Grundlagen der Blockchain Technologie

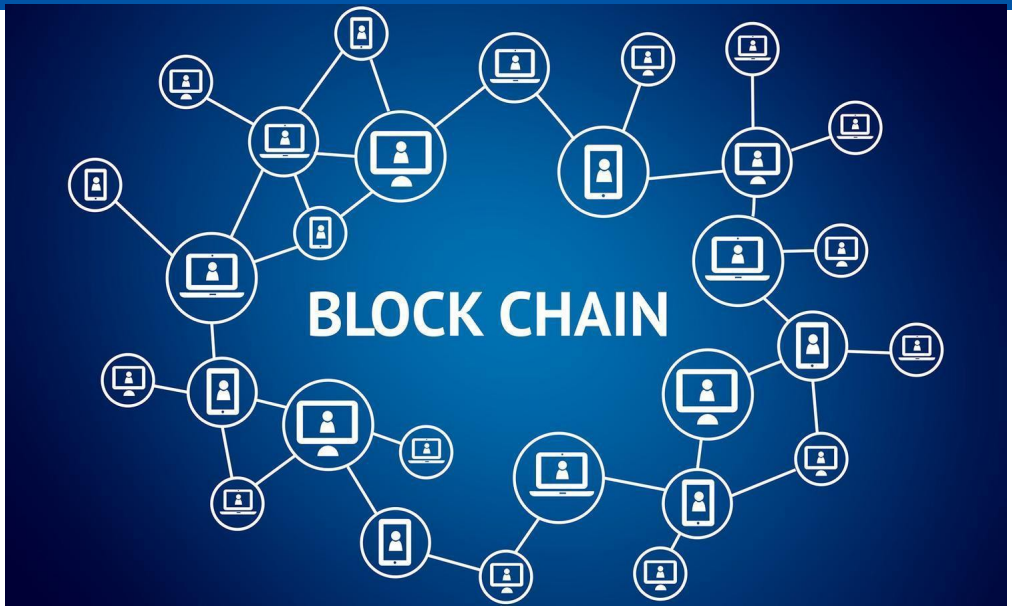
Albert-Ludwigs-Universität Freiburg

Prof. Dr. Peter Thiemann

16 Nov 2022

UNI FREIBURG

Blockchain ist in aller Munde

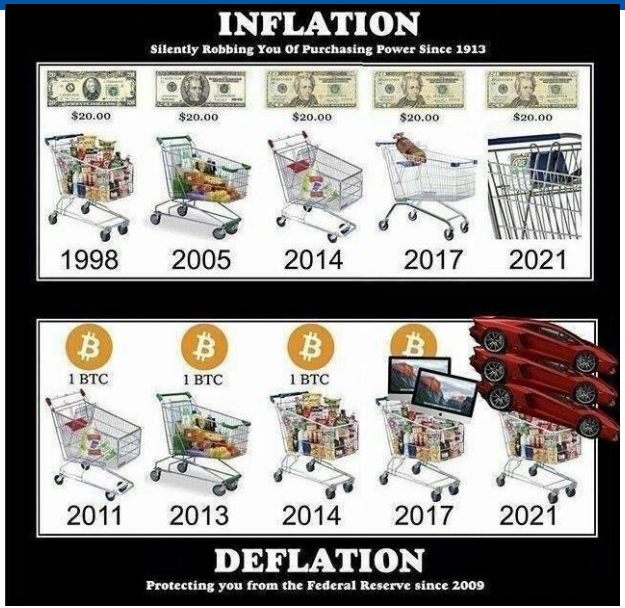


Blockchain ist in aller Munde

Blockchain ist in aller Munde

Blockchain ist in aller Munde

Blockchain ist in aller Munde



Blockchain ist in aller Munde

SPIEGEL ONLINE SPIEGEL+ Anmelden

Kryptogeld

Bitcoin-Schürfer verbrauchen mehr Strom als ganz Dänemark

Die Produktion der virtuellen Währung Bitcoin verbraucht enorme Strommengen - im Jahr 2018 mehr als die gesamte dänische Volkswirtschaft. Die Energie kommt oft aus schmutzigen Kohlekraftwerken.

REUTERS

Bitcoin-Rechner (Archivbild)

Blockchain ist in aller Munde

RP ONLINE NRW POLITIK SPORT PANORAMA KULTUR WIRTSCHAFT DIGITAL LEBEN MENÜ

Wirtschaft / Andreas von Bechtolsheim zweifelt an Blockchain

Silicon Valley

Keine Kommentare

„Blockchain ist der größe Hype aller Zeiten“

18. September 2018 um 19:18 Uhr | Lesedauer: 5 Minuten

Der deutsche Investor Andreas von Bechtolsheim beim Frühstück im Four Seasons Hotel im kalifornischen Palo Alto.

Also:

Also:

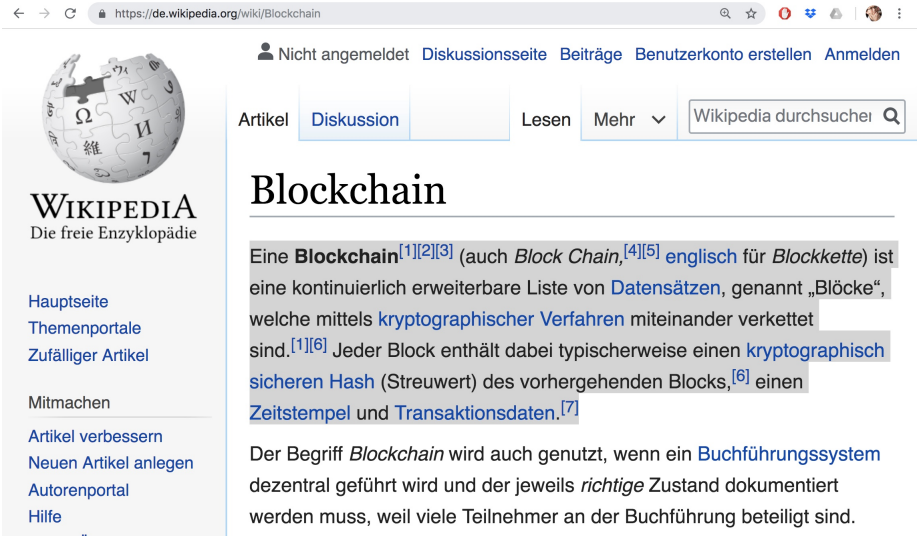
Was heißt

und

zu welchem Ende studiert man

Blockchain?

Was sagt Wikipedia?



https://de.wikipedia.org/wiki/Blockchain

Nicht angemeldet Diskussionsseite Beiträge Benutzerkonto erstellen Anmelden

WIKIPEDIA
Die freie Enzyklopädie

Artikel Diskussion Lesen Mehr Wikipedia durchsuchen

Hauptseite
Themenportale
Zufälliger Artikel

Mitmachen
Artikel verbessern
Neuen Artikel anlegen
Autorenportal
Hilfe

Blockchain

Eine **Blockchain**[1][2][3] (auch *Block Chain*,[4][5] englisch für *Blockkette*) ist eine kontinuierlich erweiterbare Liste von Datensätzen, genannt „Blöcke“, welche mittels kryptographischer Verfahren miteinander verkettet sind.[1][6] Jeder Block enthält dabei typischerweise einen kryptographisch sicheren Hash (Streuwert) des vorhergehenden Blocks,[6] einen Zeitstempel und Transaktionsdaten.[7]

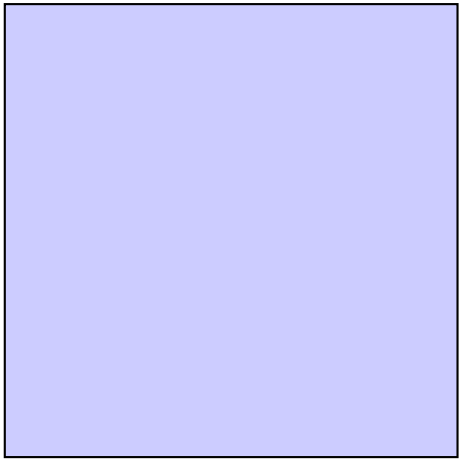
Der Begriff *Blockchain* wird auch genutzt, wenn ein Buchführungssystem dezentral geführt wird und der jeweils *richtige* Zustand dokumentiert werden muss, weil viele Teilnehmer an der Buchführung beteiligt sind.

Was sagt Wikipedia?

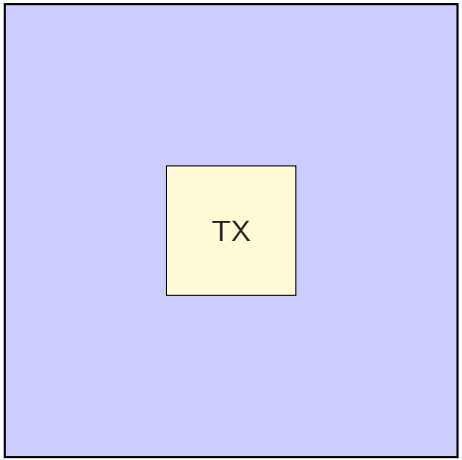
Da stelle mehr uns janz dumm. . .

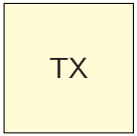
Plan

Am Anfang war der Block



Am Anfang war der Block





ist eine Transaktion

Was ist eine Transaktion?

Was ist eine Transaktion?

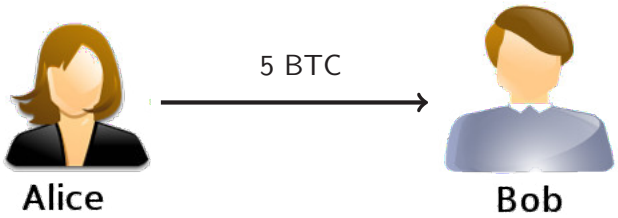
“Geld” wird bewegt!

Was ist eine Transaktion?

“Geld” wird bewegt!

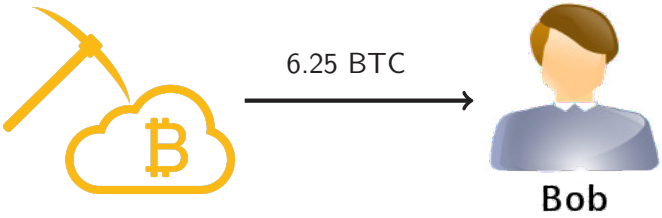
Und mehr . . .

Transaktion “Überweisung”



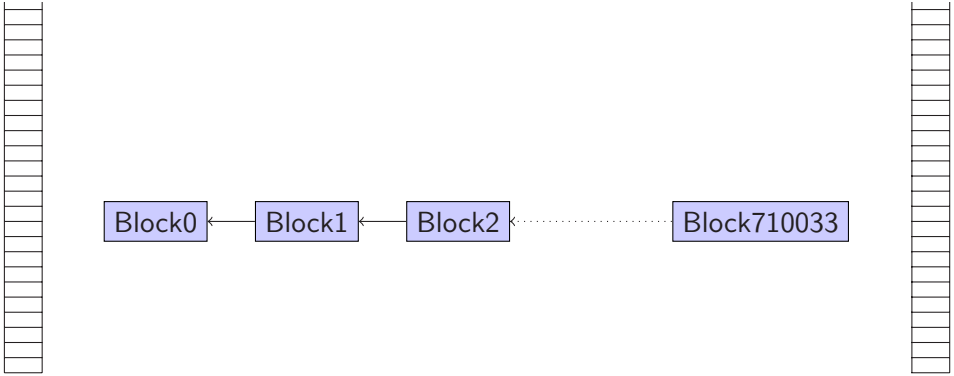
- Alice überweist 5 BTC an Bob.

Transaktion “Schürfen” (Mining)



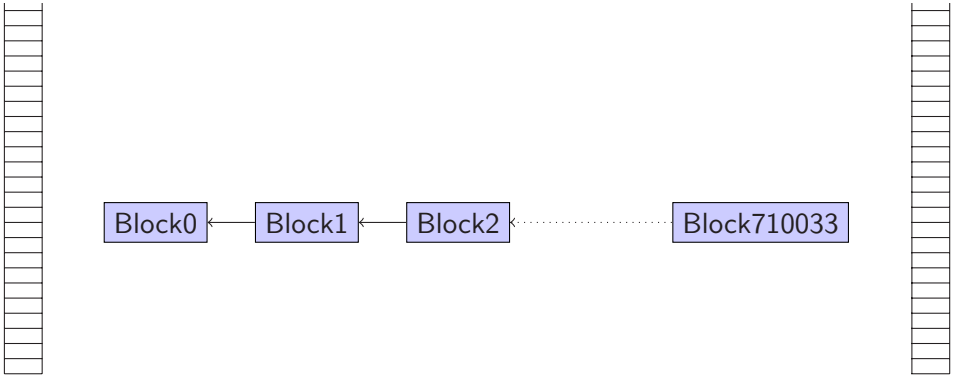
- Neue BTC entstehen durch **Schürfen**.
- Der Schürfer erhält eine Belohnung (seit 11.5.2020: 6.25 BTC).
- Beim aktuellen Kurs 16430.50 EUR/BTC: 102690.625 EUR.

Die Geschichte der Bitcoin-Blockchain



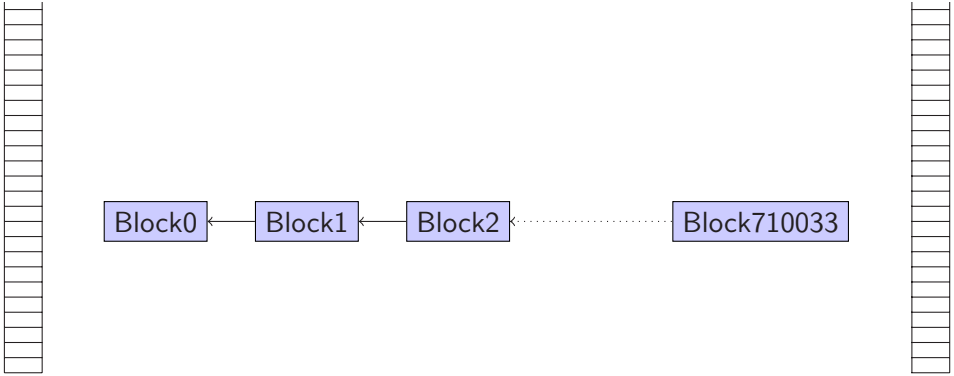
- Urknall: Januar 2009

Die Geschichte der Bitcoin-Blockchain



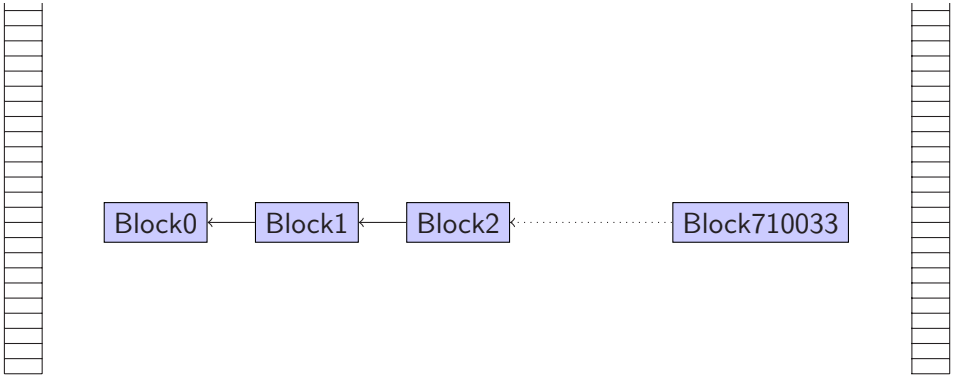
- Urknall: Januar 2009
- Alle Konten auf 0

Die Geschichte der Bitcoin-Blockchain



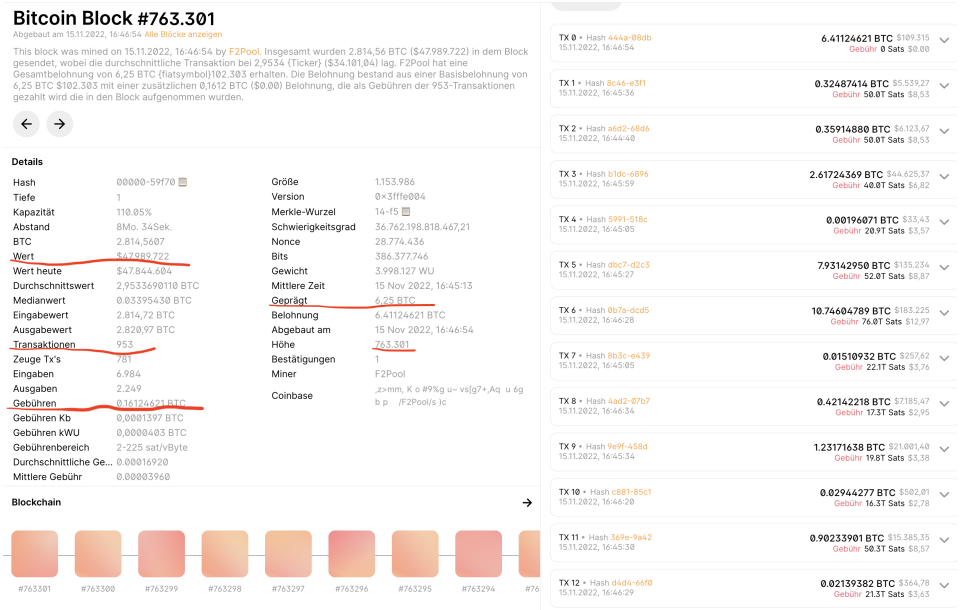
- Urknall: Januar 2009
- Alle Konten auf 0
- 16.11.2021

Die Geschichte der Bitcoin-Blockchain



- Urknall: Januar 2009
- Alle Konten auf 0

- 16.11.2021
- Kontostände gemäß Transaktionsgeschichte



Quelle: https://www.blockchain.com/explorer/blocks/btc/763301

Transaktionsgeschichte (vereinfacht)

Transaktionen	Kontostände			
	A	B	C	···
Urknall Januar 2009	0	0	0	···

Transaktionsgeschichte (vereinfacht)

Transaktionen	Kontostände			
	A	B	C	···
Urknall Januar 2009	0	0	0	···
Mining: 50 BTC → B	0	50	0	···

Transaktionsgeschichte (vereinfacht)

Transaktionen	Kontostände			
	A	B	C	···
Urknall Januar 2009	0	0	0	···
Mining: 50 BTC $\rightarrow$ B	0	50	0	···
Transfer: 7.5 BTC B $\rightarrow$ A	7.5	42.5	0	···

Transaktionsgeschichte (vereinfacht)

Transaktionen	Kontostände			
	A	B	C	···
Urknall Januar 2009	0	0	0	···
Mining: 50 BTC $\rightarrow$ B	0	50	0	···
Transfer: 7.5 BTC B $\rightarrow$ A	7.5	42.5	0	···
Transfer: 2.5 BTC A,B $\rightarrow$ C	5	40	5	···

Transaktionsgeschichte (vereinfacht)

Transaktionen	Kontostände			
	A	B	C	$\cdots$
Urknall Januar 2009	0	0	0	$\cdots$
Mining: 50 BTC $\rightarrow$ B	0	50	0	$\cdots$
Transfer: 7.5 BTC B $\rightarrow$ A	7.5	42.5	0	$\cdots$
Transfer: 2.5 BTC A,B $\rightarrow$ C	5	40	5	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Kryptowährung

- Transaktionsgeschichte ist öffentlich.

Kryptowährung

- Transaktionsgeschichte ist öffentlich.
- Jeder kann jeden Kontostand nachvollziehen.

Kryptowährung

- Transaktionsgeschichte ist öffentlich.
- Jeder kann jeden Kontostand nachvollziehen.
- Jeder kann jede Transaktion prüfen.

Kryptowährung

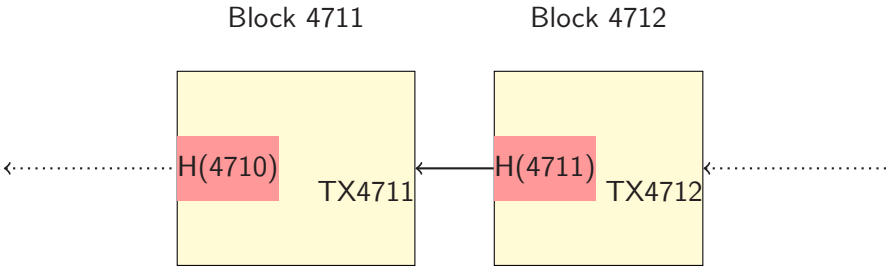
- Transaktionsgeschichte ist öffentlich.
- Jeder kann jeden Kontostand nachvollziehen.
- Jeder kann jede Transaktion prüfen.
- Wenn man sich über die Abfolge der Transaktionen einig ist!

Kryptowährung

- Transaktionsgeschichte ist öffentlich.
- Jeder kann jeden Kontostand nachvollziehen.
- Jeder kann jede Transaktion prüfen.
- Wenn man sich über die Abfolge der Transaktionen einig ist!
- Dabei hilft Kryptographie!

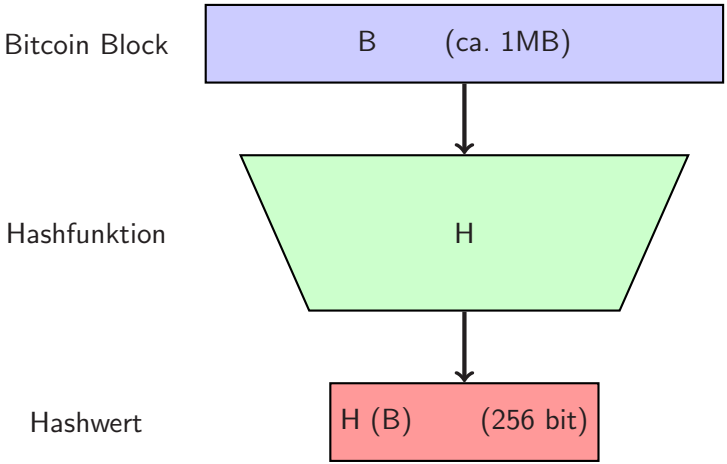
Plan

Hasch mich



- Jeder Block besteht u.a. aus dem Text der Transaktionen und dem Hashwert des vorangehenden Blocks.

(Kryptographischer) Hashwert



Eigenschaften einer kryptographischen Hashfunktion

UNI FREIBURG

Kollisionsresistenz

Wenn $B_1 \neq B_2$, dann ist fast sicher $H(B_1) \neq H(B_2)$.

Eigenschaften einer kryptographischen Hashfunktion

UNI FREIBURG

Kollisionsresistenz

Wenn $B_1 \neq B_2$, dann ist fast sicher $H(B_1) \neq H(B_2)$.

Beispiel (H=SHA-256)

Eigenschaften einer kryptographischen Hashfunktion

UNI FREIBURG

Kollisionsresistenz

Wenn $B_1 \neq B_2$, dann ist fast sicher $H(B_1) \neq H(B_2)$.

Beispiel (H=SHA-256)

- B_1 = "Zwei Warzenschweine spielen Fussball im Regen."

Eigenschaften einer kryptographischen Hashfunktion

Kollisionsresistenz

Wenn $B_1 \neq B_2$, dann ist fast sicher $H(B_1) \neq H(B_2)$.

Beispiel (H=SHA-256)

- B_1 = "Zwei Warzenschweine spielen Fussball im Regen."
- $H(B_1)$ = `7f2c6d75c99218fe6f4b742b469c0e67b319387e3a12dadb4d9dea4cd9143611`

Eigenschaften einer kryptographischen Hashfunktion

Kollisionsresistenz

Wenn $B_1 \neq B_2$, dann ist fast sicher $H(B_1) \neq H(B_2)$.

Beispiel (H=SHA-256)

- B_1 = "Zwei Warzenschweine spielen Fussball im Regen."
- $H(B_1)$ = `7f2c6d75c99218fe6f4b742b469c0e67b319387e3a12dadb4d9dea4cd9143611`
- B_2 = "Zwei Warzenschwehne spielen Fussball im Regen!"

Eigenschaften einer kryptographischen Hashfunktion

Kollisionsresistenz

Wenn $B_1 \neq B_2$, dann ist fast sicher $H(B_1) \neq H(B_2)$.

Beispiel (H=SHA-256)

- B_1 = "Zwei Warzenschweine spielen Fussball im Regen."
- $H(B_1)$ = `7f2c6d75c99218fe6f4b742b469c0e67b319387e3a12dadb4d9dea4cd9143611`
- B_2 = "Zwei Warzenschwehne spielen Fussball im Regen!"
- $H(B_2)$ = `92293fc39ecd24a05998f11f2cd8a7b007885b2b57f0581805b06419173c5fe8`

Eigenschaften einer kryptographischen Hashfunktion

Kollisionsresistenz

Wenn $B_1 \neq B_2$, dann ist fast sicher $H(B_1) \neq H(B_2)$.

Beispiel (H=SHA-256)

- B_1 = "Zwei Warzenschweine spielen Fussball im Regen."
- $H(B_1)$ = `7f2c6d75c99218fe6f4b742b469c0e67b319387e3a12dadb4d9dea4cd9143611`
- B_2 = "Zwei Warzenschwehne spielen Fussball im Regen!"
- $H(B_2)$ = `92293fc39ecd24a05998f11f2cd8a7b007885b2b57f0581805b06419173c5fe8`
- Nur ein Bit Unterschied zwischen B_1 und B_2!

Eigenschaften des kryptographischen Hashwerts, II

UNI FREIBURG

Urbildresistenz

Es ist extrem aufwändig, zu einem vorliegenden Hashwert $H(B)$ einen anderen Block $B' \neq B$ zu bestimmen, so dass $H(B) = H(B')$.

Eigenschaften des kryptographischen Hashwerts, II

Urbildresistenz

Es ist extrem aufwändig, zu einem vorliegenden Hashwert $H(B)$ einen anderen Block $B' \neq B$ zu bestimmen, so dass $H(B) = H(B')$.

Wie aufwändig?

Eigenschaften des kryptographischen Hashwerts, II

Urbildresistenz

Es ist extrem aufwändig, zu einem vorliegenden Hashwert $H(B)$ einen anderen Block $B' \neq B$ zu bestimmen, so dass $H(B) = H(B')$.

Wie aufwändig?

- Mit 2^{256} Versuchen kommt man sicher zum Ziel. (Bitcoin: H = SHA-256)

Eigenschaften des kryptographischen Hashwerts, II

Urbildresistenz

Es ist extrem aufwändig, zu einem vorliegenden Hashwert $H(B)$ einen anderen Block $B' \neq B$ zu bestimmen, so dass $H(B) = H(B')$.

Wie aufwändig?

- Mit 2^{256} Versuchen kommt man sicher zum Ziel. (Bitcoin: H = SHA-256)
- $2^{256} \approx 1.2 \cdot 10^{78}$ Versuche

Eigenschaften des kryptographischen Hashwerts, II

Urbildresistenz

Es ist extrem aufwändig, zu einem vorliegenden Hashwert $H(B)$ einen anderen Block $B' \neq B$ zu bestimmen, so dass $H(B) = H(B')$.

Wie aufwändig?

- Mit 2^{256} Versuchen kommt man sicher zum Ziel. (Bitcoin: H = SHA-256)
- $2^{256} \approx 1.2 \cdot 10^{78}$ Versuche
- bei einer Million Versuche pro Sekunde: $\approx 3.6 \cdot 10^{63}$ Jahre

Eigenschaften des kryptographischen Hashwerts, II

Urbildresistenz

Es ist extrem aufwändig, zu einem vorliegenden Hashwert $H(B)$ einen anderen Block $B' \neq B$ zu bestimmen, so dass $H(B) = H(B')$.

Wie aufwändig?

- Mit 2^{256} Versuchen kommt man sicher zum Ziel. (Bitcoin: H = SHA-256)
- $2^{256} \approx 1.2 \cdot 10^{78}$ Versuche
- bei einer Million Versuche pro Sekunde: $\approx 3.6 \cdot 10^{63}$ Jahre
- Alter des Universums: $\approx 1.4 \cdot 10^{10}$ Jahre

Eigenschaften des kryptographischen Hashwerts, II

Urbildresistenz

Es ist extrem aufwändig, zu einem vorliegenden Hashwert $H(B)$ einen anderen Block $B' \neq B$ zu bestimmen, so dass $H(B) = H(B')$.

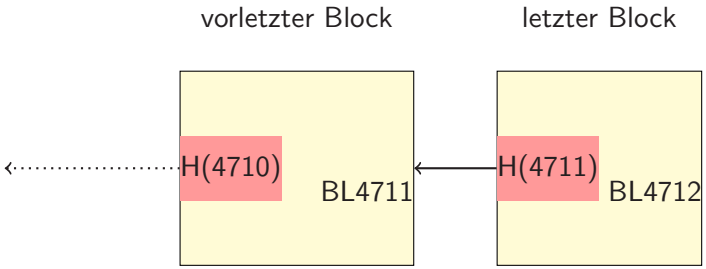
Wie aufwändig?

- Mit 2^{256} Versuchen kommt man sicher zum Ziel. (Bitcoin: H = SHA-256)
- $2^{256} \approx 1.2 \cdot 10^{78}$ Versuche
- bei einer Million Versuche pro Sekunde: $\approx 3.6 \cdot 10^{63}$ Jahre
- Alter des Universums: $\approx 1.4 \cdot 10^{10}$ Jahre

Schlussfolgerung

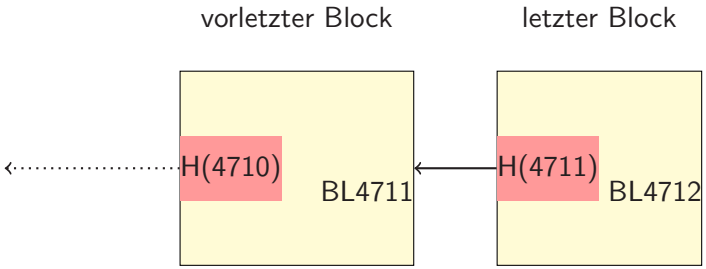
Bei vorliegendem Hashwert ist das Fälschen eines Blocks praktisch nicht möglich.

Was heisst das für die Blockchain?



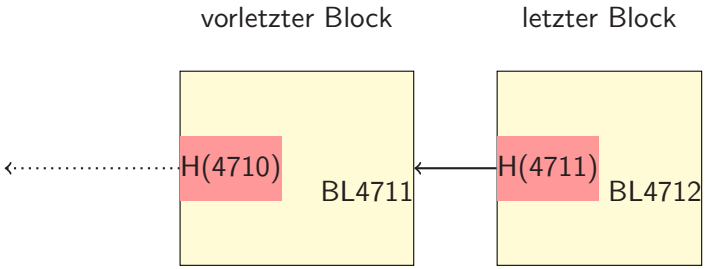
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.

Was heisst das für die Blockchain?



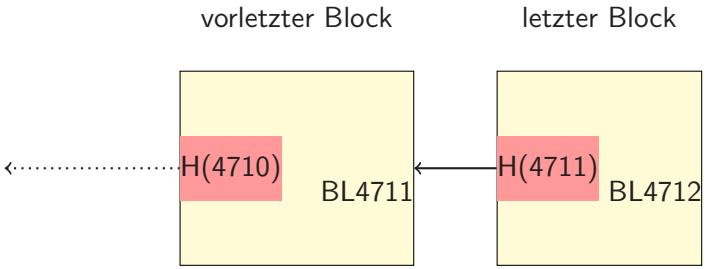
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.

Was heisst das für die Blockchain?



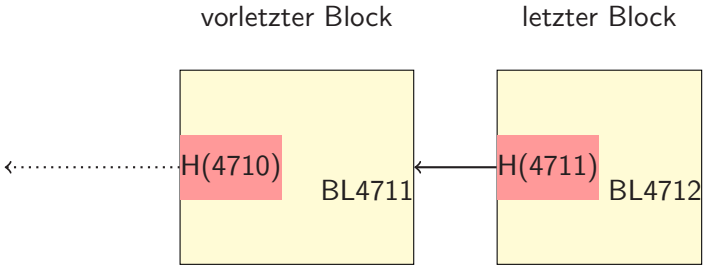
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.
- $H(4709)$ garantiert für den vor-vor-vorletzten Block und $H(4708)$.

Was heisst das für die Blockchain?



- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.
- $H(4709)$ garantiert für den vor-vor-vorletzten Block und $H(4708)$.
- ...

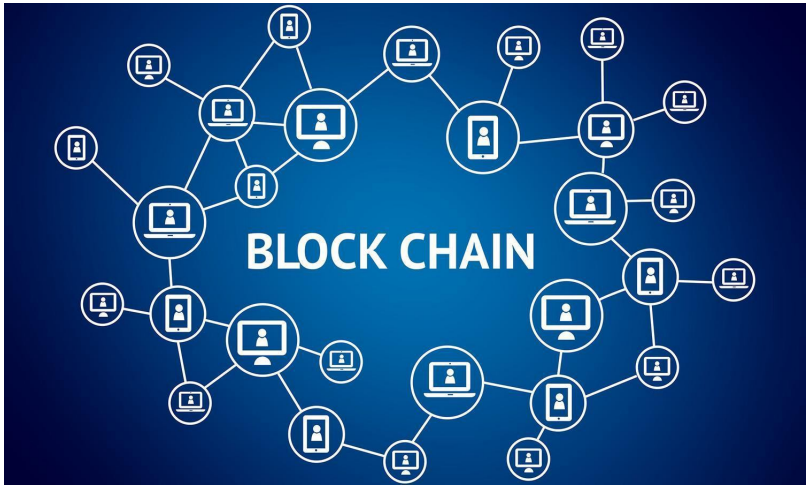
Was heisst das für die Blockchain?



- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.
- $H(4709)$ garantiert für den vor-vor-vorletzten Block und $H(4708)$.
- ...
- Also: Der letzte Blockhash garantiert für die ganze Kette!

Plan

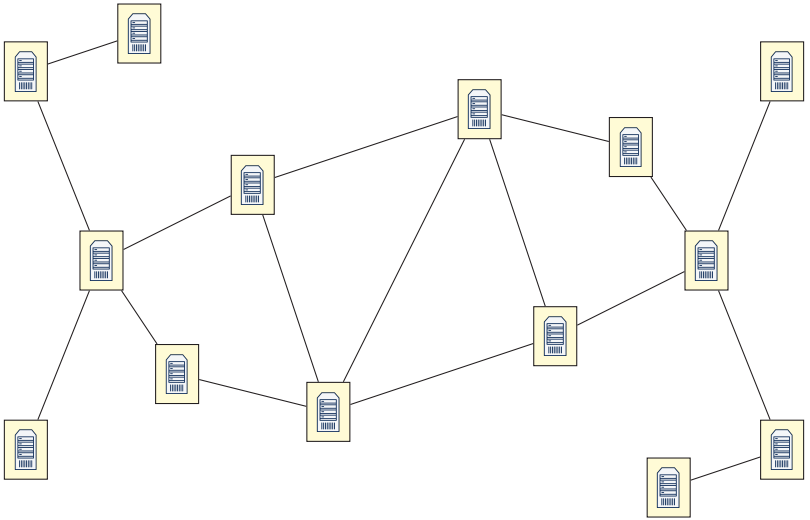
Einigkeit



Netzwerk

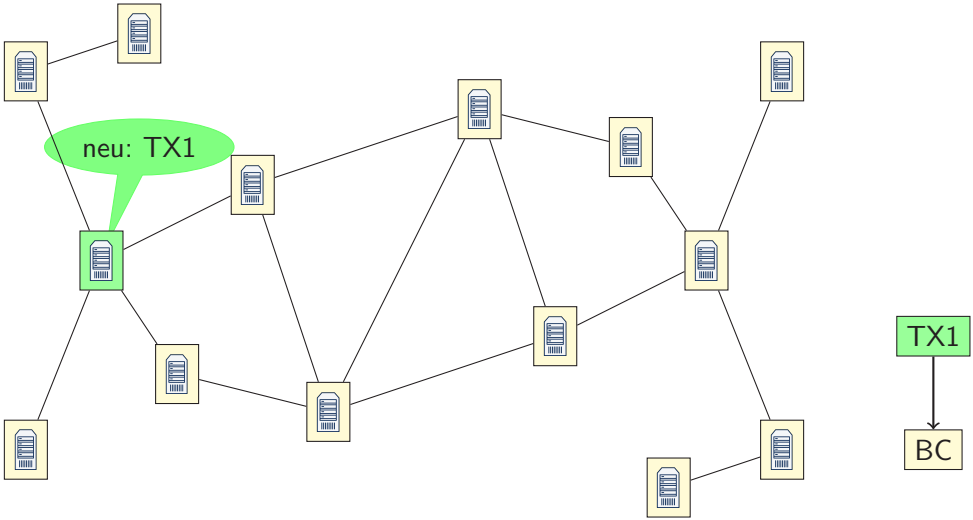
- Die Blockchain wird von einem Netz gleichwertiger Rechner unterhalten.
- Jeder Rechner hält die vollständige Blockchain.
- Jeder Rechner kann neue Transaktionen vorschlagen und schickt sie dafür an alle.
- Jeder Rechner weist unzulässige Transaktionen zurück!
- Die Mehrheit entscheidet, welche Transaktion zuerst akzeptiert wird.
  (je nach Blockchain)

Transaktionen vorschlagen

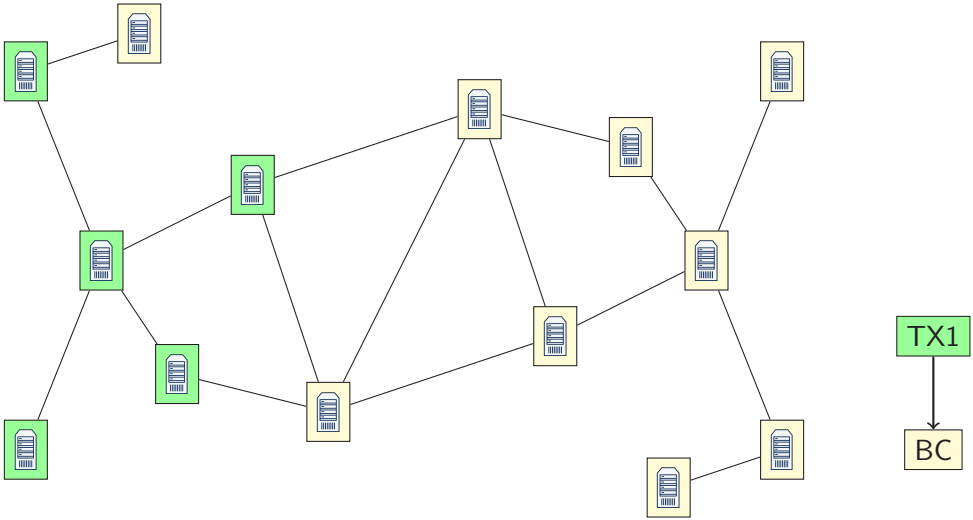


BC

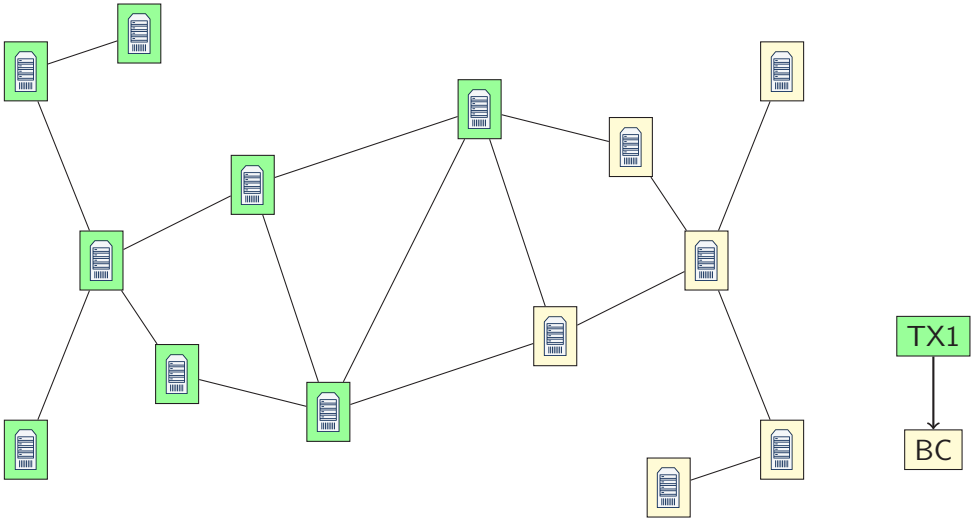
Transaktionen vorschlagen



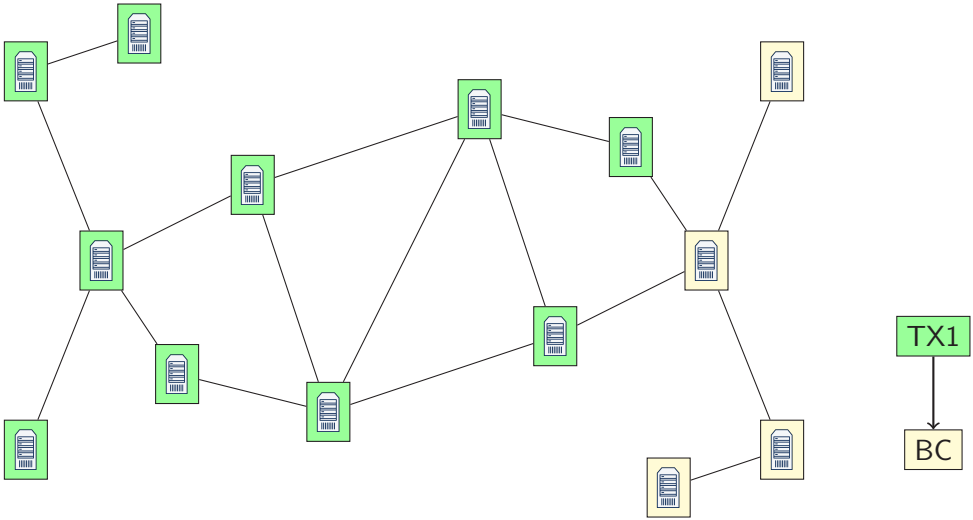
Transaktionen vorschlagen



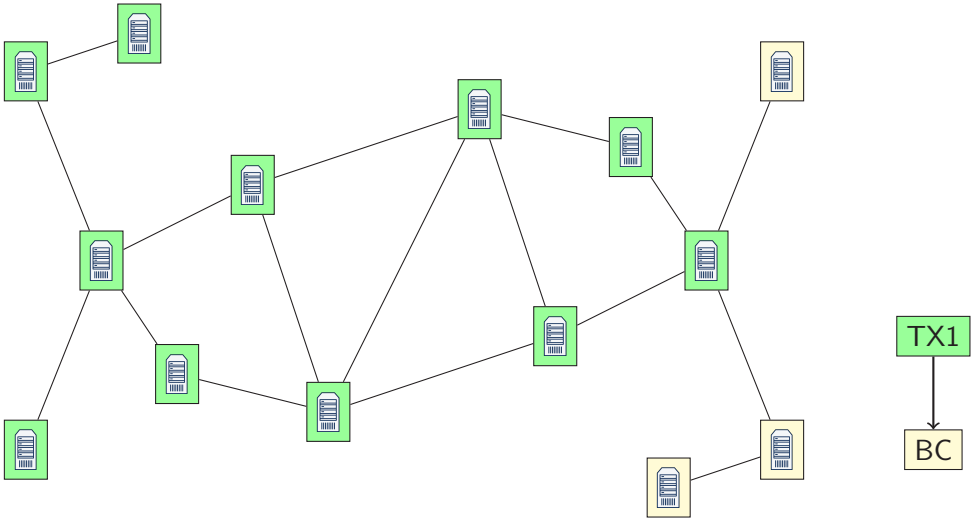
Transaktionen vorschlagen



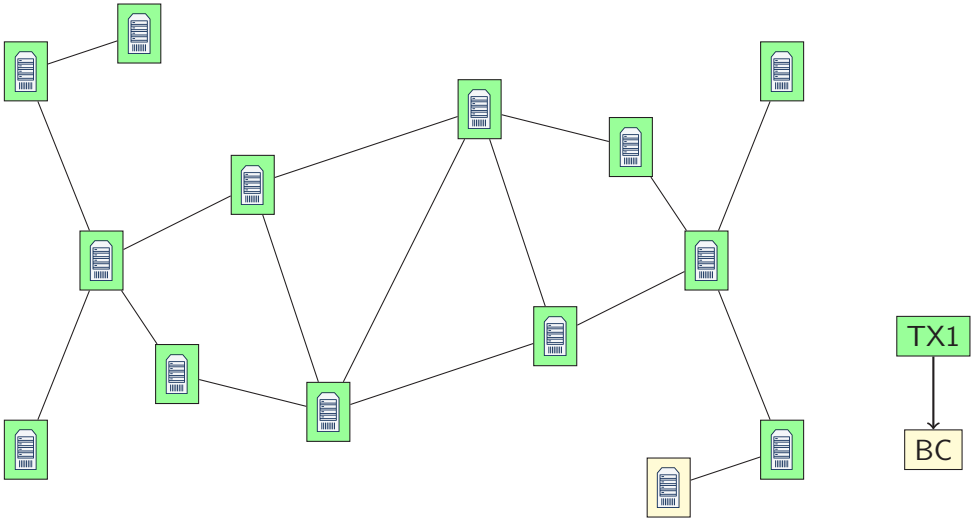
Transaktionen vorschlagen



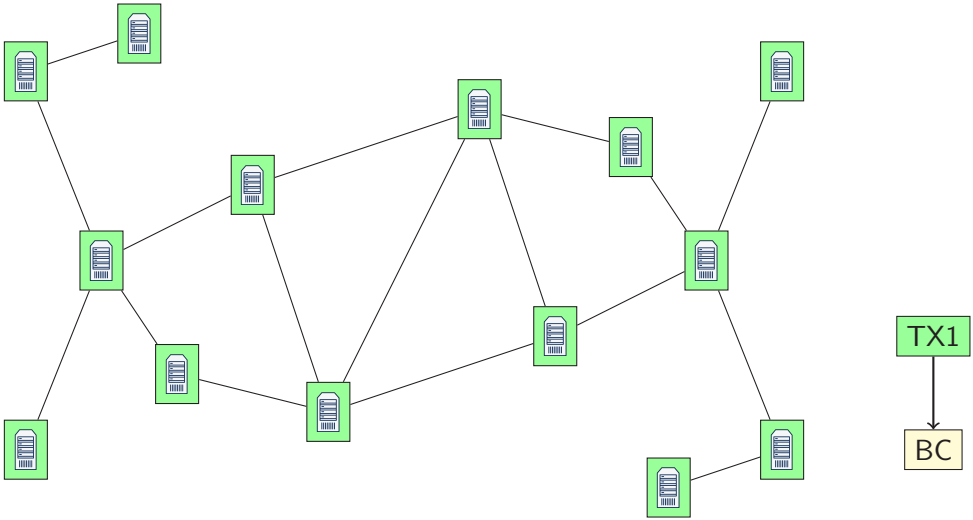
Transaktionen vorschlagen



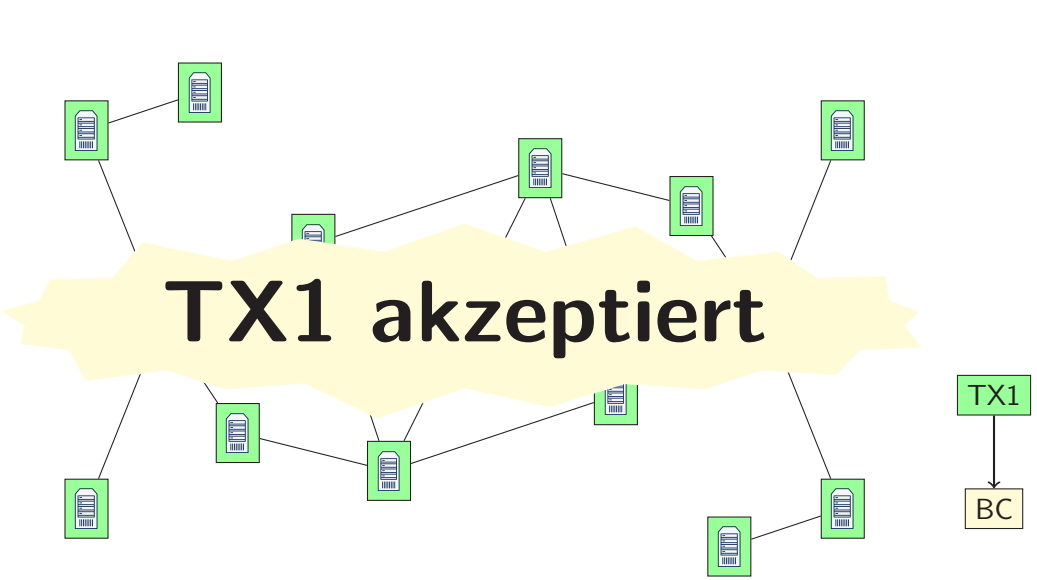
Transaktionen vorschlagen



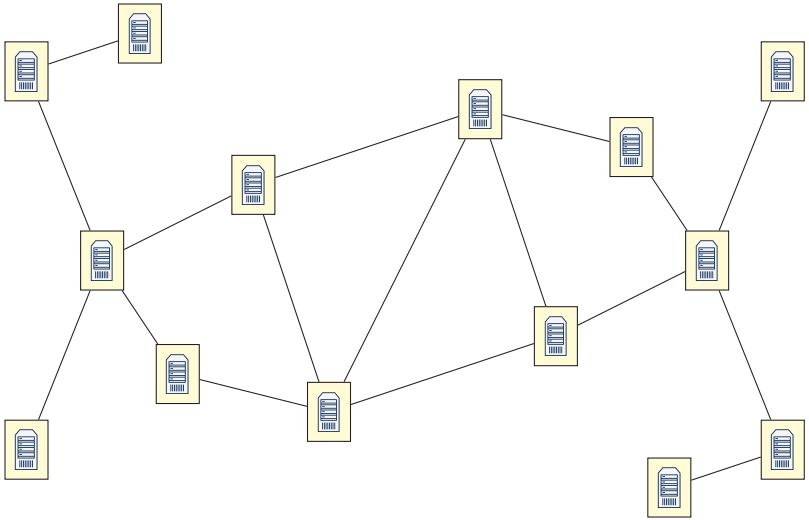
Transaktionen vorschlagen



Transaktionen vorschlagen

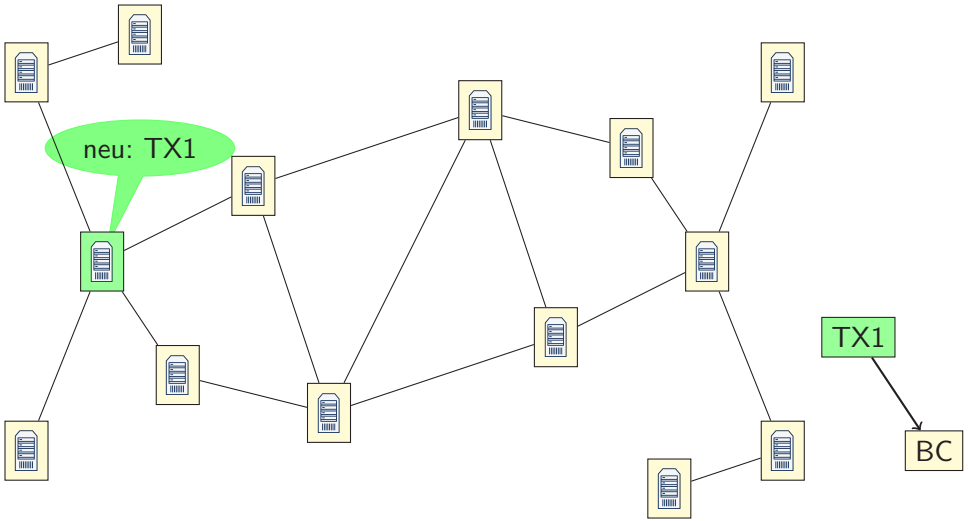


Zwei Transaktionen

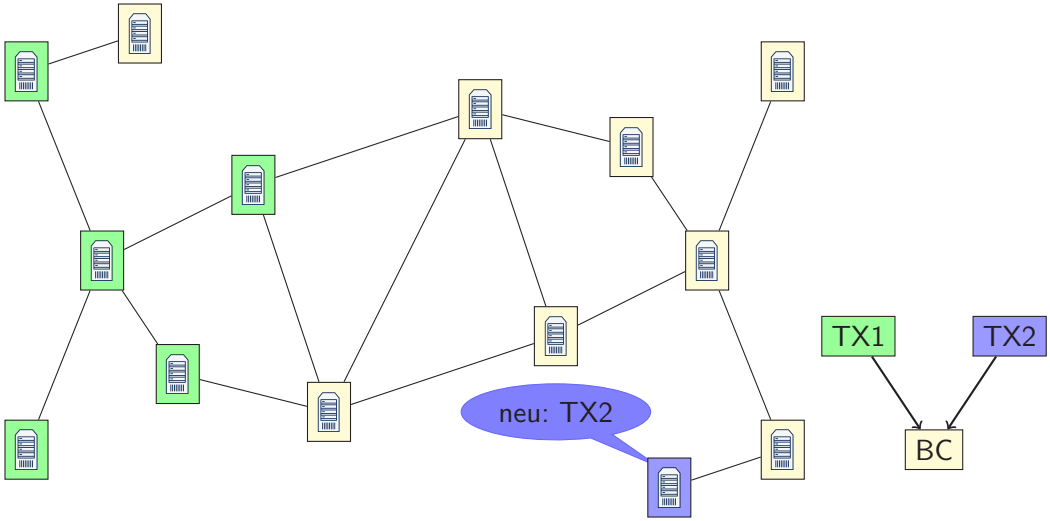


BC

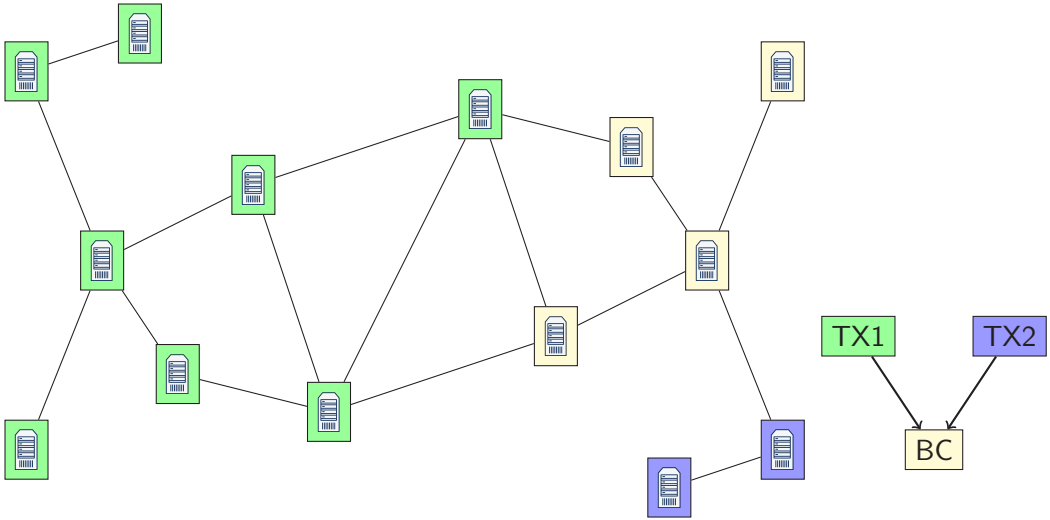
Zwei Transaktionen



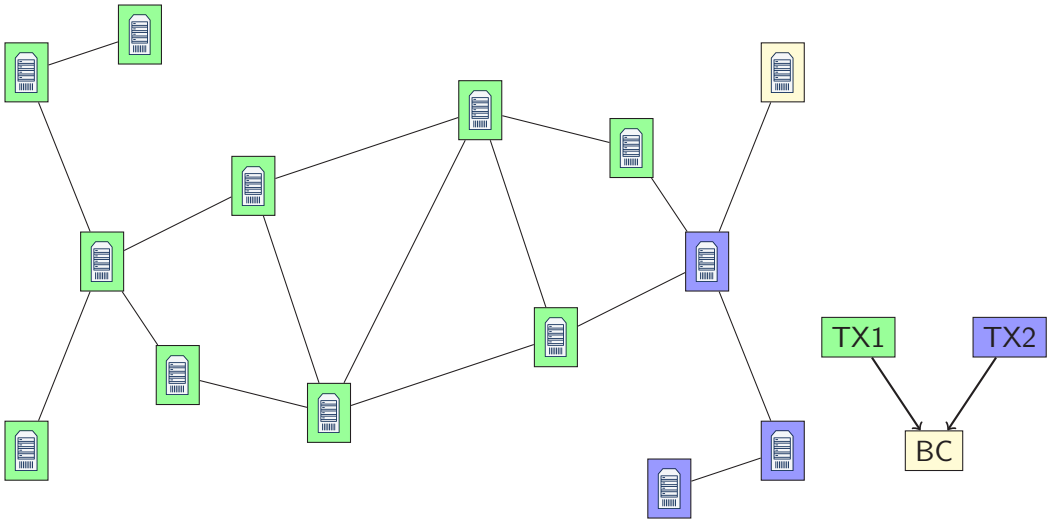
Zwei Transaktionen



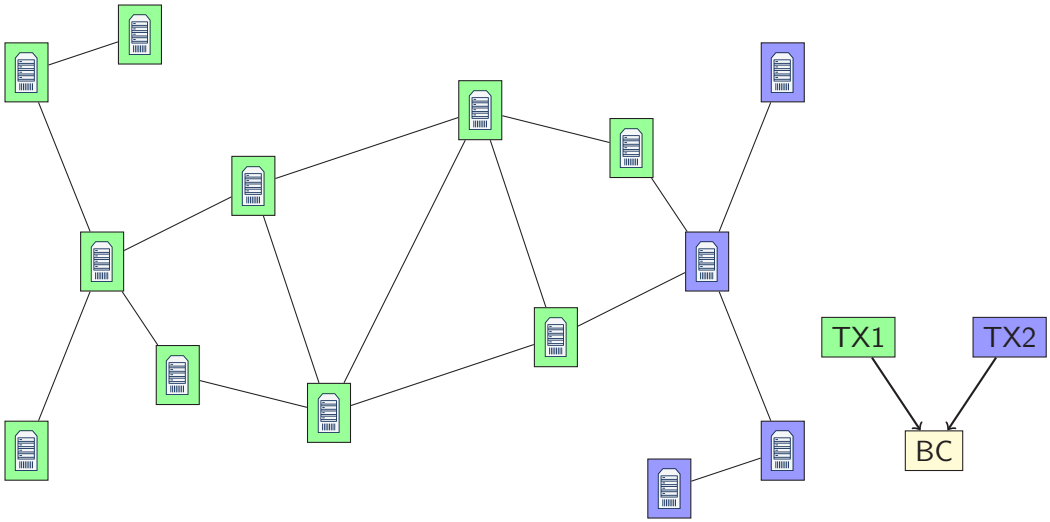
Zwei Transaktionen



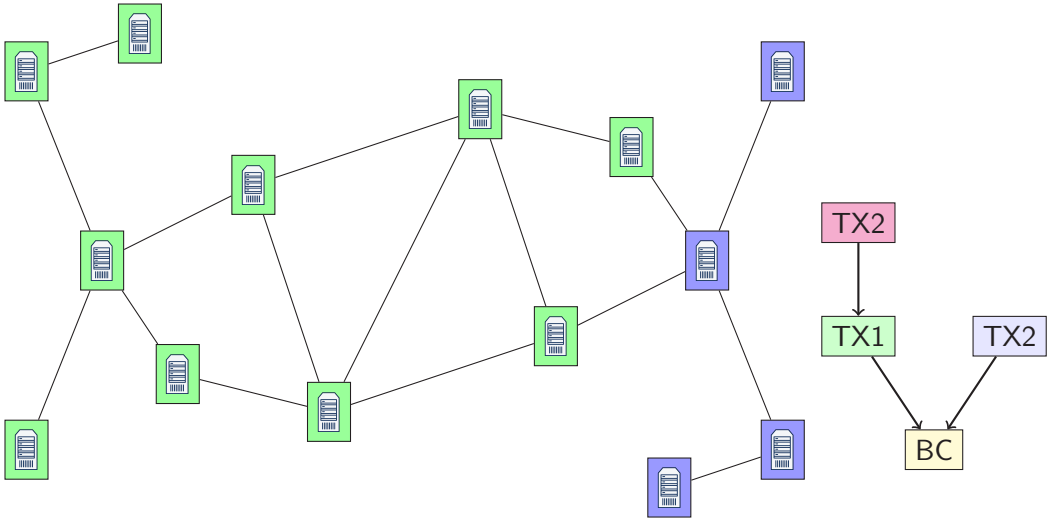
Zwei Transaktionen



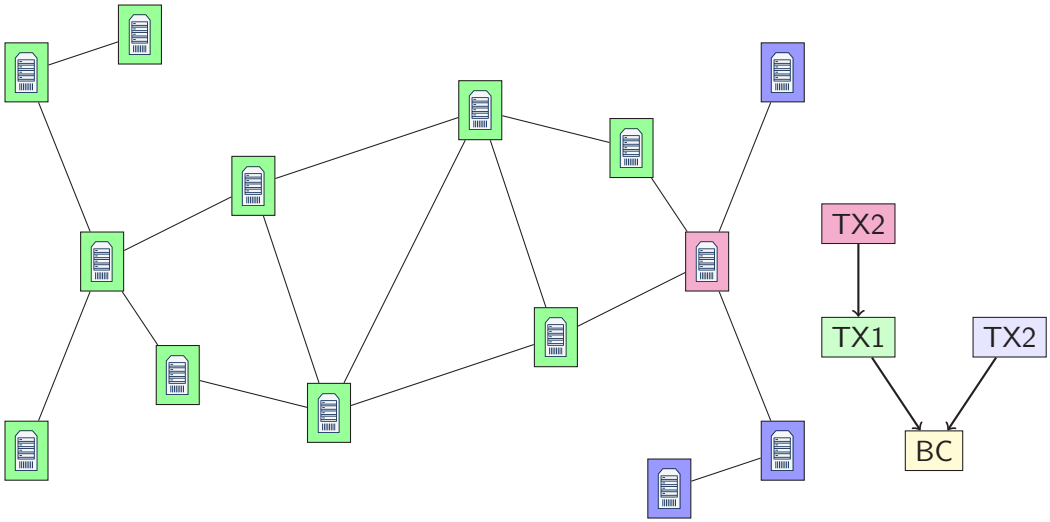
Zwei Transaktionen



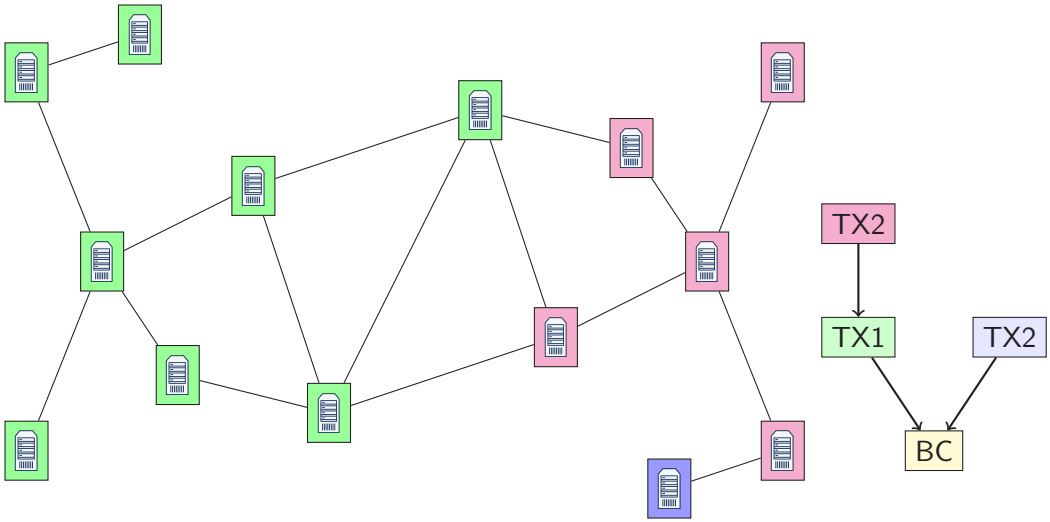
Zwei Transaktionen



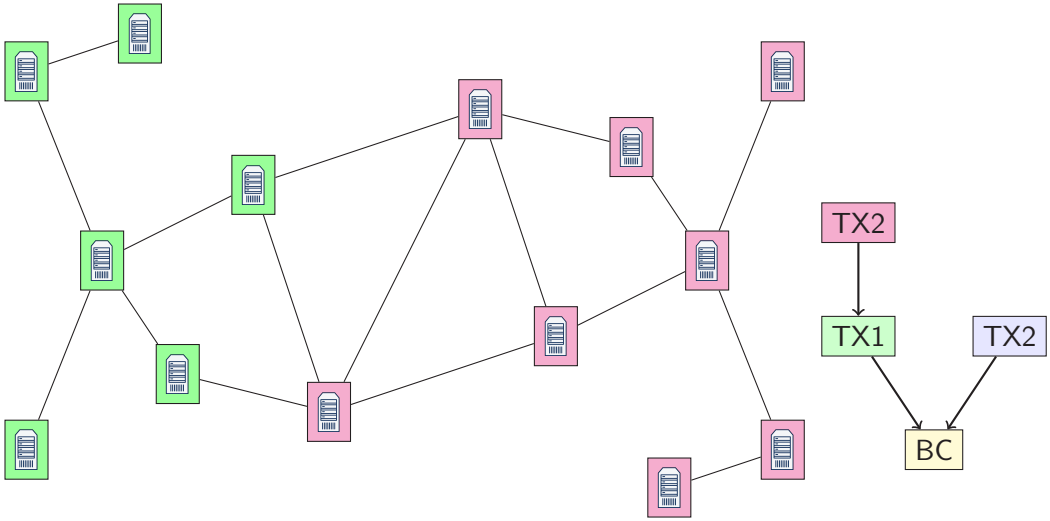
Zwei Transaktionen



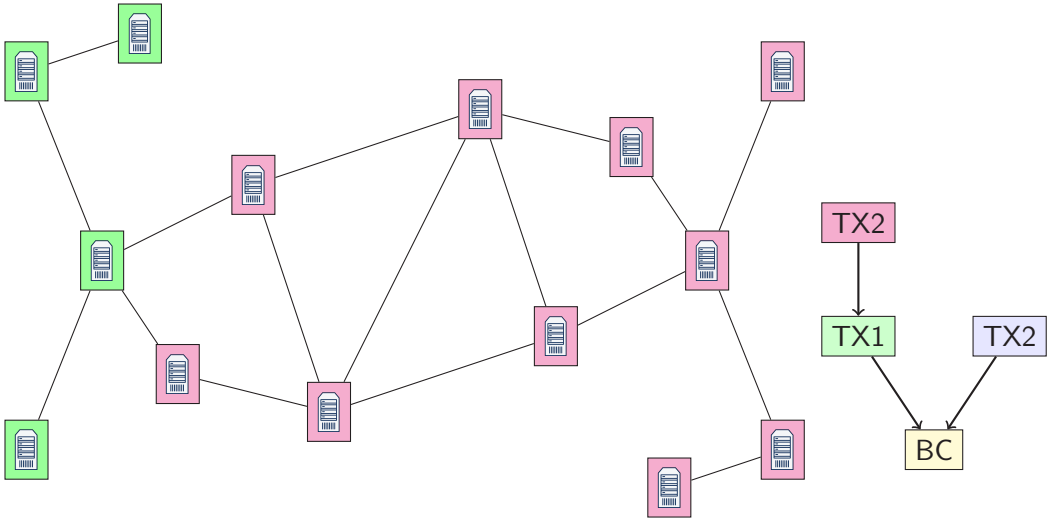
Zwei Transaktionen



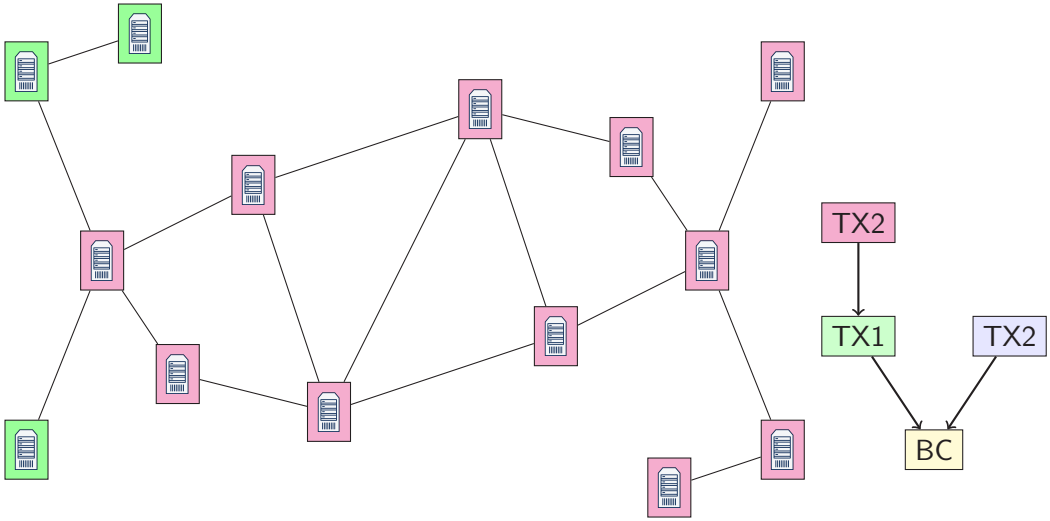
Zwei Transaktionen



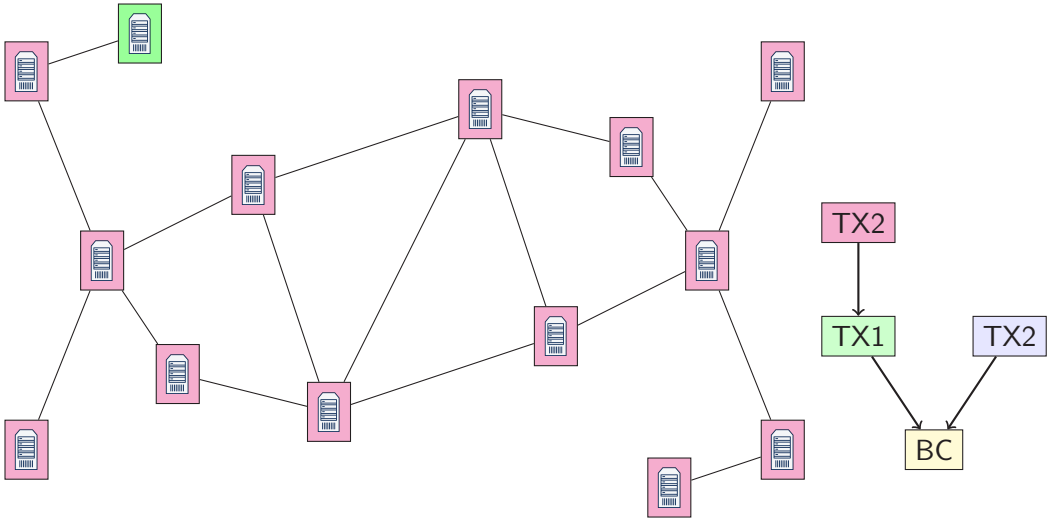
Zwei Transaktionen



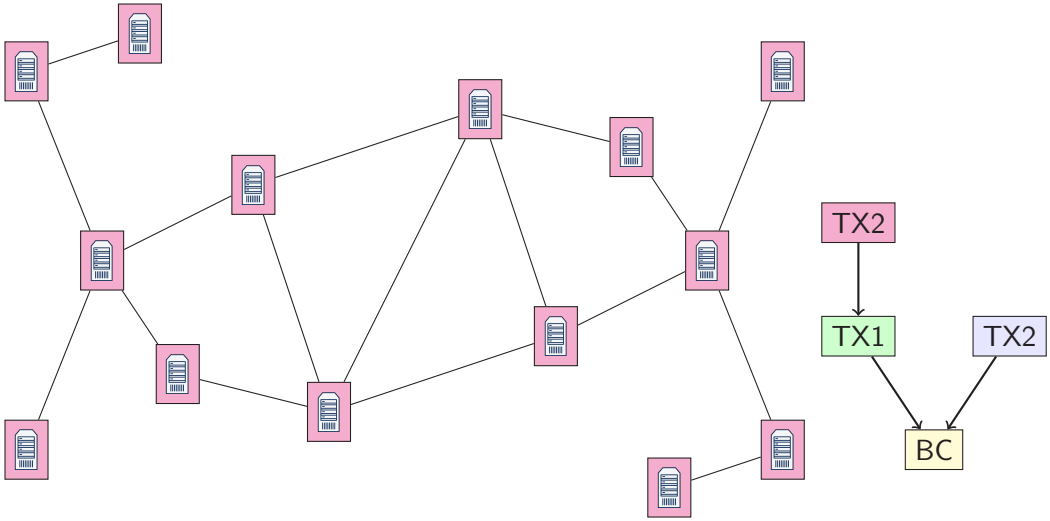
Zwei Transaktionen



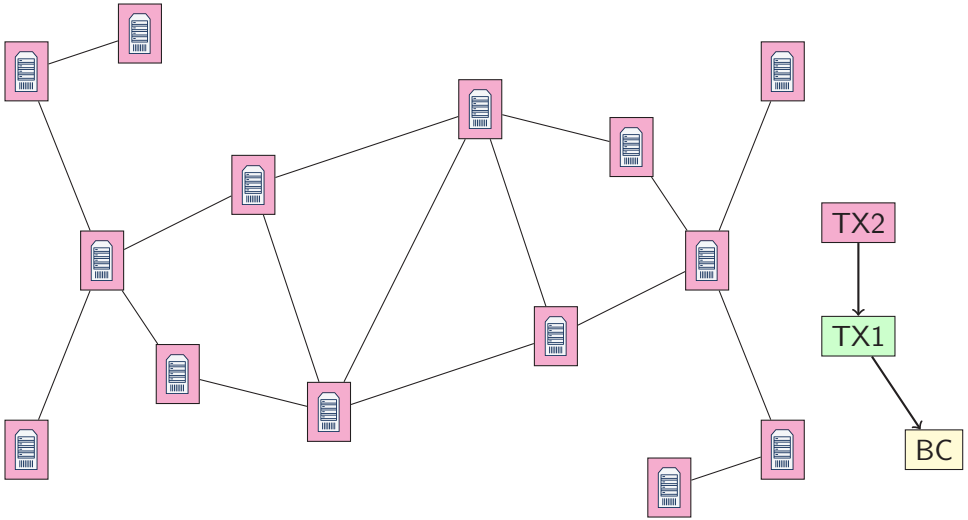
Zwei Transaktionen



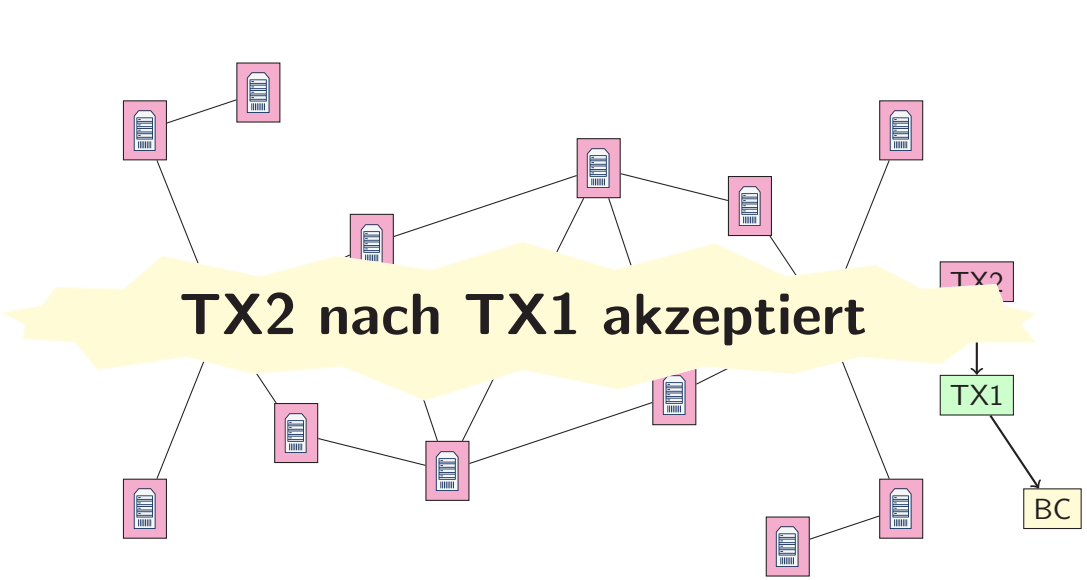
Zwei Transaktionen



Zwei Transaktionen



Zwei Transaktionen

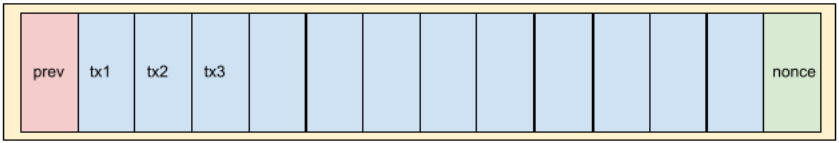


Plan

Wobei Bitcoin Strom verbraucht

- Schürfen eines Blocks: Wettbewerb aller Rechner im Bitcoinnetzwerk
- Gewinner
  - bestimmt den nächsten Block (Konsens)
  - erhält die Belohnung (block reward)
- Verfahren: **Proof of Work**
- Gleiche Aufgabe für alle Rechner: Löse ein rechenintensives Puzzle, was aber leicht zu verifizieren ist!
- Wer als erster eine Lösung findet, gewinnt.
- Alle anderen verifizieren.

Das Bitcoin Puzzle



- Ein Block besteht aus (u.a.)
  - prev: Hashwert des Vorgängerblocks
  - tx1, . . . : Transaktionen
  - nonce: ein frei wählbarer Wert
- **Aufgabe des Bitcoin Puzzle**: Finde einen Wert für nonce, so dass der Hashwert des gesamten Blocks kleiner als eine vorgegebene Schranke ist.

Block 710033

USD | BTC

This block was mined on November 16, 2021 at 9:49 PM GMT+1 by Unknown. It currently has 1 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC ($374,104.19). The reward consisted of a base reward of 6.25000000 BTC ($374,104.19) with an additional 0.05383451 BTC ($3,222.35) reward paid as fees of the 3248 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 28,130.42414084 BTC ($1,683,793,514.76) were sent in the block with the average transaction being 8.66084487 BTC ($518,409.33). Learn more about how blocks work.

Hash	00000000000000000050311490a7b879b3ef6e3c6590251d62c1c125280cfc6
Confirmations	1
Timestamp	2021-11-16 21:49
Height	710033
Miner	Unknown
Number of Transactions	3,248
Difficulty	22,674,148,233,453.11
Merkle root	da3debfc46fdf8d608e6d6bb0003386237fc2d321dd4cc2f6e27711db0a173f4
Version	0x20004004
Bits	386,689,514
Weight	3,999,812 WU
Size	1,549,358 bytes
Nonce	2,237,267,554
Transaction Volume	28130.42414084 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.05383451 BTC

Quelle: https://www.blockchain.com/btc/block/00000000000000000050311490a7b879b3ef6e3c6590251d62c1c125280cfc6

Schwere des Bitcoin Puzzle

- Je kleiner die Schranke, desto schwerer das Puzzle!
- Aktuell (Nov. 2022) muss die Binärdarstellung mit 76 Nullen beginnen.
- Die Wahrscheinlichkeit, dass ein Hashwert diese Eigenschaft hat, ist 2^{-76}.
- D.h. unter $2^{76} \approx 10^{23}$ Versuchen erwarten wir einen Treffer.
- Die Schwere stellt sich so ein, dass durchschnittlich alle 10 Minuten ein Treffer zu erwarten ist.
- also 1.6e22 Hashes pro Sekunde

Bitcoin Hash Rate

Quelle: https://www.blockchain.com/charts/hash-rate

Nochmal zum Stromverbrauch

- Stromverbrauch für das Hashpuzzle: ca 130 TWh pro Jahr
- Bruttojahresverbrauch Norwegen 125.7 TWh, Argentinien 132.7 TWh, Deutschland 544 TWh
- Gesamtproduktion elektrische Energie weltweit in 2018: 26,6 PWh
  - davon verbraucht Bitcoin 0.5%
  - elektrische Geräte in Standby (USA) 0.85%
  - weltweiter Verlust beim Stromtransport 8.251%

Quelle: https://www.watson.ch/wissen/wirtschaft/957154209-bitcoin-und-der-energieverbrauch-13-punkte-die-du-kennen-musst

Alternative: Proof of Stake

- Neuere Blockchains verwenden andere Verfahren für den Konsens.
- **Proof of Stake** verteilt das Recht, den nächsten Block zu bestimmen, gemäß des Kontostandes.
- Drei Ansätze
  - Ethereum (Belohnung und Strafe)

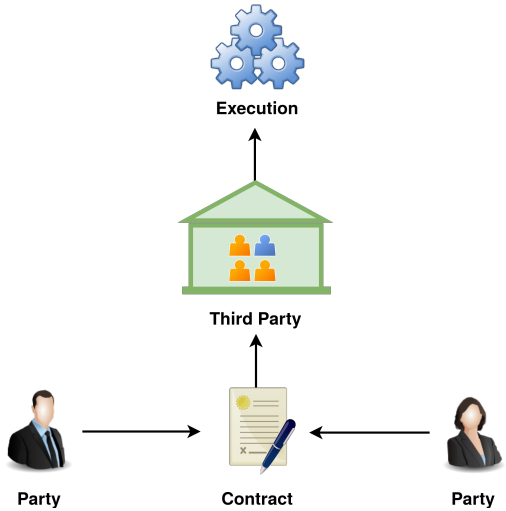
    Quelle https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
  - Tezos (Belohnung und Strafe)

    Quelle: https://tezos.gitlab.io/active/proof_of_stake.html
  - Algorand (Verifiable Random Functions, Silvio Micali)

    Quelle: https://www.algorand.com/technology/white-papers

Plan

Traditionelle Verträge



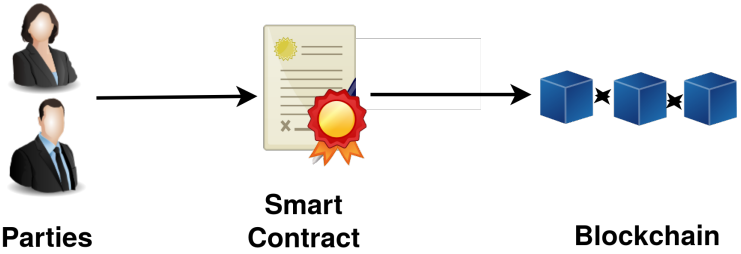
Definition

- Vertragspartner
- Gemeinsames Ziel
- Verpflichtungen
- Weitere Vertragsklauseln
- Willenserklärung

Smart Contracts

Smart Contract: Programm, das auf der Blockchain abgelegt ist und dort automatisch abläuft.

- Nick Szabo 1997 (dry code)
- Vertrag in ausführbarer Form
  (Lawrence Lessig: Code is law)
- Selbst-vollstreckende Regeln

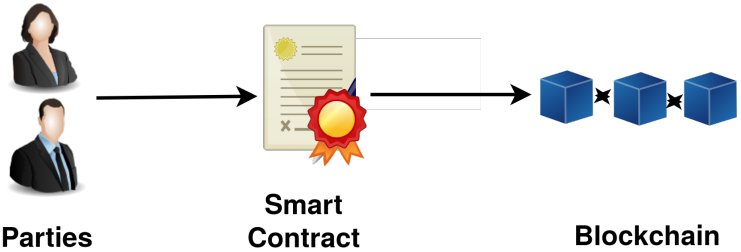


Smart Contract: Programm, das auf der Blockchain abgelegt ist und dort automatisch abläuft.

- Nick Szabo 1997 (dry code)
- Vertrag in ausführbarer Form (Lawrence Lessig: Code is law)
- Selbst-vollstreckende Regeln

Ziele:

- Vertrauenswürdige Ausführung ohne Dritte
- Sicherheit, niedrige Transaktionskosten



UNI FREIBURG

Eigenschaften

- Code gespeichert auf der Blockchain $\Rightarrow$ **unveränderlich**
- Ausgeführt im Netz $\Rightarrow$ **verteilter weltweiter Computer**
- Transparenz
  - Zugriff, Interaktion und Verifikation (jeder)
  - Konsens über Ergebnisse
  - Daten gespeichert auf der Blockchain

Smart Contracts

Eigenschaften

- Code gespeichert auf der Blockchain $\Rightarrow$ **unveränderlich**
- Ausgeführt im Netz $\Rightarrow$ **verteilter weltweiter Computer**
- Transparenz
  - Zugriff, Interaktion und Verifikation (jeder)
  - Konsens über Ergebnisse
  - Daten gespeichert auf der Blockchain

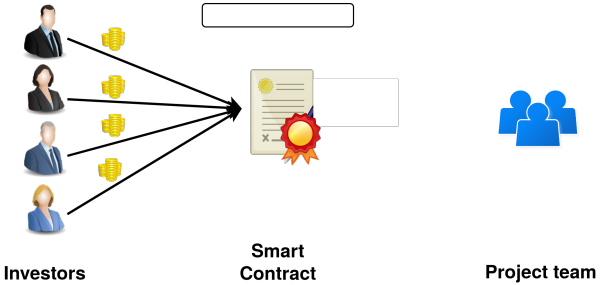
Funktionen

- Geld senden und empfangen
- Interaktion mit anderen Smart Contracts

Bespiel: Crowdfunding

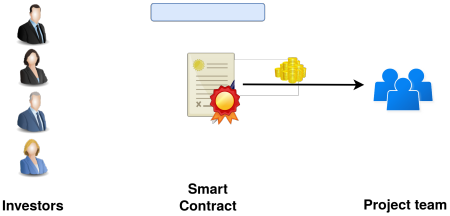
Geld einsammeln von Investoren zur Unterstützung eines Projekts

- Projektteam: definiert Projekt, setzt Zielbetrag und Termin
- Investor: setzt Geld auf ein Projekt

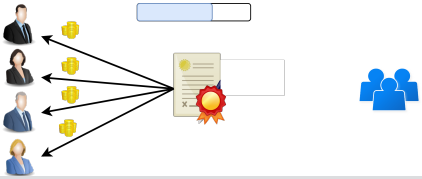


1. Wenn der Zielbetrag bis zum Termin erreicht ist, dann wird automatisch das gesammelte Geld ans Projektteam überwiesen

1. Wenn der Zielbetrag bis zum Termin erreicht ist, dann wird automatisch das gesammelte Geld ans Projektteam überwiesen



2. Wenn der Zielbetrag nicht erreicht wird, dann erhält jeder Investor seinen Einsatz zurück



Plan

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens
- Mechanik des Schürfens

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens
- Mechanik des Schürfens
- Transaktionsprogramme “smart contracts”

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens
- Mechanik des Schürfens
- Transaktionsprogramme “smart contracts”
- Viele Dinge nicht angesprochen

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens
- Mechanik des Schürfens
- Transaktionsprogramme “smart contracts”
- Viele Dinge nicht angesprochen
  - Konsens-Protokolle

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens
- Mechanik des Schürfens
- Transaktionsprogramme “smart contracts”
- Viele Dinge nicht angesprochen
  - Konsens-Protokolle
  - Ökonomie des Schürfens

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens
- Mechanik des Schürfens
- Transaktionsprogramme “smart contracts”
- Viele Dinge nicht angesprochen
  - Konsens-Protokolle
  - Ökonomie des Schürfens
  - Identifizierung von Konten und Anwendern durch digitale Unterschriften (Kryptographie)

Zusammenfassung

- Kleiner Einblick in die Blockchain Technologie
- Blöcke, Transaktionen, Konten, Kryptographischer Hash, Konsens
- Mechanik des Schürfens
- Transaktionsprogramme “smart contracts”
- Viele Dinge nicht angesprochen
  - Konsens-Protokolle
  - Ökonomie des Schürfens
  - Identifizierung von Konten und Anwendern durch digitale Unterschriften (Kryptographie)
- Viele spannende Anwendungen