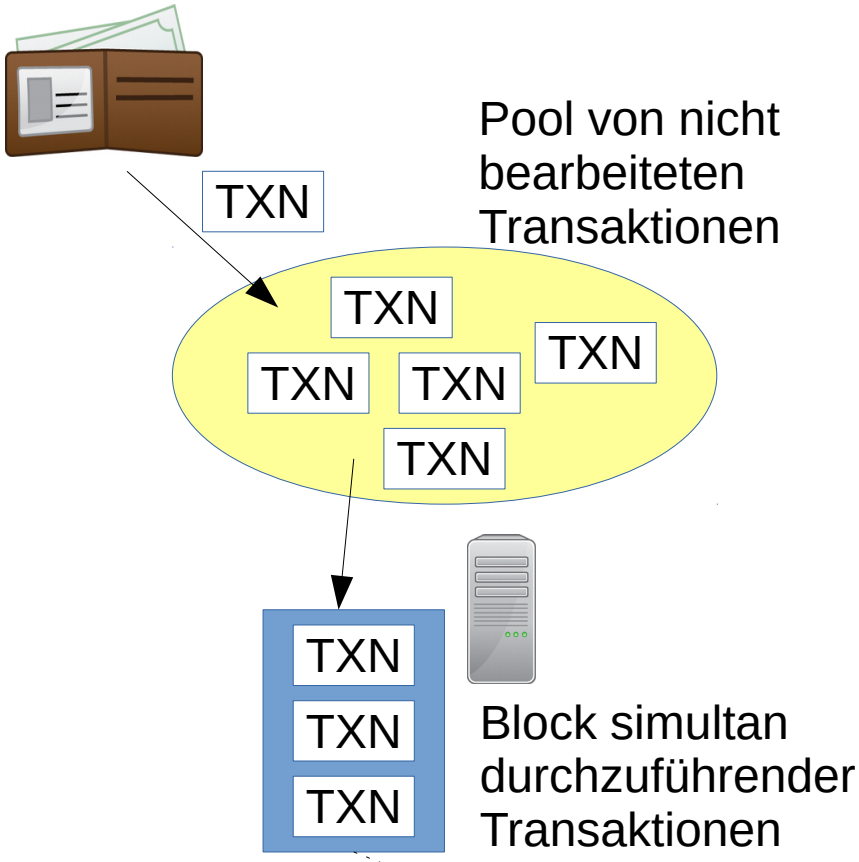


- keine Zentrale Instanz
- kein Streitschlichter
- keine Beschwerde Instanz

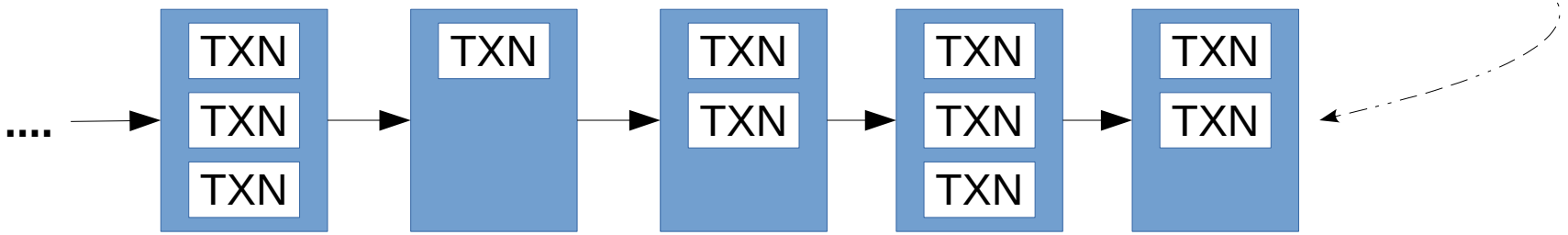
Vertraue Niemandem! Überprüfe alles!

Verarbeitung von Transaktionen

- Klient stößt Transaktion an
  - ➔ Pool von wartenden (nicht bestätigten) Transaktionen
- Bitcoin Rechner
  - nimmt Menge von Transaktionen aus Pool
  - „verarbeitet“ Menge von Transaktionen als gleichzeitig durch geführt
  - hängt sie an Blockkette (= Journal) an



Journal = Blockkette (block chain)

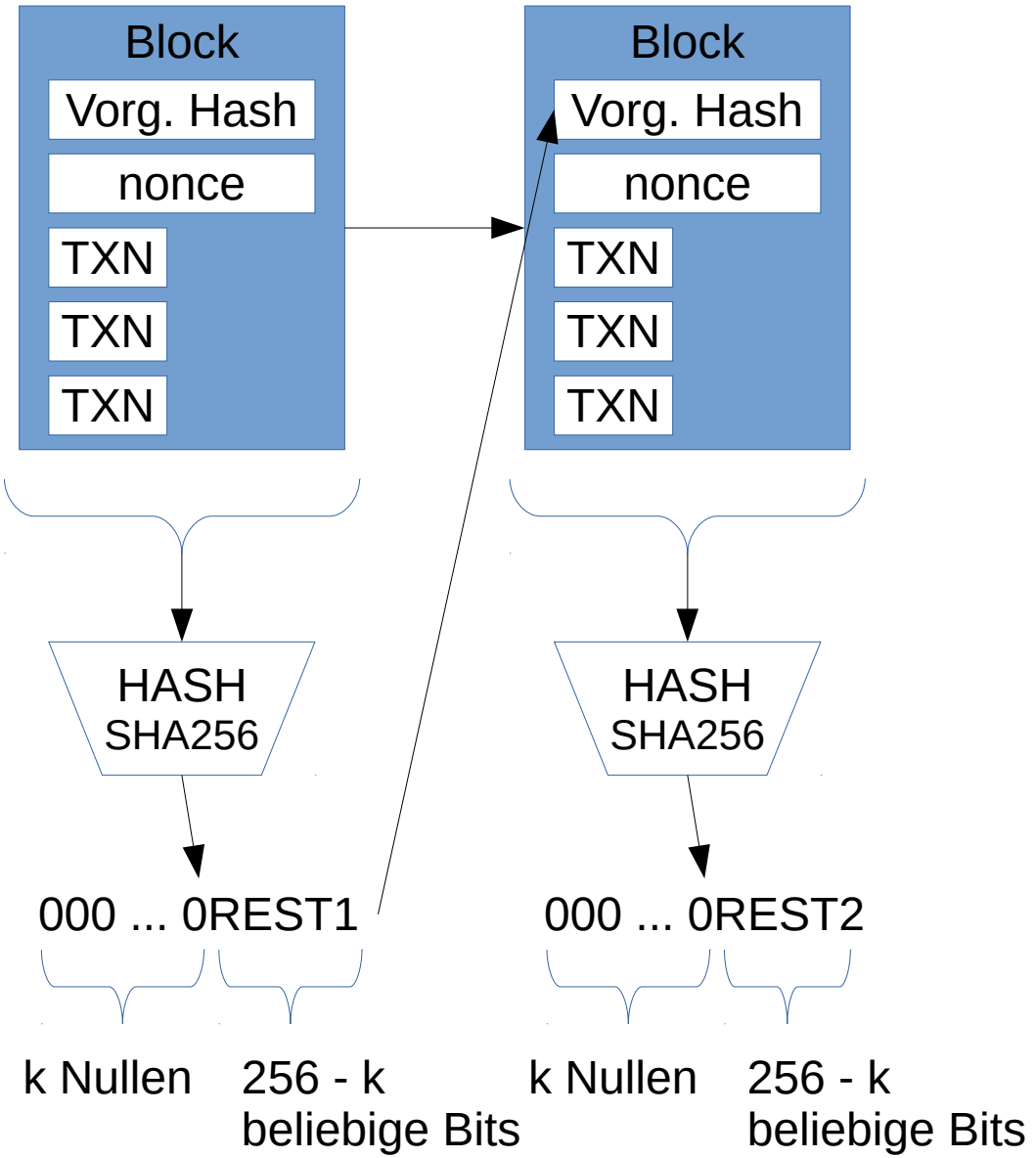


Arbeitsbeweis (Proof of Work)

Bearbeitung eines Blocks, so dass er an Blockkette angehängt werden kann.

- Aufgabe: finde einen Wert für Komponente des Blocks (nonce), so dass der Hash des Blocks mit mindestens k Nullen beginnt

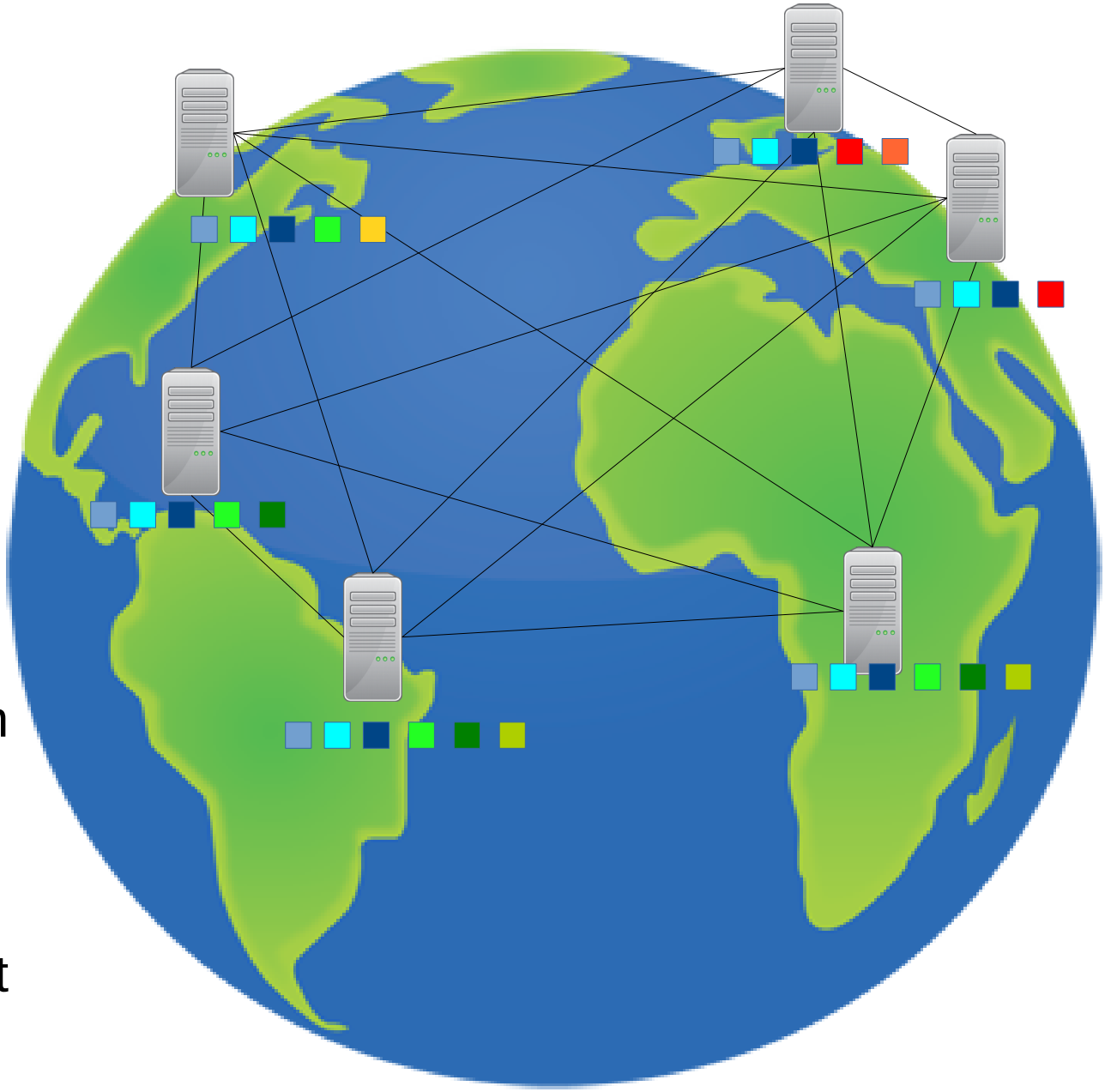
- k kallibrierbar
  - wird so angepasst, dass mit vorhandener Technologie die Bearbeitung eines Blocks ca 10 min dauert
- Block enthält Hash des Vorgängers in der Kette:
  - manifestiert Reihenfolge
  - kein Block in der Kette kann (einfach) ausgetauscht werden
  - strenge Sequenzialisierung der Arbeit: Block kann nicht bearbeitet werden, bevor Vorgängerblock berechnet ist



Blockketten Konsens

die meiste Arbeit gewinnt

- jeder Knoten verteilt seine Blockkette an alle anderen Knoten
- jeder Knoten nutzt die längste ihm bekannte Blockkette für weitere Berechnungen
- Transaktionen aus verworfenen Blöcken gehen zurück in den Pool
- Der Knoten, der die Blockkette verlängert wird belohnt



Konsequenzen des Proof of Work Konzepts

- Es kann passieren dass es unterschiedliche Knoten verschiedene Ketten für die Längste halten
- Die letzte in einer Kette enthaltene Transaktionen wird eventuell wieder verworfen
- Die Mehrheit der (fairen) Knoten wird die längste(n) Kette(n) bearbeiten
- Je mehr Knoten (Rechenkraft) versuchen, eine Kette zu bearbeiten, desto höher die Wahrscheinlichkeit, dass diese Kette als nächste verlängert wird
- Wenn eine Kette viel länger als andere Ketten ist, kann sie von den kürzeren Ketten nur mit äußerst geringer Wahrscheinlichkeit eingeholt werden.
- Nur wer die längste Kette bearbeitet, kann beeinflussen welche Transaktionen als nächstes bestätigt werden.
- Einzelne fehlerhafte Knoten können nicht mit der Mehrheit der Knoten konkurrieren
- Der Ausfall weniger Knoten hat keinen Einfluss auf das System
- Unfaire Knoten benötigen >50% der Rechenkraft des Bitcoin Netzes um die Blockketten manipulieren zu können (Mehrfachausgabe von Bitcoins)
- Eine Transaktion ist nie 100%ig bestätigt.
- Man wartet üblicherweise bis eine Transaktion durch 6 Folgeblöcke abgesichert ist (ca. 1h), bevor man sie als bestätigt erachtet.

Belohnung

- Warum sollte jemand Rechenzeit investieren um Blockketten zu verlängern?
- Startphase
  - für jeden bestätigten Block gibt es eine Belohnung (neue Bitcoins werden geschöpft, „mining“)
  - Belohnung wird alle 4 Jahre halbiert
  - maximal 21 Millionen BTCs
  - ab ca 2140 wird es keine neue BTCs durch mining geben
- Jederzeit, insbesondere nach Startphase
  - wird eine (freiwillige) Gebühr für die Bearbeitung von Transaktionen erhoben
  - Höhe der gewährten Gebühr wird Bearbeitungsgeschwindigkeit beeinflussen

Anonymität von Bitcoins

- Jeder Nutzer kann alle Transaktionen mit allen Sendern und Empfängern sehen
- Jeder Nutzer wird im Rahmen einer Transaktion durch seinen öffentlichen Schlüssel repräsentiert
- Den Beweis, dass er der Besitzer des öffentlichen Schlüssels ist, führt er durch den Besitz des assoziierten privaten Schlüssels durch.
- Jeder Nutzer kann beliebig viele private und öffentliche Schlüsselpaare (erzeugen und) besitzen
- Analyse der Transaktionen kann allerdings Zusammenhänge zwischen Schlüsseln finden
- Die Herkunft von Transaktionen (IP Adresse) kann durch Anonymisierungsdienste (z.B. TOR) verschleiert werden.

Blockchain

allgemeines Konzept einer Datenbank

- öffentlich
- verteilt
- synchronisiert
- kryptographisch abgesichert

Blockchain Infrastruktur Systeme

- Etherum
  - smart contracts
- open blockchain / Hyperledger
  - vertrauliche aber überprüfbare Verträge