TNG TECHNOLOGY CONSULTING

Blockchain

Eine Einführung in Funktionsweise und Nutzen

Martin Kreidenweis, TNG Technology Consulting

2018-07-06

Tag der Informatiklehrerinnen und -lehrer

Was ist Bitcoin?

	A	B	C
1	Alice	1 BTC	
2	Bob	2 BTC	
3	Charlie	3 BTC	
4	Donald	4 BTC	
5	…		
6			
7			
8			

	A	B
1	15kur3zjNTZoESMenAXAzRWxnXoo9s6kgu	2.9995 BTC
2	1GW38UbCvxyhRzYm5GykKCDThnCcuzbzk9	2.9935 BTC
3	13zQLKadEMAVhturQDkoXyVJdQJgZvSTPi	0 BTC
4	1QJZPdkDaaegr4Rt39Rkjhm41posTbbpJL	0.01154235 BTC
5	18xBD5PA5eeWipiEyKuwe9kCopYqr4g2u7	0.04 BTC
6		
7		
8		

Was ist Bitcoin

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

bitcoin.org/bitcoin.pdf

Double-Spending Problem

Reihenfolge

Wie funktioniert Blockchain?

Zutaten

Hashes

Kryptologische Hashfunktionen

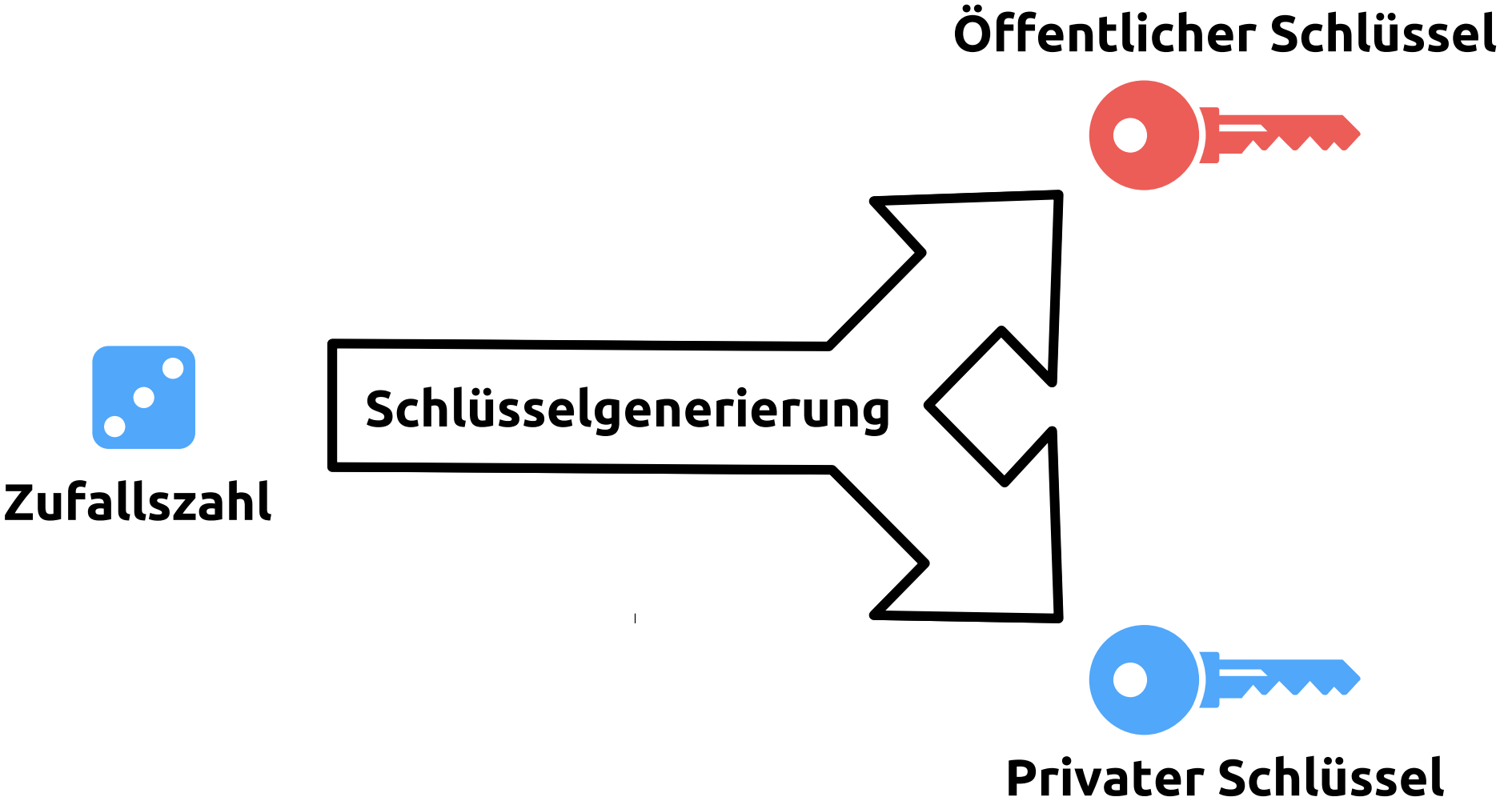
```
"Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!1" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
```

- Einwegfunktion
- Kollisionsresistent

Public-Private-Key-Kryptographie

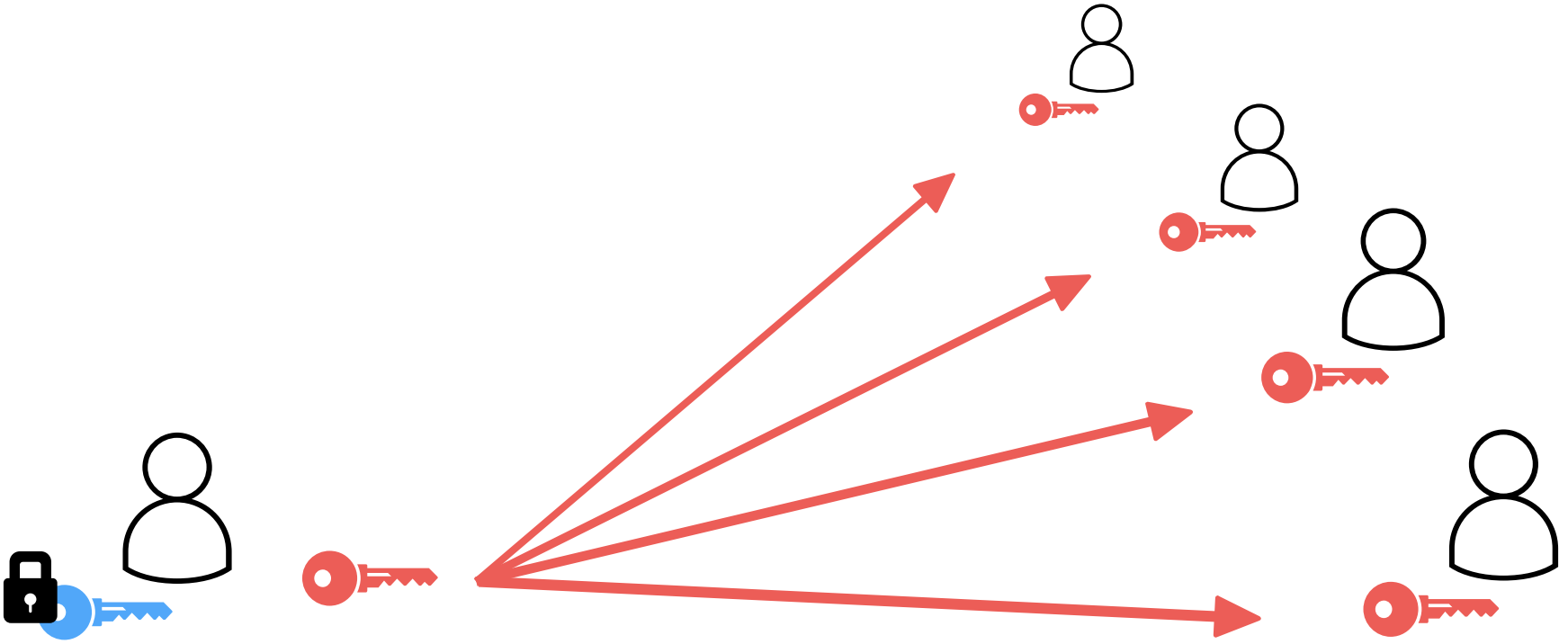
Asymmetrische Kryptosysteme

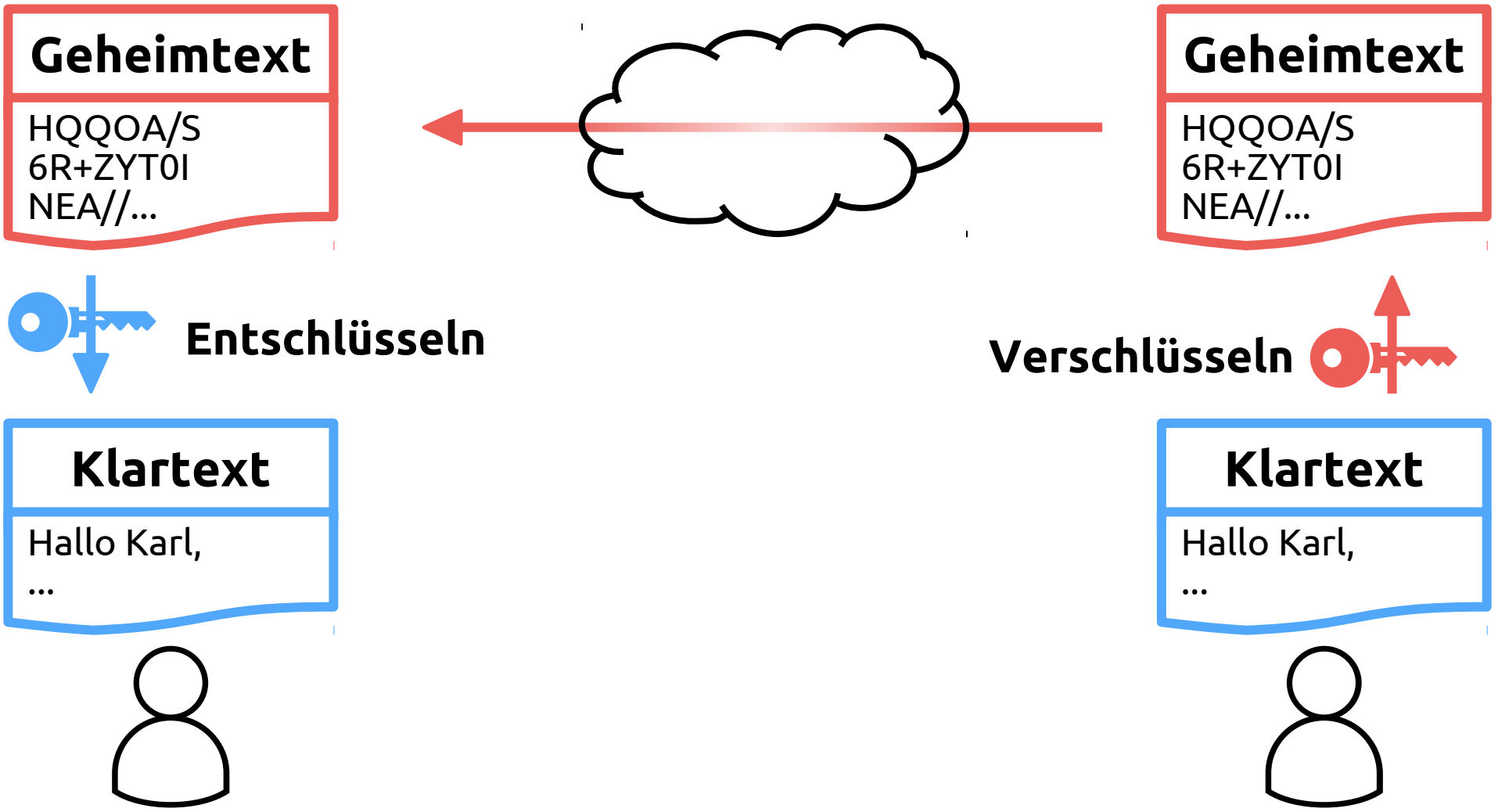

Öffentlicher Schlüssel
Schlüsselgenerierung
Zufallszahl
Privater Schlüssel

Schlüsselverteilung

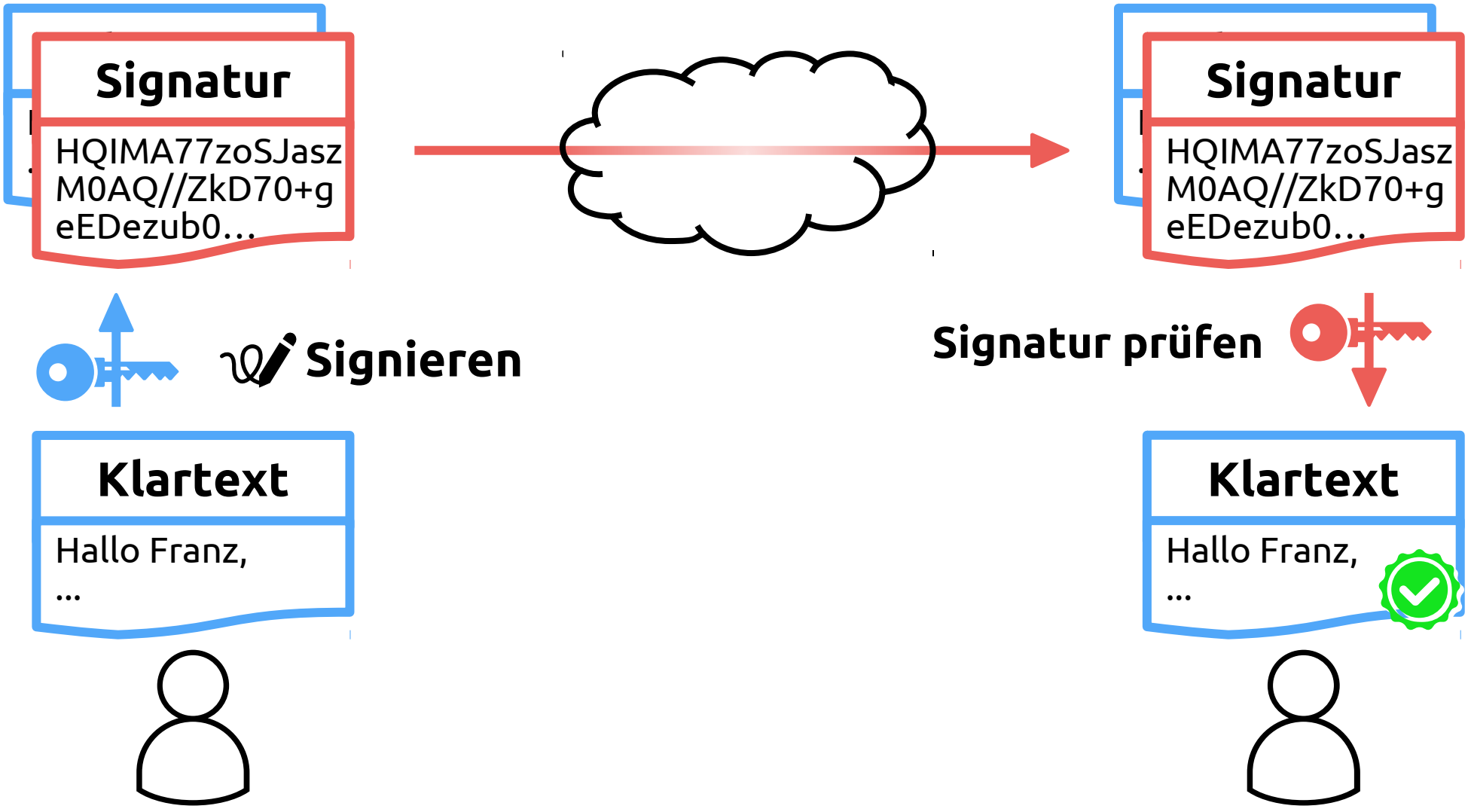
Schlüsselverteilung

Schlüsselverteilung




Geheimtext
HQQOA/S
6R+ZYT0I
NEA//...
Geheimtext
HQQOA/S
6R+ZYT0I
NEA//...
Entschlüsseln
Verschlüsseln
Klartext
Hallo Karl,
...
Klartext
Hallo Karl,
...

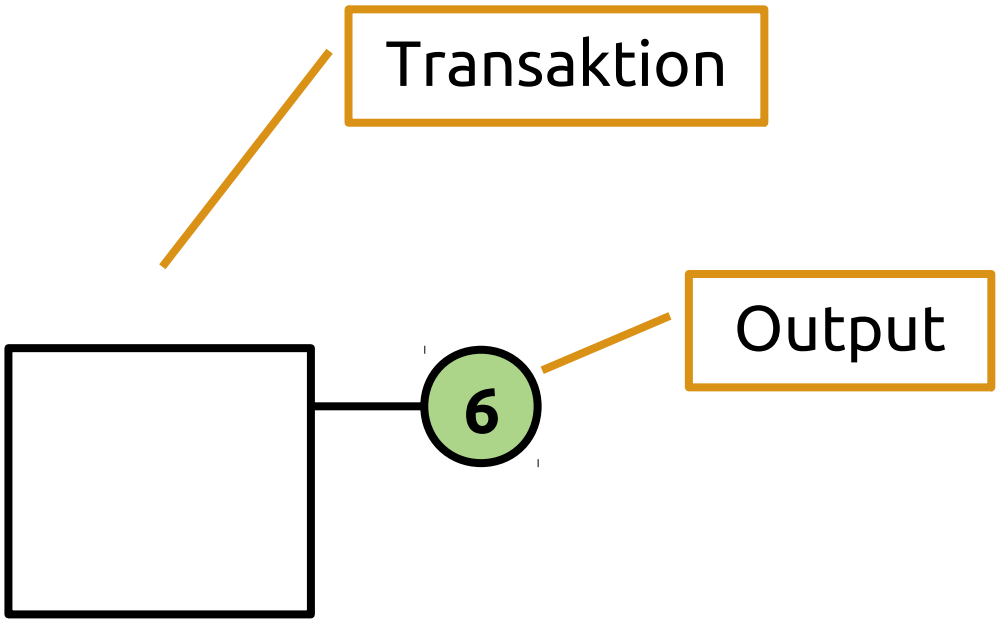
Elektronische Signaturen

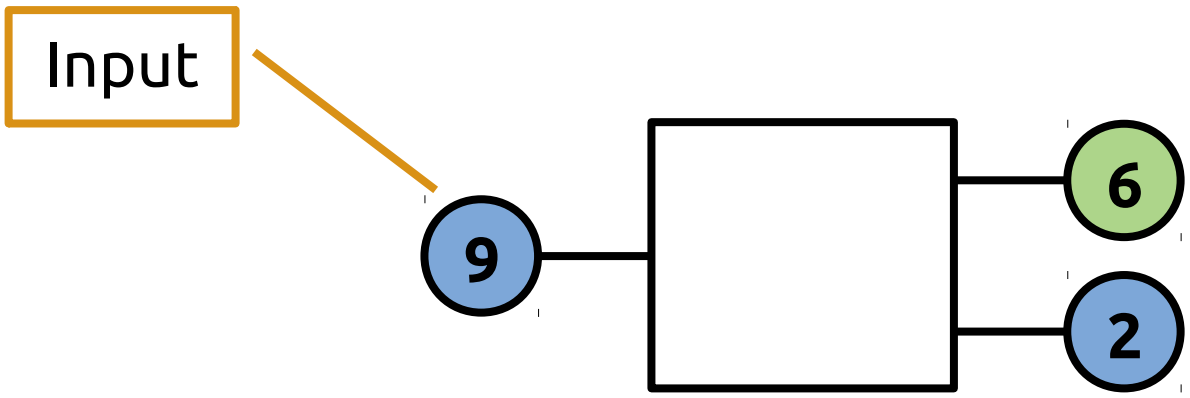

Signatur
HQIMA77zoSJasz
M0AQ//ZkD70+g
eEDezub0…
Signieren
Klartext
Hallo Franz,
…
Signatur
HQIMA77zoSJasz
M0AQ//ZkD70+g
eEDezub0…
Signatur prüfen
Klartext
Hallo Franz,
…

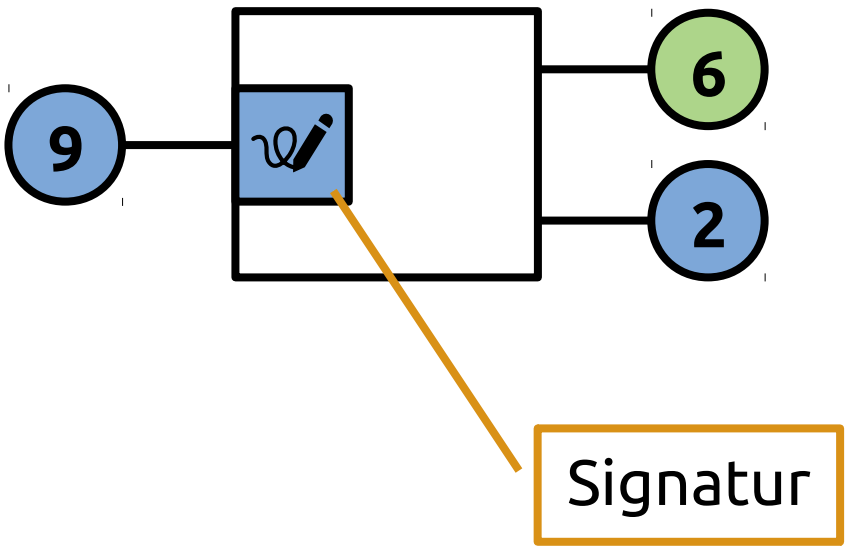

bitcoin

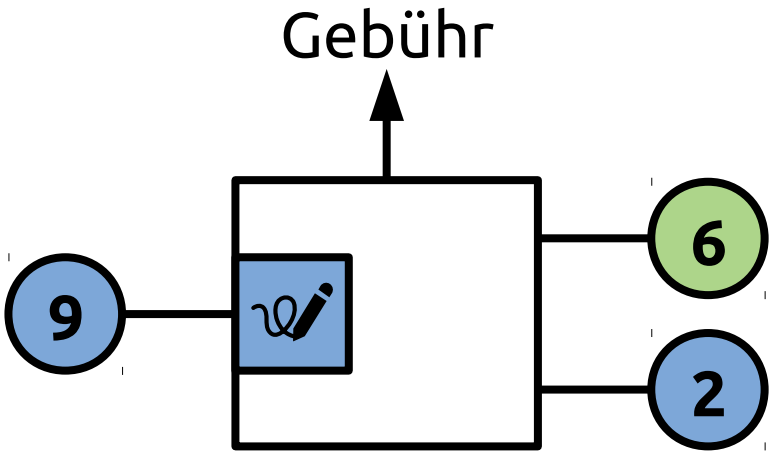
	A	B
1	15kur3zjNTZoESMenAXAzRWxnXoo9s6kgu	2.9995 BTC
2	1GW38UbCvxyhRzYm5GykKCDThnCcuzbzk9	2.9935 BTC
3	13zQLKadEMAVhturQDkoXyVJdQJgZvSTPi	0 BTC
4	1QJZPdkDaaegr4Rt39Rkjhm41posTbbpJL	0.01154235 BTC
5	18xBD5PA5eeWipiEyKuwe9kCopYqr4g2u7	0.04 BTC
6		
7		
8		

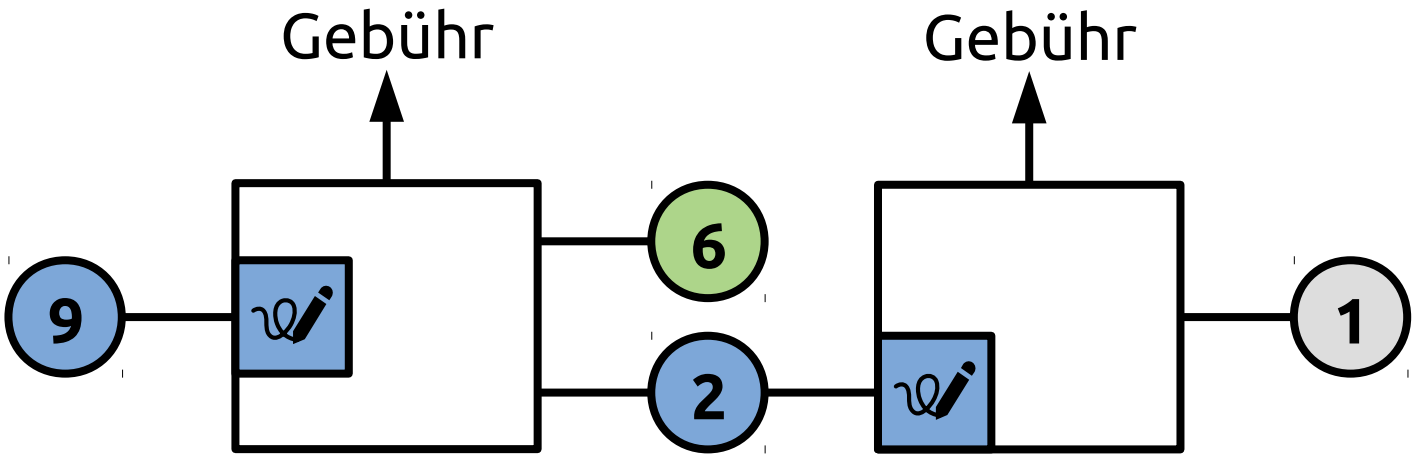
Transaktionen

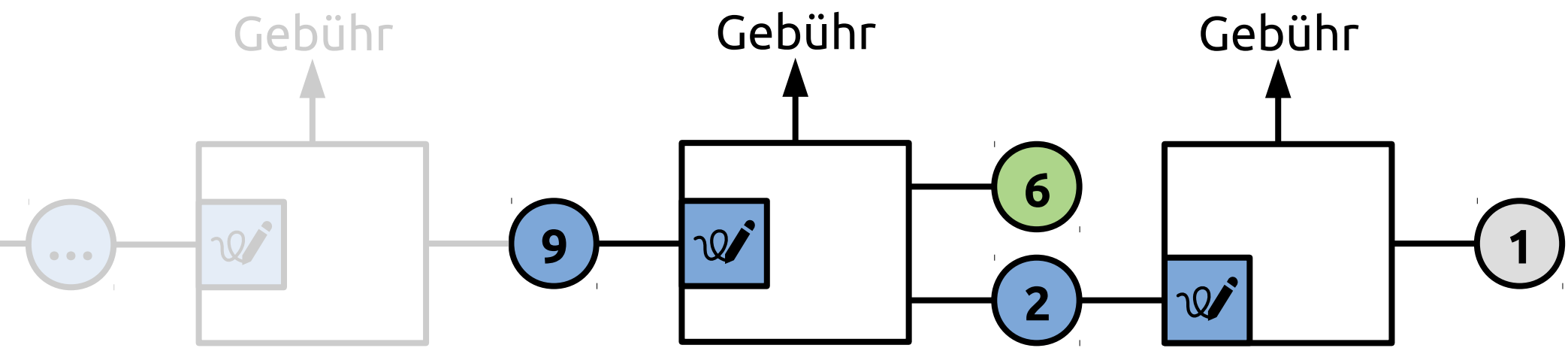

Transaktion
Output
6


Input
9
6
2

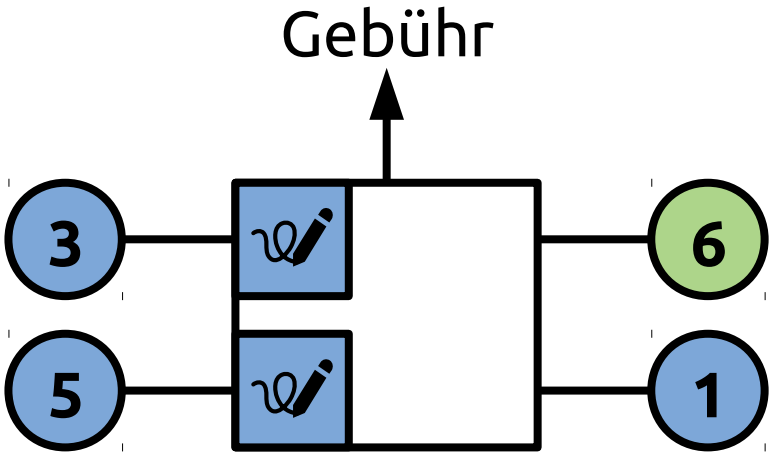

9
6
2
Signatur

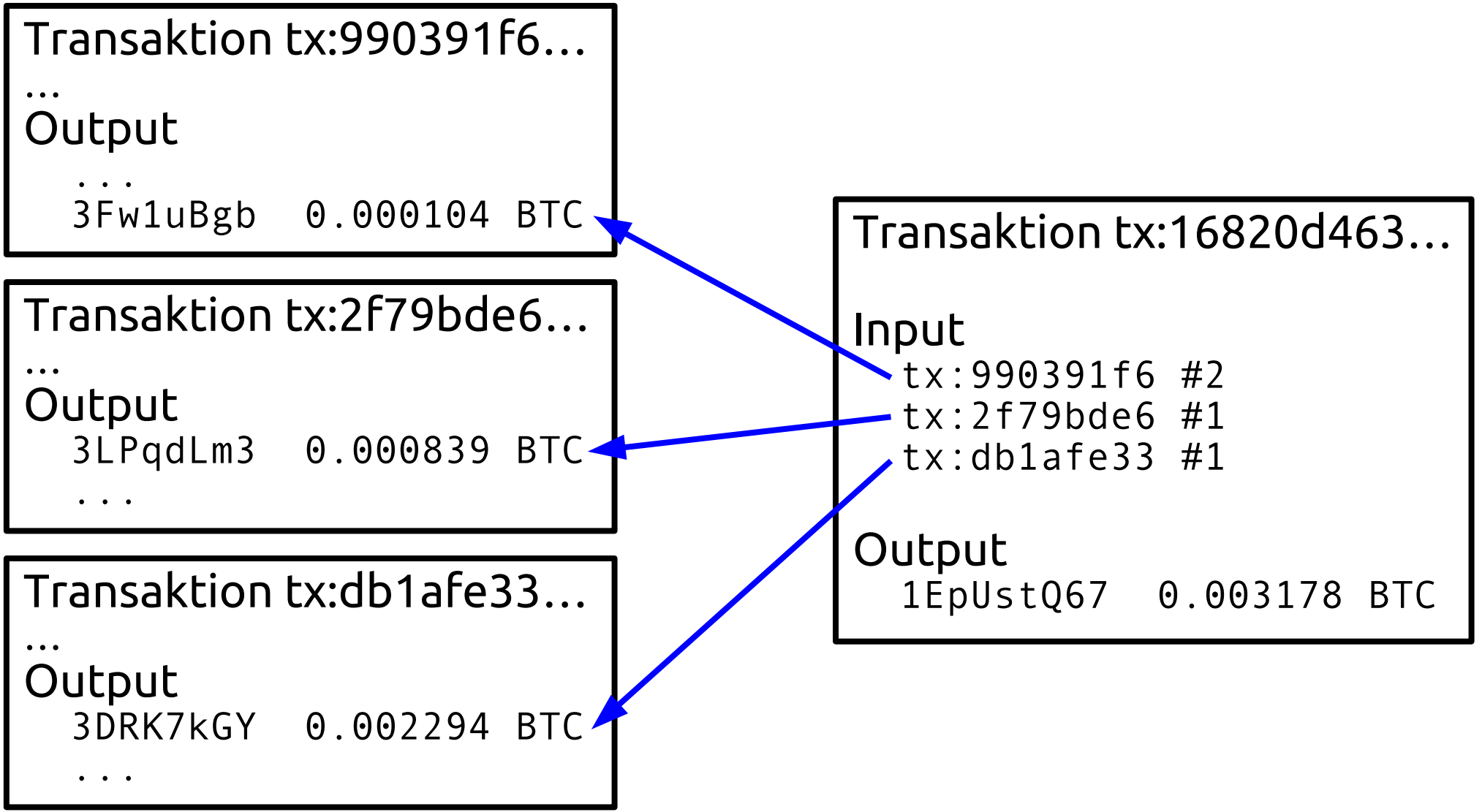

Gebühr
9
6
2


Gebühr
Gebühr
9
6
2
1


Gebühr
Gebühr
Gebühr
...
9
6
2
1

Mehrere Inputs


Gebühr
3
5
6
1

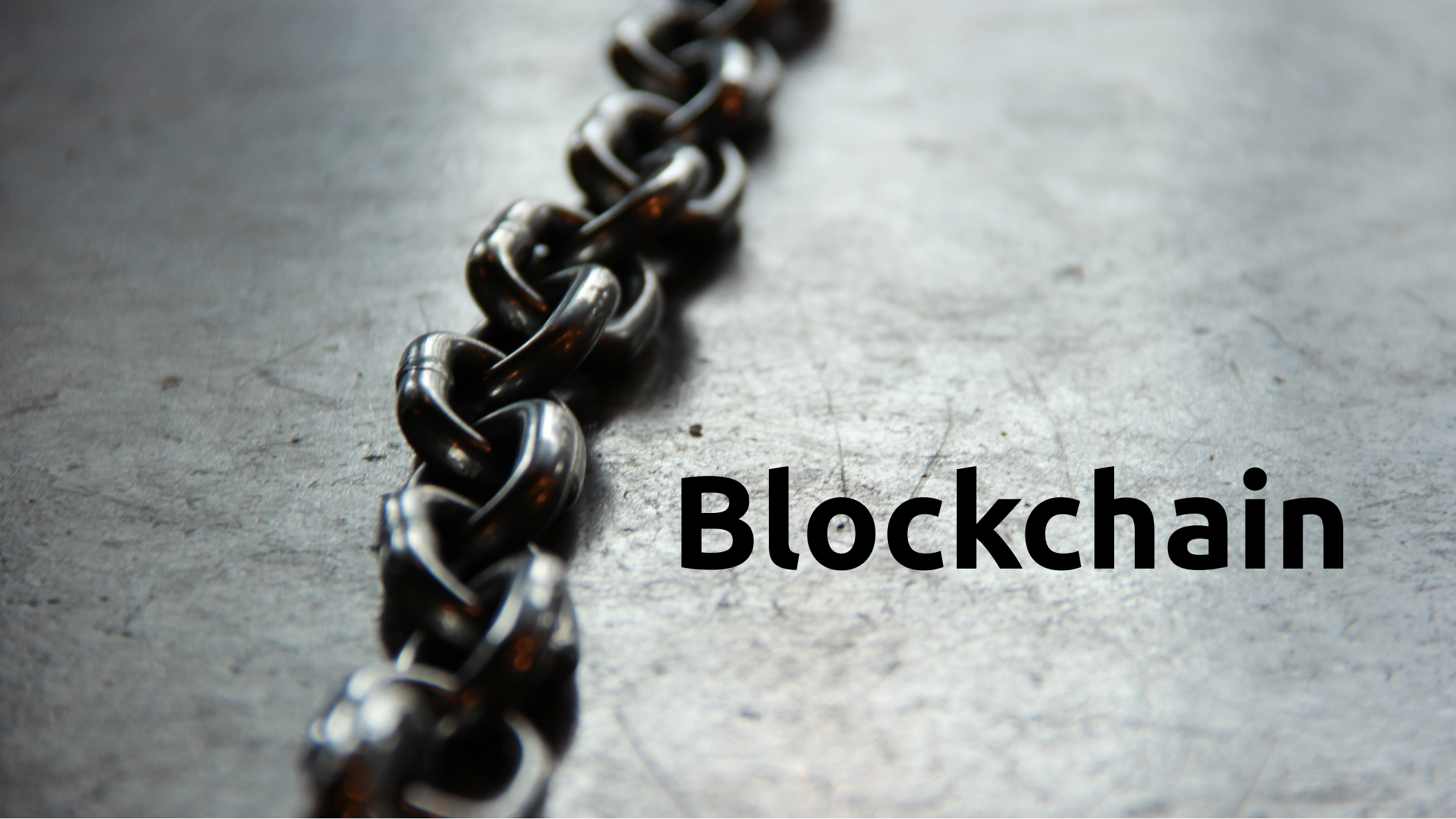

Transaktion tx:990391f6…
…
Output
...
3Fw1uBgb 0.000104 BTC
Transaktion tx:2f79bde6…
…
Output
3LPqdLm3 0.000839 BTC
...
Transaktion tx:db1afe33…
…
Output
3DRK7kGY 0.002294 BTC
...
Transaktion tx:16820d463…
Input
tx:990391f6 #2
tx:2f79bde6 #1
tx:db1afe33 #1
Output
1EpUstQ67 0.003178 BTC

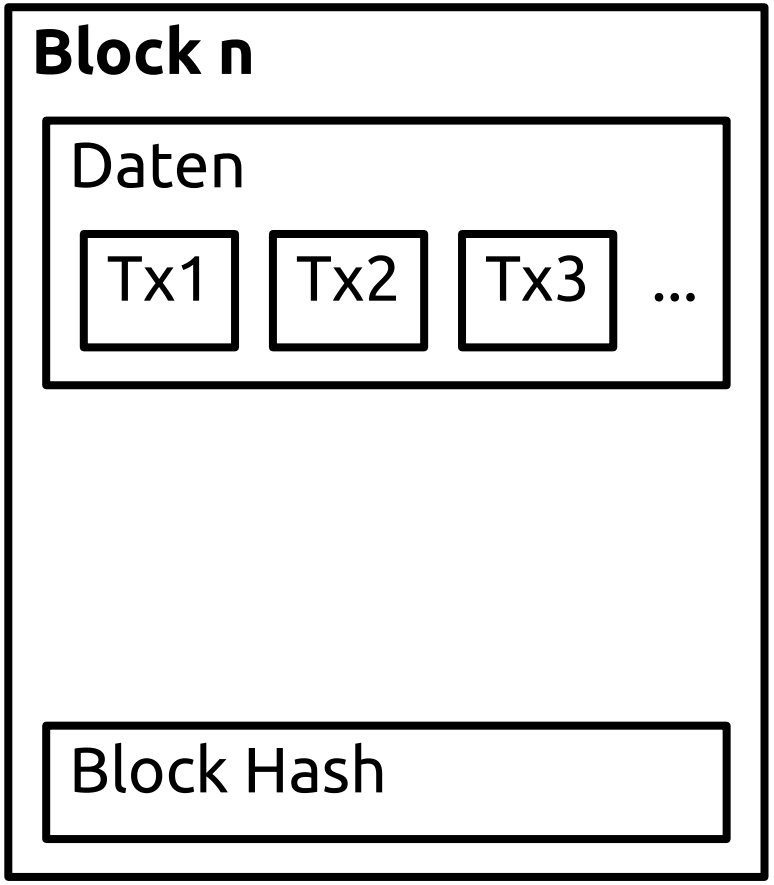
Wo kommen die Bitcoins her?

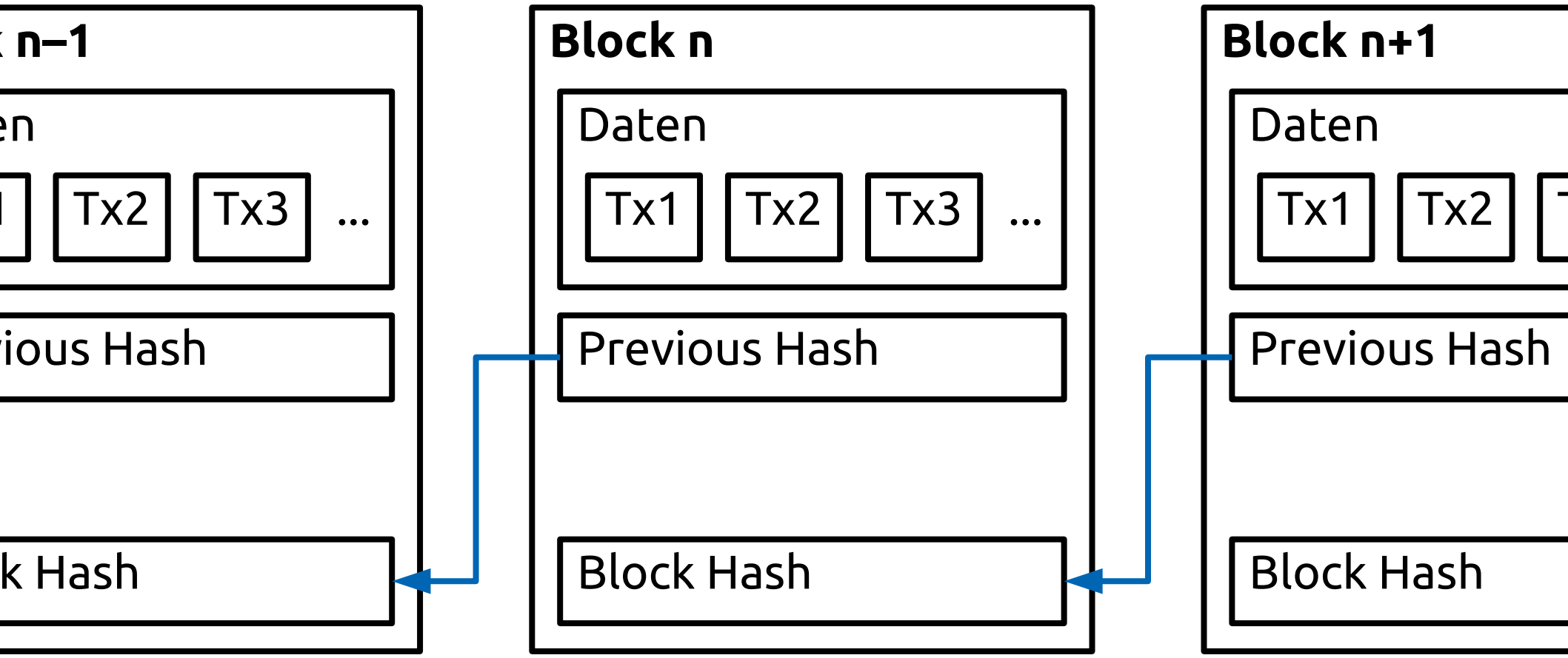
Mining

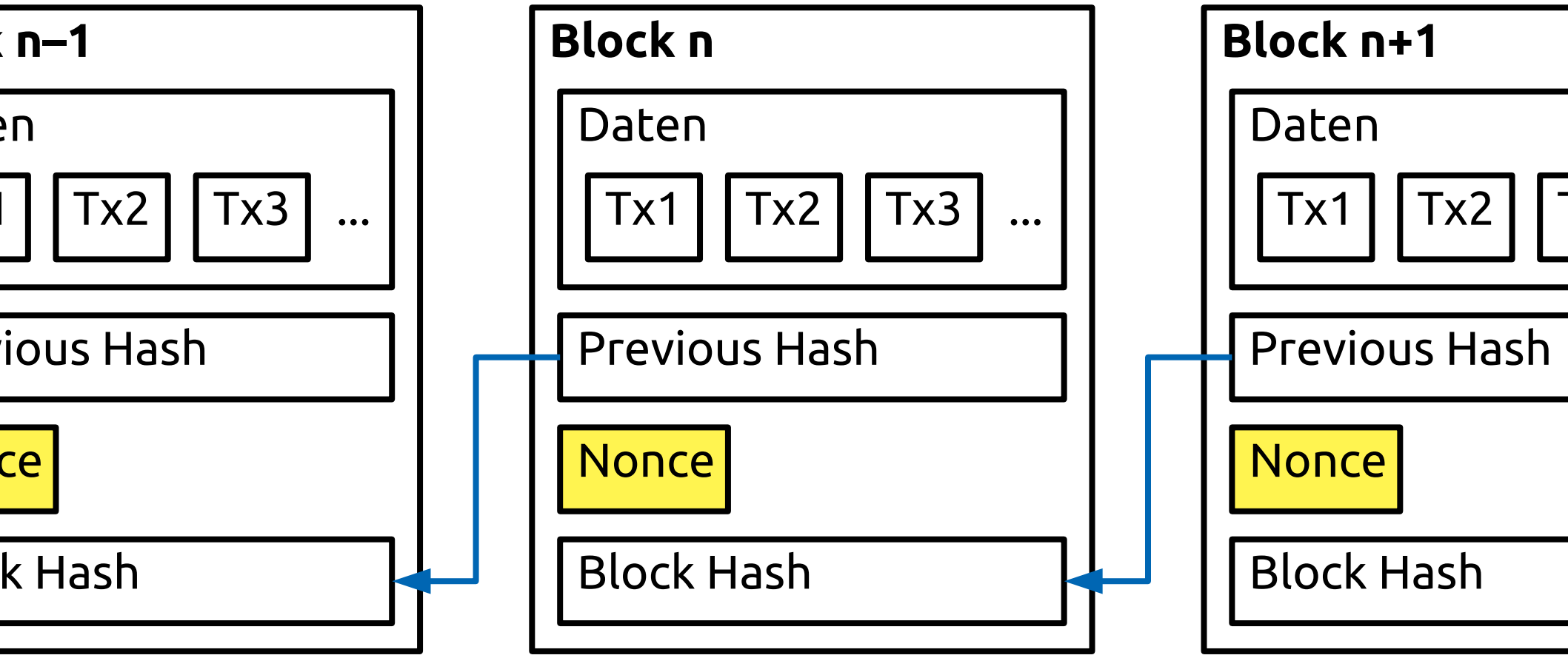
Mining
= Transaktionsverarbeitung

Double-Spending Problem


Blockchain


Block n
Daten
Tx1
Tx2
Tx3
...
Block Hash


n–1
en
Tx2
Tx3
...
ious Hash
k Hash
Block n
Daten
Tx1
Tx2
Tx3
...
Previous Hash
Block Hash
Block n+1
Daten
Tx1
Tx2
Previous Hash
Block Hash


n–1
en
Tx2
Tx3
...
ious Hash
ce
k Hash
Block n
Daten
Tx1
Tx2
Tx3
...
Previous Hash
Nonce
Block Hash
Block n+1
Daten
Tx1
Tx2
Previous Hash
Nonce
Block Hash

Proof of Work

Proof of Work: Difficulty

Proof of Work: Difficulty

```
"Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
```

Proof of Work: Difficulty

"Hello, world!**0**" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!**1**" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

Proof of Work: Difficulty

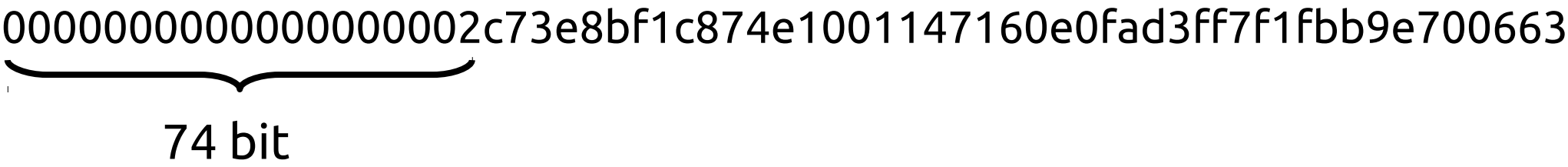
"Hello, world!**0**" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!**1**" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

...

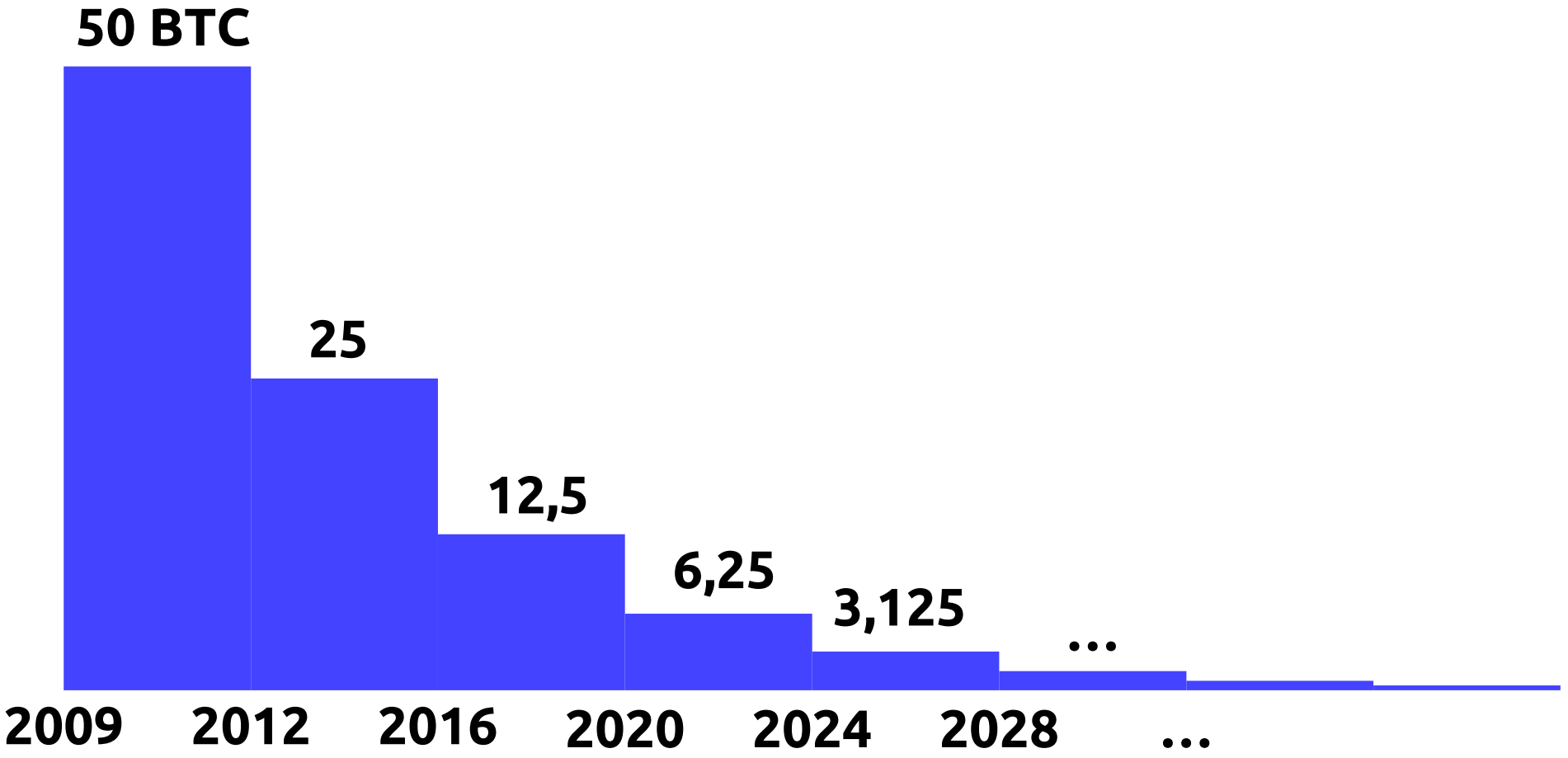
"Hello, world!**4249**" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6

"Hello, world!**4250**" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

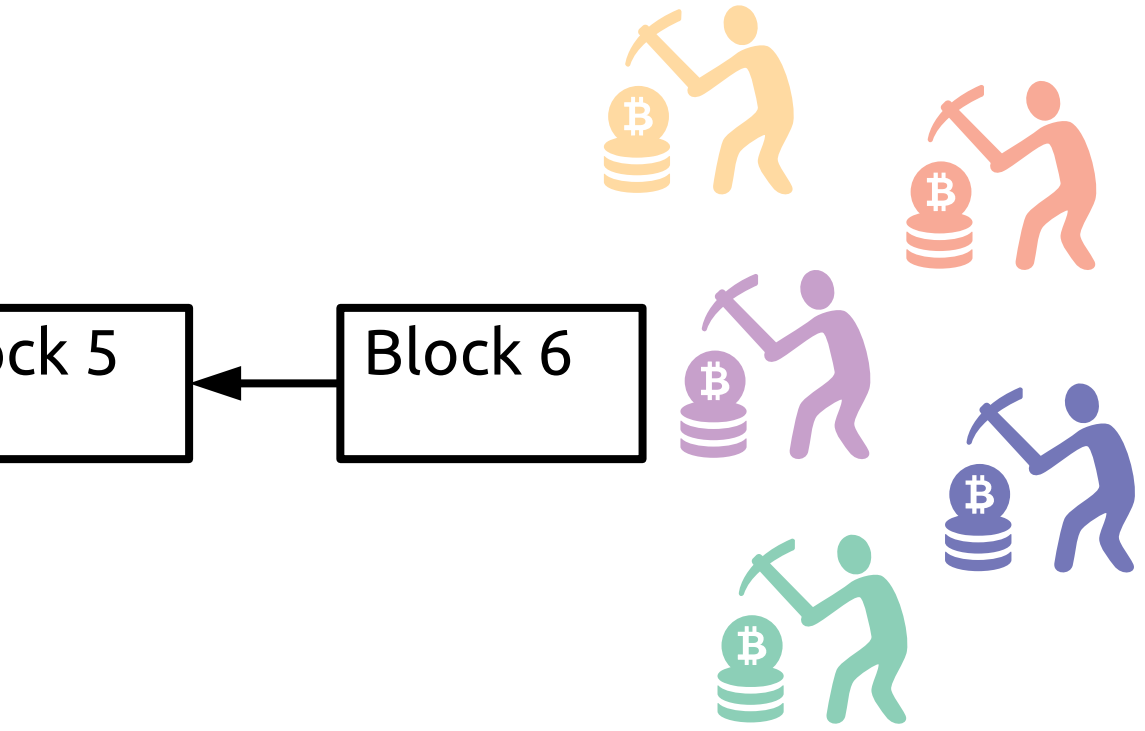

0000000000000000002c73e8bf1c874e1001147160e0fad3ff7f1fbb9e700663
74 bit

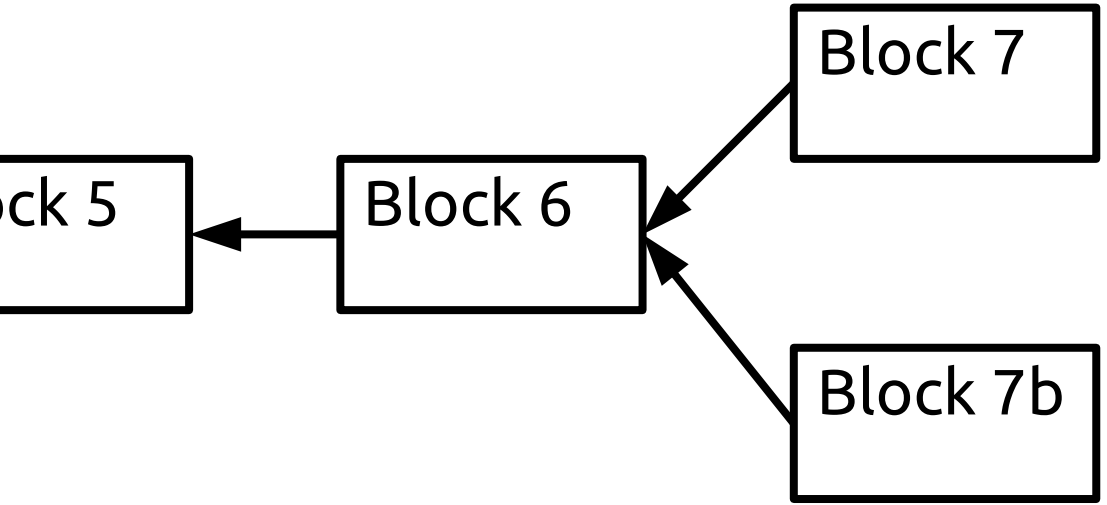
Block Reward

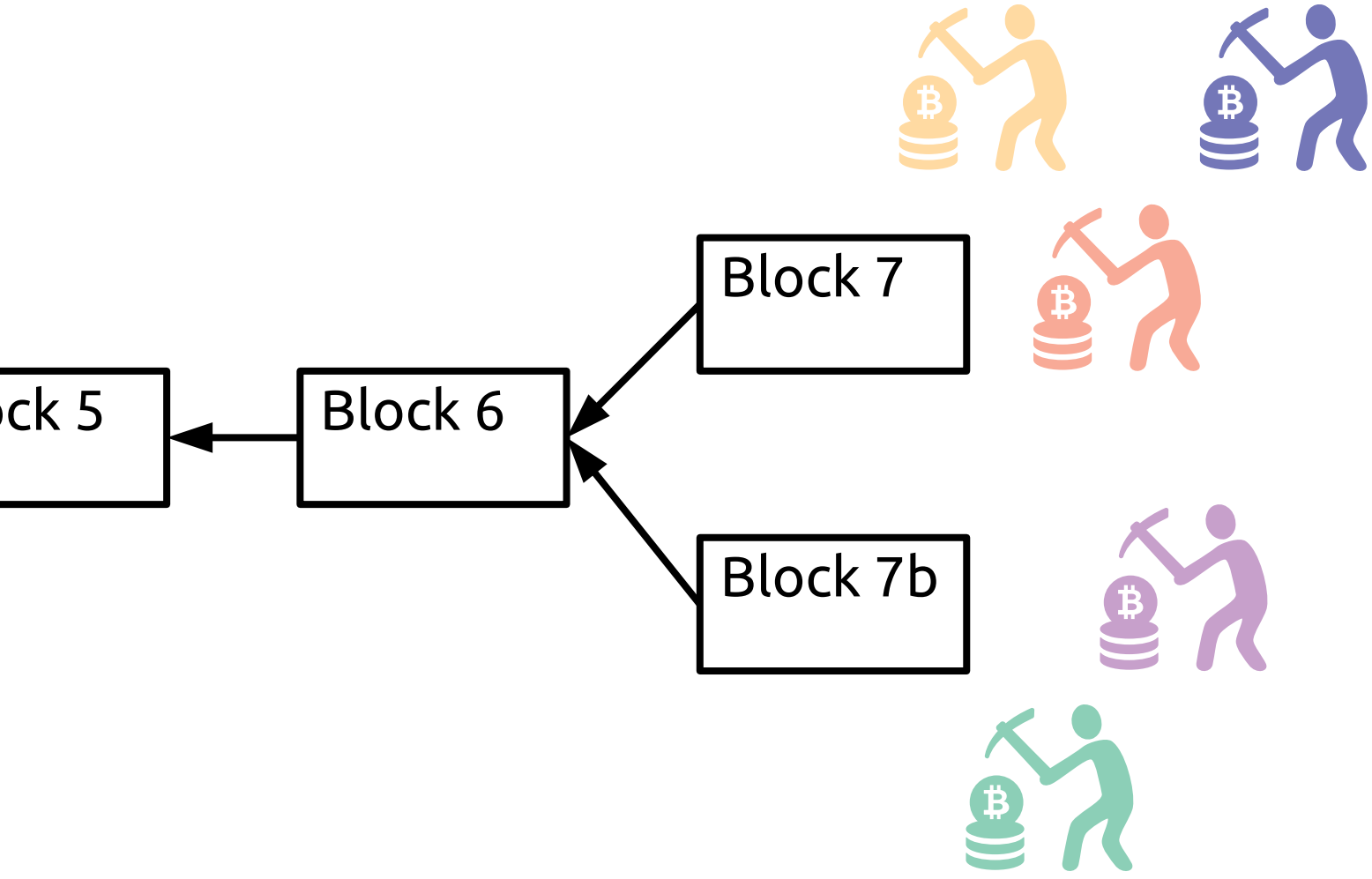
Halfing of Block Subsidy

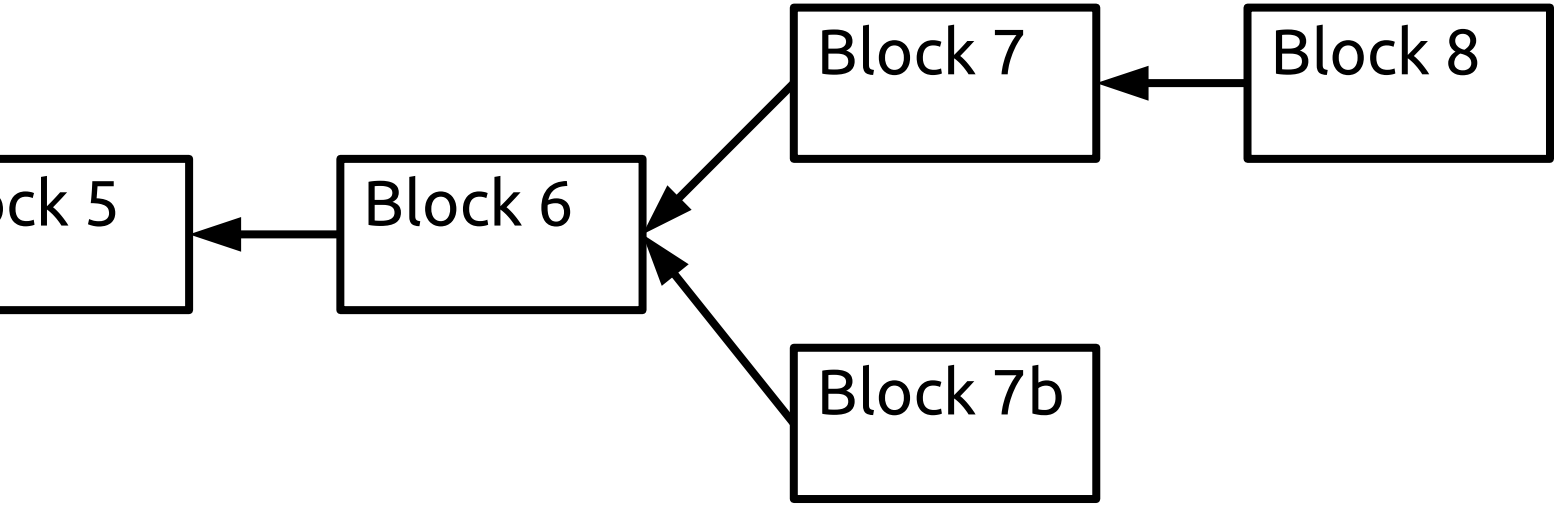


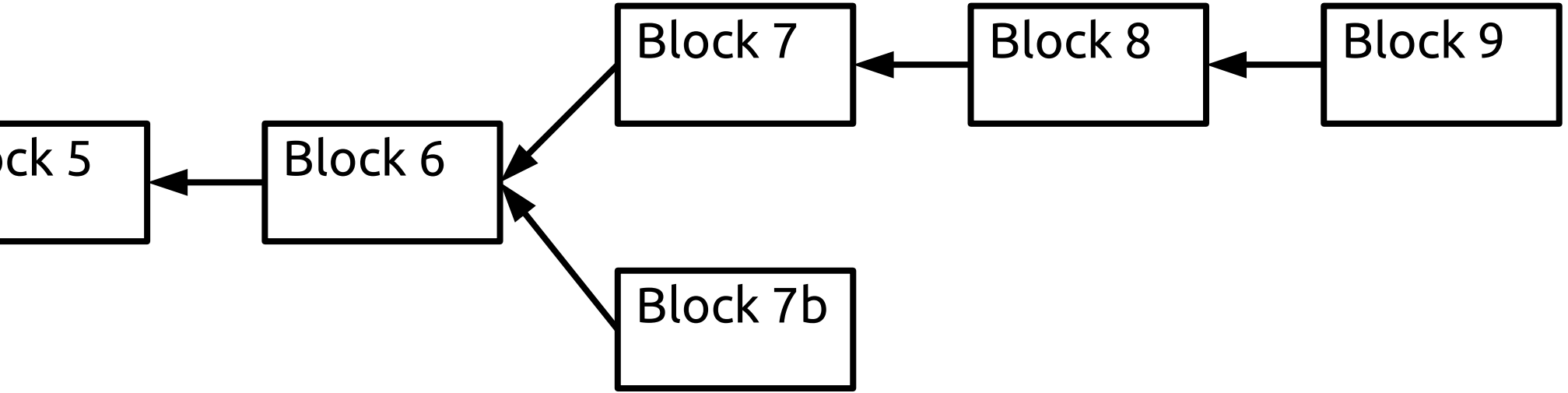
Forks


ck 5
Block 6


ock 5
Block 6
Block 7
Block 7b

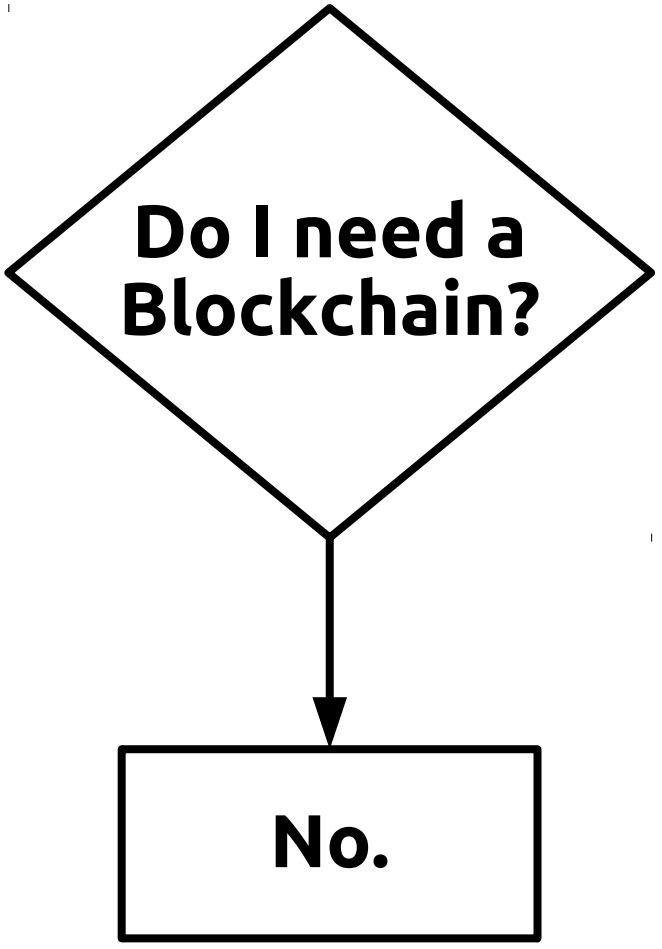

ck 5
Block 6
Block 7
Block 7b


ock 5
Block 6
Block 7
Block 8
Block 7b


ck 5
Block 6
Block 7
Block 8
Block 9
Block 7b

wahrscheinlich

Wo ist Blockchain sinnvoll?

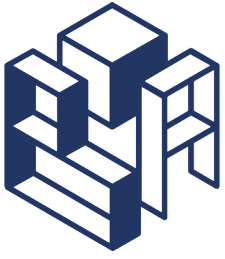


David Birch Blockchain Decision Model – https://twitter.com/dgwbirch/status/757976191487934464

Blockchains for Business

HYPERLEDGER

c·rda



BlockApps™

...

Dezentralisierung

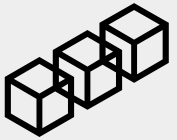
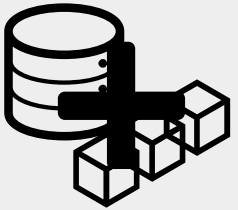
Disintermediation

Gründe für Blockchain

- Notwendigkeit Zustand zu speichern
- Geteilter Schreibzugriff
- Interaktion zwischen Transaktionen
- Kein Vertrauen zwischen den Parteien
- Kein vertrauter Intermediär
- Marketing

Manipulationssicherung privater Datenbanken mittels öffentlicher Blockchains

Warum?

	Blockchain	Datenbank	Kombination
			
Manipulationssicherheit	✓		✓
Datenschutz		✓	✓
Kosten		✓	✓
Performance		✓	✓

Wie?

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. **Daten → Hash**
2. **Hash → Blockchain**
3. **fertig**

Transaction View information about a bitcoin transaction

a83b021fb1033c65749416831a4f52a5a4cae970fa94e1e92a5df4cac41bee39

3KaDVRxq7NjFLBkU82qdLLL9KhodzsfoXV (0.00442736 BTC - Output) →

1734HkZaKJqCoA3utLTmYs8Kr5TcG55RMB - (Unspent)	0.00002 BTC
3KaDVRxq7NjFLBkU82qdLLL9KhodzsfoXV - (Spent)	0.00438536 BTC
Unable to decode output address - (Unspent)	0 BTC
	0.00440536 BTC

Summary	
Size	341 (bytes)
Weight	1037
Received Time	2018-04-06 21:55:50
Included In Blocks	516948 (2018-04-06 22:01:46 + 6 minutes)
Confirmations	5602 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.00442736 BTC
Total Output	0.00440536 BTC
Fees	0.000022 BTC
Fee per byte	6.452 sat/B
Fee per weight unit	2.122 sat/WU
Estimated BTC Transacted	0 BTC
Scripts	Hide scripts & coinbase

Input Scripts

ScriptSig: PUSHDATA(22)[00145298
Witness:
02473044022061f7f2d54bb f9262ca

RETURN
PUSHDATA1[2e2e2e2e2e2e2e2e2e2e2e2e2e2e536565207468652066756
(decoded) ....See the full picture at TDAmeritrade.com/Blockchain

Output Scripts

DUP HASH160 PUSHDATA(20)[423454fd267102b0ba7d5d14e20f0127fca30e7a] EQUALVERIFY CHECKSIG

HASH160 PUSHDATA(20)[c429020f059f5cf91a69baad624dc480e5169cbc] EQUAL

RETURN
PUSHDATA1[2e2e2e2e2e2e2e2e2e2e2e2e2e2e536565207468652066756c6c20706963747572652061742054444416d6572697472616465 ... 6c636b636861696e2e2e2e2e
(decoded) ....See the full picture at TDAmeritrade.com/Blockchain..............

Verifizierung

1. **Daten → Hash**
2. **Blockchain → Hash**
3. **Vergleich**

Datenschutz

Beweis der Nicht-Existenz

Verifizierung alter Zustände

Löschen von Daten

…