

Grundlagen der Blockchain Technologie

Albert-Ludwigs-Universität Freiburg

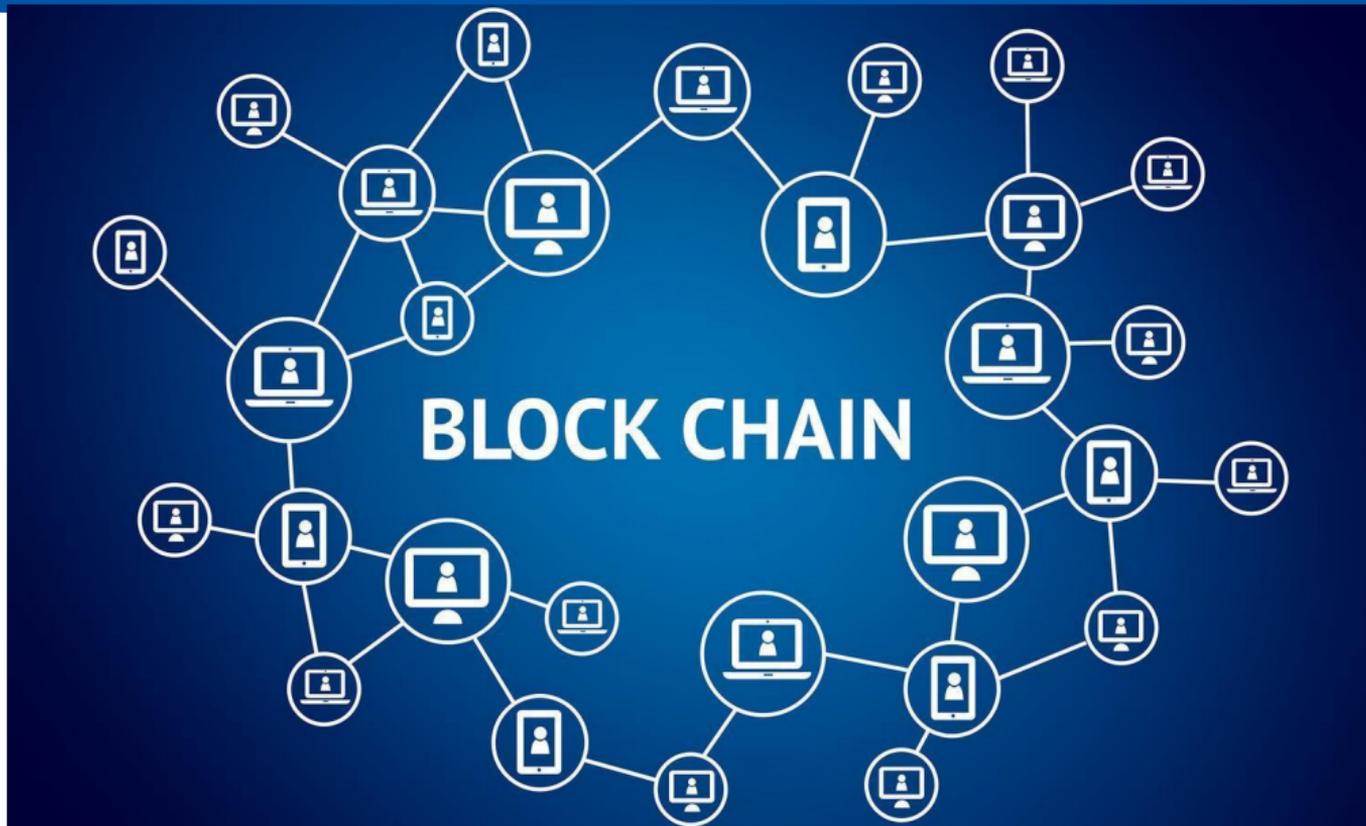
Prof. Dr. Peter Thiemann

16 Nov 2022



**UNI
FREIBURG**

Blockchain ist in aller Munde



Blockchain ist in aller Munde

SPIEGEL ONLINE **SPIEGEL**

[Alle Texte](#) | [Anmelden](#)



ConsenSys-Gründer Lubin im Interview

Die Neuerfindung des Internets - dank Blockchain

Blockchain ist in aller Munde



Blockchain ist in aller Munde



The Independent ✓

@Independent

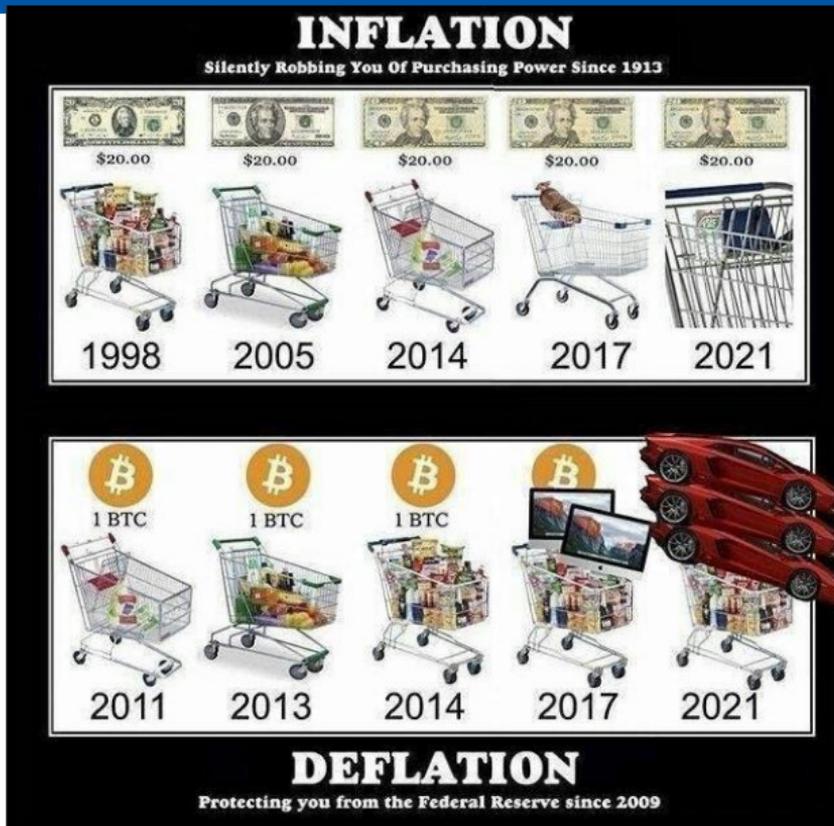


IT man accidentally threw away bitcoin drive worth £63 million

[independent.co.uk/life-style/gad...](https://www.independent.co.uk/life-style/gad...)

♡ 14 8:26 PM - Dec 4, 2017

Blockchain ist in aller Munde



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.



Bitcoin-Rechner (Archivbild)

REUTERS

Blockchain ist in aller Munde



Silicon Valley

Keine Kommentare

„Blockchain ist der größte 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?



The screenshot shows the German Wikipedia page for 'Blockchain'. At the top, there is a navigation bar with the URL 'https://de.wikipedia.org/wiki/Blockchain' and user status 'Nicht angemeldet'. Below this, there are tabs for 'Artikel' and 'Diskussion', and a search bar containing 'Wikipedia durchsuche'. The main heading is 'Blockchain'. The first paragraph defines it as a 'Blockchain' (also 'Block Chain' in English) which is a continuously expandable list of 'Datensätzen' (data sets) called 'Blöcke' (blocks), linked together using 'kryptographischer Verfahren' (cryptographic methods). Each block contains a 'kryptographisch sicheren Hash' (cryptographically secure hash) of the previous block, a 'Zeitstempel' (timestamp), and 'Transaktionsdaten' (transaction data). The second paragraph explains that the term 'Blockchain' is also used for a 'Buchführungssystem' (accounting system) that is decentralized and documents the 'richtige' (correct) state, as many participants are involved in the bookkeeping.



The screenshot shows the German Wikipedia page for 'Blockchain'. The page title is 'Blockchain' and it is currently on the 'Diskussion' (Discussion) tab. The main text describes a blockchain as a 'kontinuierlich erweiterbare Liste von Blöcken' (continuously extensible list of blocks) which are 'kryptographisch verknüpft' (cryptographically linked). A large, 3D purple question mark is overlaid on the right side of the page, partially obscuring the text. The browser address bar shows 'https://de.wikipedia.org/wiki/Blockchain'.

← → ↻ <https://de.wikipedia.org/wiki/Blockchain> 🔍 ☆ 📄 📧 👤 ⋮

Nicht angemeldet [Diskussionsseite](#) [Beiträge](#) [Benutzerkonto erstellen](#) [Anmelden](#)

Artikel [Diskussion](#) 🔍

Blockchain

Eine **Blockchain**^{[1][2][3]} (auch *Block Chain* oder *Blockkette*) ist eine kontinuierlich erweiterbare Liste von Blöcken, die durch sogenannte „Blöcke“, welche mittels **kryptographischer Verfahren** miteinander verknüpft sind.^{[1][6]} Jeder Block enthält dabei typischerweise einen **kryptographisch sicheren Hash** (Streuwert) des vorhergehenden Blocks,^[6] einen **Zeitstempel** und **Transaktionsdaten**.^[7]

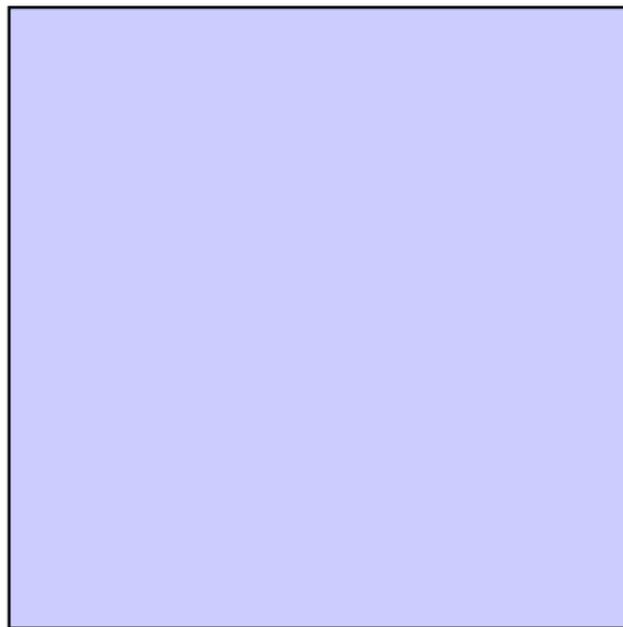
Der Begriff *Blockchain* wird auch genutzt für ein **Buchführungssystem**, das dezentral geführt wird und der jeweils *richtige* Zustand dokumentiert werden muss, weil viele Teilnehmer an der Buchführung beteiligt sind.



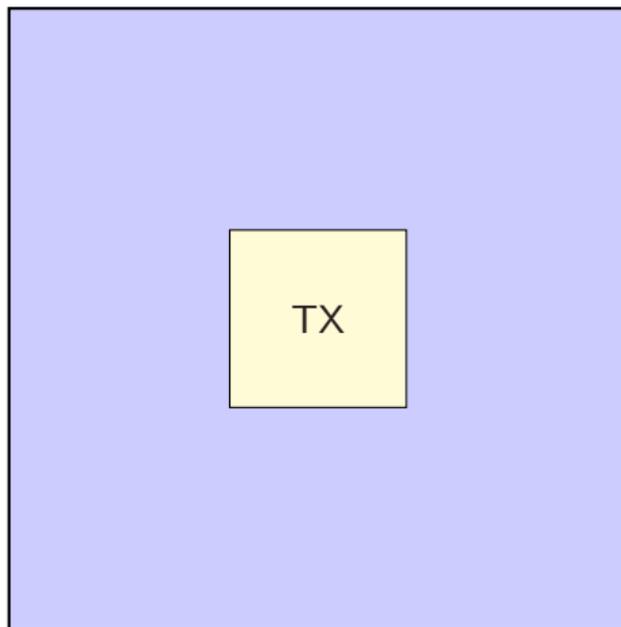
Da stelle mehr uns ganz dumm...

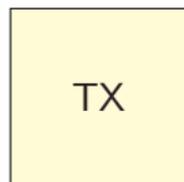
- 1 Blöcke und Transaktionen
- 2 Hashing
- 3 Konsens
- 4 Arbeitsbeweis
- 5 Kode ist Gesetz
- 6 Zusammenfassung

Am Anfang war der Block



Am Anfang war der Block





ist eine **Transaktion**

Was ist eine Transaktion?





Was ist eine Transaktion?

“Geld” wird bewegt!

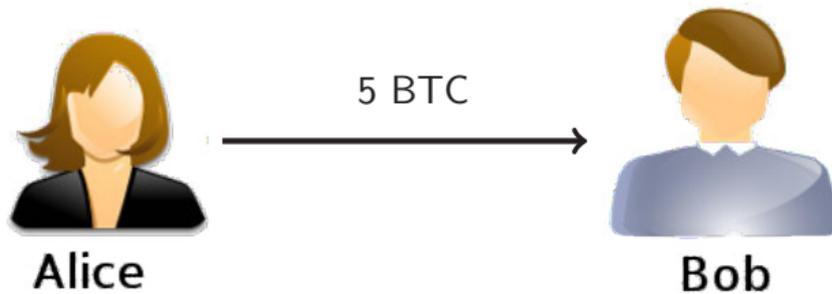


Was ist eine Transaktion?

“Geld” wird bewegt!

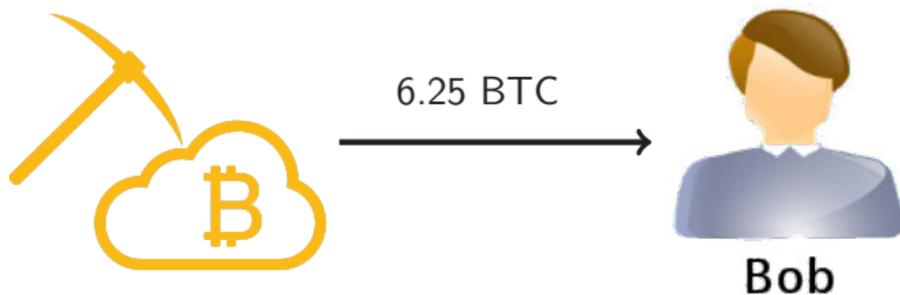
Und mehr . . .

Transaktion “Überweisung”



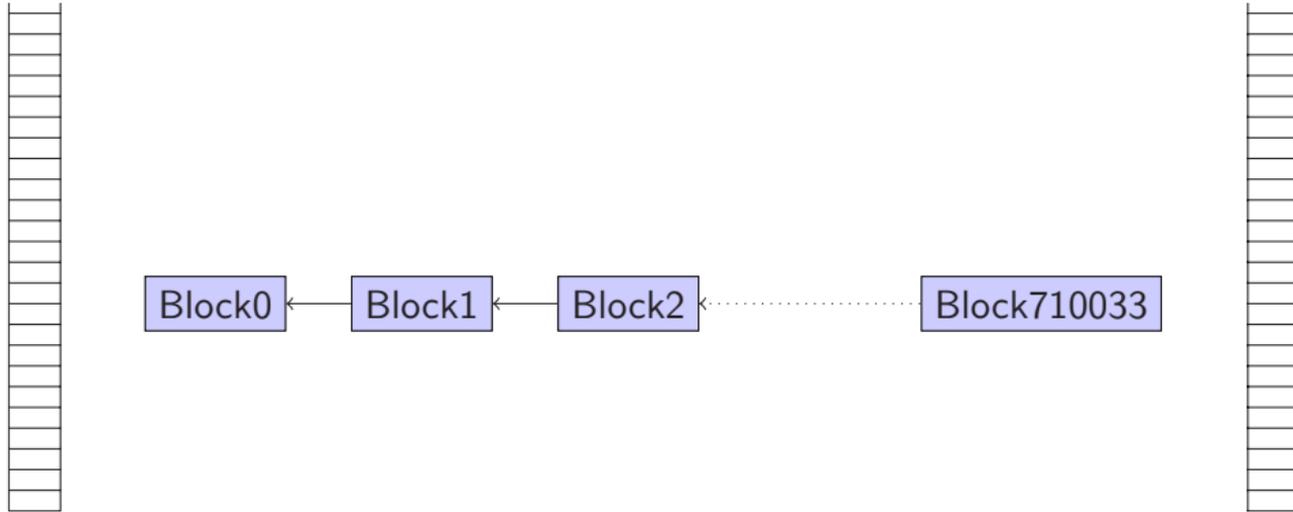
- Alice überweist 5 BTC an Bob.

Transaktion "Schürfen" (Mining)



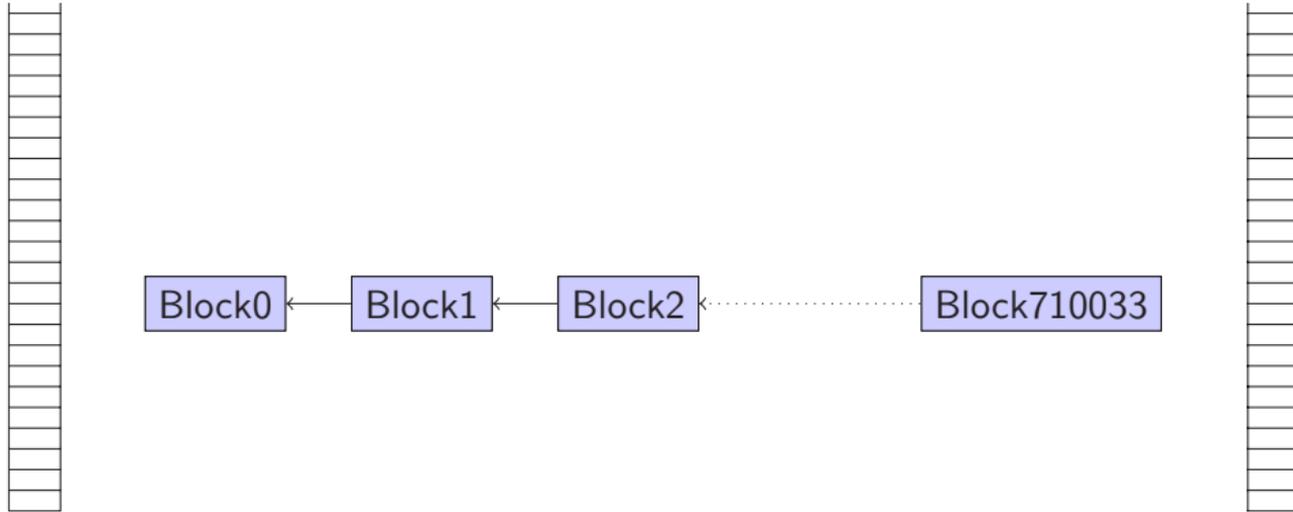
- Neue BTC entstehen durch **Schürfen**.
- Der Schürfer erhält eine Belohnung (seit 11.5.2020: 6.25 BTC).
- Beim aktuellen Kurs 16430.50 EUR/BTC: 102690.625 EUR.

Die Geschichte der Bitcoin-Blockchain



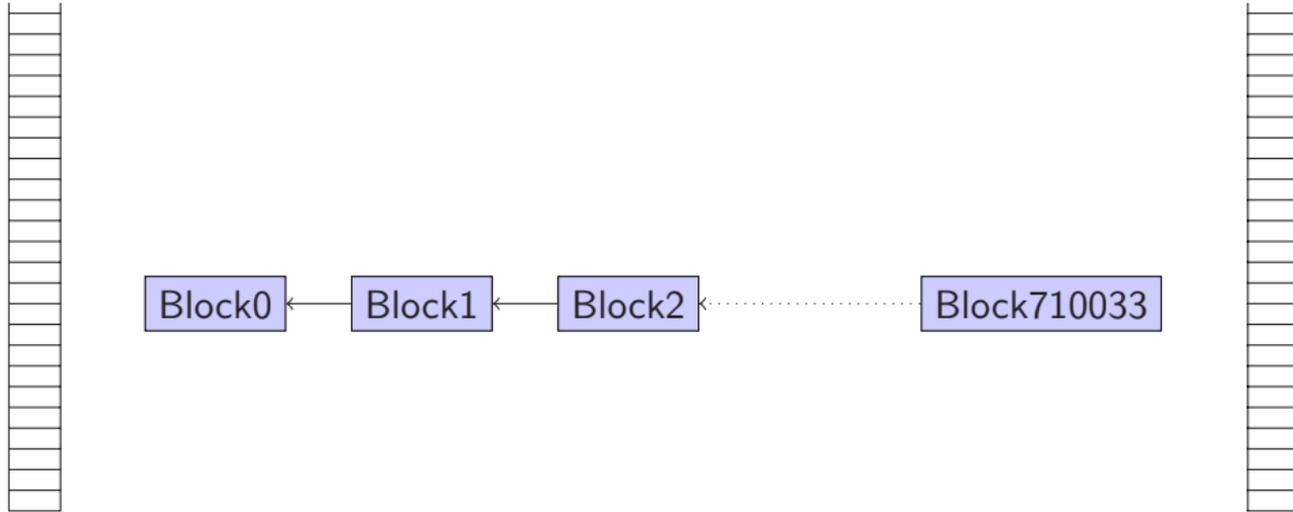
- Urknall: Januar 2009

Die Geschichte der Bitcoin-Blockchain



- Urknall: Januar 2009
- Alle Konten auf 0

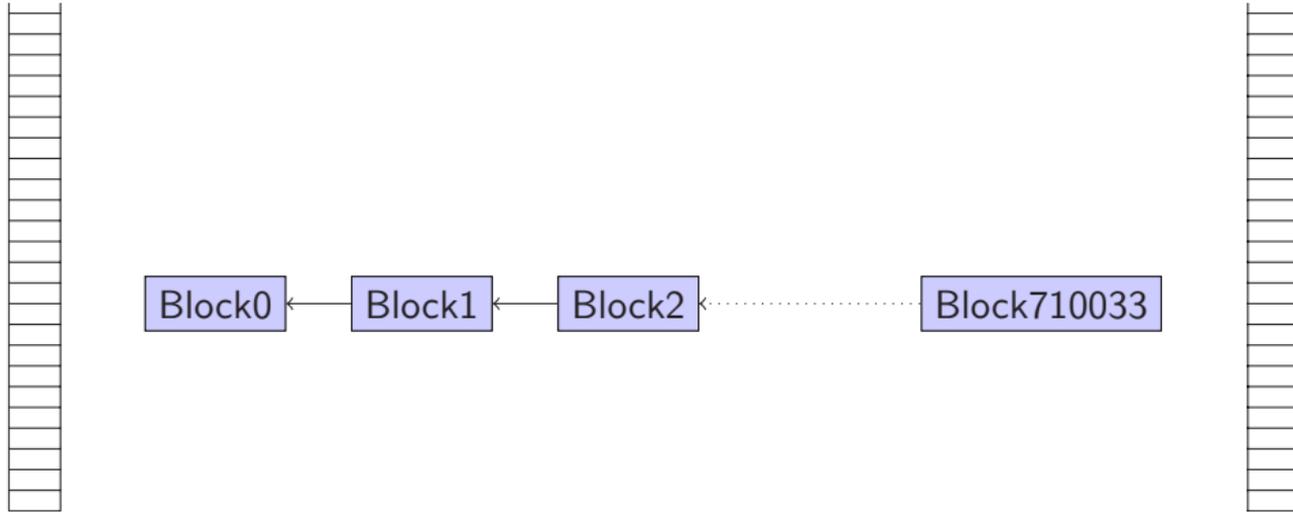
Die Geschichte der Bitcoin-Blockchain



- 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

Bitcoin Block #763.301

Abgebaut am 15.11.2022, 16:46:54 [Alle Blöcke anzeigen](#)

This block was mined on 15.11.2022, 16:46:54 by [F2Pool](#). Insgesamt wurden 2.814,56 BTC (\$47.989.722) in dem Block gesendet, wobei die durchschnittliche Transaktion bei 2,9534 (Ticker) (\$34.101,04) lag. F2Pool hat eine Gesamtbelohnung von 6,25 BTC (fiatsymbol)102.303 erhalten. Die Belohnung bestand aus einer Basisbelohnung von 6,25 BTC \$102.303 mit einer zusätzlichen 0,1612 BTC (\$0.00) Belohnung, die als Gebühren der 953-Transaktionen gezahlt wird die in den Block aufgenommen wurden.



Details

Hash	00000-59f70	Größe	1.153.986
Tiefe	1	Version	0x3ffffe004
Kapazität	110.05%	Merkle-Wurzel	14-15
Abstand	8Mo, 34Sek.	Schwierigkeitsgrad	36.762.198.818.467.21
BTC	2.814,5607	Nonce	28.774.436
<u>Wert</u>	<u>\$47.989.722</u>	Bits	386.377.746
Wert heute	\$47.844.604	Gewicht	3.998.127 WU
Durchschnittswert	2,9533690110 BTC	Mittlere Zeit	15 Nov 2022, 16:45:13
Medianwert	0,03395430 BTC	<u>Geprägt</u>	<u>6,25 BTC</u>
Eingabewert	2.814,72 BTC	Belohnung	6.41124621 BTC
Ausgabewert	2.820,97 BTC	Abgebaut am	15 Nov 2022, 16:46:54
<u>Transaktionen</u>	<u>953</u>	Höhe	<u>763.301</u>
Zeuge Tx's	781	Bestätigungen	1
Eingaben	6.984	Miner	F2Pool
Ausgaben	2.249	Coinbase	>=mm, K o #9%g u- vs[g7+, Aq u 6g b p /F2Pool/s)c
<u>Gebühren</u>	<u>0,16124621 BTC</u>		
Gebühren Kb	0,0001397 BTC		
Gebühren kWU	0,0000403 BTC		
Gebührenbereich	2-225 sat/vByte		
Durchschnittliche Ge...	0,00016920		
Mittlere Gebühr	0,00003960		

Blockchain



TX 0 • Hash 444a-08db 15.11.2022, 16:46:54	6.41124621 BTC \$109,315 Gebühr 0 Sats \$0,00
TX 1 • Hash 8c46-e3f1 15.11.2022, 16:45:36	0.32487414 BTC \$5.539,27 Gebühr 50.0T Sats \$8,53
TX 2 • Hash a6d2-68d6 15.11.2022, 16:44:40	0.35914880 BTC \$6.123,67 Gebühr 50.0T Sats \$8,53
TX 3 • Hash b1dc-6896 15.11.2022, 16:45:59	2.61724369 BTC \$44.625,37 Gebühr 40.0T Sats \$6,82
TX 4 • Hash 5991-518c 15.11.2022, 16:45:05	0.00196071 BTC \$33,43 Gebühr 20.9T Sats \$3,57
TX 5 • Hash dbc7-d2c3 15.11.2022, 16:45:27	7.93142950 BTC \$135.234 Gebühr 52.0T Sats \$8,87
TX 6 • Hash 0b7a-dcd5 15.11.2022, 16:46:28	10.74604789 BTC \$183.225 Gebühr 76.0T Sats \$12,97
TX 7 • Hash 8b3c-e439 15.11.2022, 16:45:05	0.01510932 BTC \$257,62 Gebühr 22.1T Sats \$3,76
TX 8 • Hash 4ad2-07b7 15.11.2022, 16:46:34	0.42142218 BTC \$7185,47 Gebühr 17.3T Sats \$2,95
TX 9 • Hash 9e9f-458d 15.11.2022, 16:45:34	1.23171638 BTC \$21.001,40 Gebühr 19.8T Sats \$3,38
TX 10 • Hash c881-85c1 15.11.2022, 16:46:20	0.02944277 BTC \$502,01 Gebühr 16.3T Sats \$2,78
TX 11 • Hash 369e-9a42 15.11.2022, 16:45:30	0.90233901 BTC \$15.385,35 Gebühr 50.3T Sats \$8,57
TX 12 • Hash d4d4-66f0 15.11.2022, 16:46:29	0.02139382 BTC \$364,78 Gebühr 21.3T Sats \$3,63

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 → B	0	50	0	...
Transfer: 7.5 BTC B → A	7.5	42.5	0	...

Transaktionsgeschichte (vereinfacht)



Transaktionen	Kontostände			
	A	B	C	...
Urknall Januar 2009	0	0	0	...
Mining: 50 BTC → B	0	50	0	...
Transfer: 7.5 BTC B → A	7.5	42.5	0	...
Transfer: 2.5 BTC A,B → C	5	40	5	...

Transaktionsgeschichte (vereinfacht)



Transaktionen	Kontostände			
	A	B	C	...
Urknall Januar 2009	0	0	0	...
Mining: 50 BTC → B	0	50	0	...
Transfer: 7.5 BTC B → A	7.5	42.5	0	...
Transfer: 2.5 BTC A,B → C	5	40	5	...
⋮	⋮	⋮	⋮	⋮



- Transaktionsgeschichte ist öffentlich.

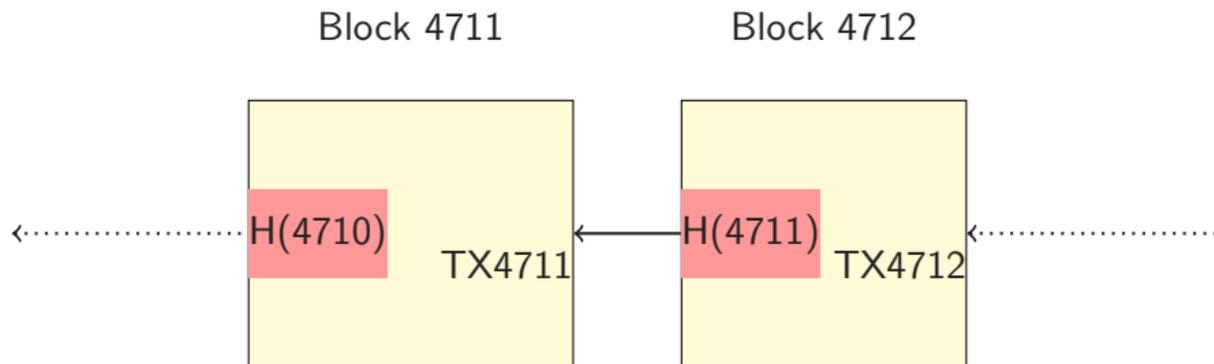
- Transaktionsgeschichte ist öffentlich.
- Jeder kann jeden Kontostand nachvollziehen.

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

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

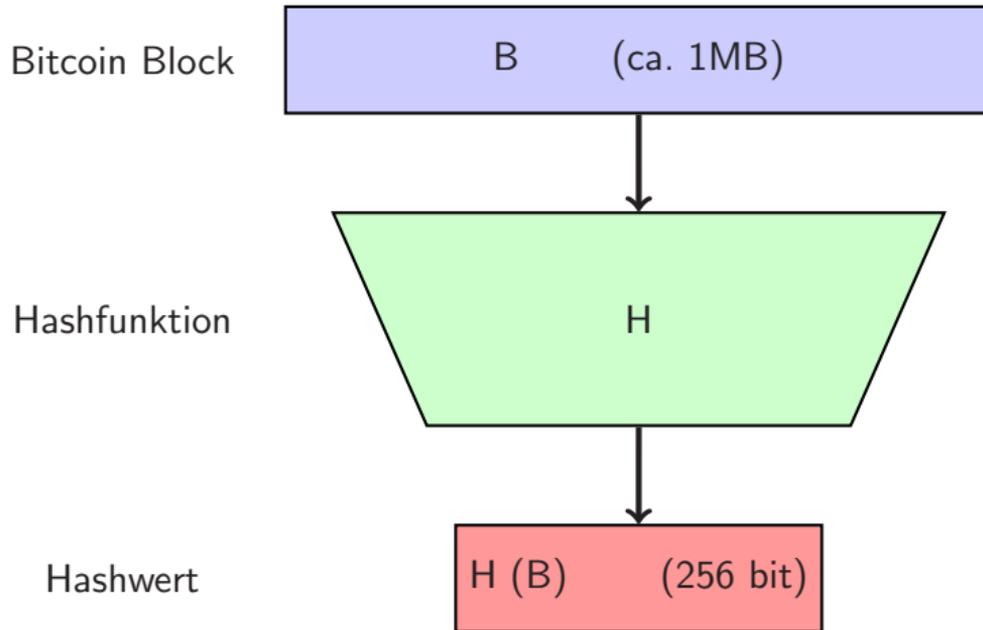
- Transaktionsgeschichte ist öffentlich.
- Jeder kann jeden Kontostand nachvollziehen.
- Jeder kann jede Transaktion prüfen.
- Wenn man sich über die Abfolge der Transaktionen einig ist!
- Dabei hilft Kryptographie!

- 1 Blöcke und Transaktionen
- 2 Hashing**
- 3 Konsens
- 4 Arbeitsbeweis
- 5 Kode ist Gesetz
- 6 Zusammenfassung



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

(Kryptographischer) Hashwert





Kollisionsresistenz

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

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

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."

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."
- $H(B_1) = 7f2c6d75c99218fe6f4b742b469c0e67b319387e3a12dad4d9dea4cd9143611$

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!"

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."
- $H(B_1)$ = 7f2c6d75c99218fe6f4b742b469c0e67b319387e3a12dad4d9dea4cd9143611
- B_2 = "Zwei Warzenschwehne spielen Fussball im Regen!"
- $H(B_2)$ = 92293fc39ecd24a05998f11f2cd8a7b007885b2b57f0581805b06419173c5fe8

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."
- $H(B_1)$ = 7f2c6d75c99218fe6f4b742b469c0e67b319387e3a12dadbd4d9dea4cd9143611
- B_2 = "Zwei Warzenschwehne spielen Fussball im Regen!"
- $H(B_2)$ = 92293fc39ecd24a05998f11f2cd8a7b007885b2b57f0581805b06419173c5fe8
- Nur ein Bit Unterschied zwischen B_1 und B_2 !



Urbildresistenz

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

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?

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: $H = \text{SHA-256}$)

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: $H = \text{SHA-256}$)
- $2^{256} \approx 1.2 \cdot 10^{78}$ 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: $H = \text{SHA-256}$)
- $2^{256} \approx 1.2 \cdot 10^{78}$ Versuche
- bei einer Million Versuche pro Sekunde: $\approx 3.6 \cdot 10^{63}$ Jahre

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: $H = \text{SHA-256}$)
- $2^{256} \approx 1.2 \cdot 10^{78}$ 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 $H(B) = H(B')$.

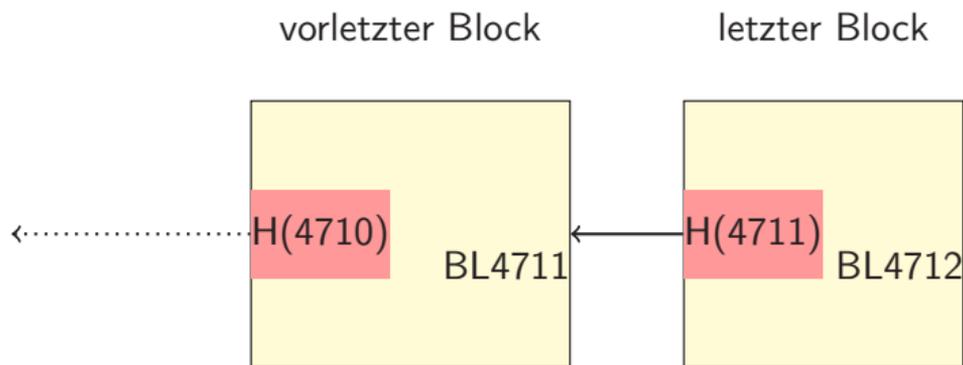
Wie aufwändig?

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

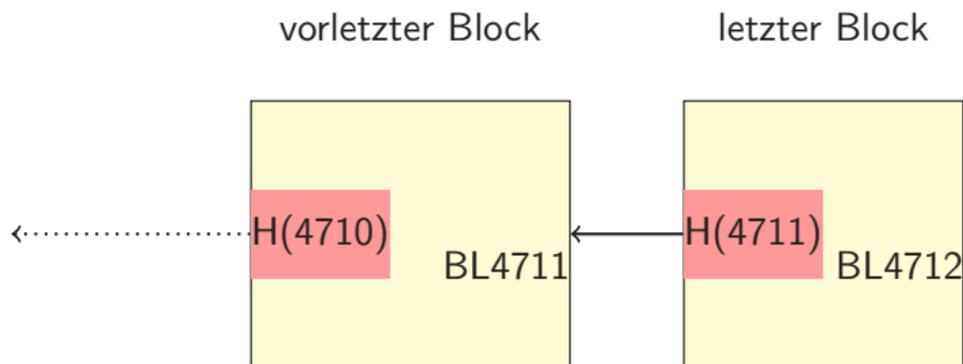
Bei vorliegendem Hashwert ist das Fälschen eines Blocks praktisch nicht möglich.

Was heisst das für die Blockchain?



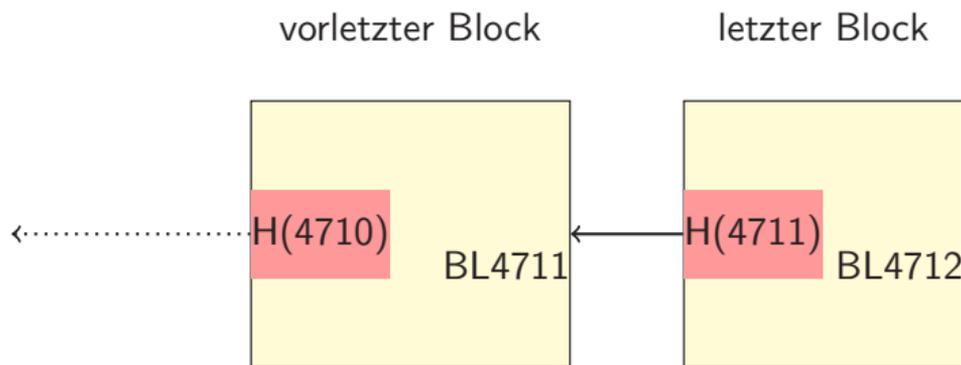
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.

Was heisst das für die Blockchain?



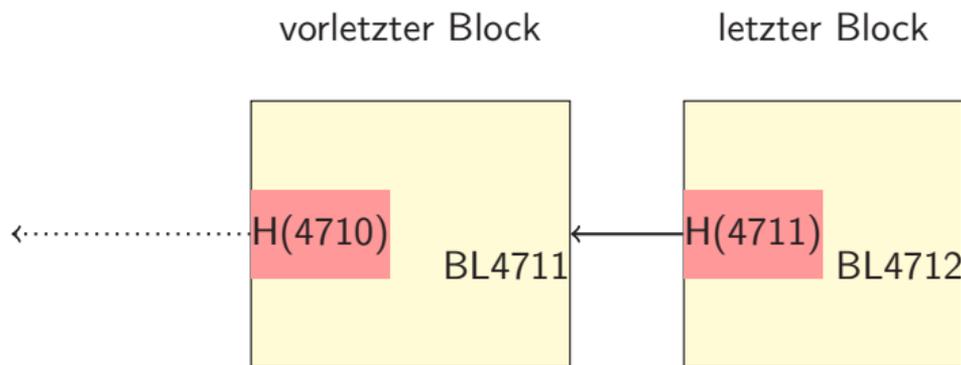
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.

Was heisst das für die Blockchain?



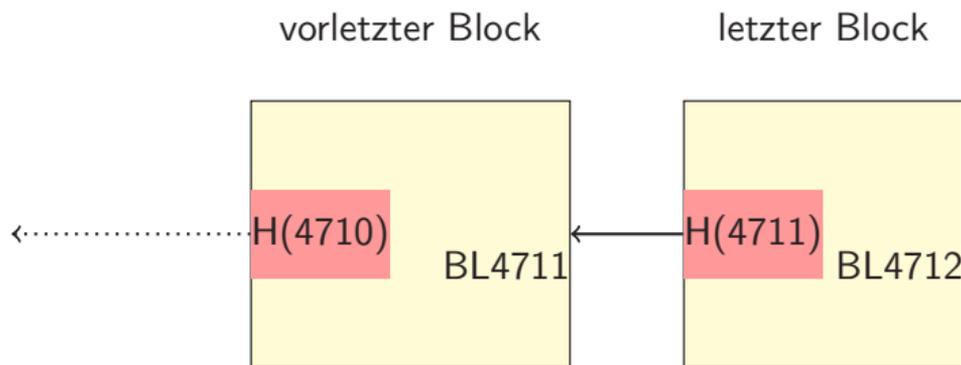
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.
- $H(4709)$ garantiert für den vor-vor-vorletzten Block und $H(4708)$.

Was heisst das für die Blockchain?



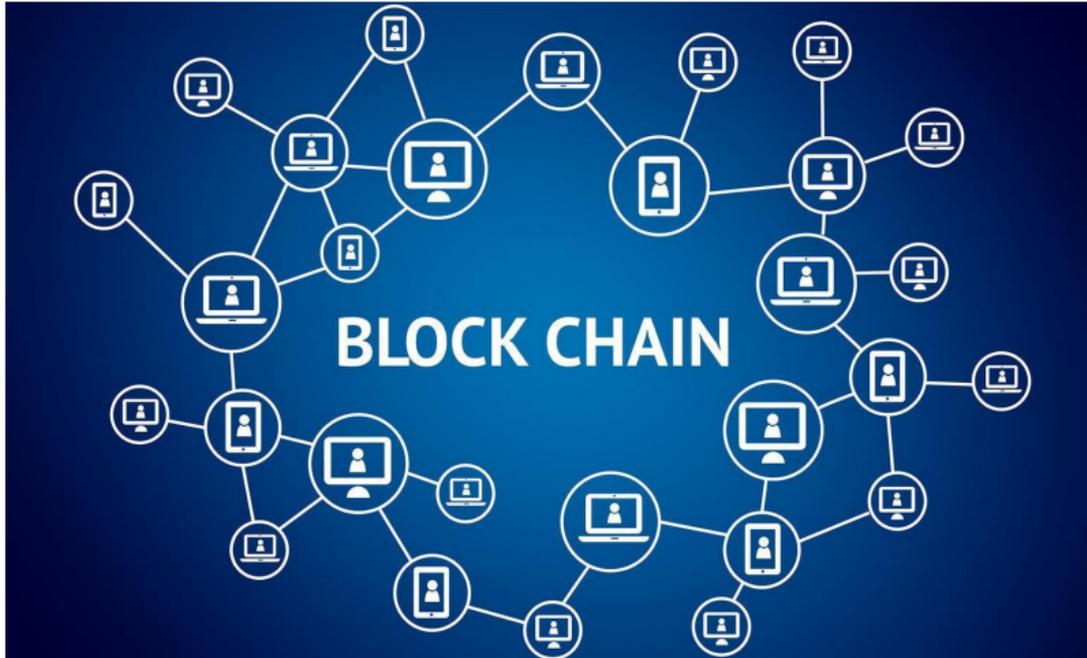
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.
- $H(4709)$ garantiert für den vor-vor-vorletzten Block und $H(4708)$.
- ...

Was heisst das für die Blockchain?



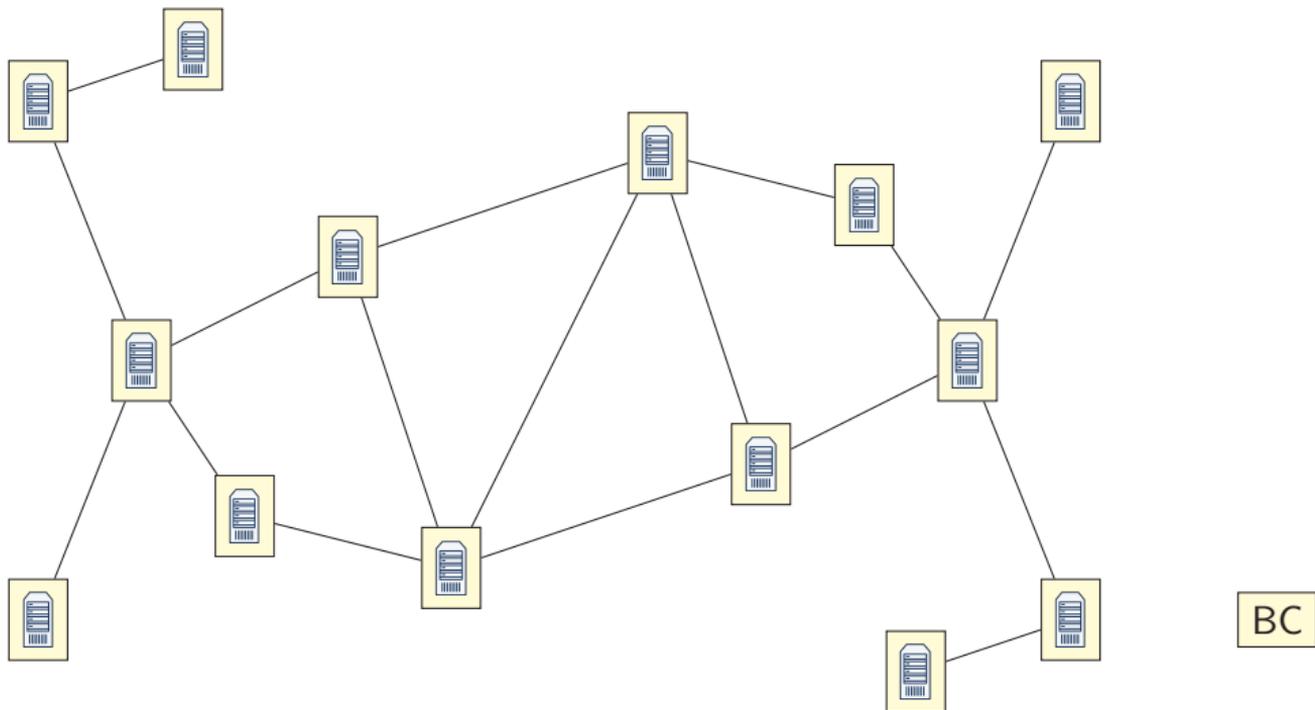
- $H(4711)$ garantiert für den vorletzten Block und $H(4710)$.
- $H(4710)$ garantiert für den vor-vorletzten Block und $H(4709)$.
- $H(4709)$ garantiert für den vor-vor-vorletzten Block und $H(4708)$.
- ...
- Also: Der letzte Blockhash garantiert für die ganze Kette!

- 1 Blöcke und Transaktionen
- 2 Hashing
- 3 Konsens**
- 4 Arbeitsbeweis
- 5 Kode ist Gesetz
- 6 Zusammenfassung

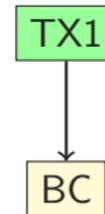
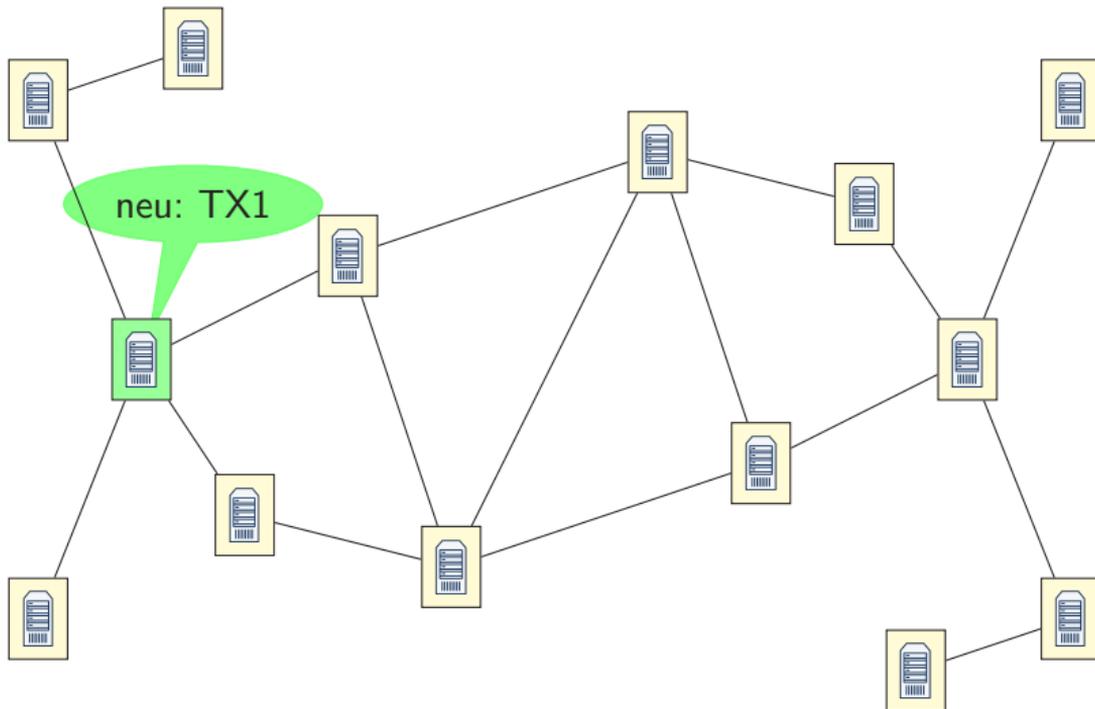


- Die Blockchain wird von einem Netz gleichwertiger Rechner unterhalten.
- Jeder Rechner hält die vollständige Blockchain.
- Jeder Rechner kann neue Transaktionen vorschlagen und schickt sie dafür an alle.
- Jeder Rechner weist unzulässige Transaktionen zurück!
- Die Mehrheit entscheidet, welche Transaktion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

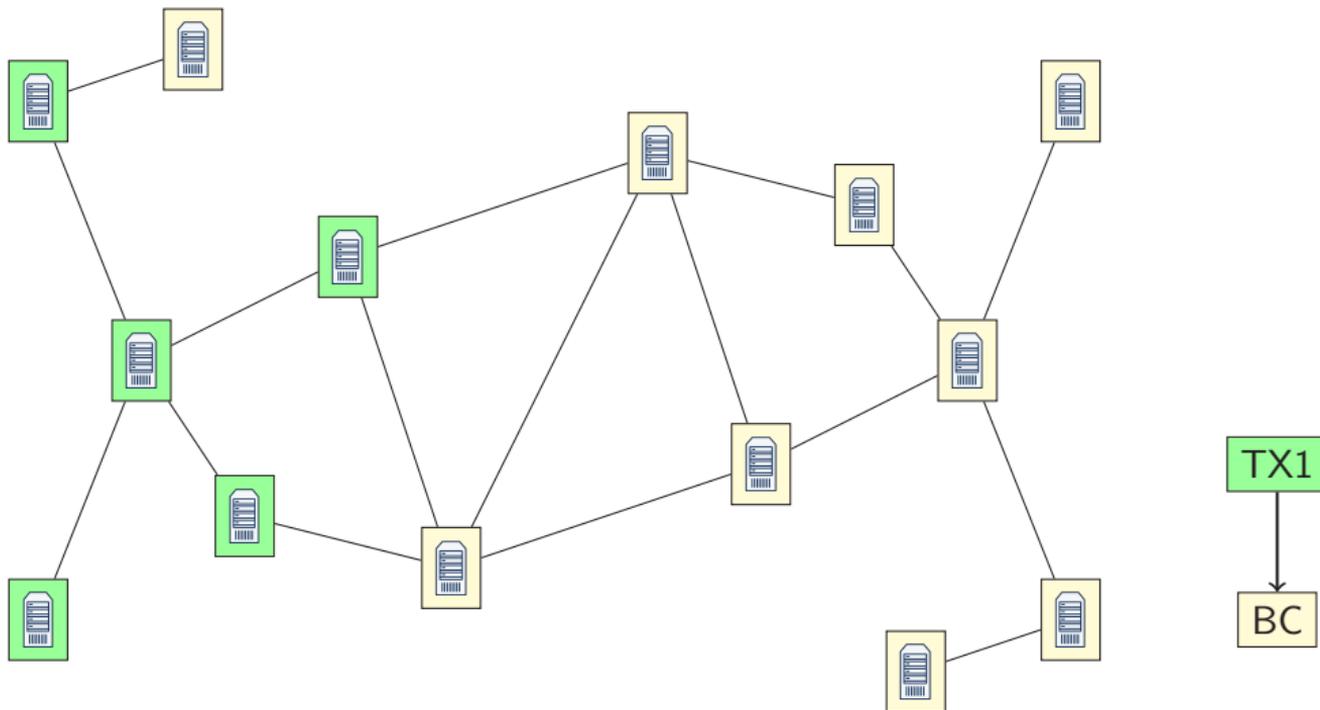
Transaktionen vorschlagen



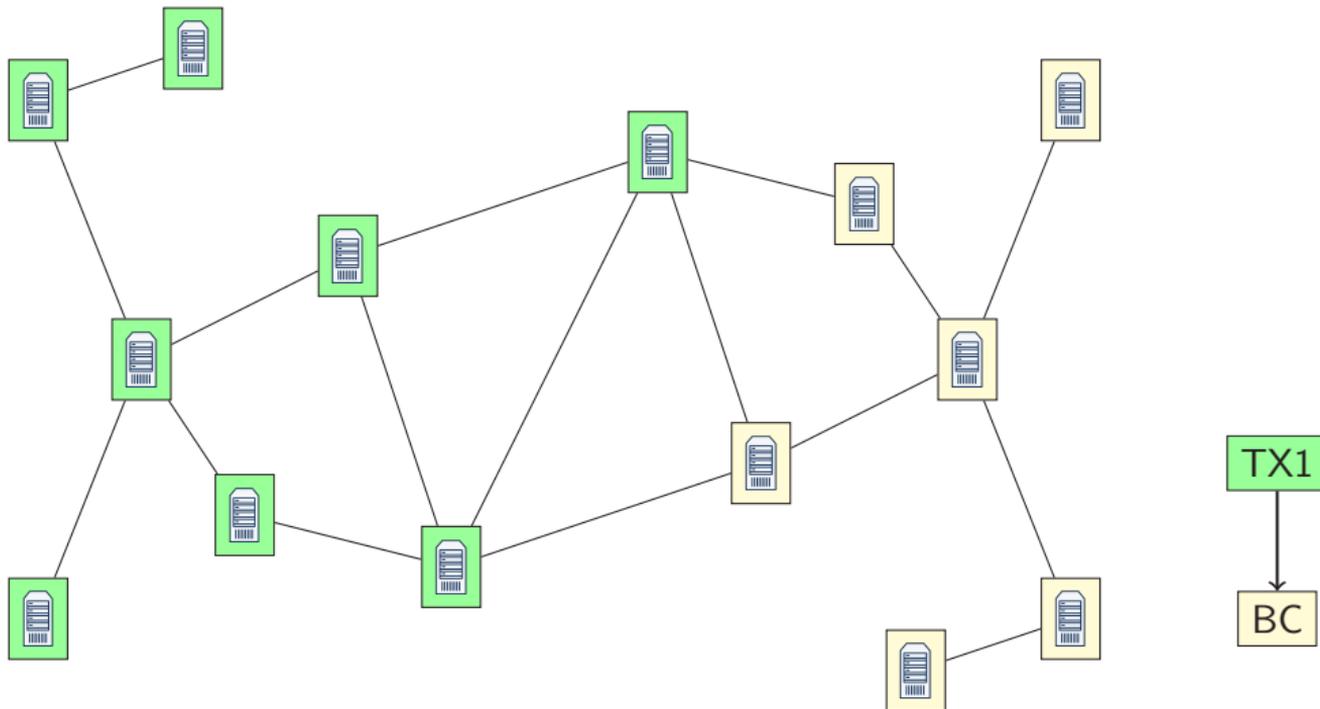
Transaktionen vorschlagen



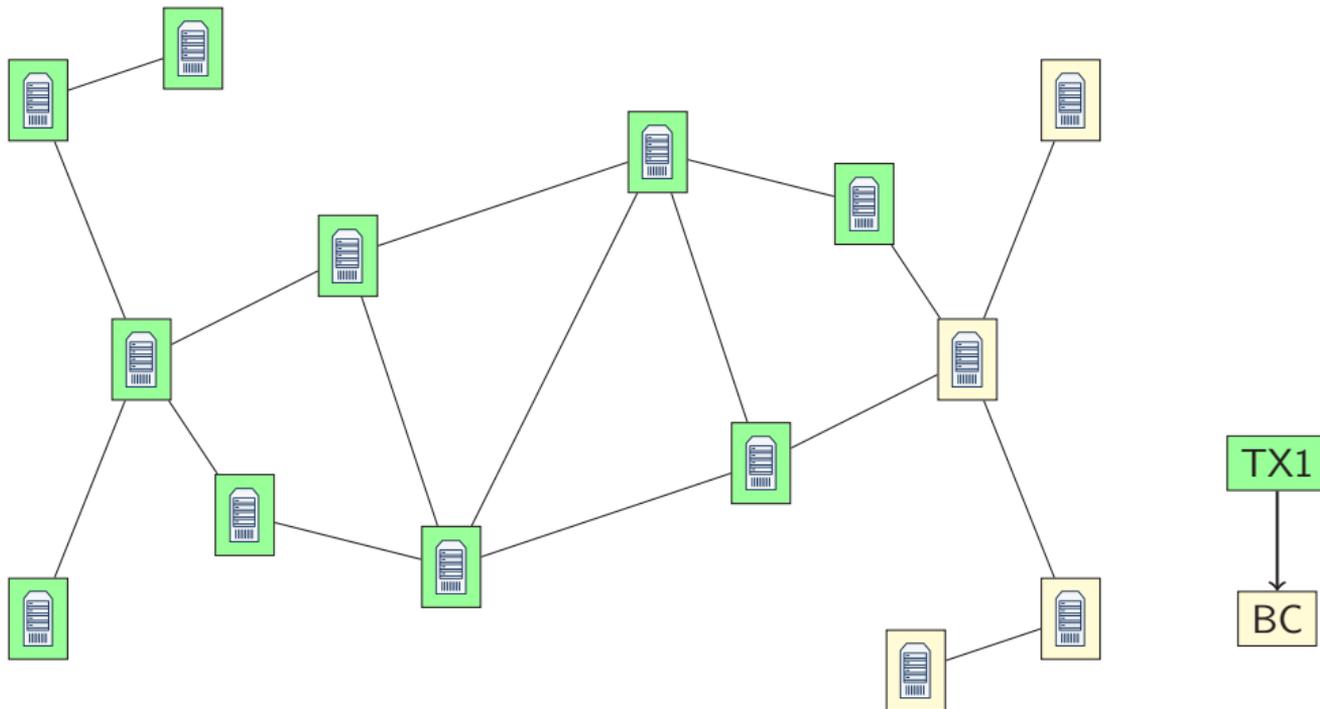
Transaktionen vorschlagen



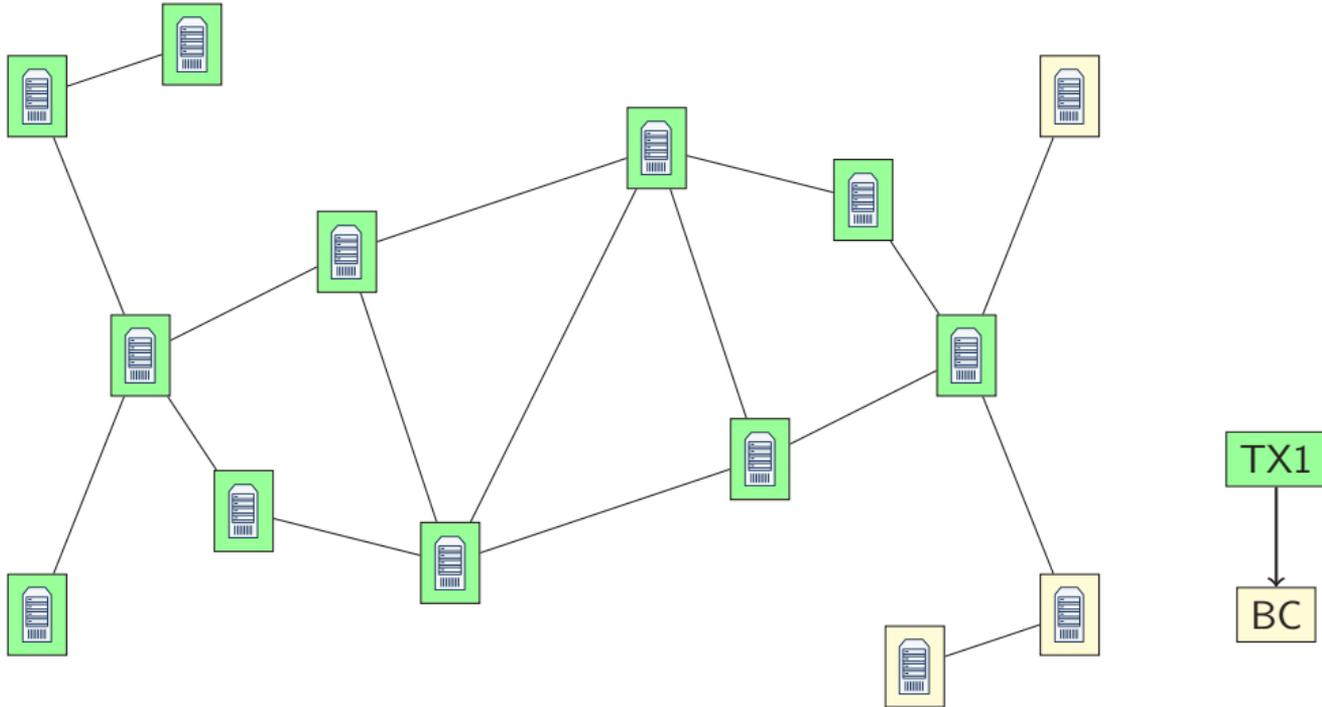
Transaktionen vorschlagen



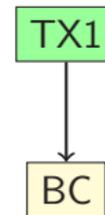
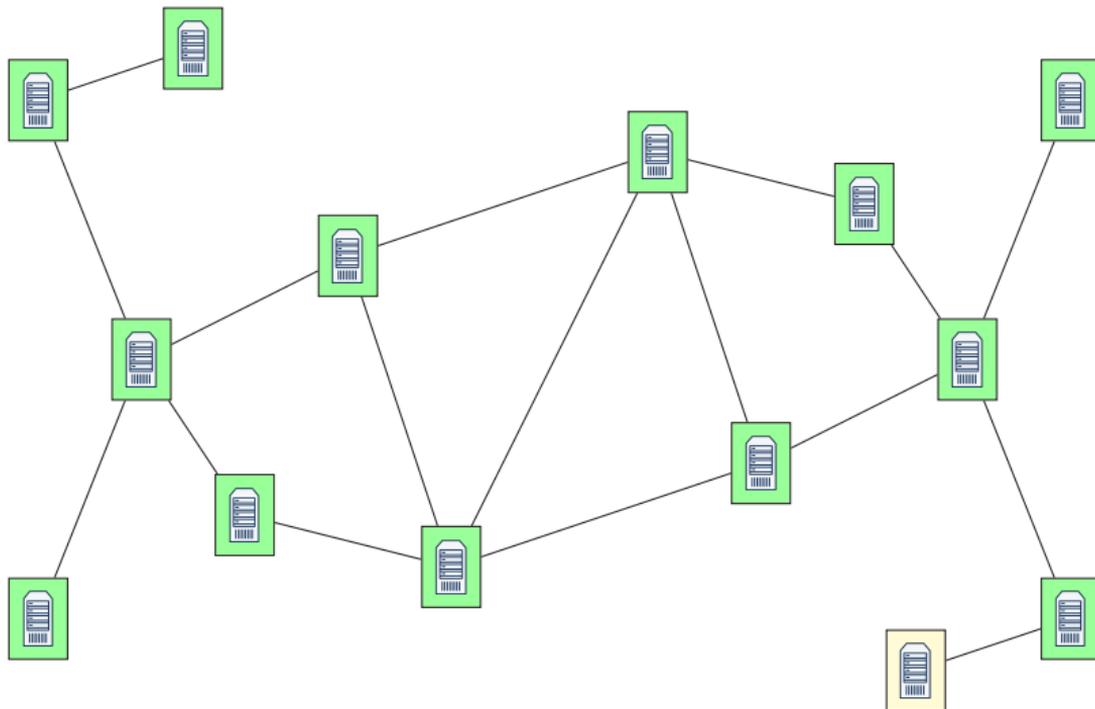
Transaktionen vorschlagen



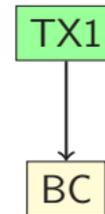
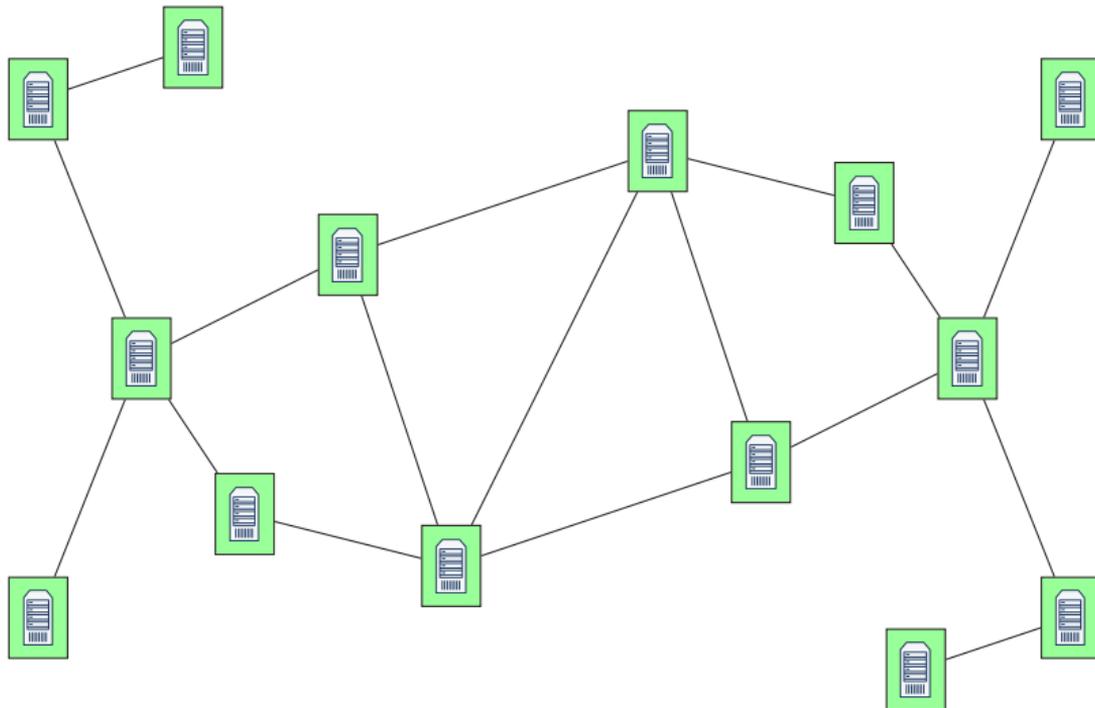
Transaktionen vorschlagen

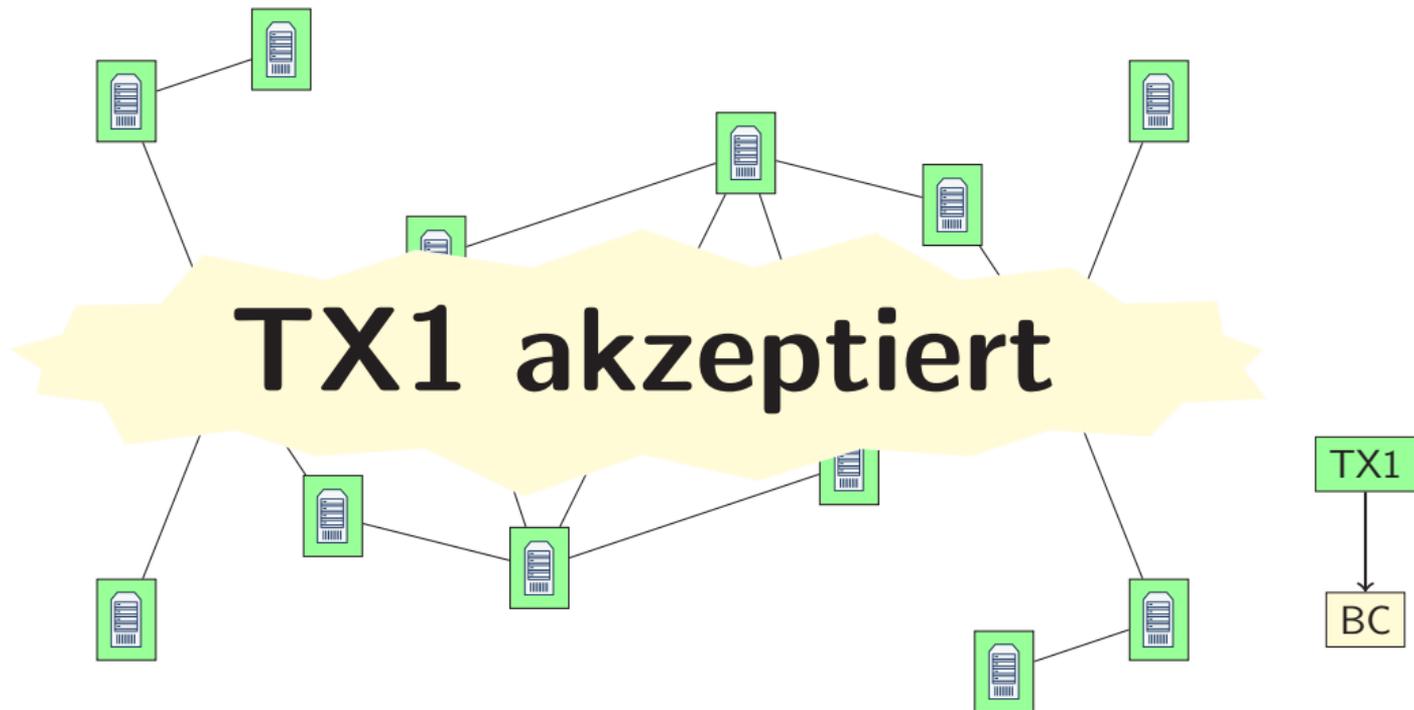


Transaktionen vorschlagen

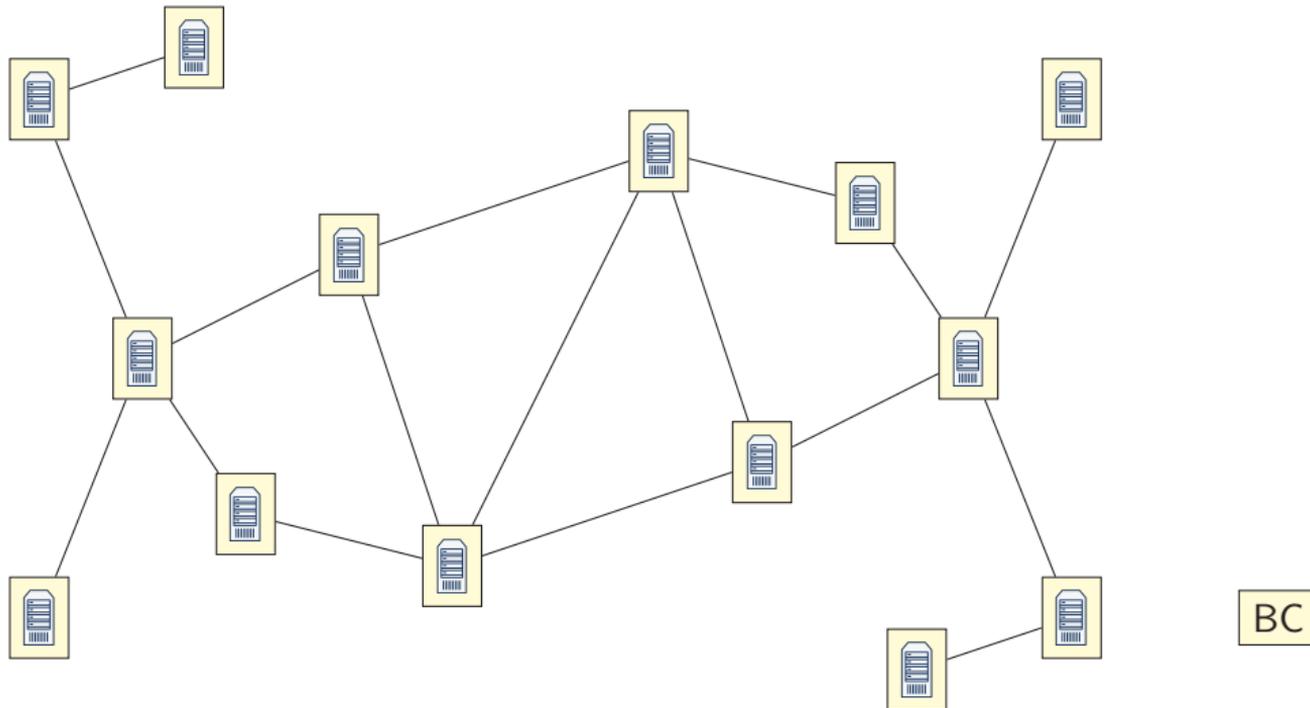


Transaktionen vorschlagen

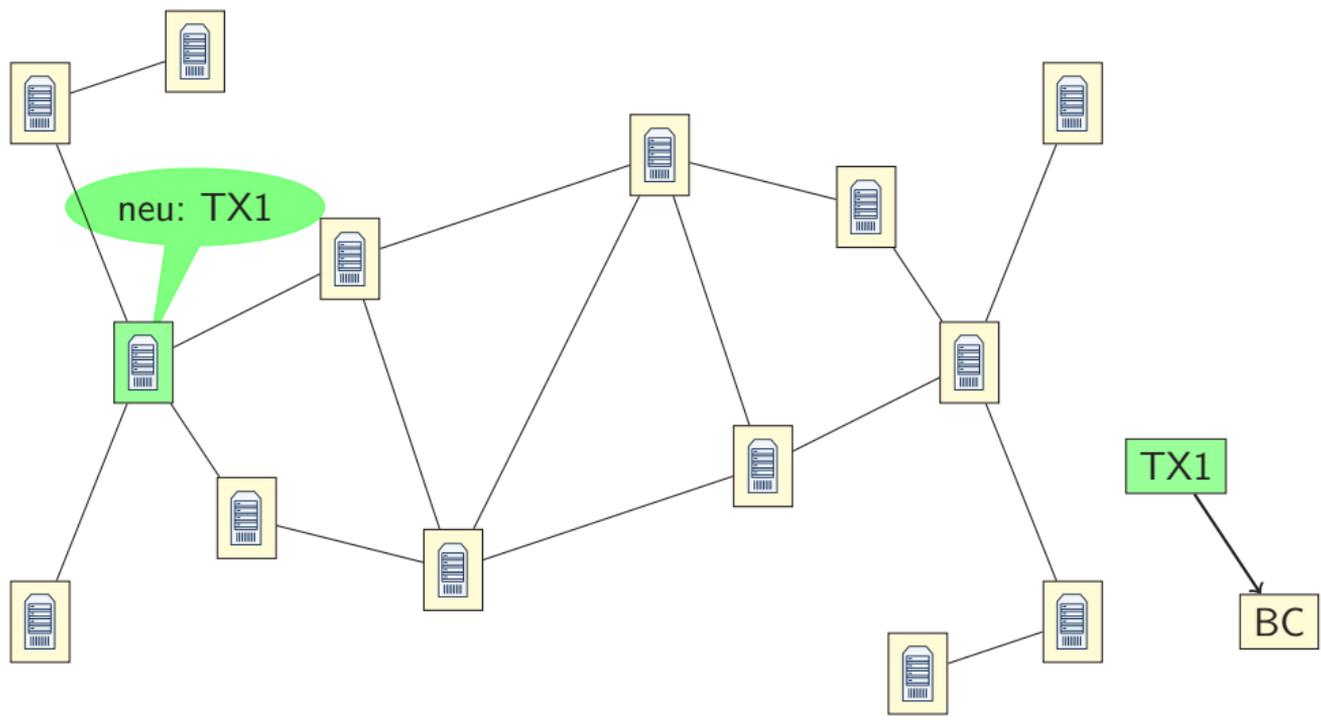




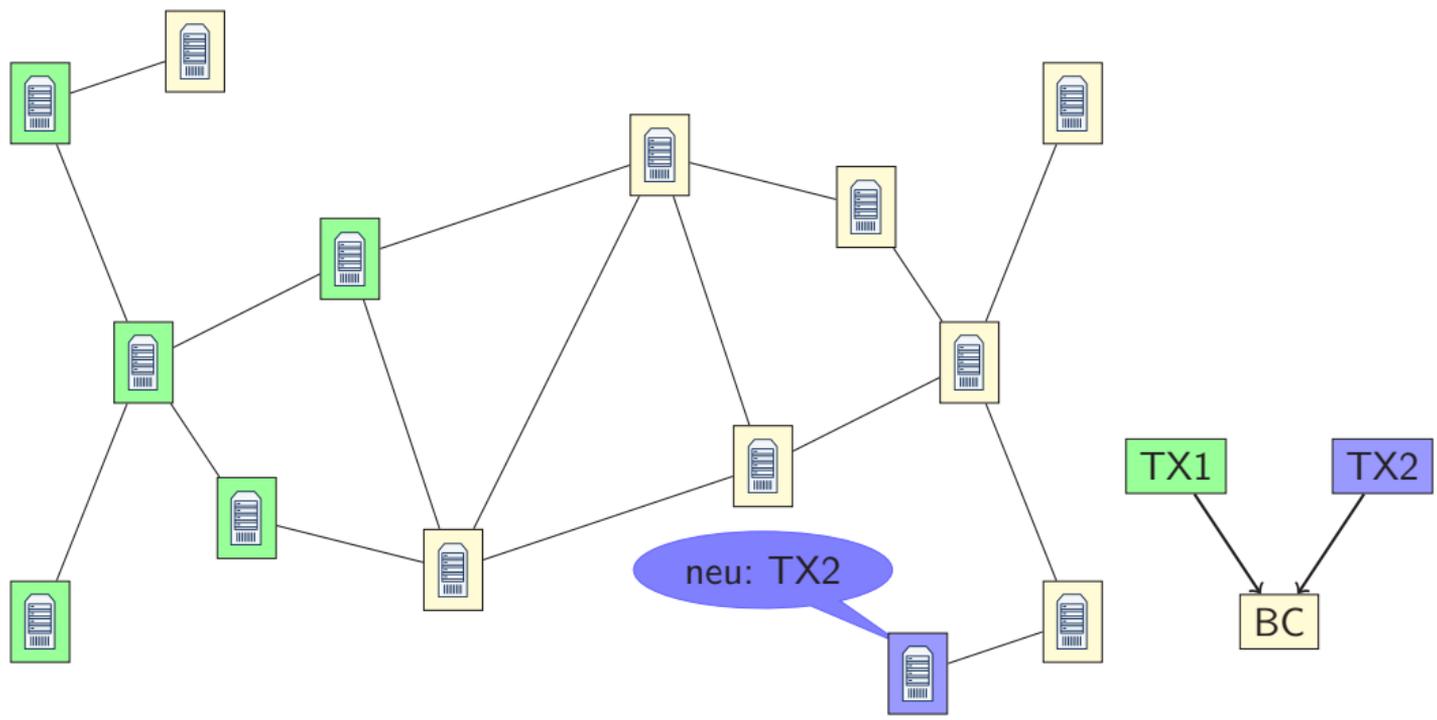
Zwei Transaktionen



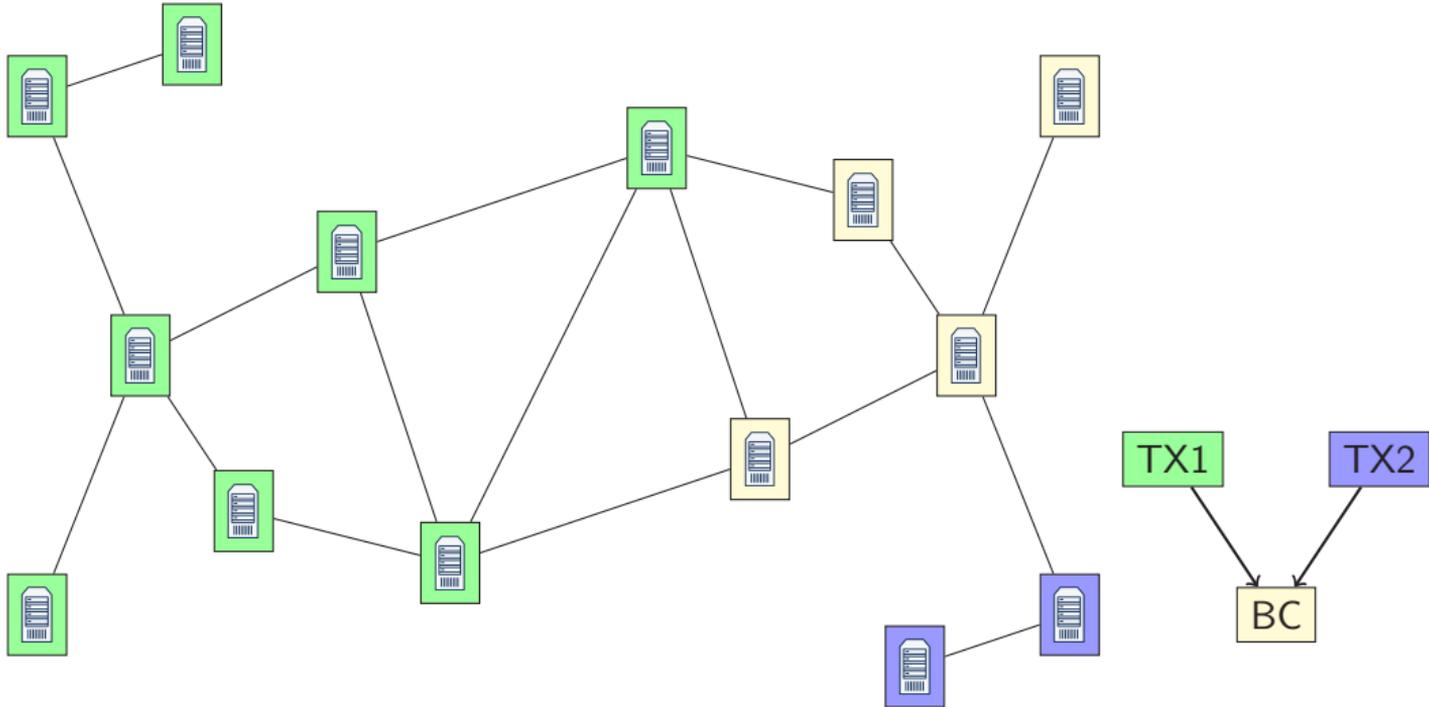
Zwei Transaktionen



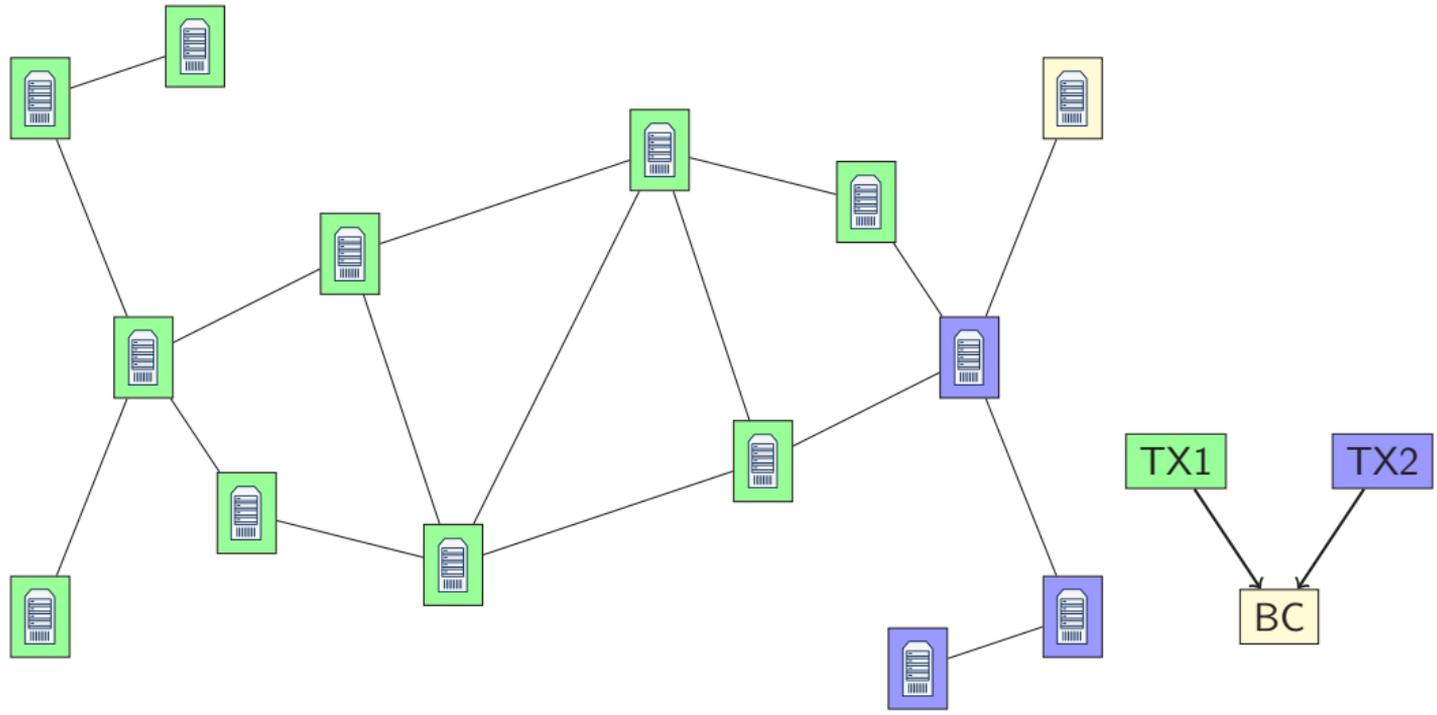
Zwei Transaktionen



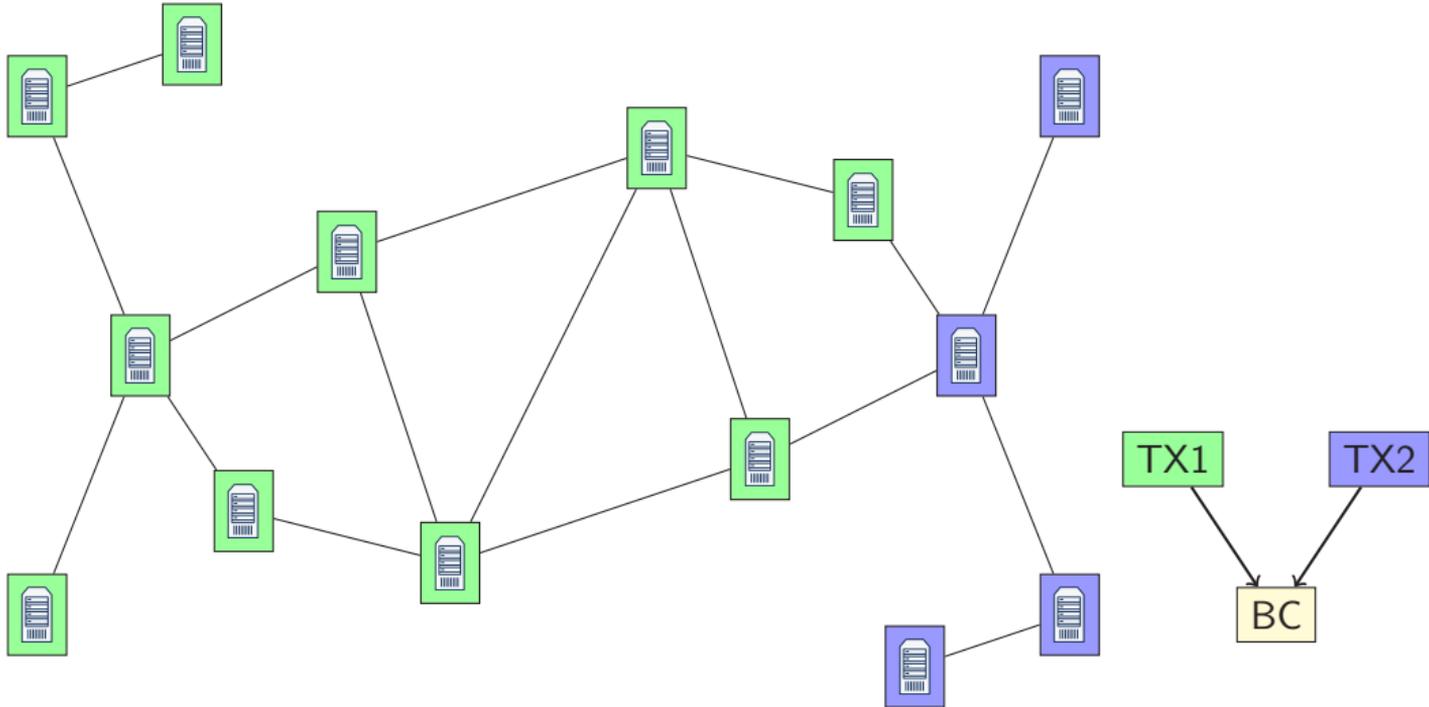
Zwei Transaktionen



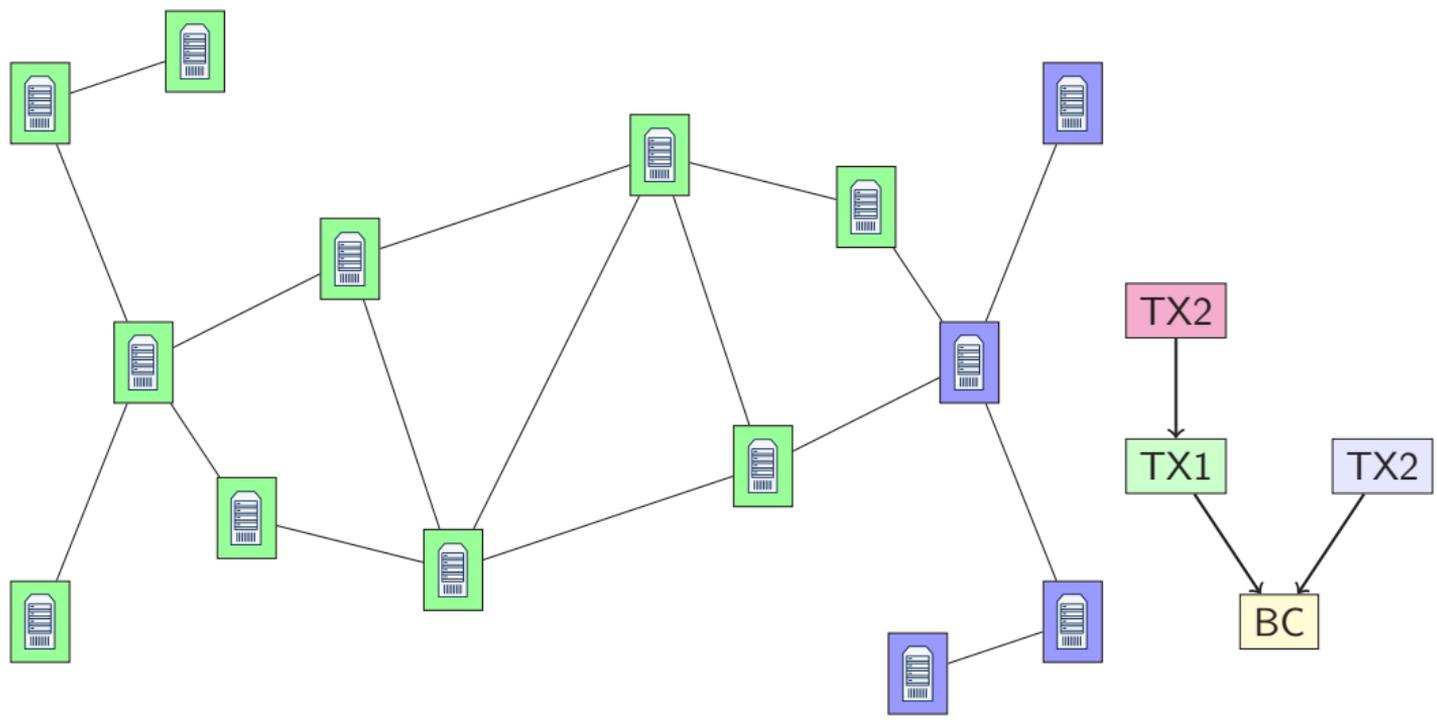
Zwei Transaktionen



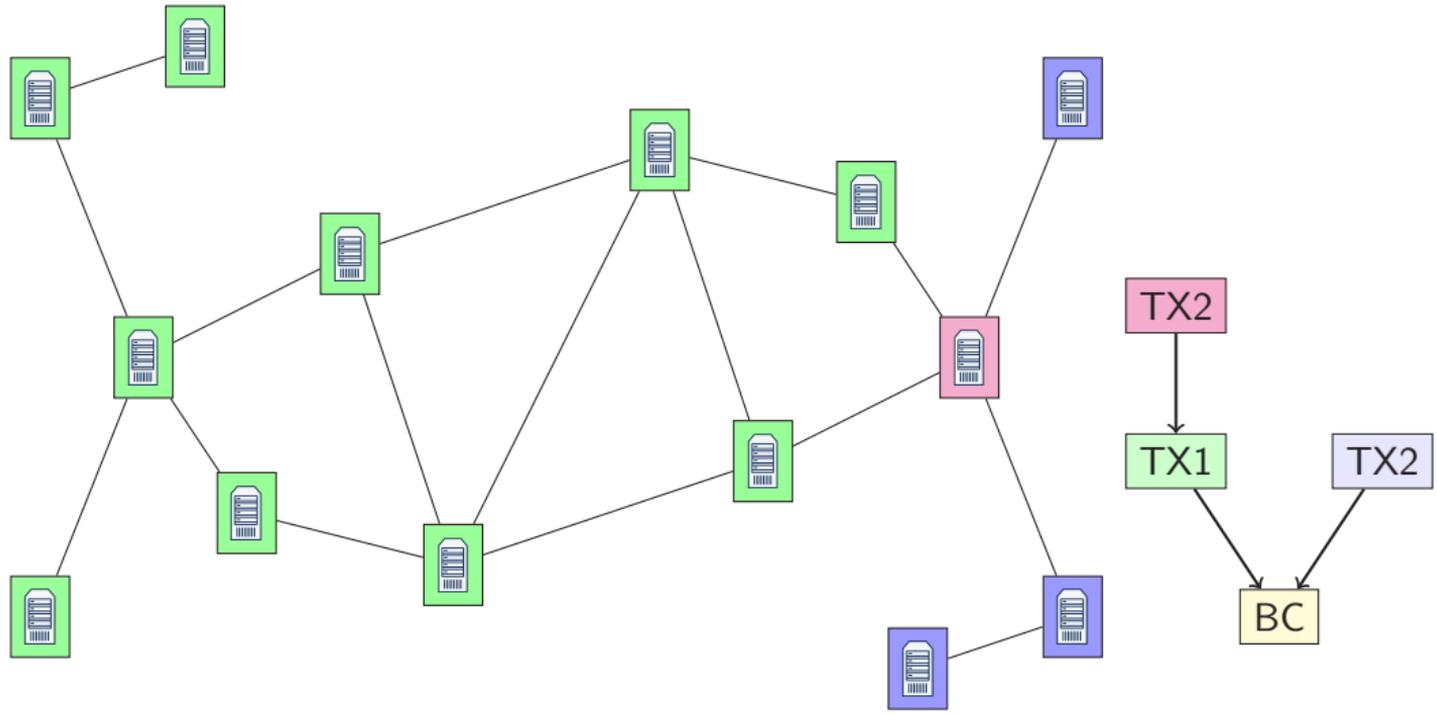
Zwei Transaktionen



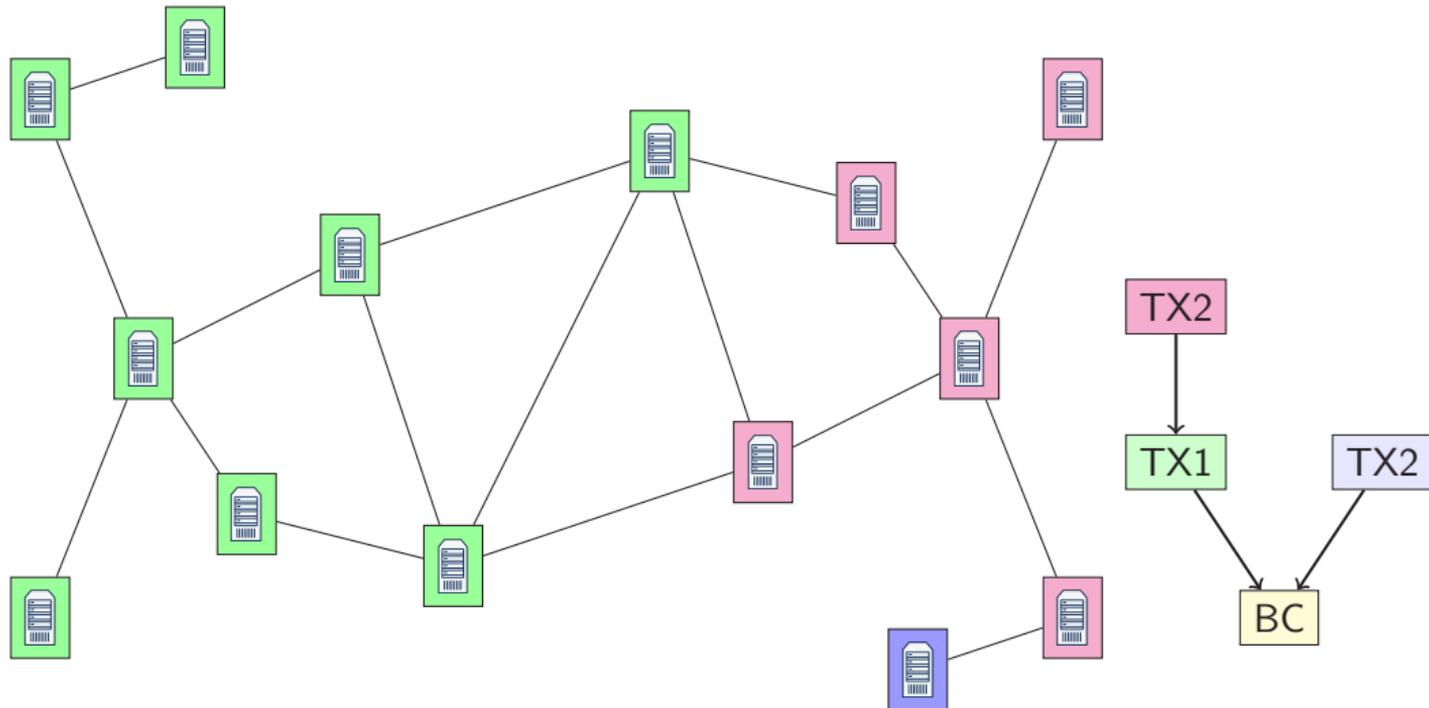
Zwei Transaktionen



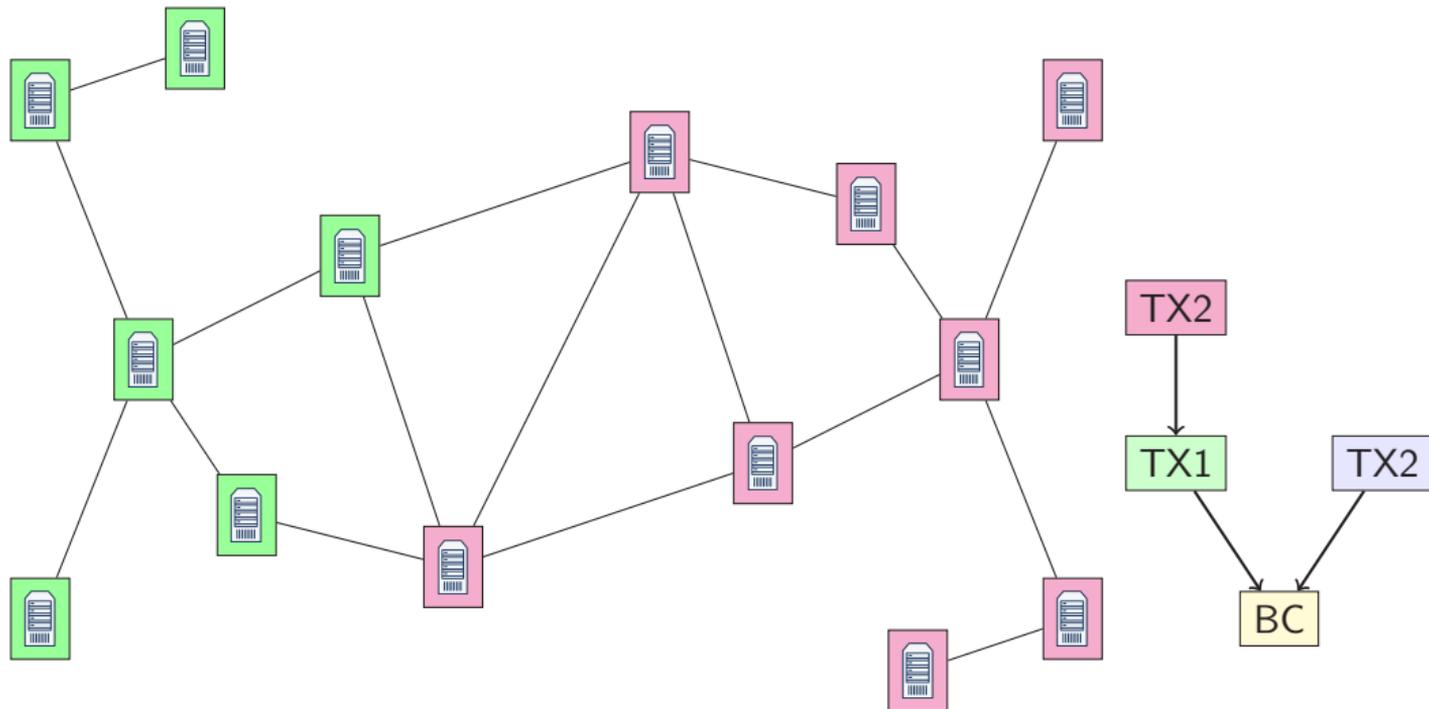
Zwei Transaktionen



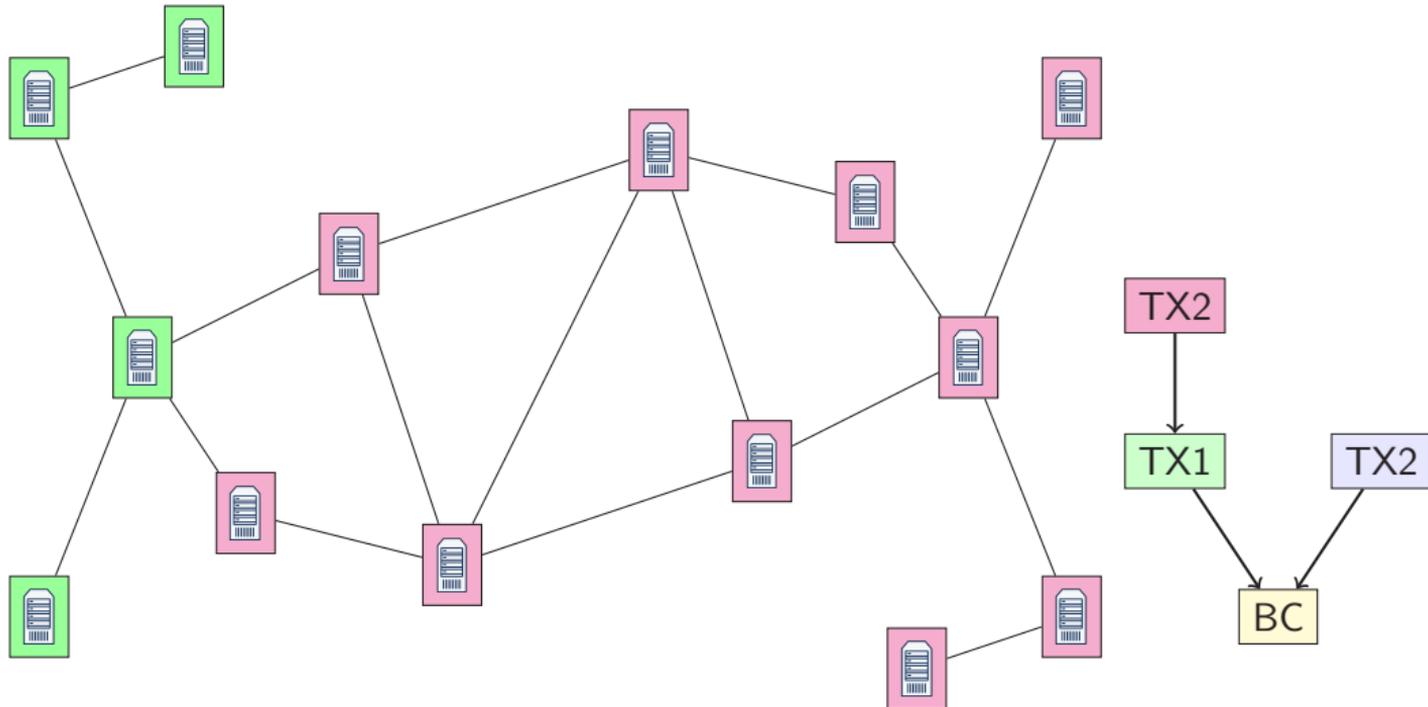
Zwei Transaktionen



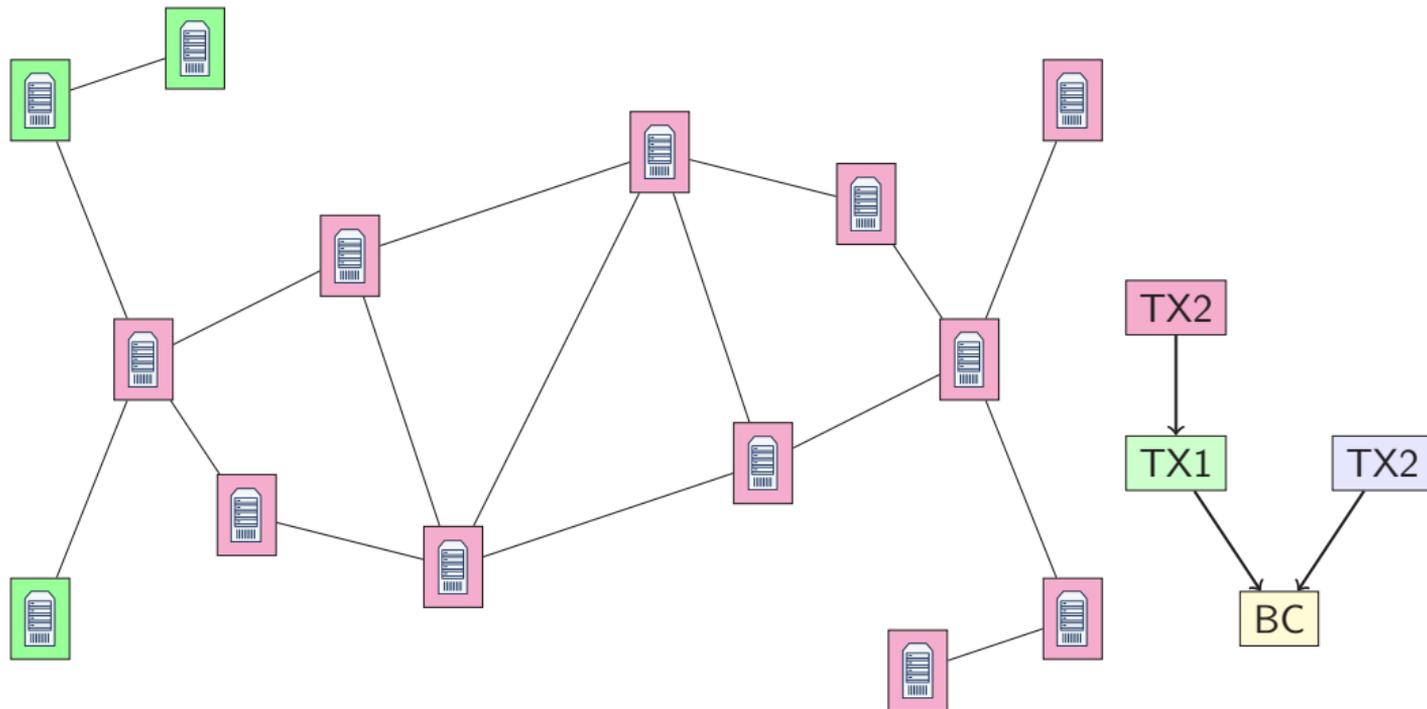
Zwei Transaktionen



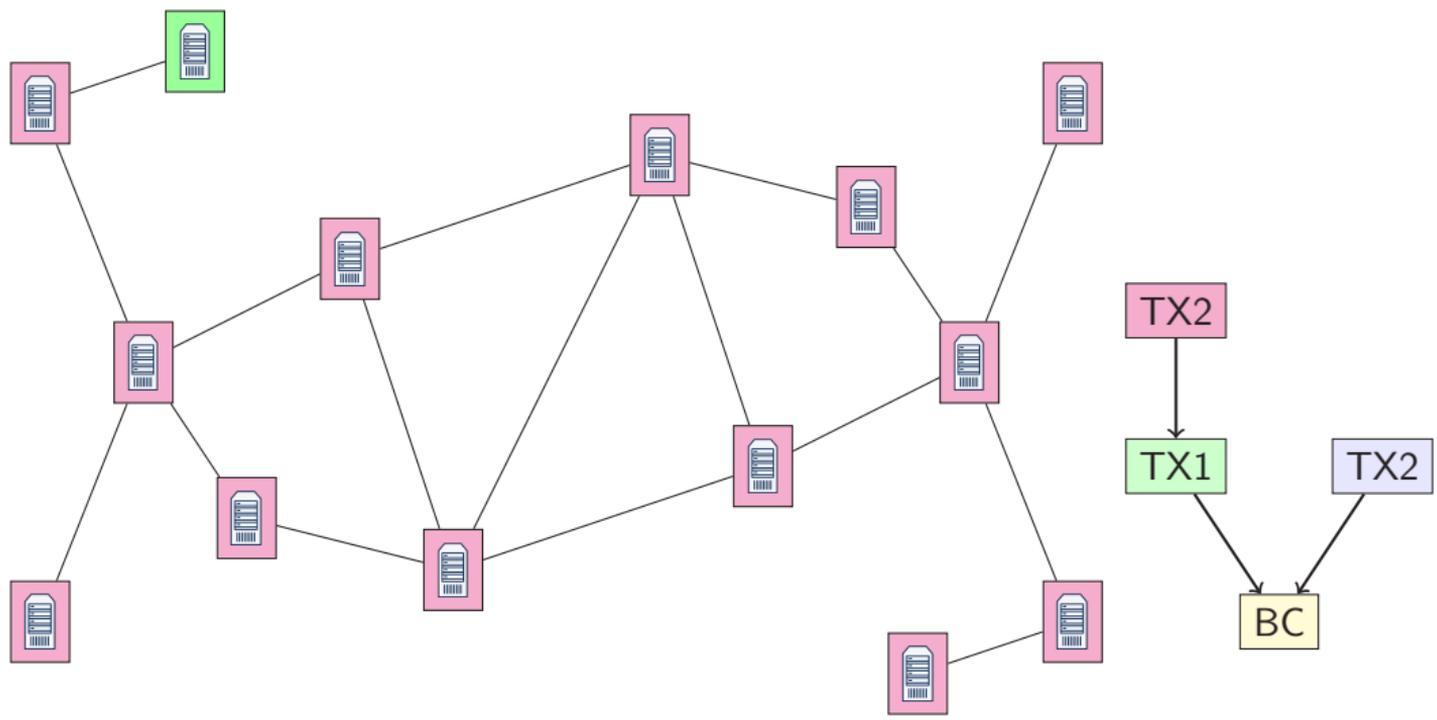
Zwei Transaktionen



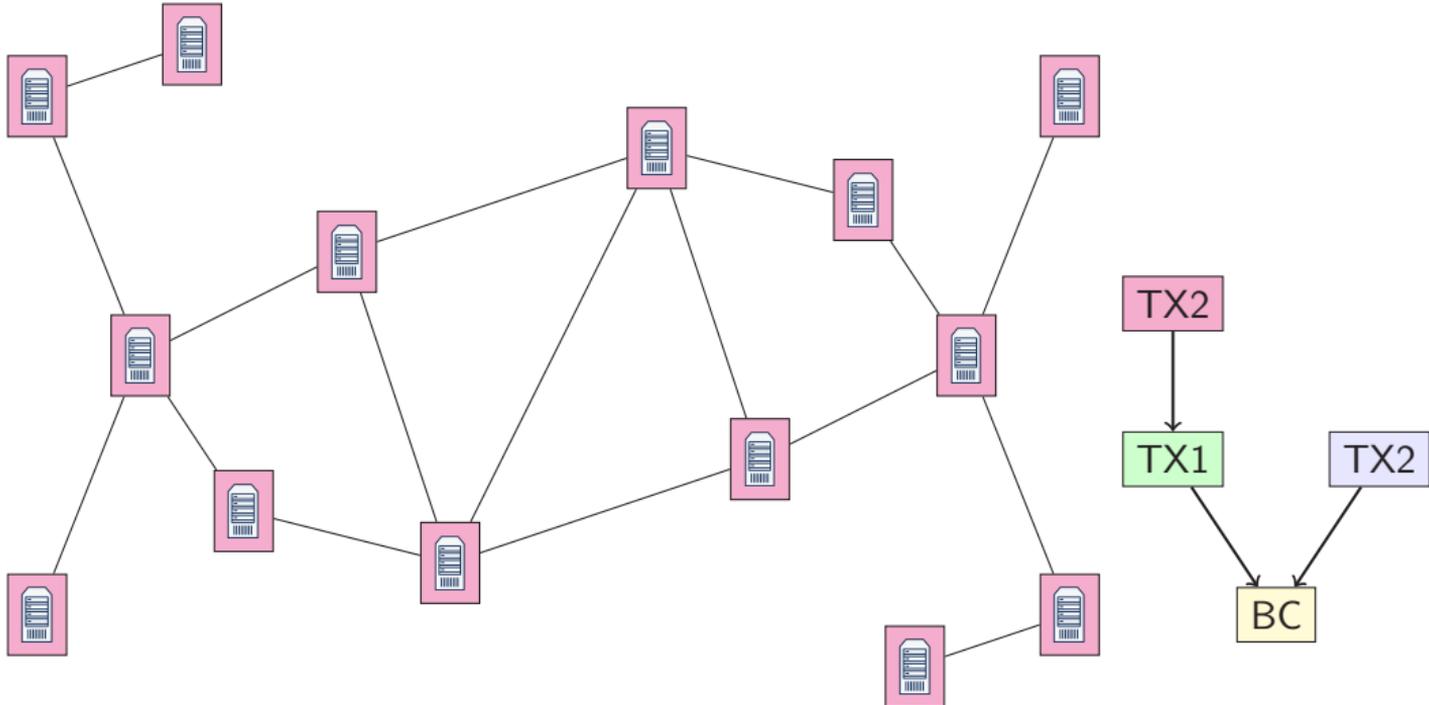
Zwei Transaktionen



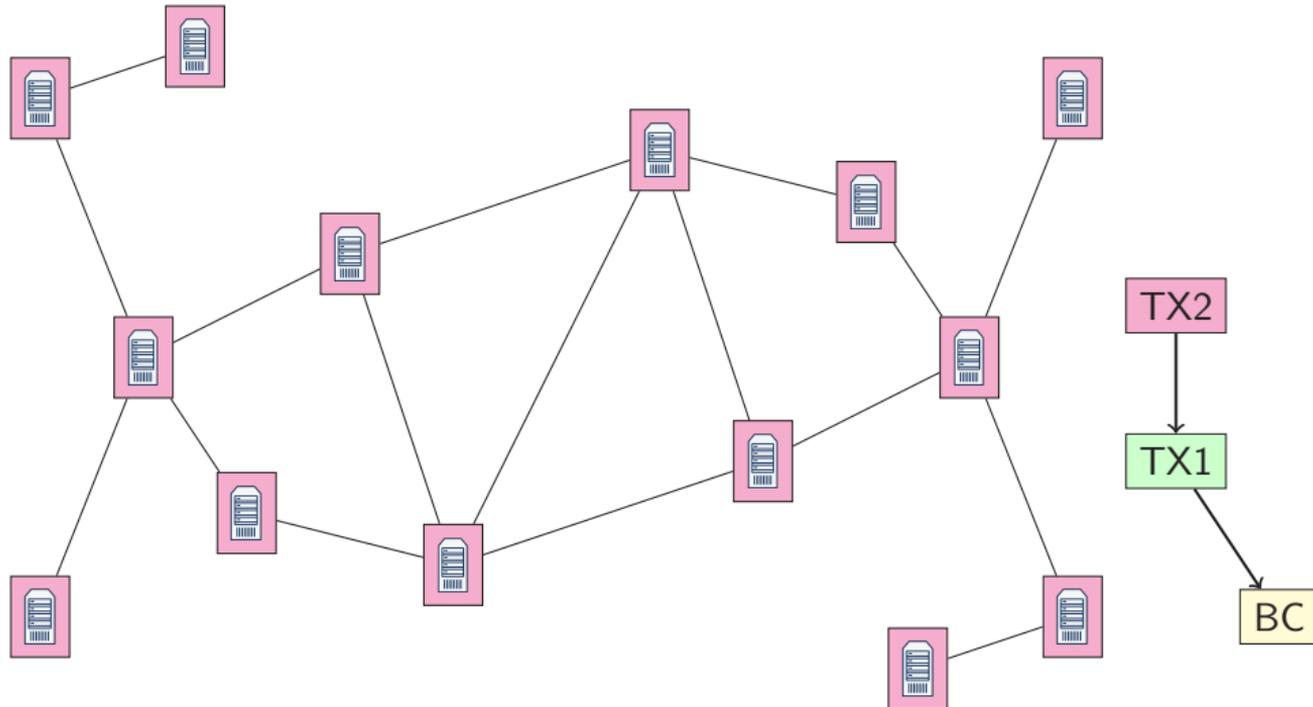
Zwei Transaktionen

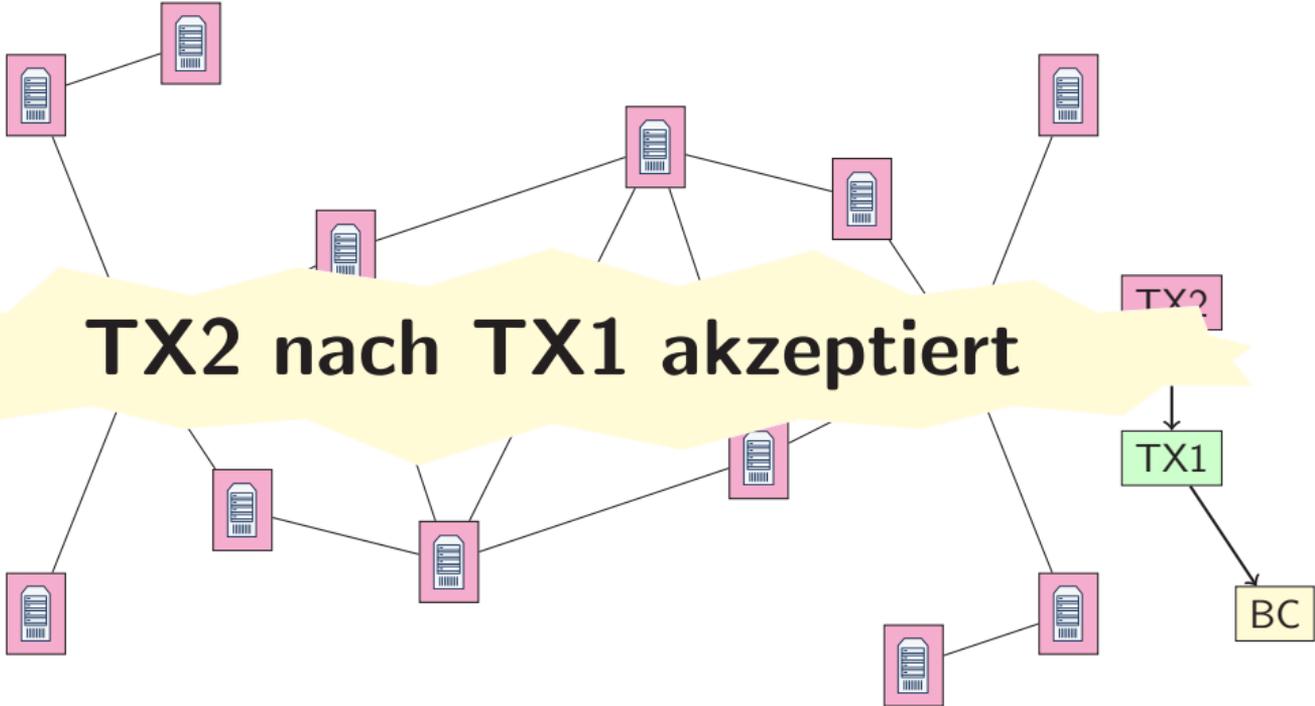


Zwei Transaktionen



Zwei Transaktionen

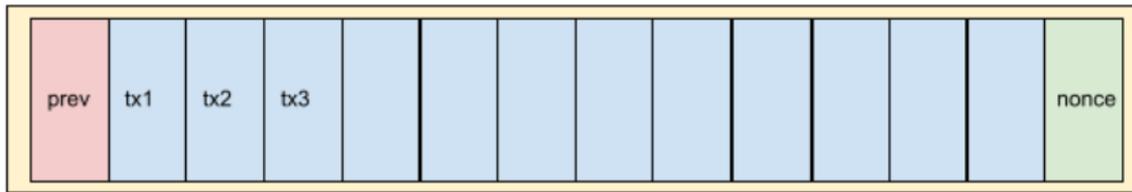




TX2 nach TX1 akzeptiert

- 1 Blöcke und Transaktionen
- 2 Hashing
- 3 Konsens
- 4 Arbeitsbeweis**
- 5 Kode ist Gesetz
- 6 Zusammenfassung

- 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.



- 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	000000000000000000050311490a7b879b3ef6e3c6590251d62c1c125280cfc6 
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/000000000000000000050311490a7b879b3ef6e3c6590251d62c1c125280cfc6>

- 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

Currency Statistics

Block Details

Mining Information

Total Hash Rate (TH/s)

Hashrate Distribution

Hashrate Distribution Over Time

Network Difficulty

Miners Revenue (USD)

Total Transaction Fees (BTC)

Total Transaction Fees (USD)

Fees Per Transaction (USD)

Cost % of Transaction Volume

Cost Per Transaction

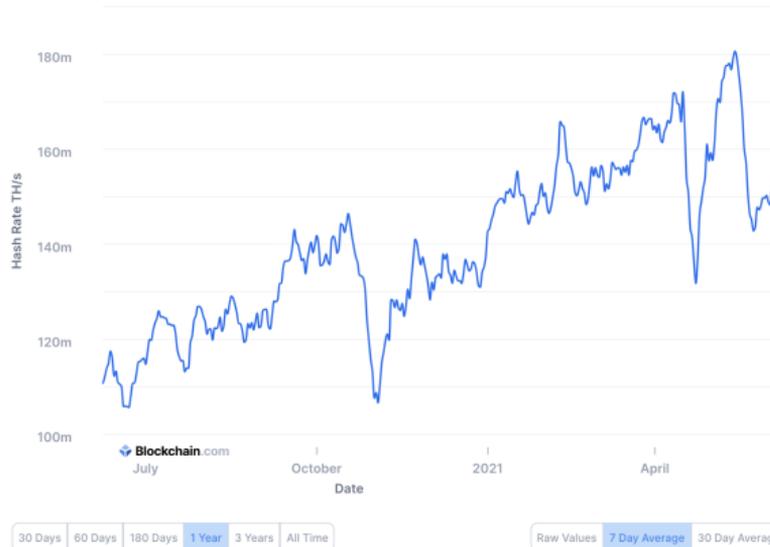
Network Activity

Wallet Activity

Market Signals

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



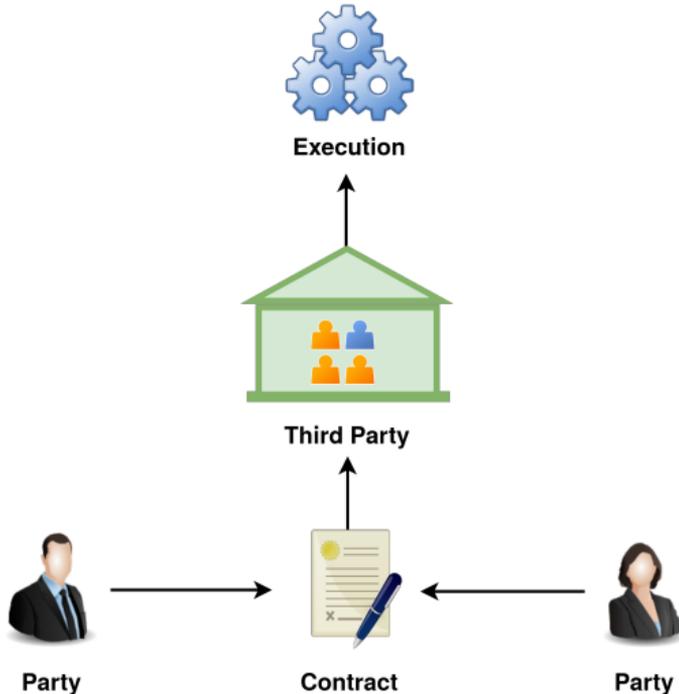
Quelle: <https://www.blockchain.com/charts/hash-rate>

- 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>

- 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>

- 1 Blöcke und Transaktionen
- 2 Hashing
- 3 Konsens
- 4 Arbeitsbeweis
- 5 Kode ist Gesetz**
- 6 Zusammenfassung

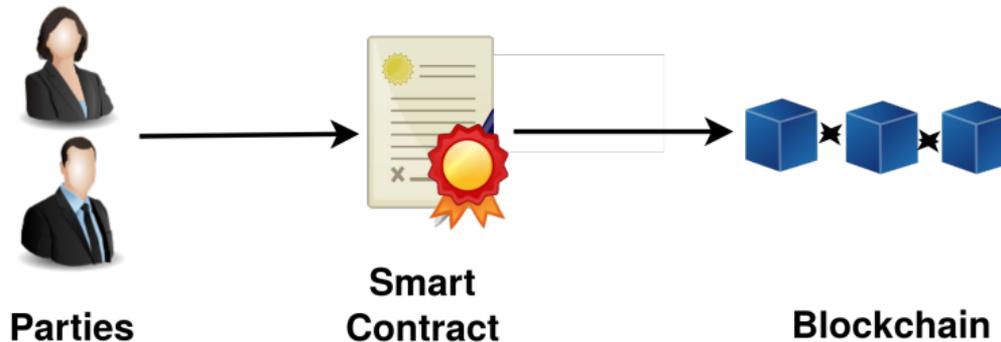


Definition

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

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

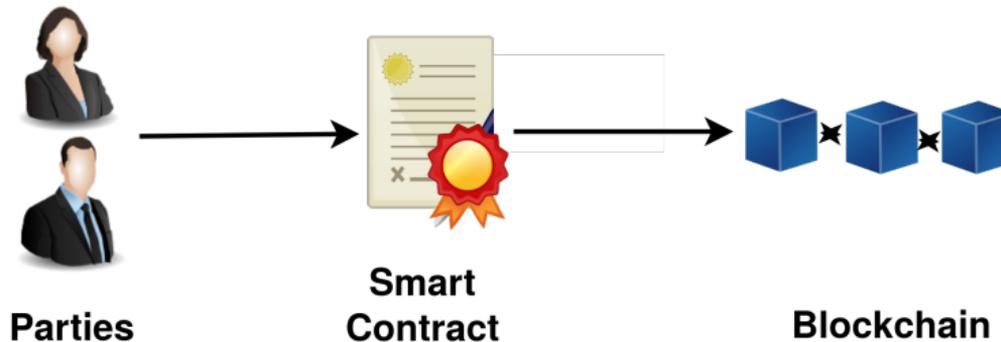


Smart Contract: Programm, das auf der Blockchain abgelegt ist und dort automatisch abläuft.

- 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



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

Eigenschaften

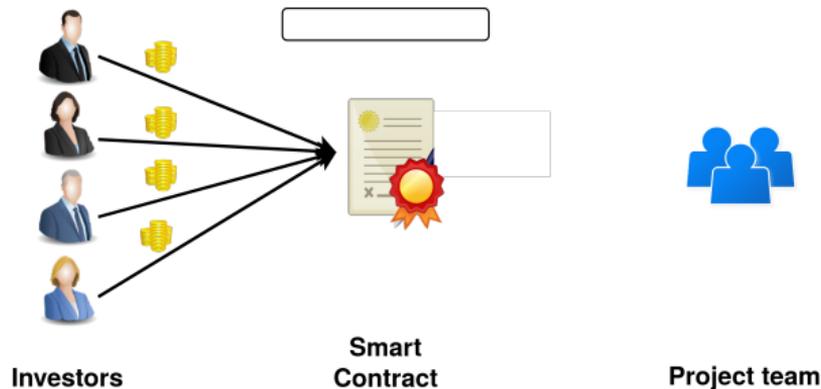
- Code gespeichert auf der Blockchain \Rightarrow **unveränderlich**
- Ausgeführt im Netz \Rightarrow **verteilter weltweiter Computer**
- Transparenz
 - Zugriff, Interaktion und Verifikation (jeder)
 - Konsens über Ergebnisse
 - Daten gespeichert auf der Blockchain

Funktionen

- Geld senden und empfangen
- Interaktion mit anderen Smart Contracts

Geld einsammeln von Investoren zur Unterstützung eines Projekts

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



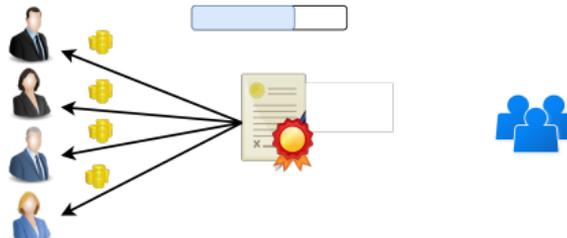
- 1 Wenn der Zielbetrag bis zum Termin erreicht ist, dann wird automatisch das gesammelte Geld ans Projektteam überwiesen



- 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



- 1 Blöcke und Transaktionen
- 2 Hashing
- 3 Konsens
- 4 Arbeitsbeweis
- 5 Kode ist Gesetz
- 6 Zusammenfassung**

- Kleiner Einblick in die Blockchain Technologie

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

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

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

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

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

- 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

- 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)

- 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