Blockchain

Eine Idee verändert die Welt

Christoph Stock

BTD11, 2018-05-18

TNG TECHNOLOGY CONSULTING

Übersicht

Geschichte

Vision

Grundlagen

Blockchain

Bitcoin

Entwicklung

Anwendungen


THE TIMES
Eat Out from £5
More than 100 great restaurants, including four Gordon Ramsay favourites from £15
Israel prepares to send tanks and troops into Gaza
Michael Sheen
Trust, Nixon
and me
Working mums
So that's how
she does it
Detox in style
The best spas
on the planer
Salman Rushdie
I won't marry
again
Giant killing?
Guide to the FA
Cup third round
Chancellor on brink of
second bailout for banks
99p
The Genesis Block
Satoshi Nakamoto

```
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
```

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

Übersicht

Geschichte
Vision
Grundlagen
Blockchain
Bitcoin
Entwicklung
Anwendungen

Vision

Dezentrales, digitales Geldsystem

Kriterien

- Keine Mittelsmänner
- Kein Vertrauen zwischen den Akteuren nötig
- Irreversible Transaktionen
- Kein "Single Point of Failure"
- Keine Beeinflussung des Systems durch einzelne Akteure

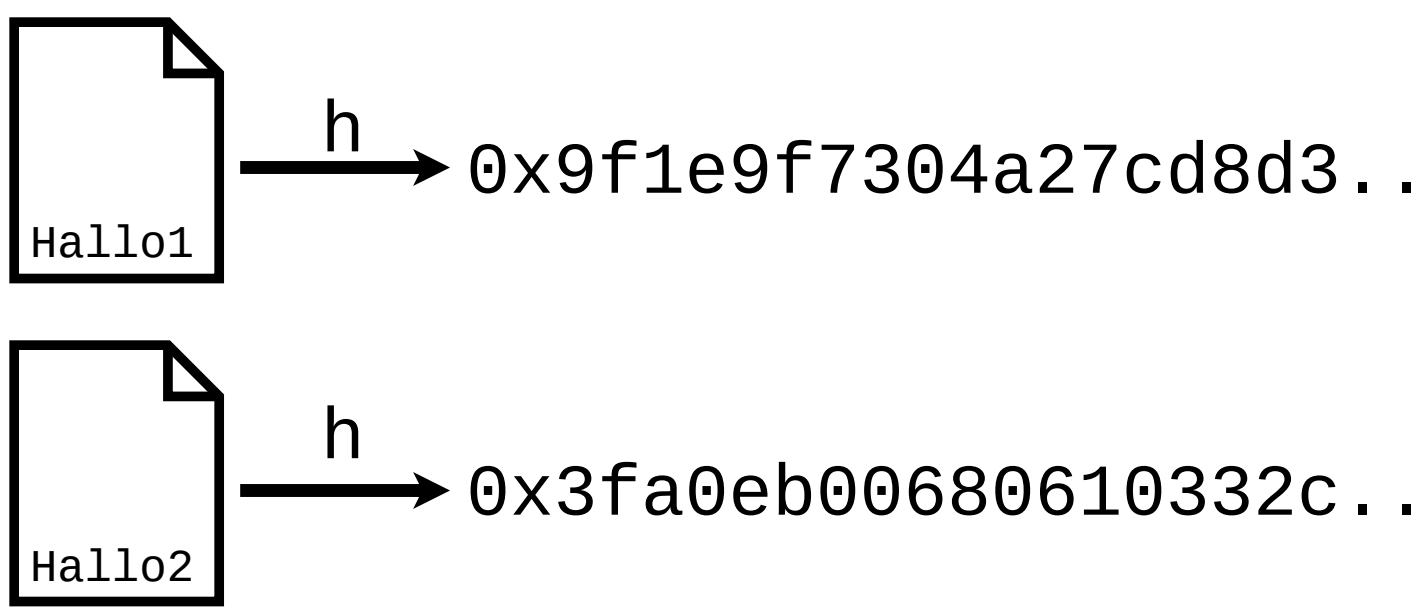
Stand 2008

- Vorhandene Bestandteile
  - Kryptographisches Hashing
  - Public-Key-Kryptographie
  - P2P-Netzwerke
- Praktisch ungelöst
  - Double-Spending-Problem

Übersicht

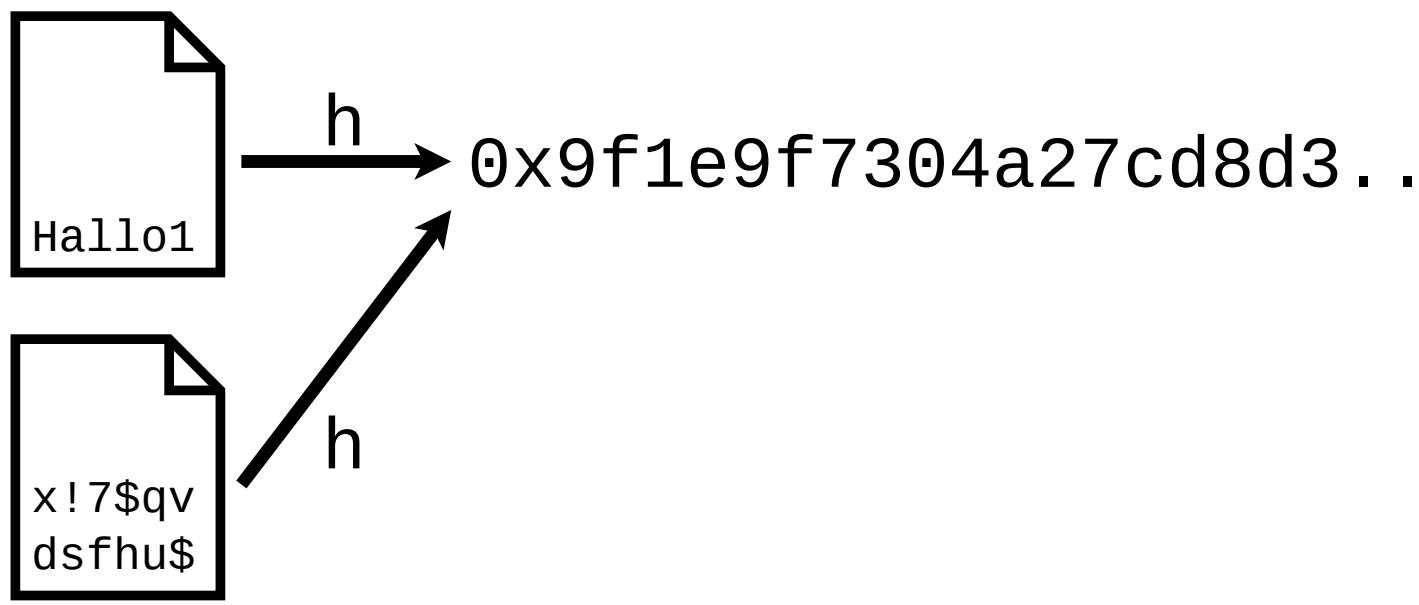
Geschichte
Vision
Grundlagen
Blockchain
Bitcoin
Entwicklung
Anwendungen

Hashfunktionen



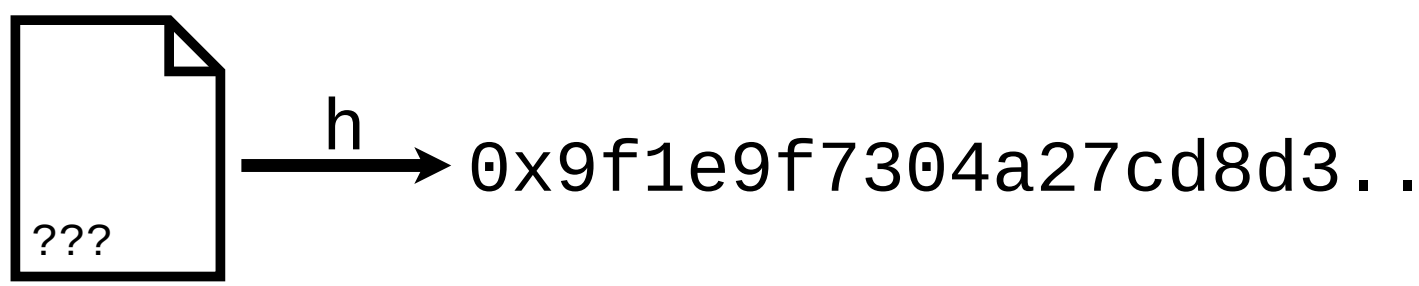
- Bilden Daten beliebiger Länge auf Zahlen fester Länge ab
- Kleine Änderungen haben große Auswirkungen
- z.B. SHA256, MD5

Hashfunktionen



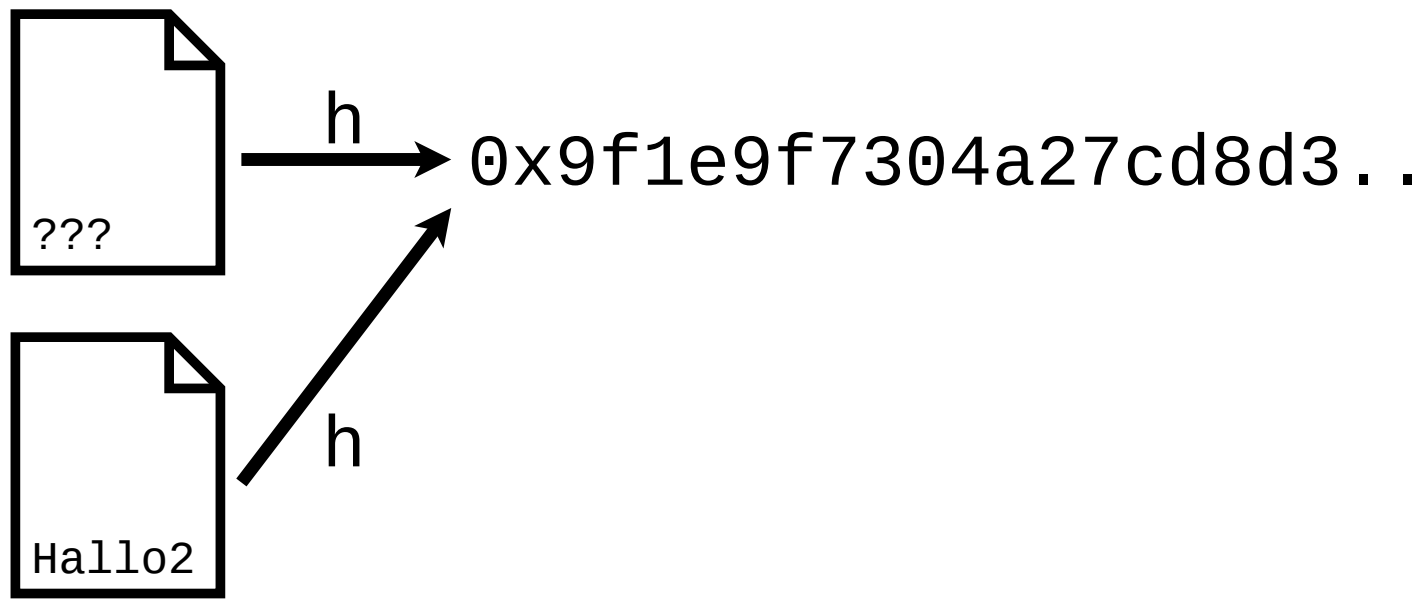
- Funktionen nicht injektiv
- Kollisionen möglich

Kryptographische Hashfunktionen



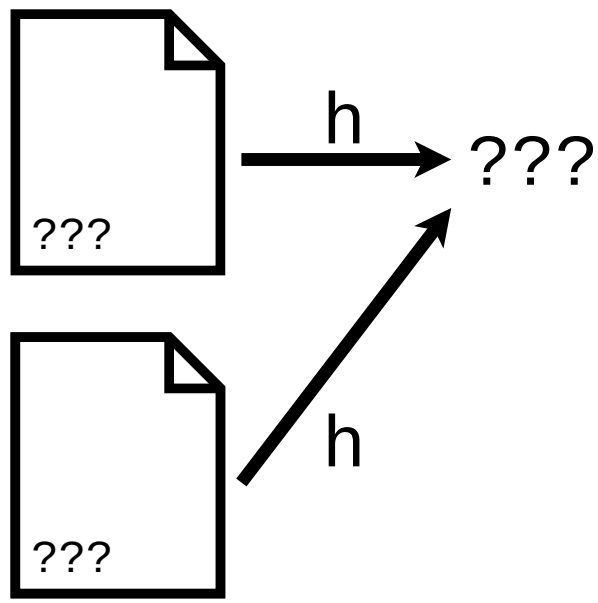
- Urbildresistenz

Kryptographische Hashfunktionen



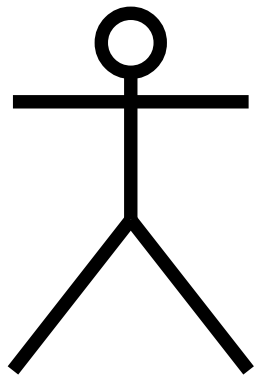
- Urbildresistenz
- 2. Urbildresistenz

Kryptographische Hashfunktionen

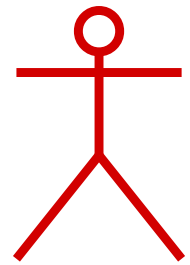


- Urbildresistenz
- 2. Urbildresistenz
- Kollisionsresistenz

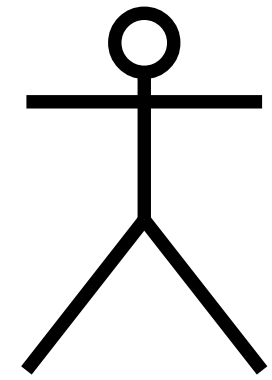
Public-Key Kryptographie



Alice

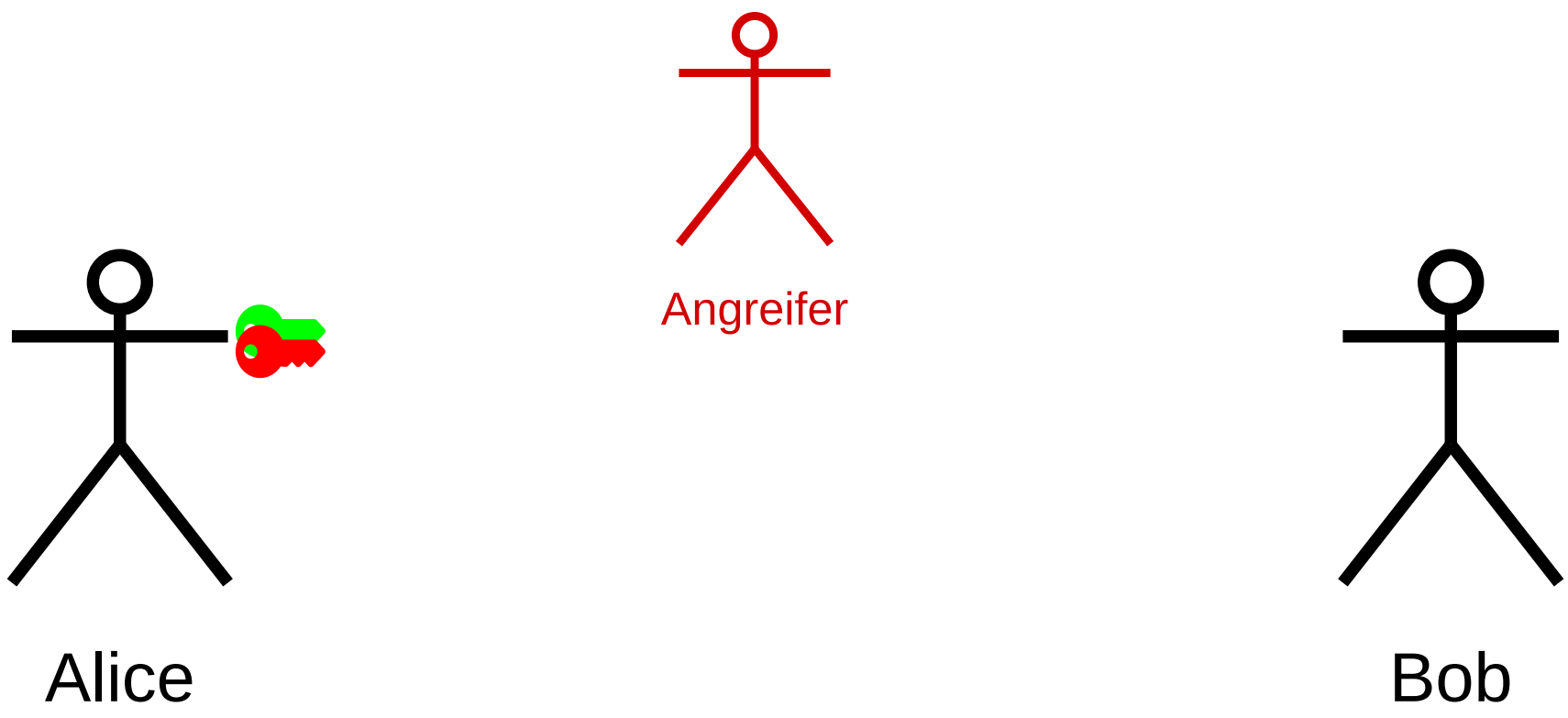


Angreifer



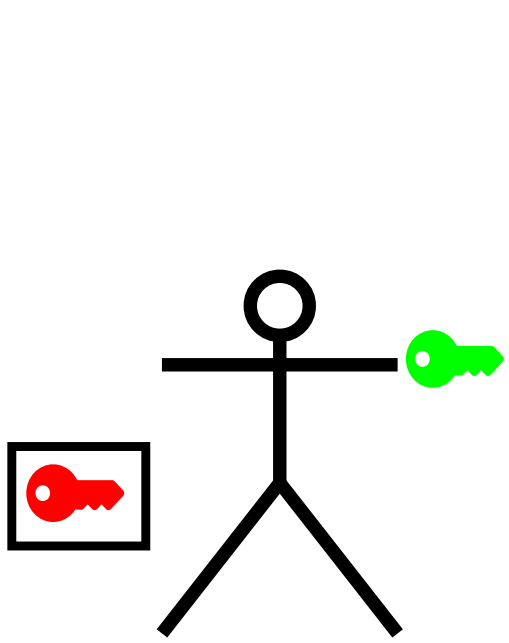
Bob

Public-Key Kryptographie

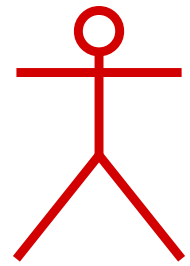


- Erzeuge privaten und öffentlichen Schlüssel

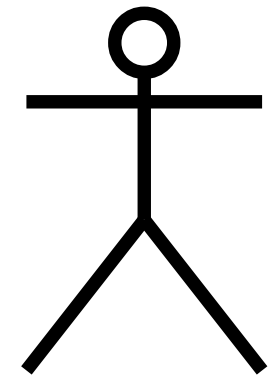
Public-Key Kryptographie



Alice



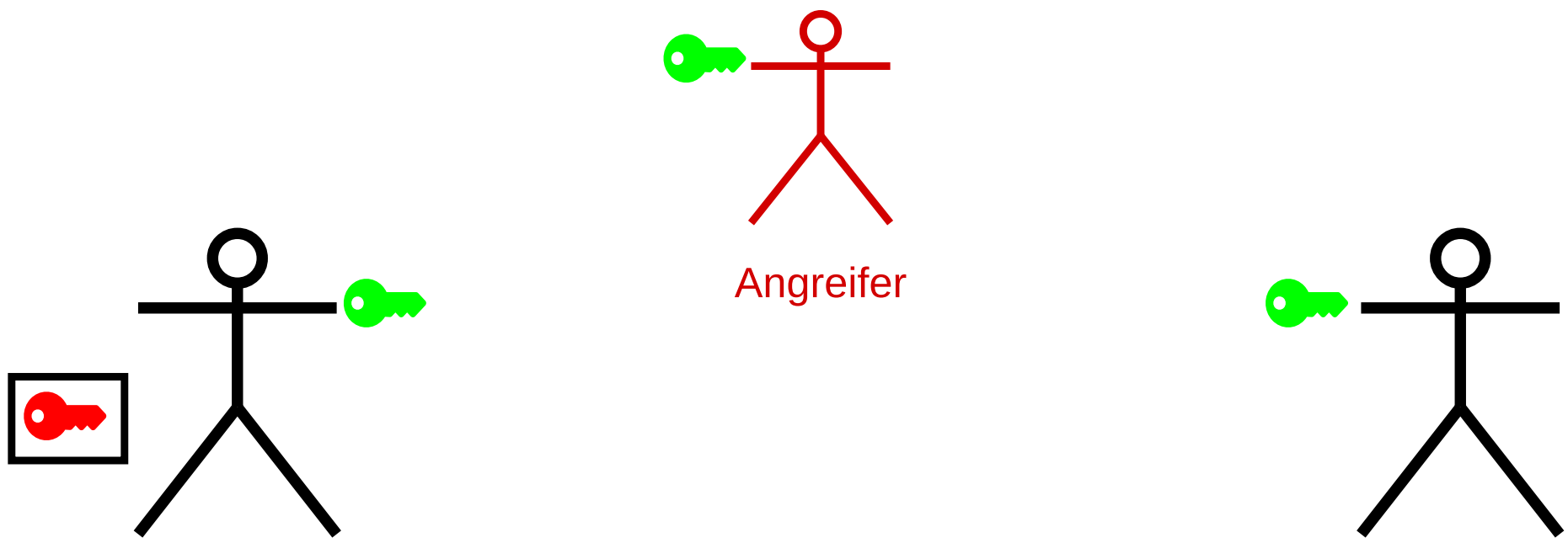
Angreifer



Bob

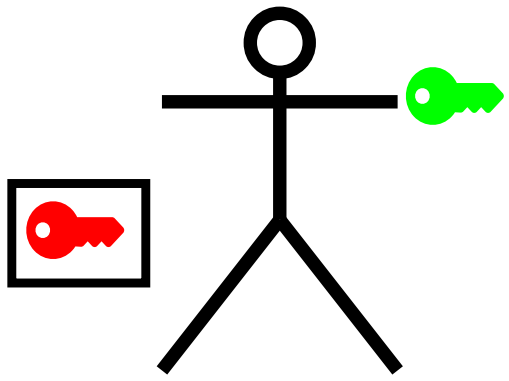
- Erzeuge privaten und öffentlichen Schlüssel
- Privater Schlüssel ist geheimzuhalten

Public-Key Kryptographie

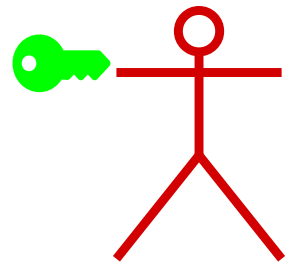


- Erzeuge privaten und öffentlichen Schlüssel
- Privater Schlüssel ist geheimzuhalten
- Öffentlicher Schlüssel wird weitergegeben

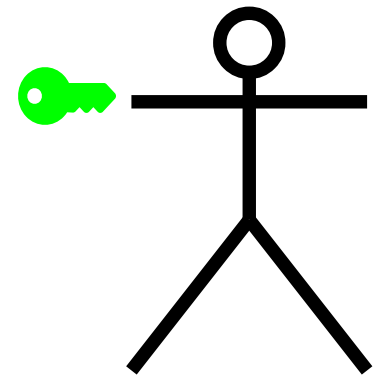
Verschlüsselung



Alice

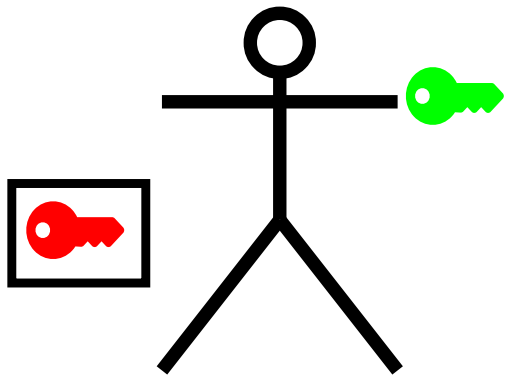


Angreifer

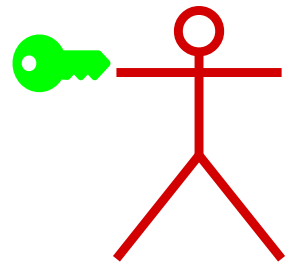


Bob

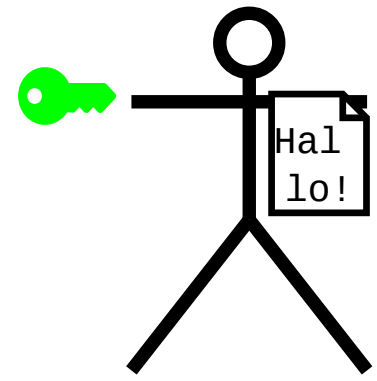
Verschlüsselung



Alice

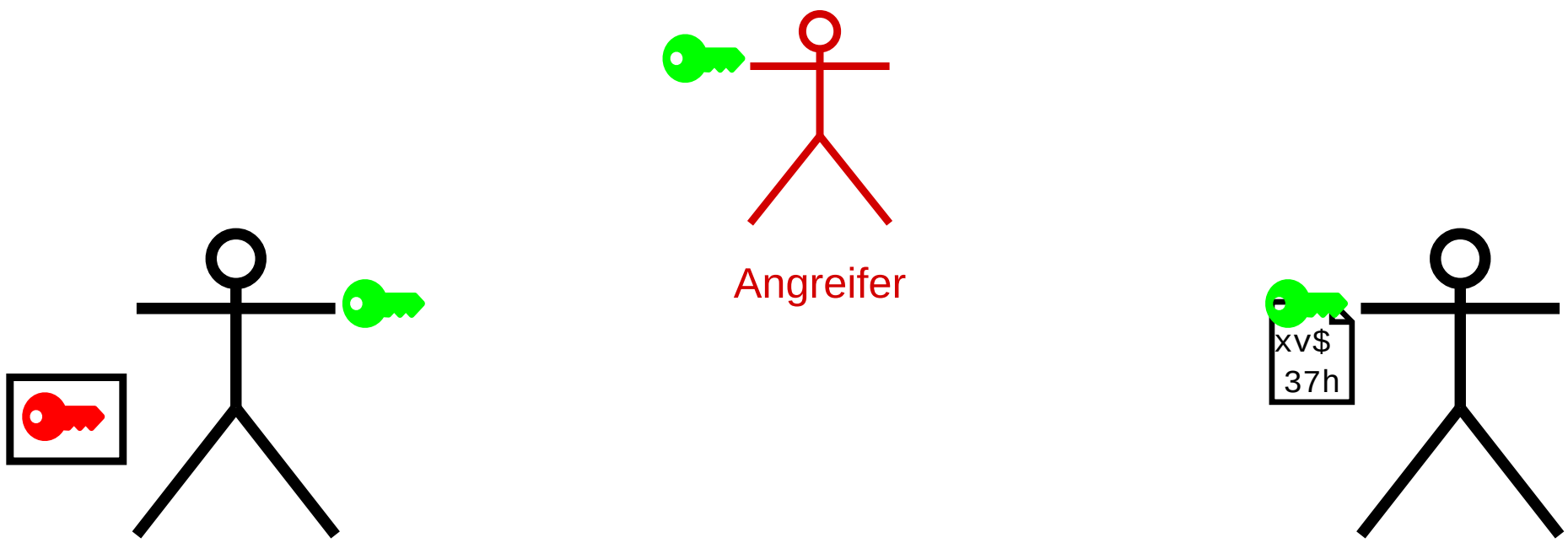


Angreifer



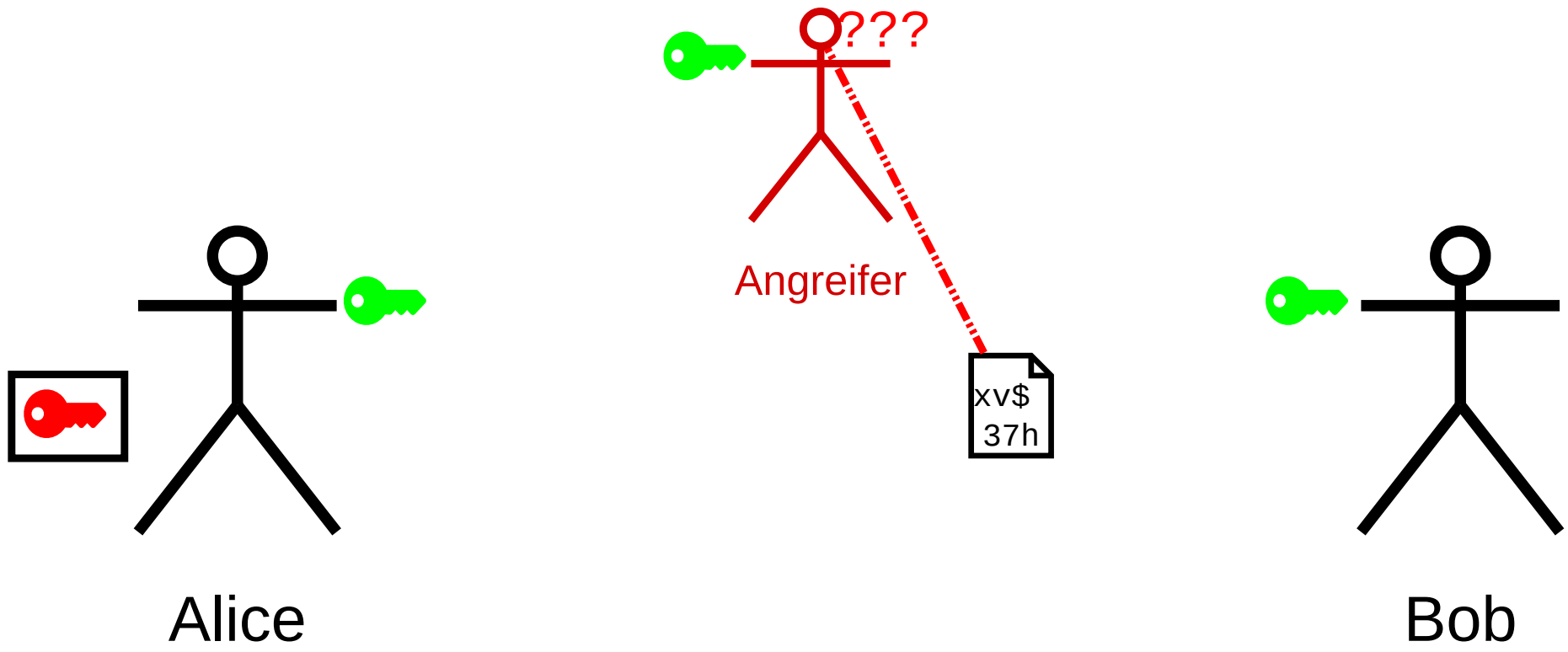
Bob

Verschlüsselung



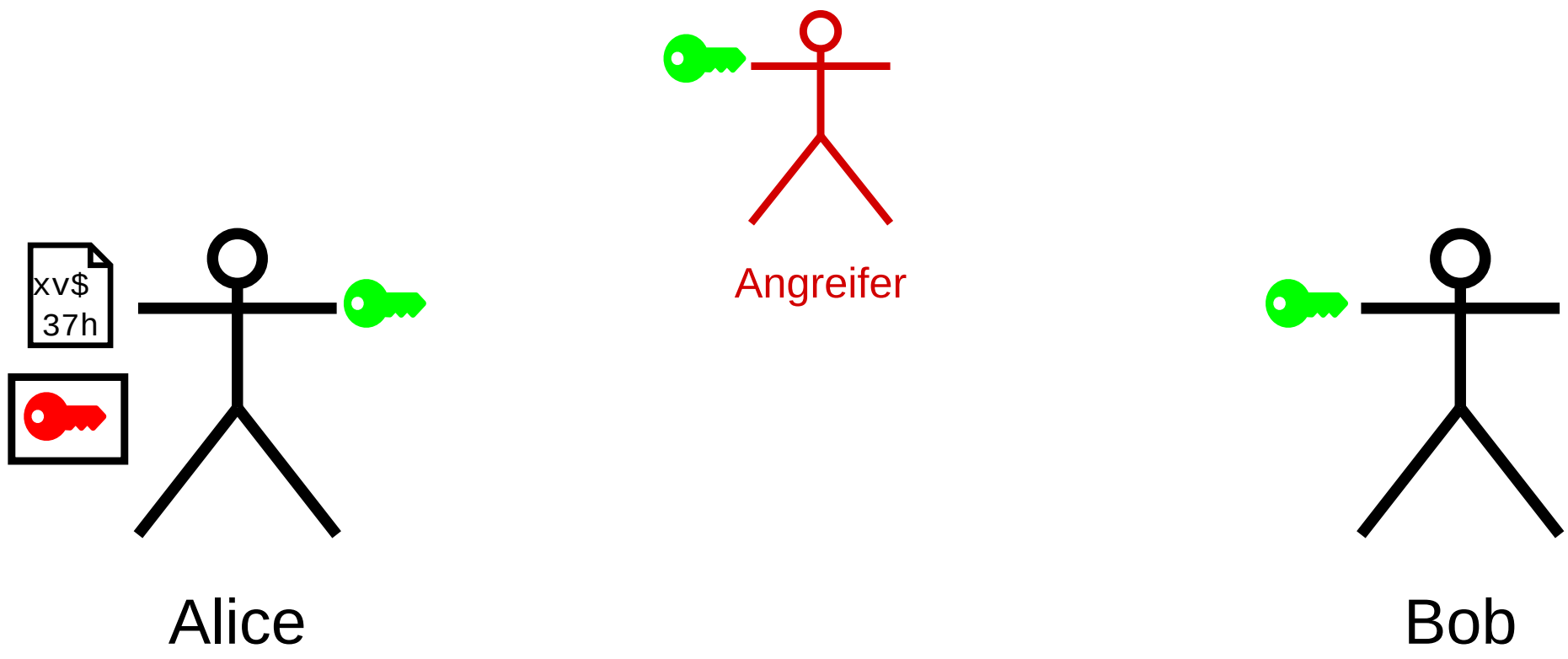
- Bob verschlüsselt Nachricht mit öffentlichem Schlüssel

Verschlüsselung



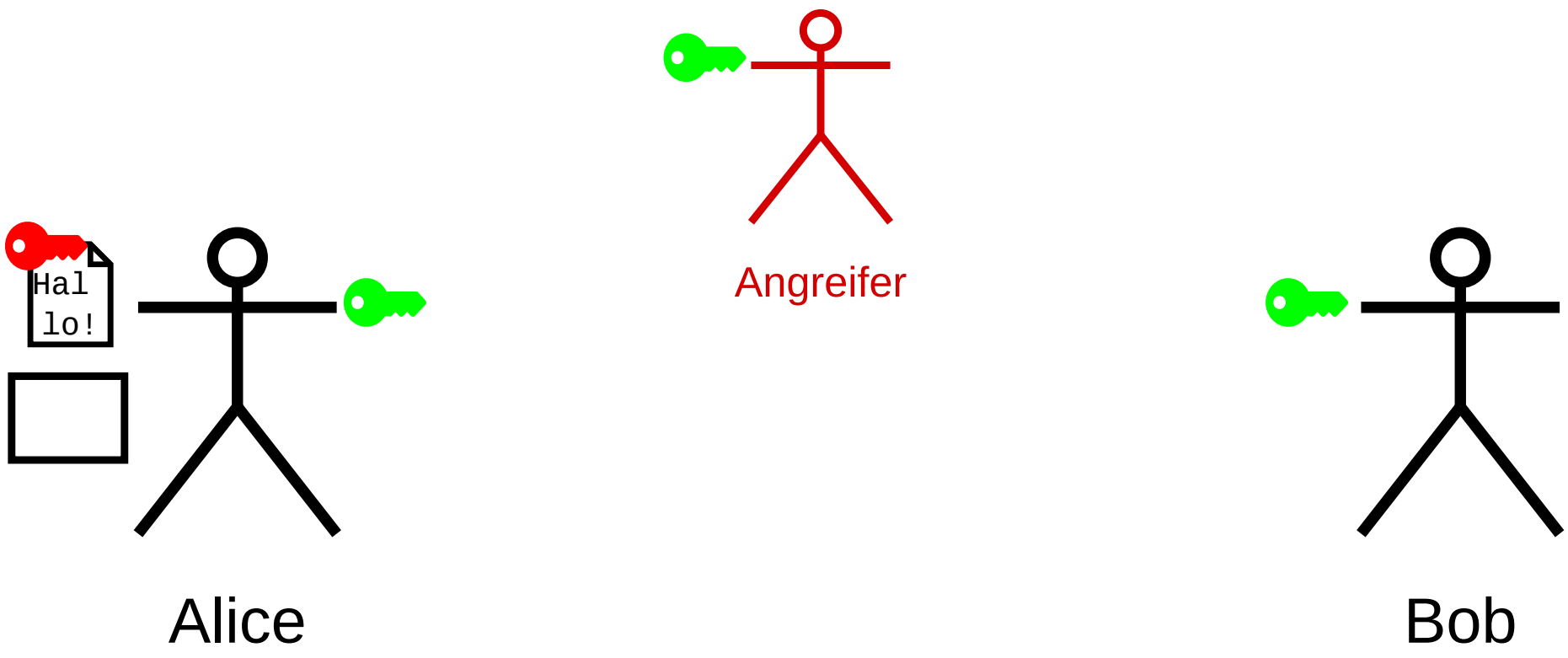
- Bob verschlüsselt Nachricht mit öffentlichem Schlüssel
- Angreifer kann Nachricht nicht entschlüsseln

Verschlüsselung



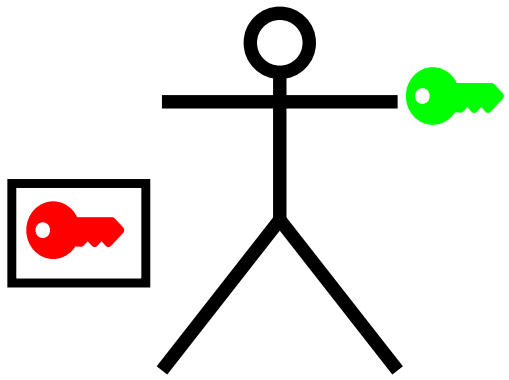
- Bob verschlüsselt Nachricht mit öffentlichem Schlüssel
- Angreifer kann Nachricht nicht entschlüsseln

Verschlüsselung

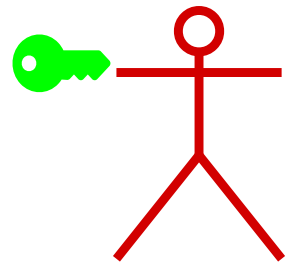


- Bob verschlüsselt Nachricht mit öffentlichem Schlüssel
- Angreifer kann Nachricht nicht entschlüsseln
- Alice entschlüsselt Nachricht mit privatem Schlüssel

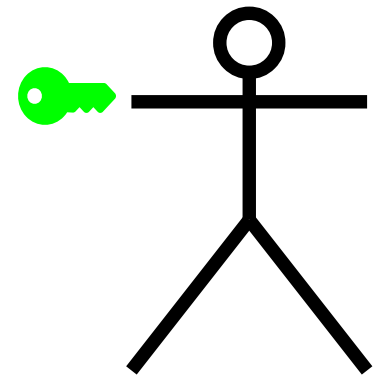
Signatur



Alice

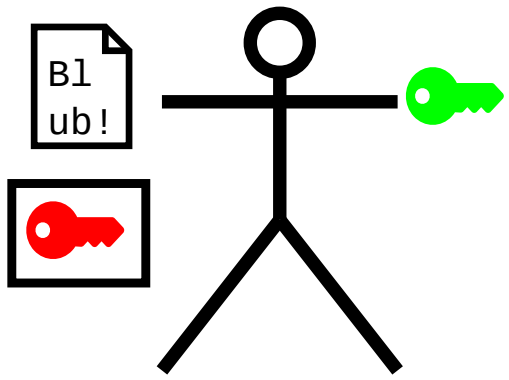


Angreifer

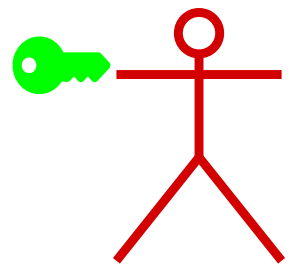


Bob

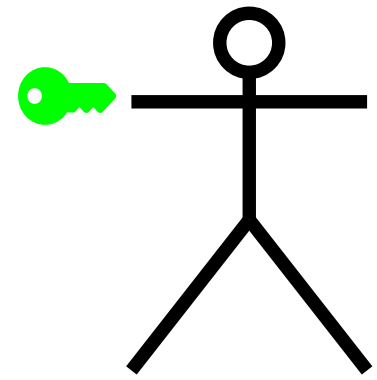
Signatur



Alice

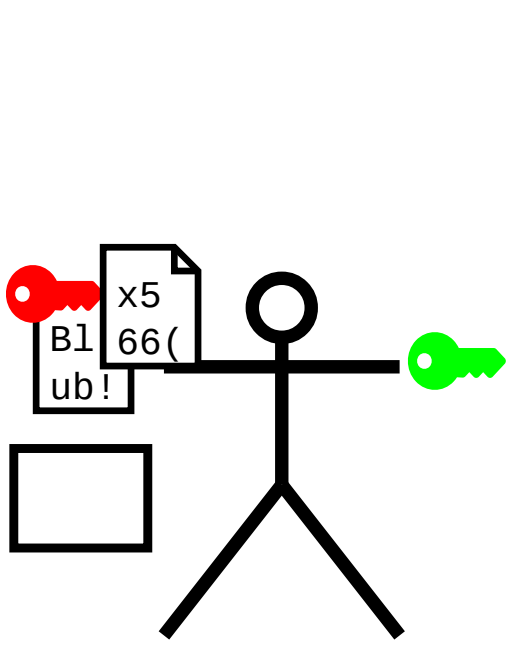


Angreifer

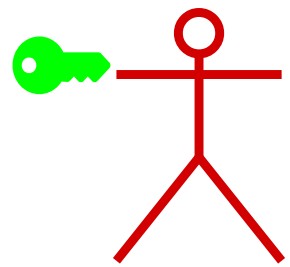


Bob

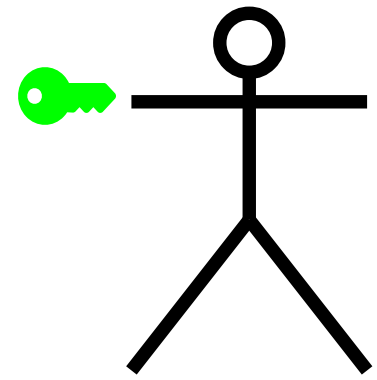
Signatur



Alice



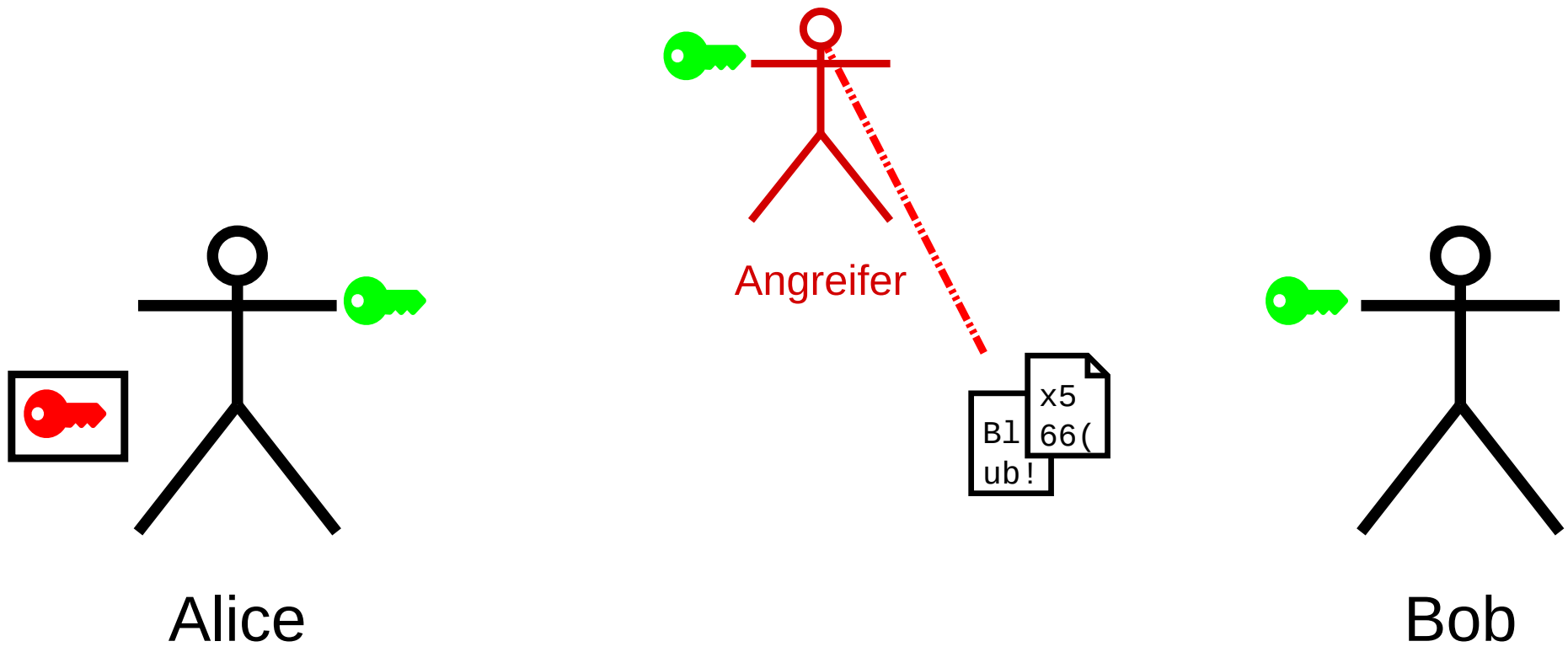
Angreifer



Bob

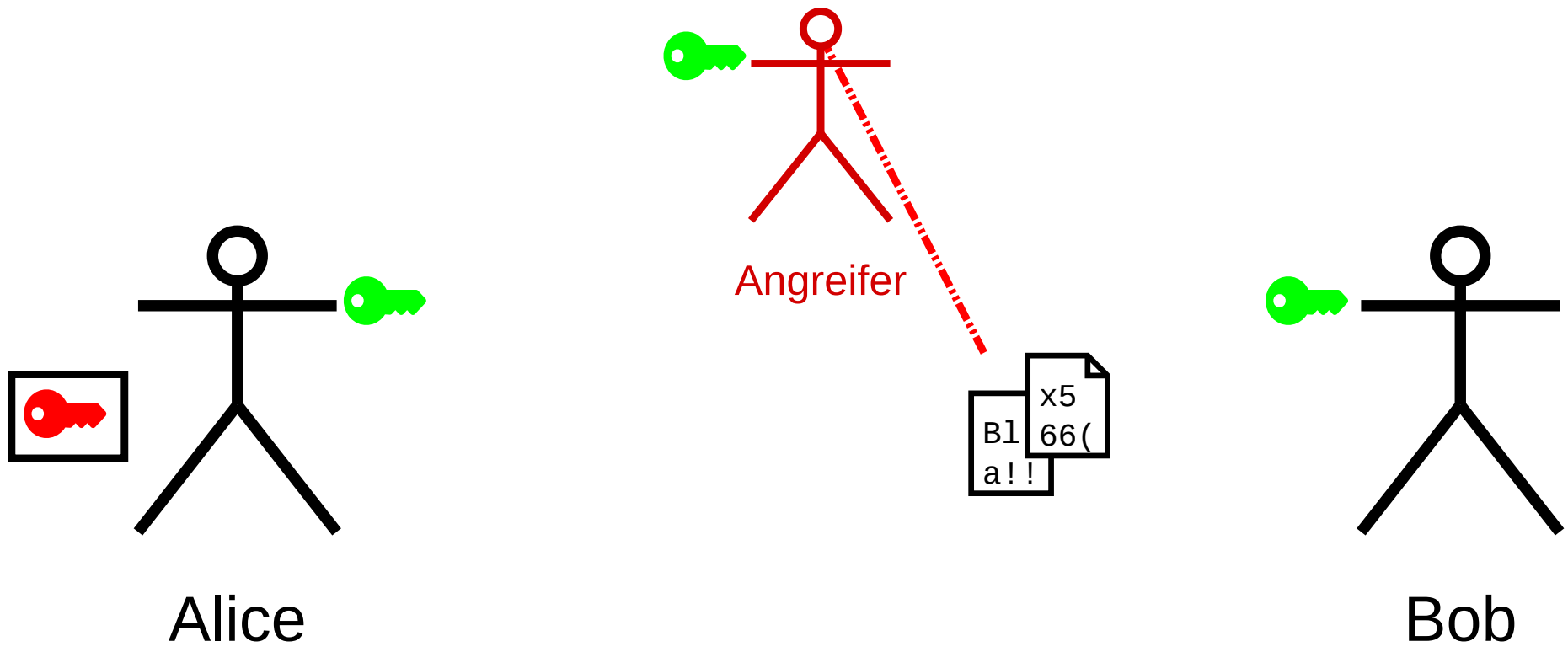
- Alice signiert die Nachricht mit privatem Schlüssel

Signatur



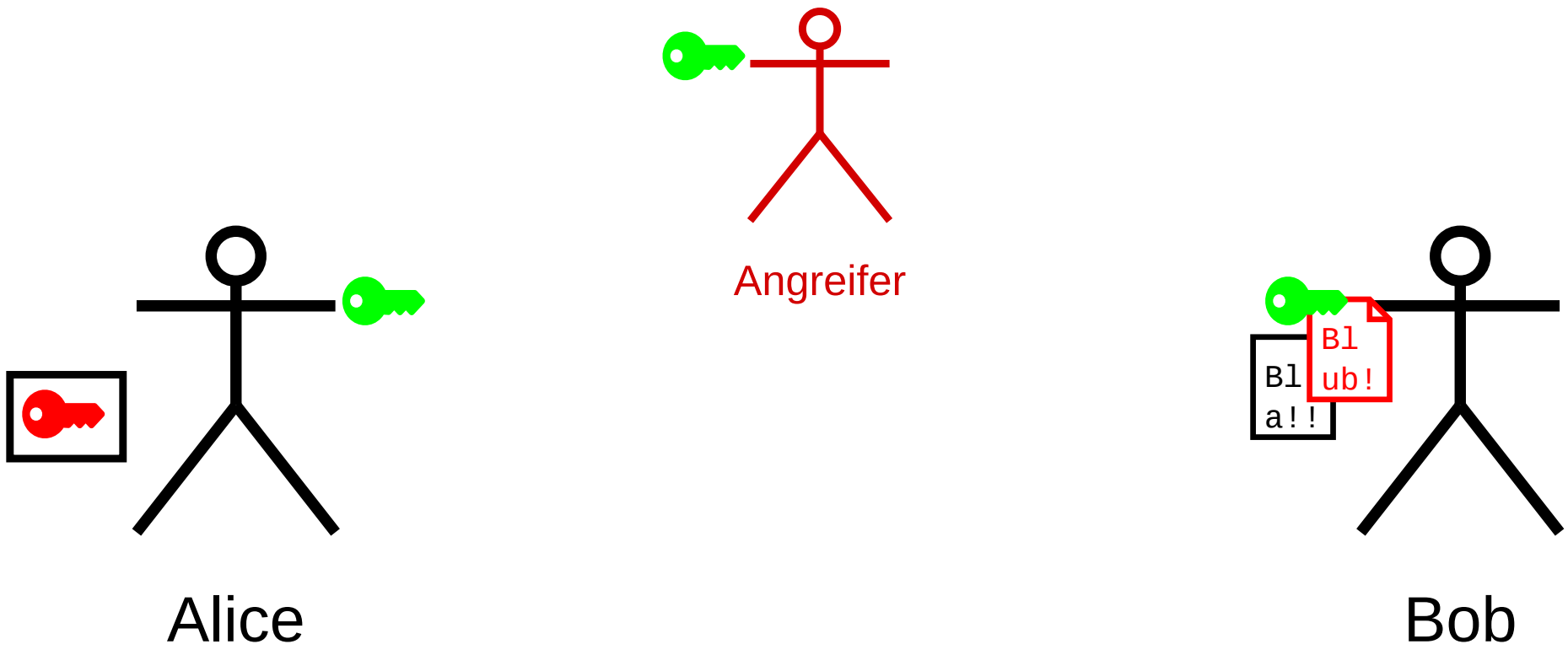
- Alice signiert die Nachricht mit privatem Schlüssel

Signatur



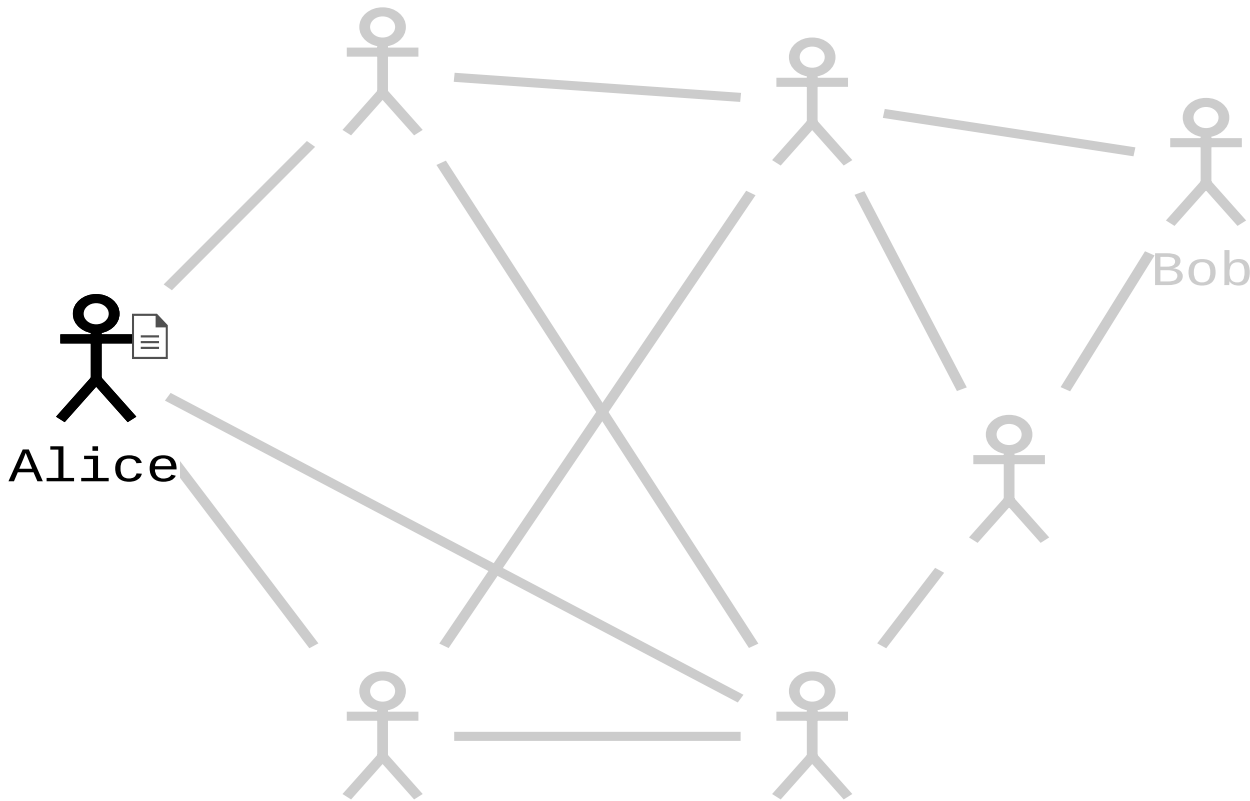
- Alice signiert die Nachricht mit privatem Schlüssel
- Der Angreifer manipuliert die Nachricht

Signatur

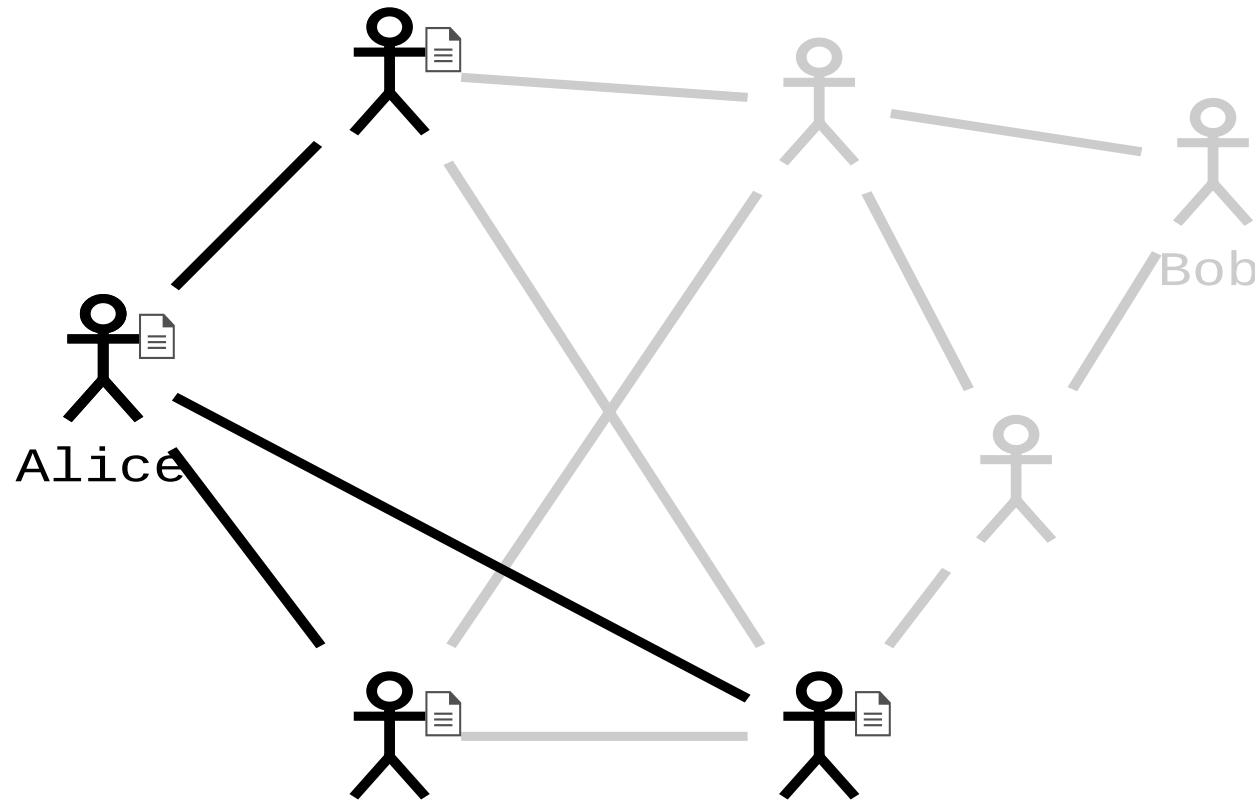


- Alice signiert die Nachricht mit privatem Schlüssel
- Der Angreifer manipuliert die Nachricht
- Bob bemerkt die Manipulation

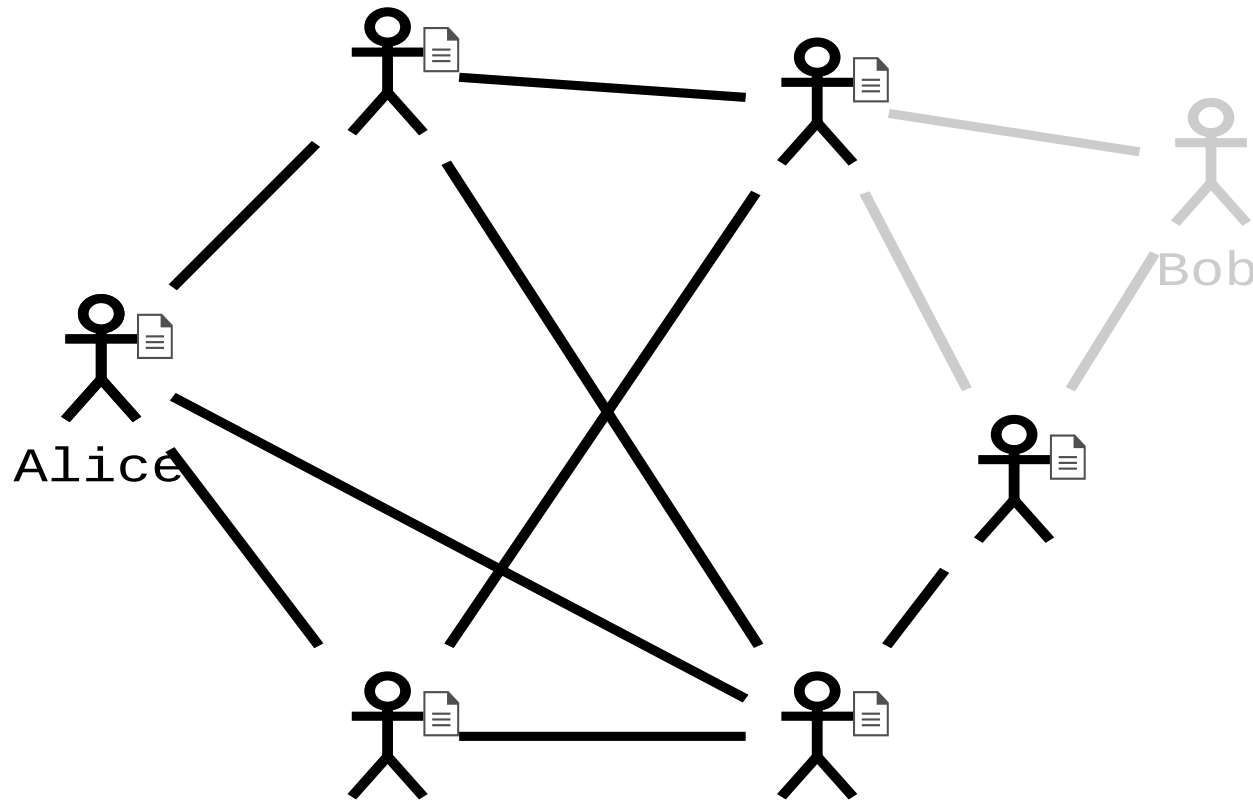
P2P-Netzwerk



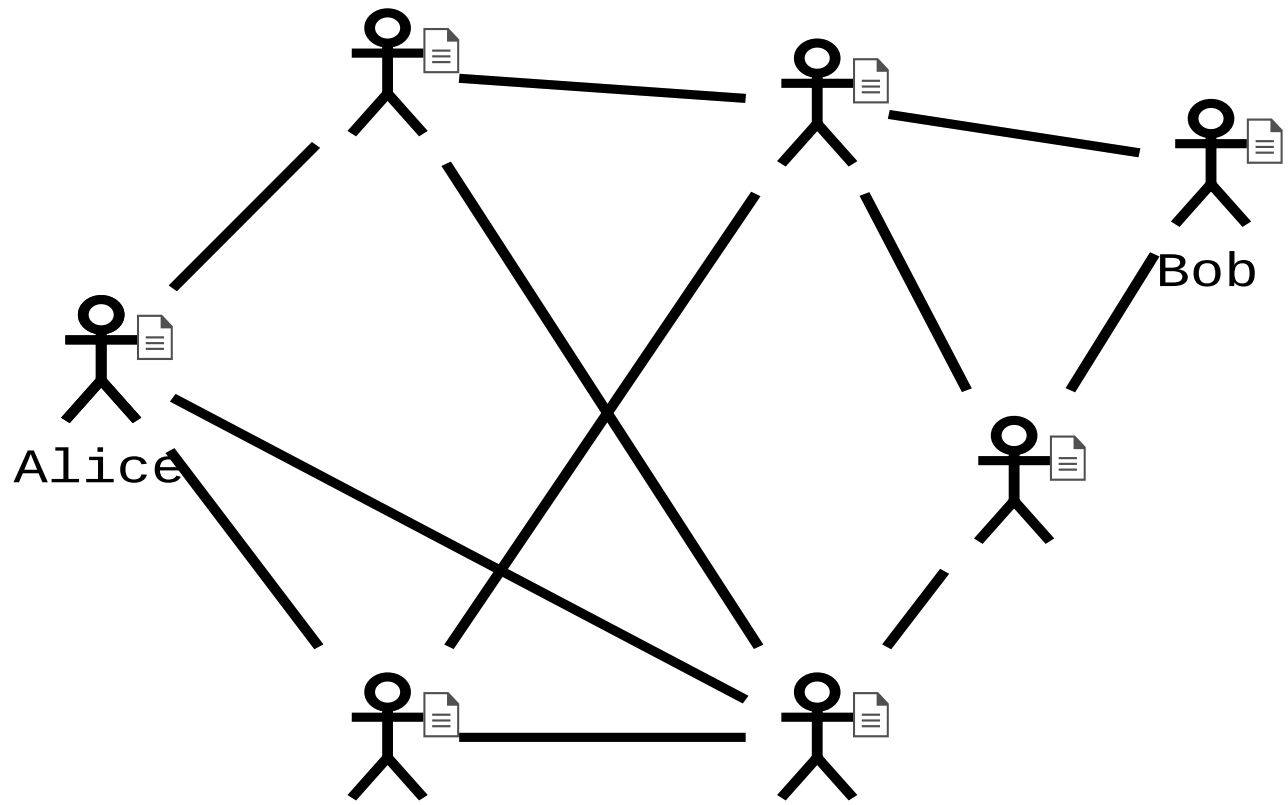
P2P-Netzwerk



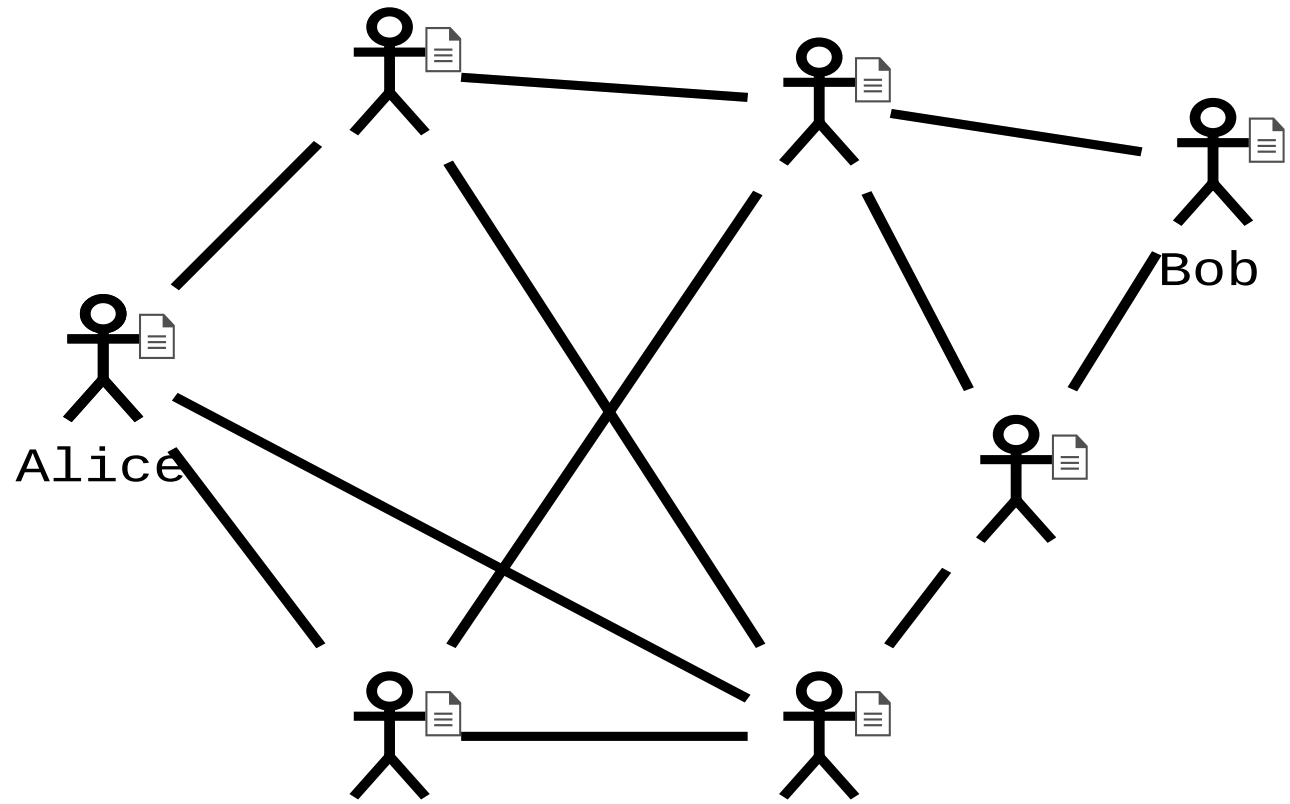
P2P-Netzwerk



P2P-Netzwerk

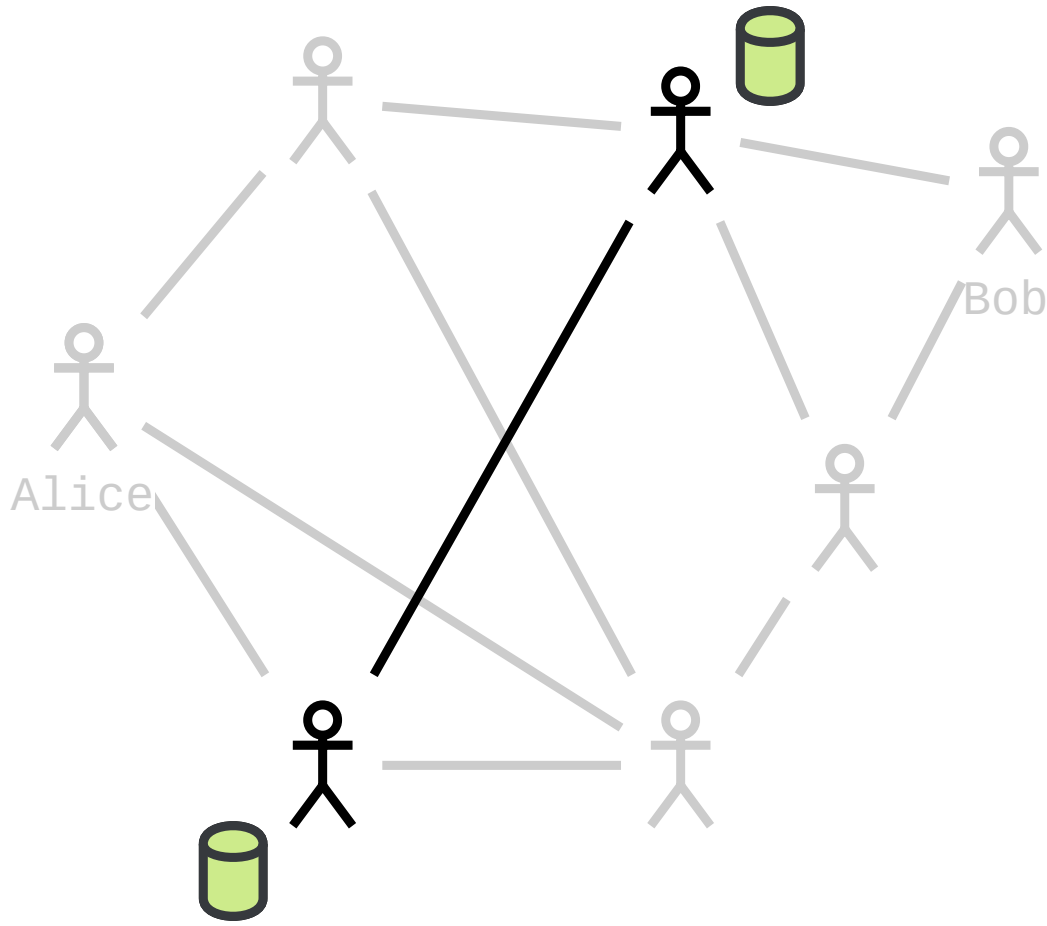


P2P-Netzwerk



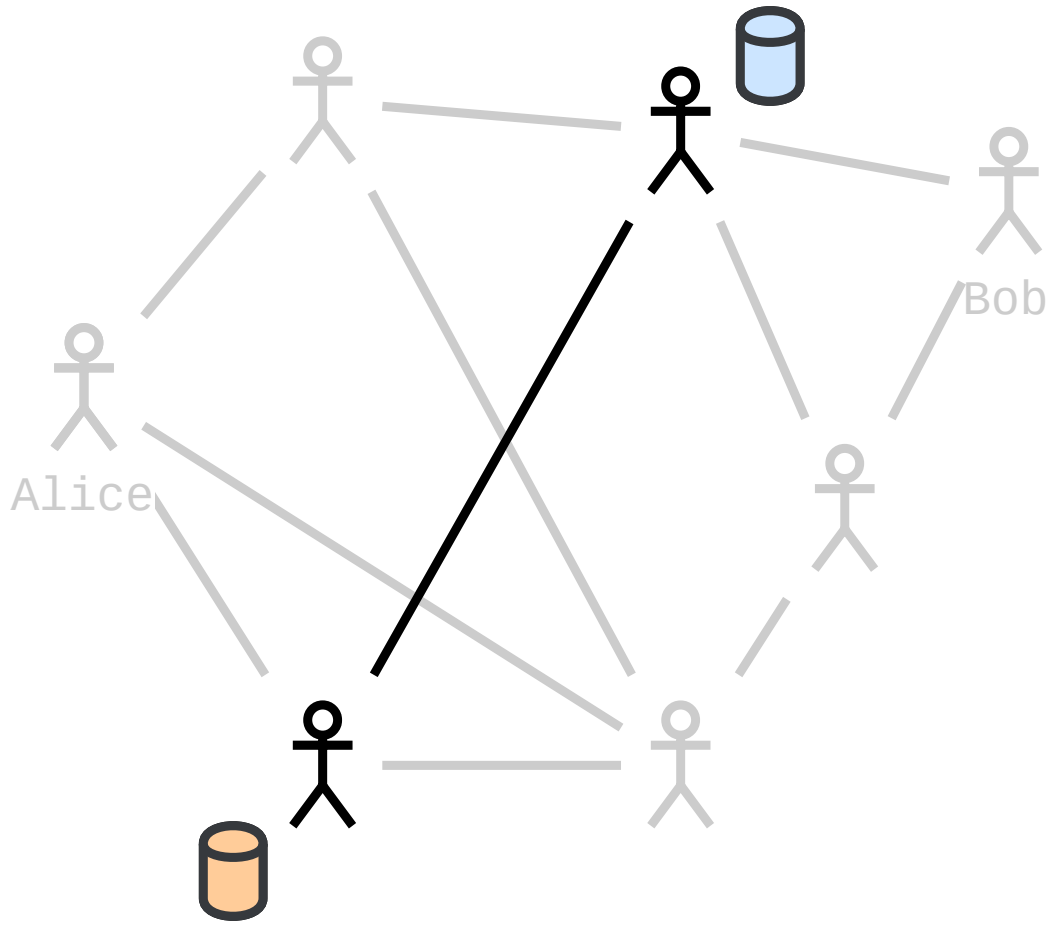
- Finanztransaktionen werden als Nachricht ausgetauscht
- Problem: Keine zentrale Instanz verhindert Double-Spending
- Transaktionen können sich gegenseitig widersprechen
- P2P-Knoten prüft Nachricht gegen lokale Historie

P2P-Netzwerk



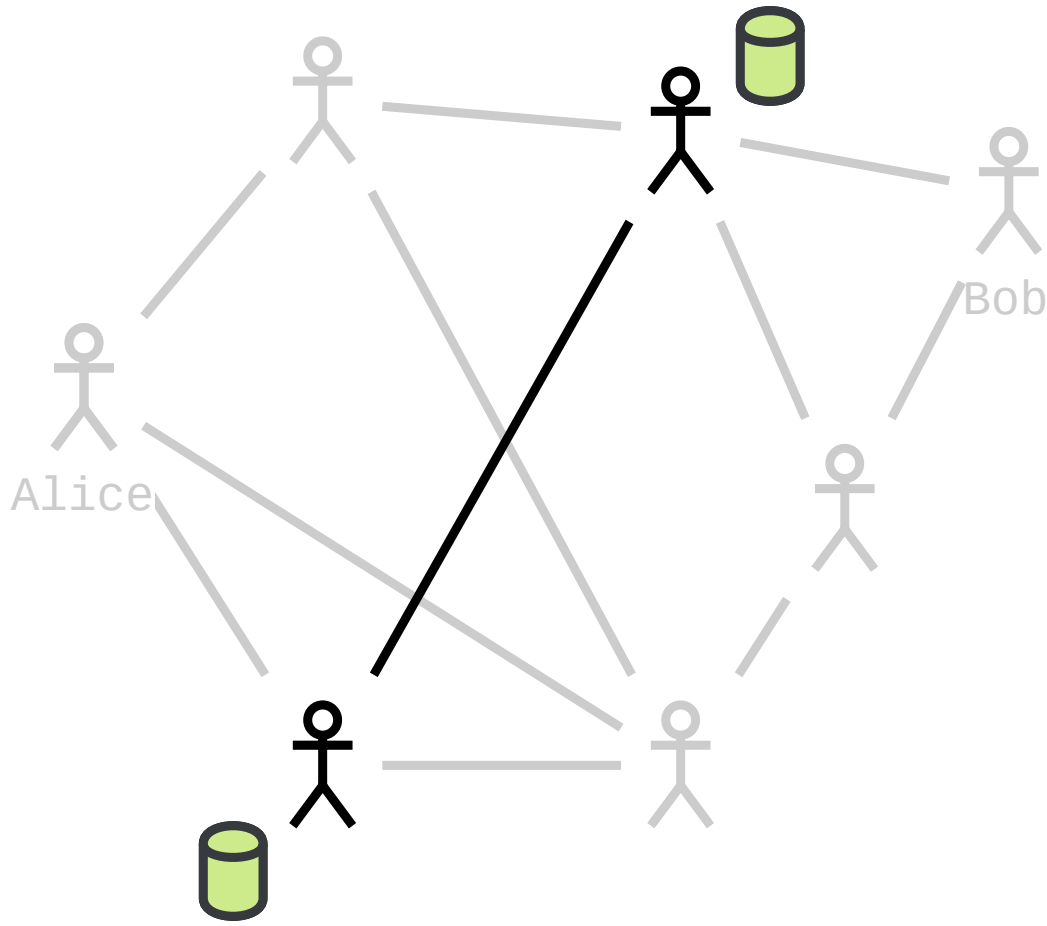
- Datenbank "gleich"

P2P-Netzwerk



- Datenbank "gleich"
- Datenbank "ungleich"
  - Zustände unterscheidbar in "schlechter" und "besser"

P2P-Netzwerk

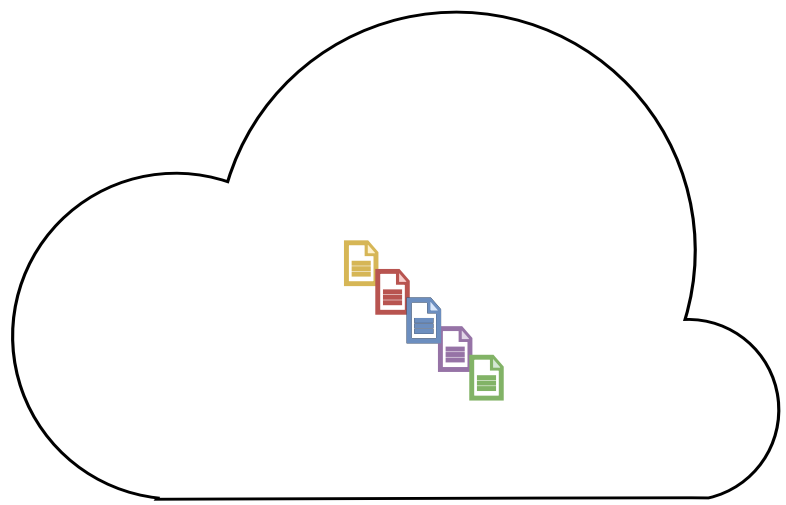


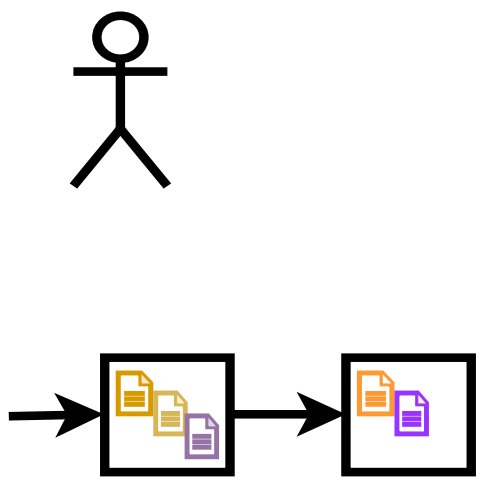
- Datenbank "gleich"
- Datenbank "ungleich"
  - Zustände unterscheidbar in "schlechter" und "besser"
  - "Schlechter" wird durch "besser" ersetzt

Übersicht

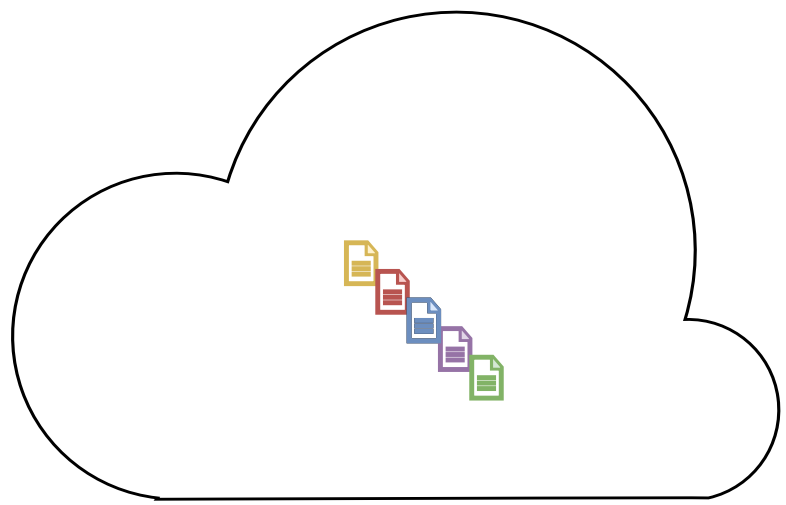
Geschichte
Vision
Grundlagen
Blockchain
Bitcoin
Entwicklung
Anwendungen

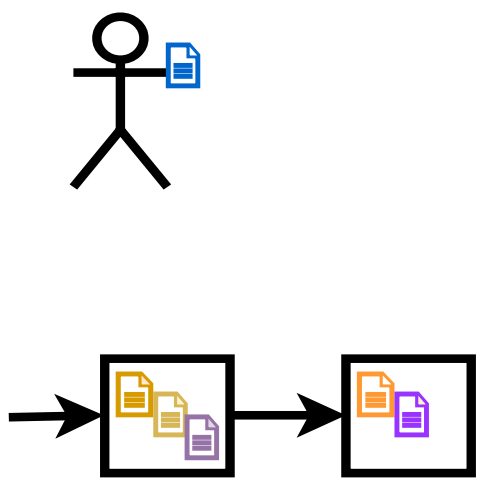
Blockchain: Funktionsweise



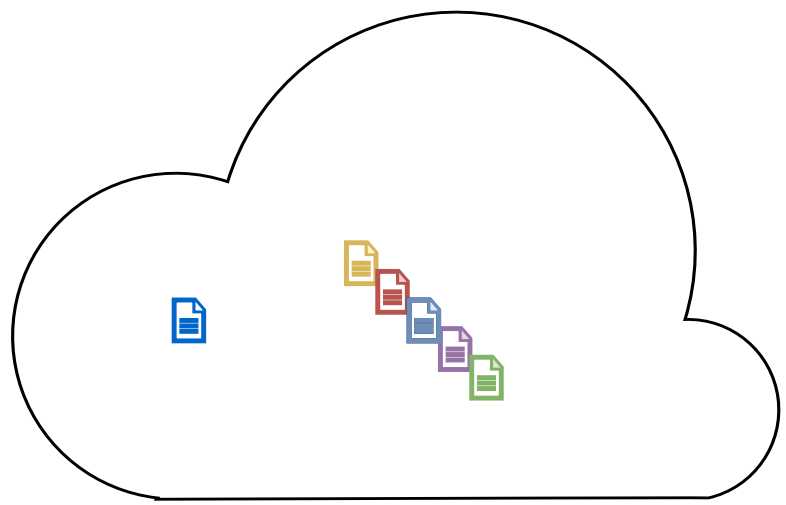


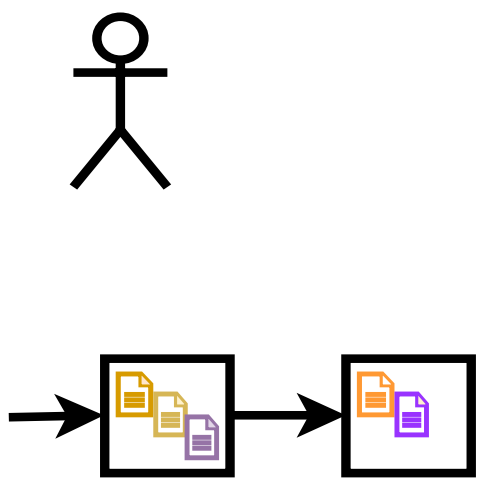
Blockchain: Funktionsweise



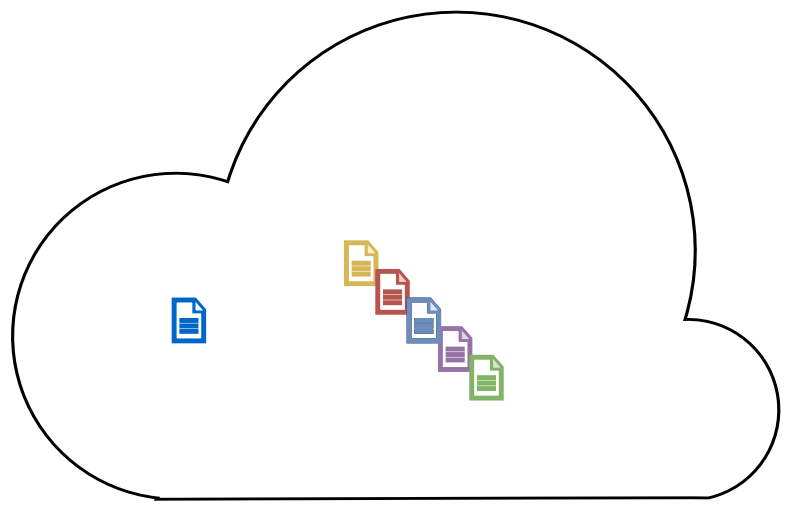


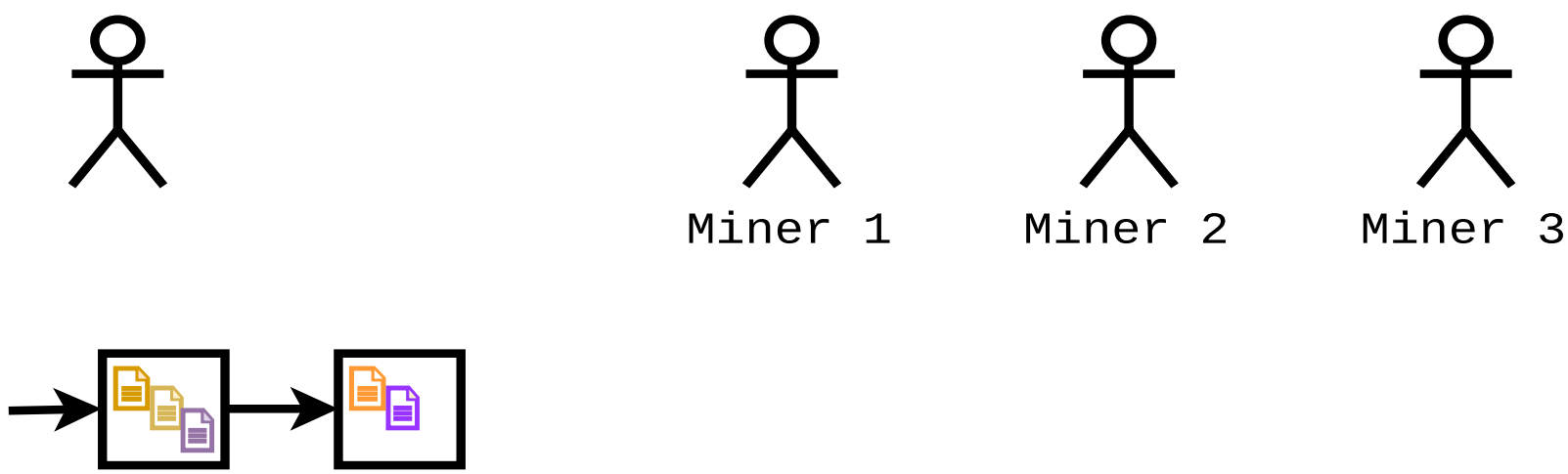
Blockchain: Funktionsweise



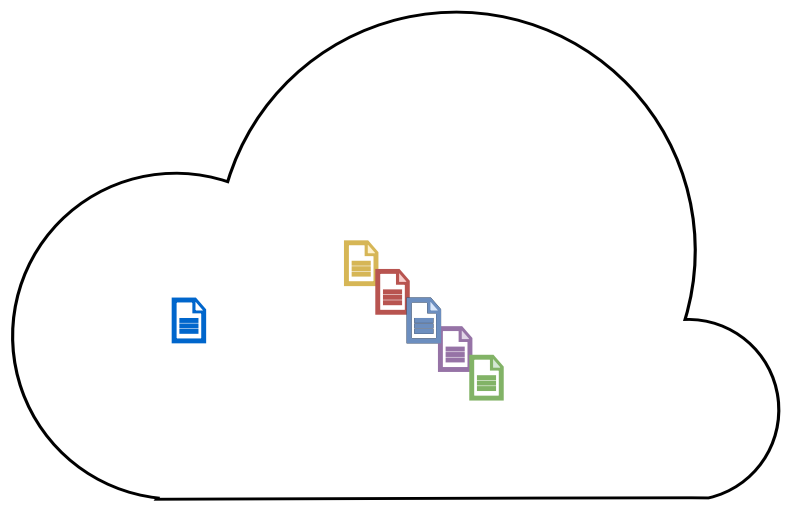


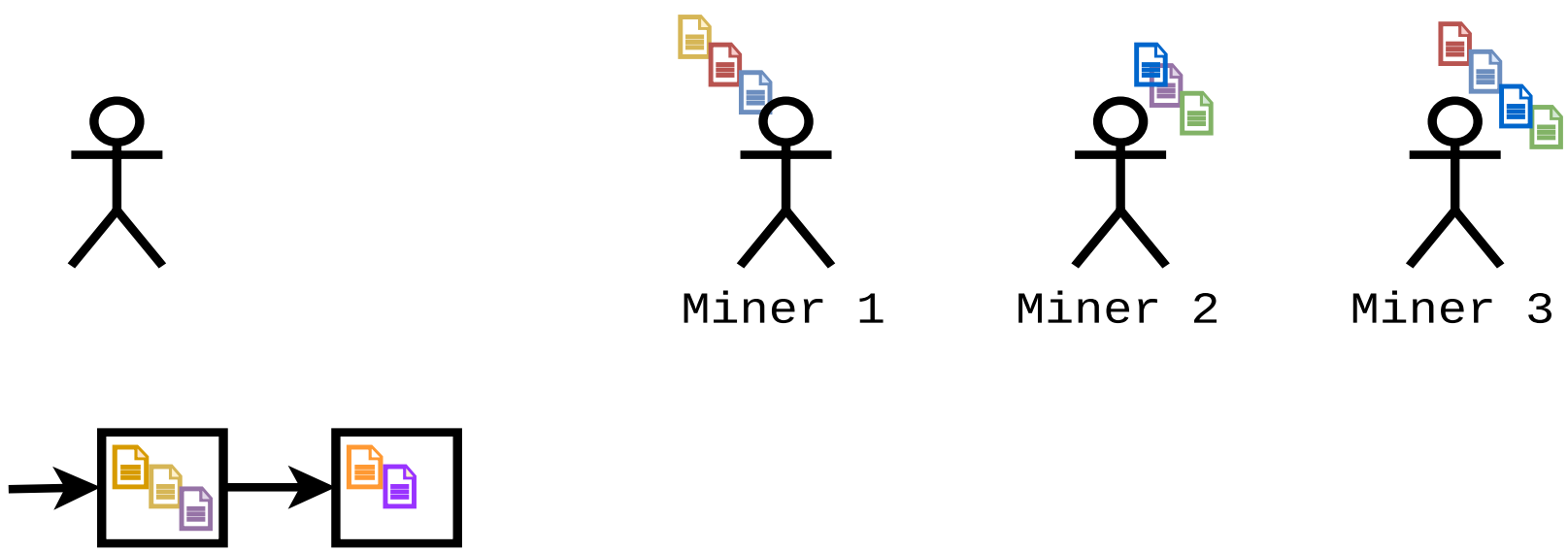
Blockchain: Funktionsweise



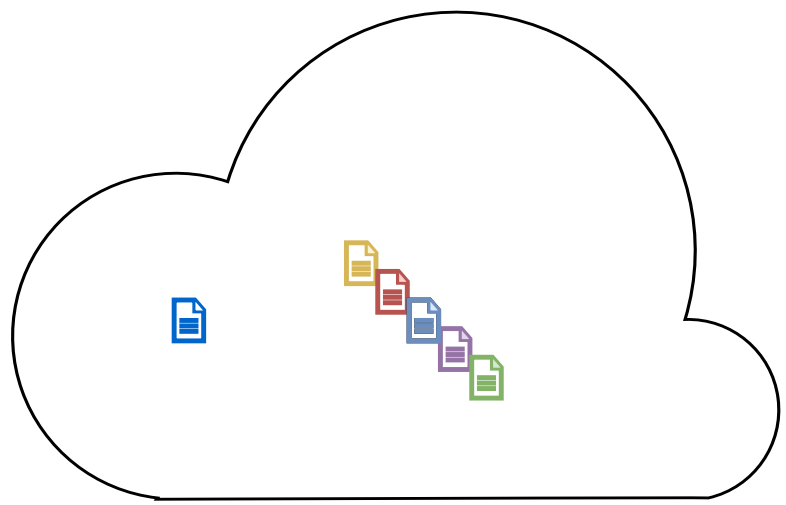


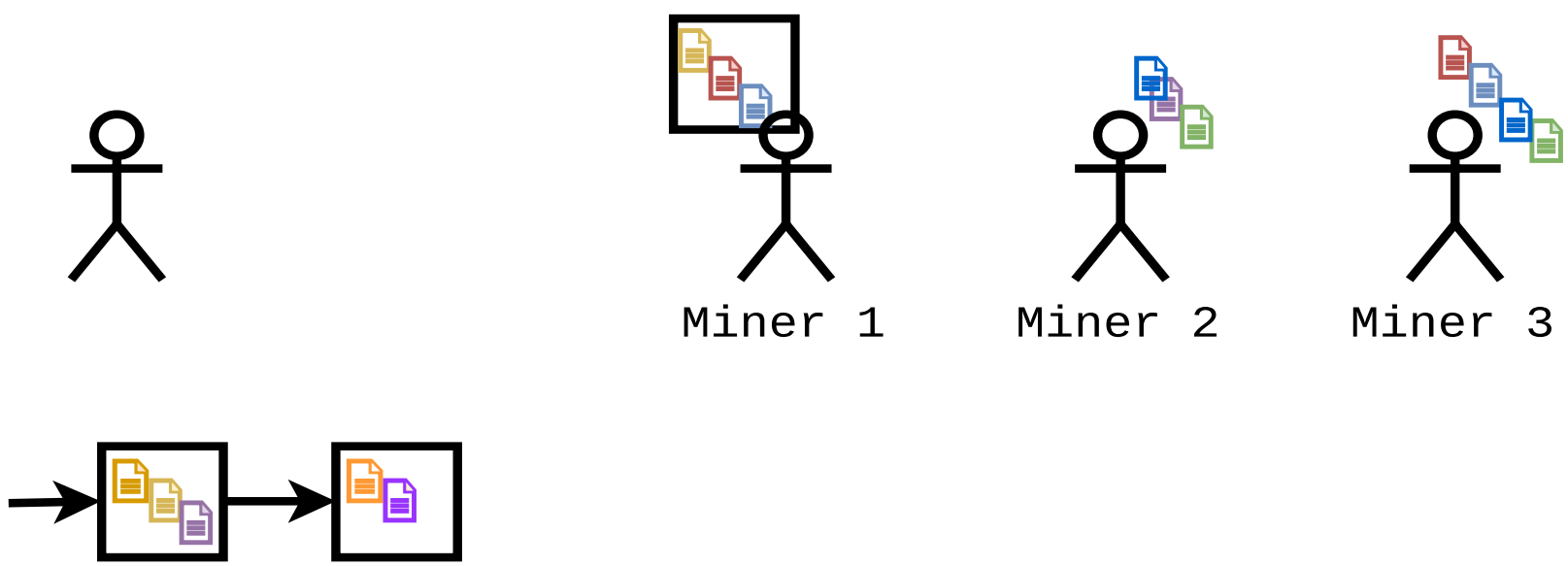
Blockchain: Funktionsweise



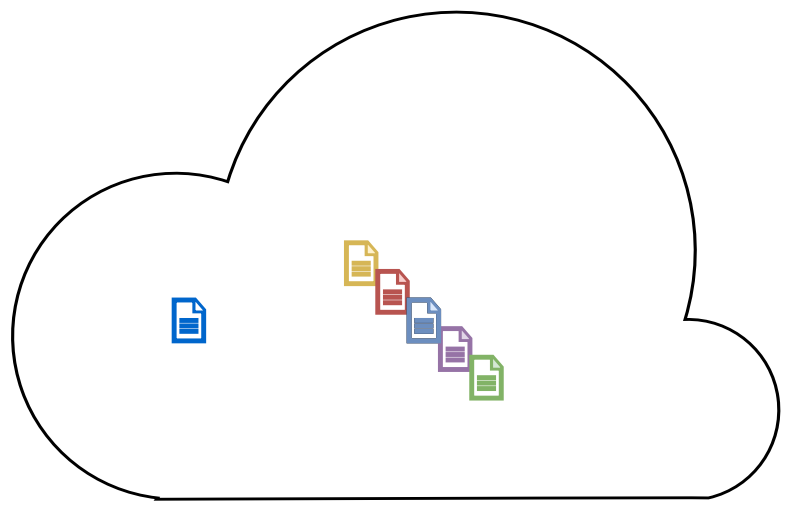


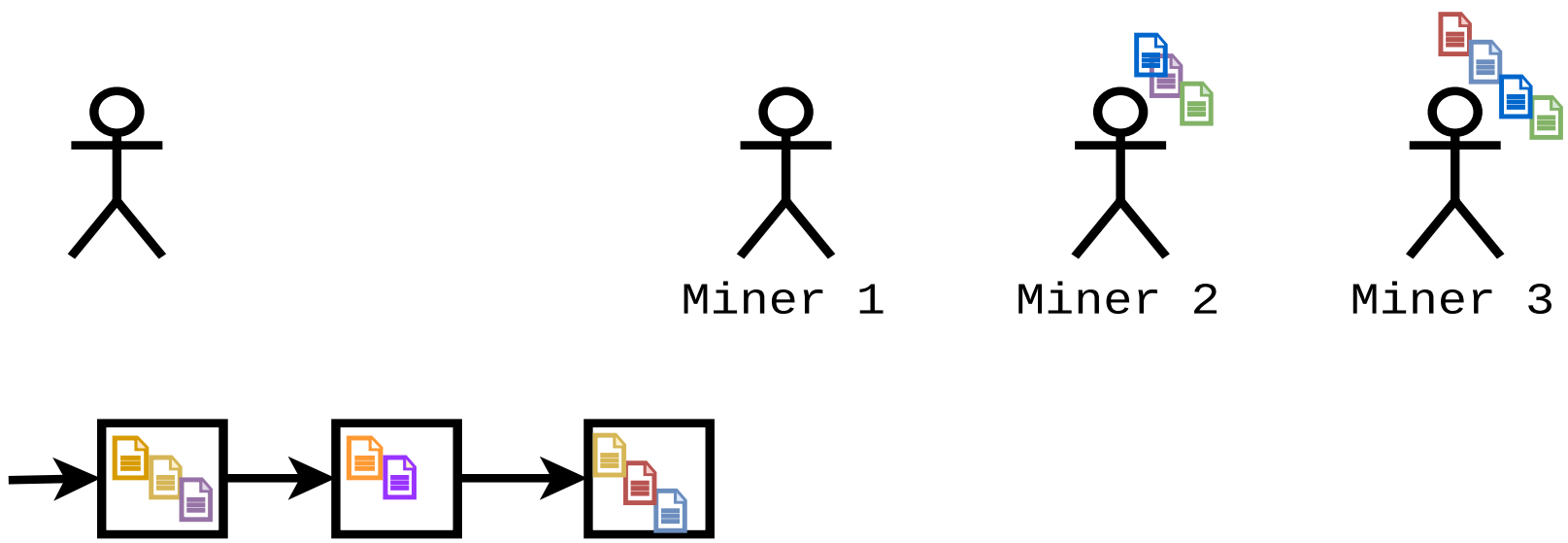
Blockchain: Funktionsweise



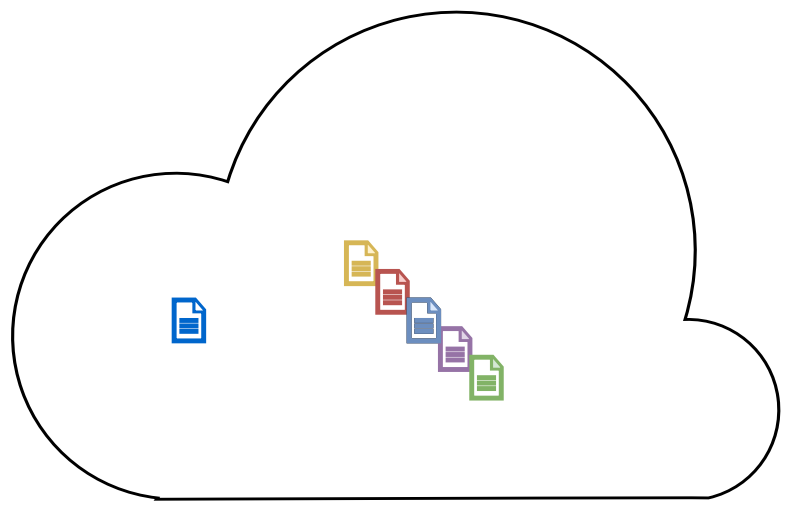


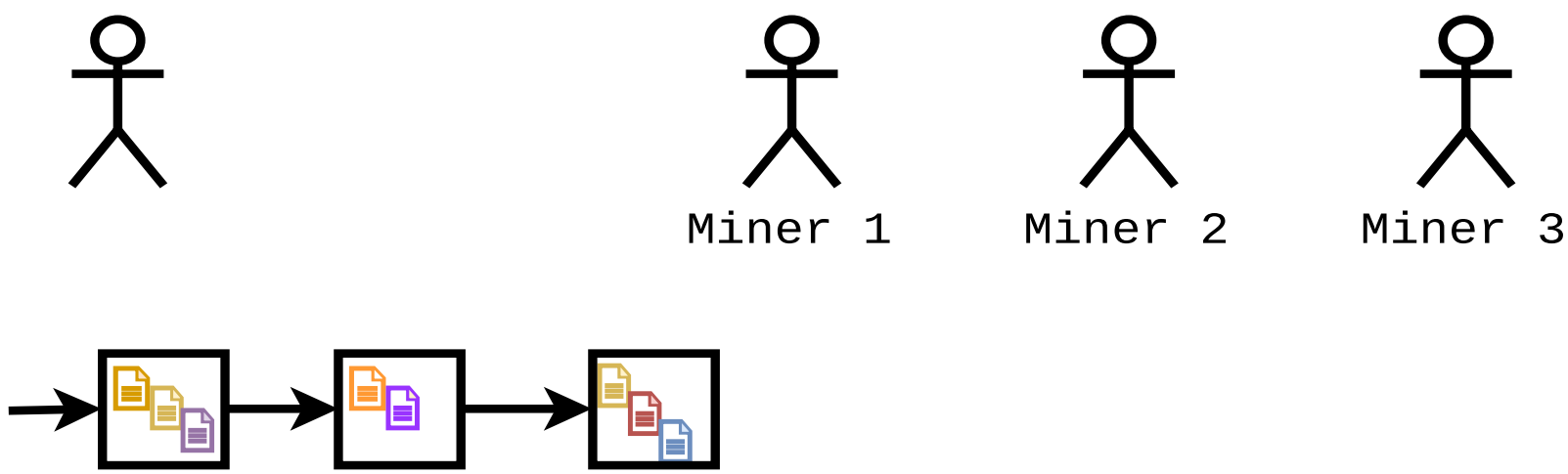
Blockchain: Funktionsweise



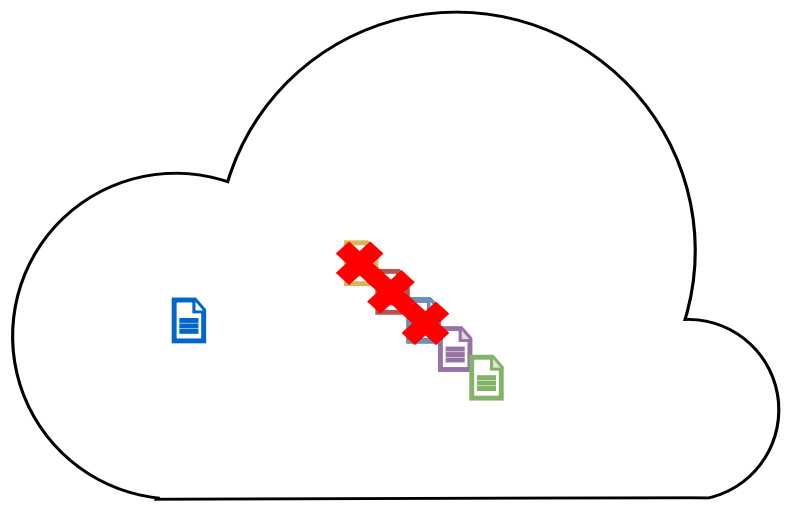


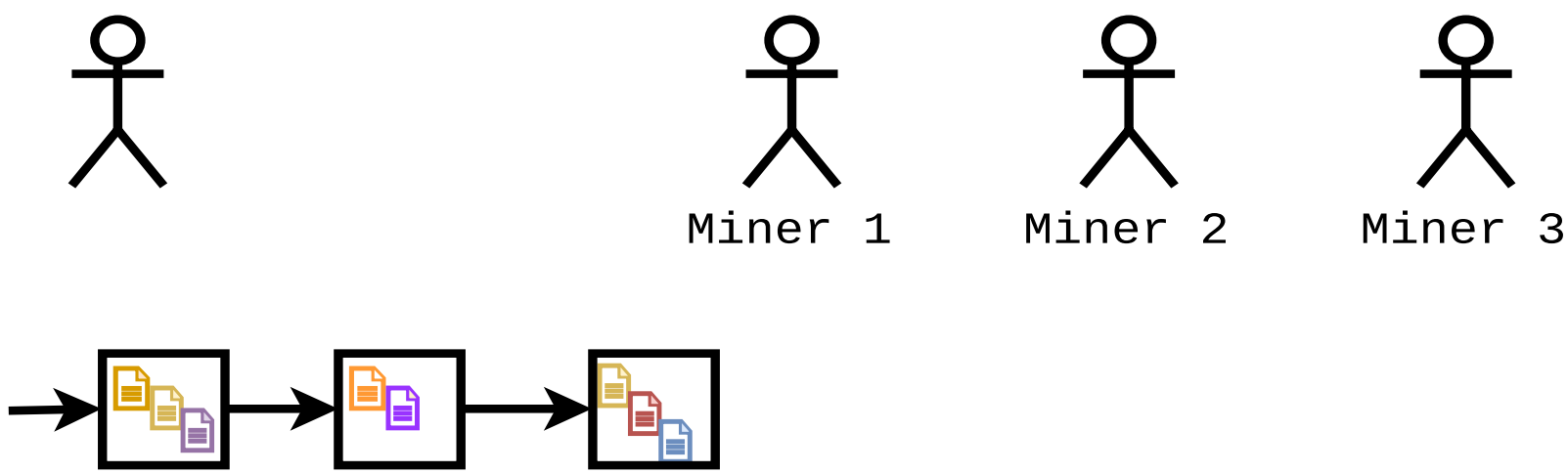
Blockchain: Funktionsweise



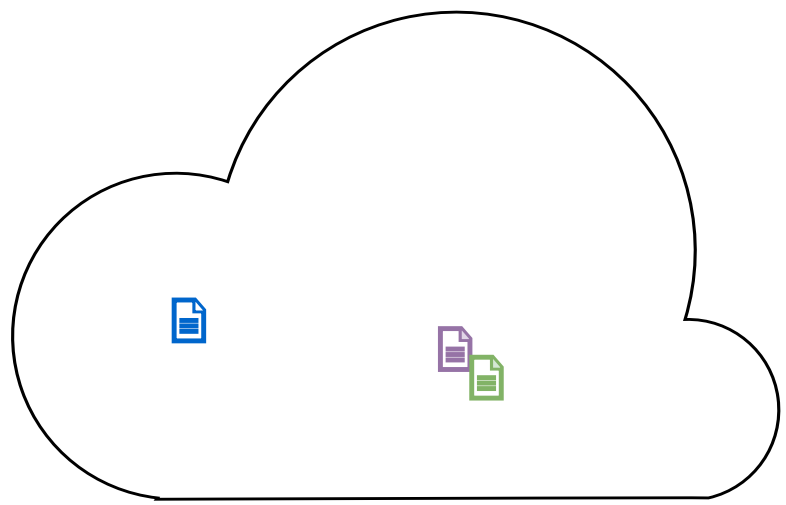


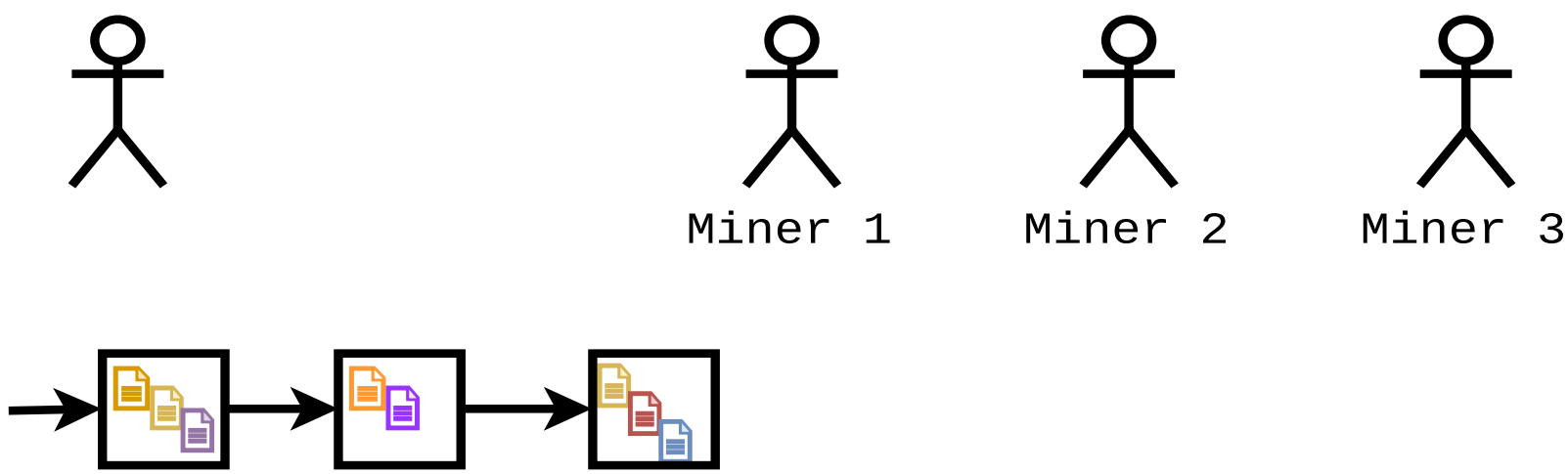
Blockchain: Funktionsweise



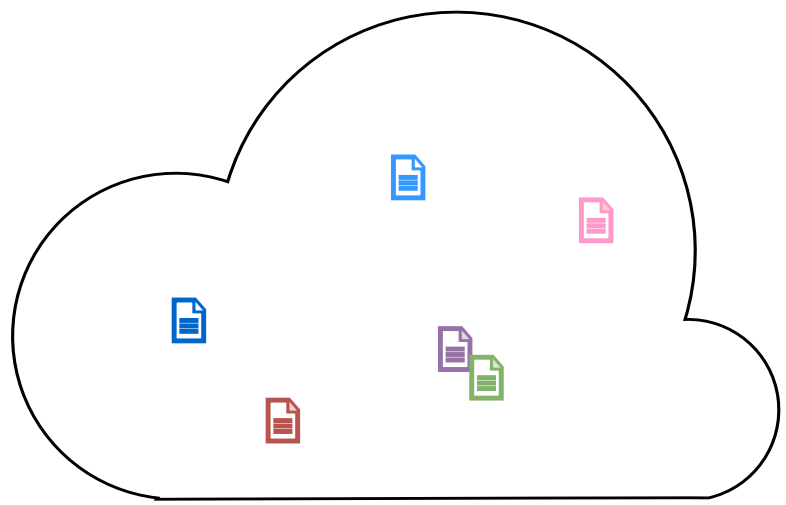


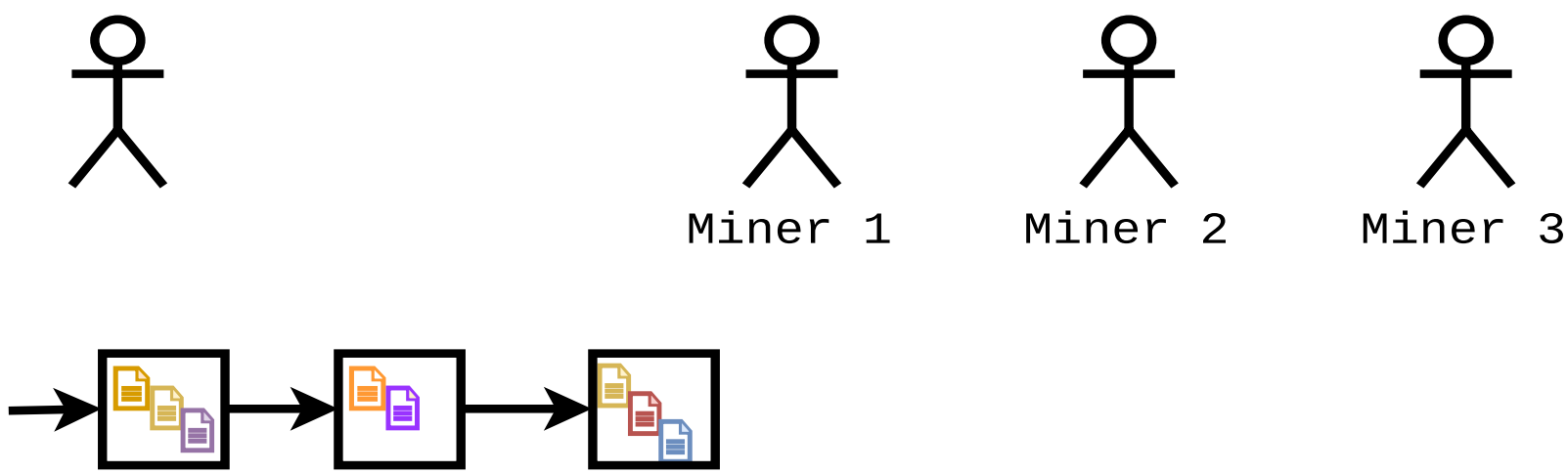
Blockchain: Funktionsweise



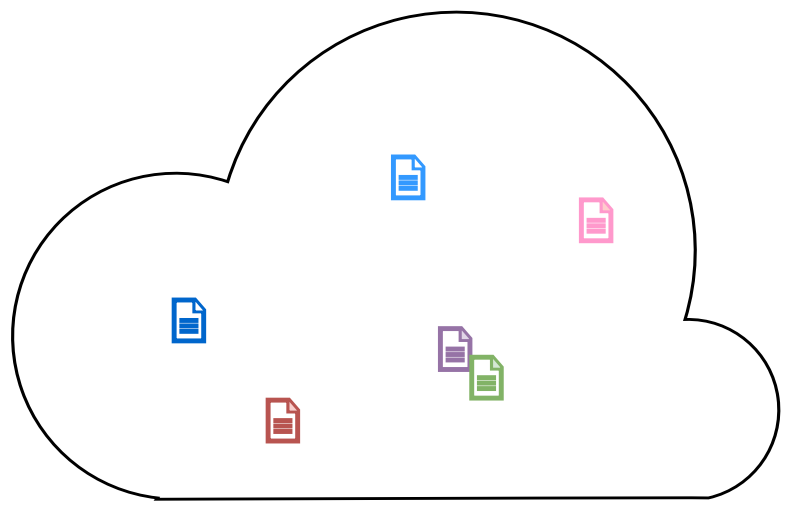


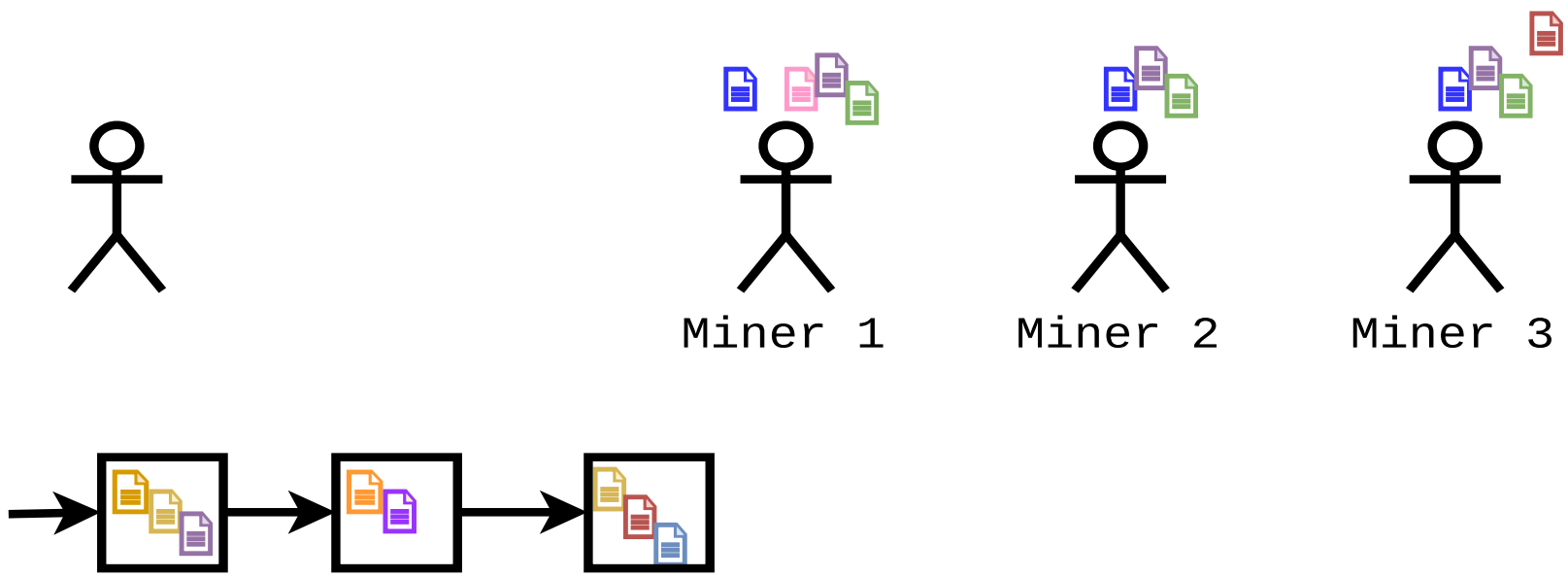
Blockchain: Funktionsweise



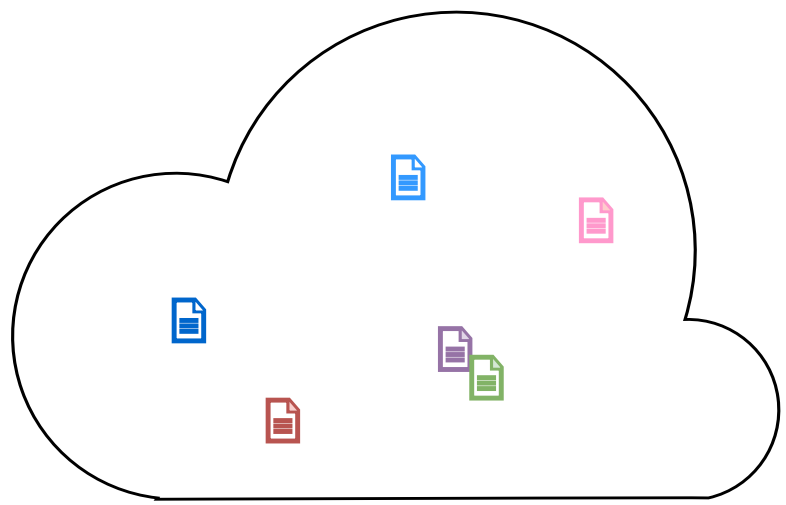


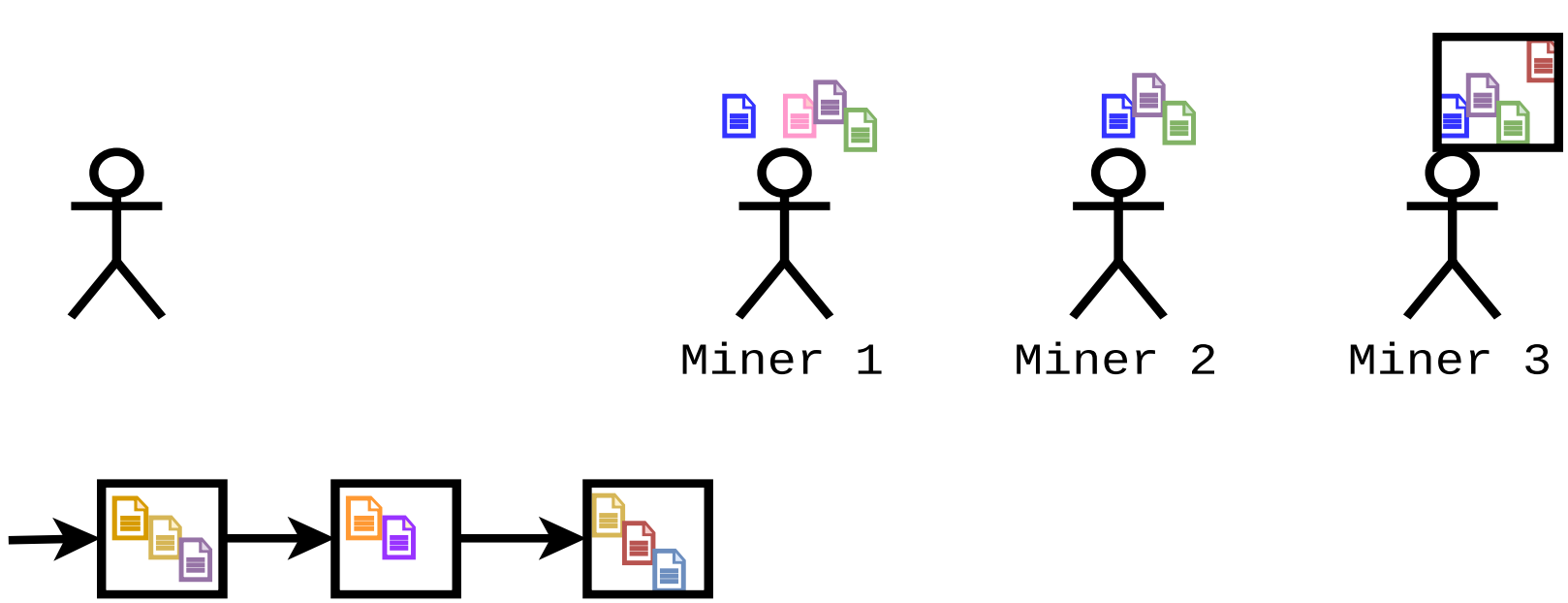
Blockchain: Funktionsweise



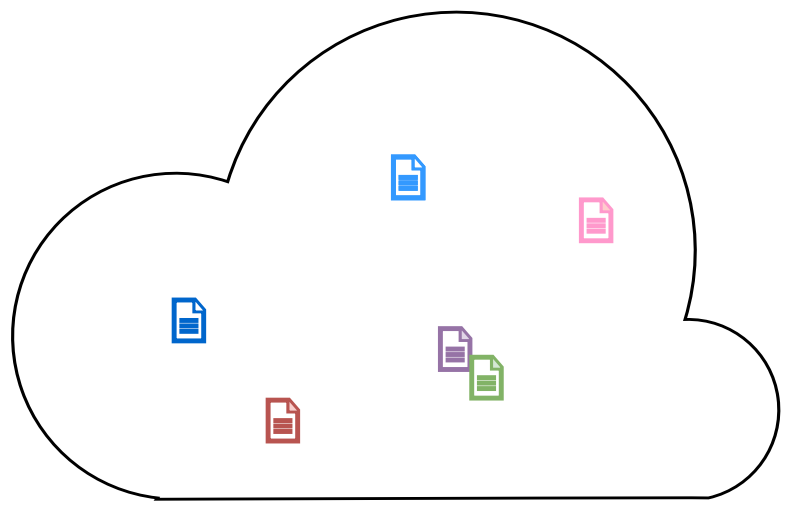


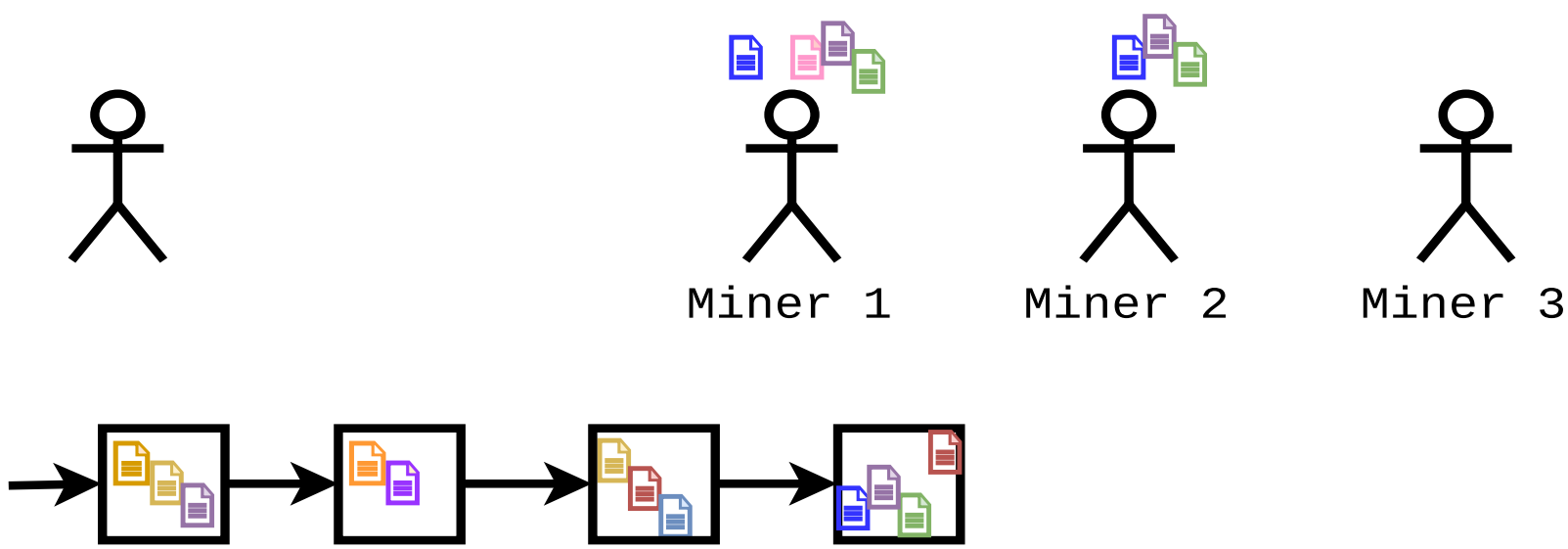
Blockchain: Funktionsweise



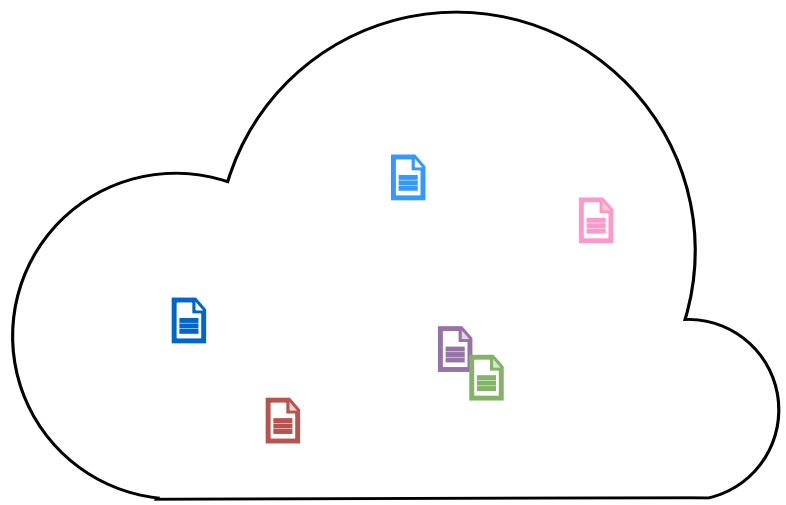


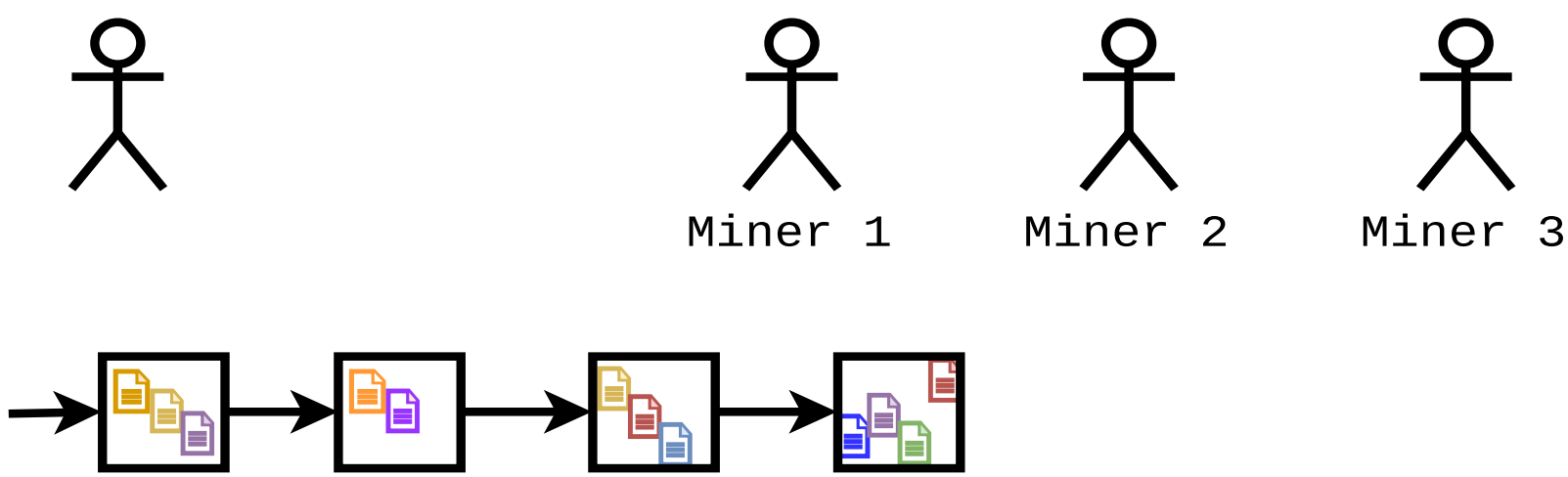
Blockchain: Funktionsweise



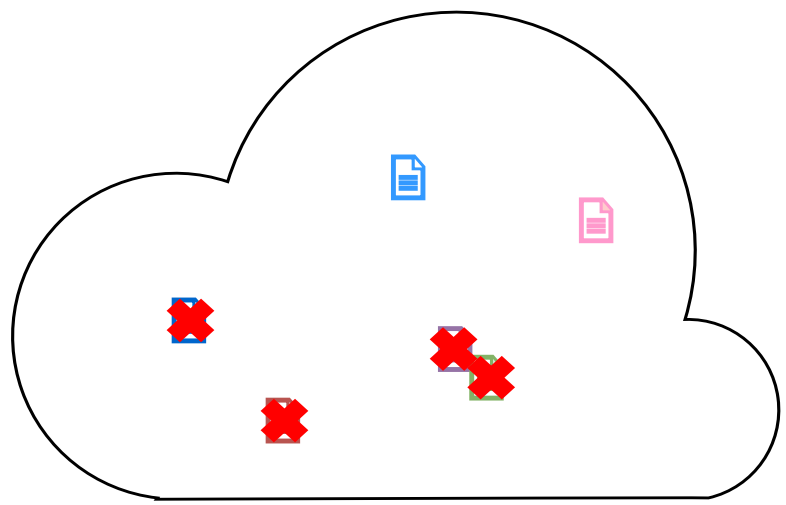


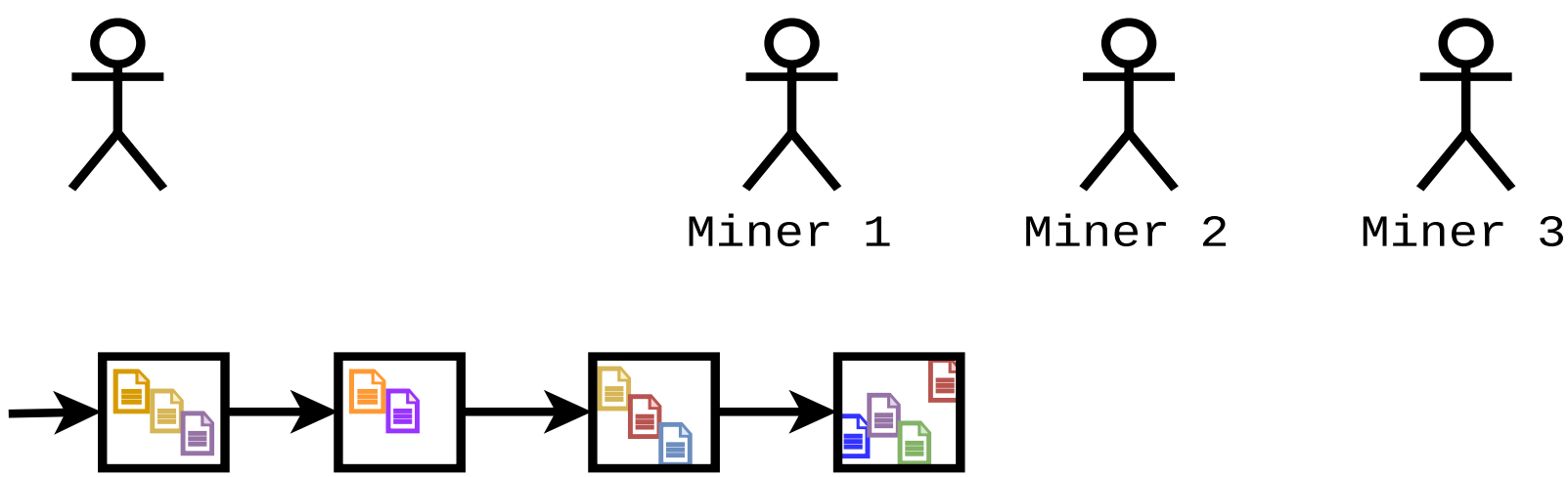
Blockchain: Funktionsweise



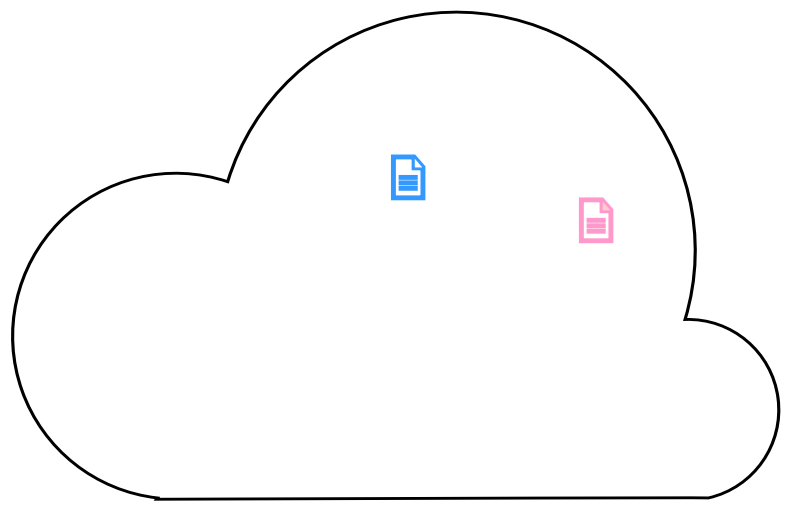


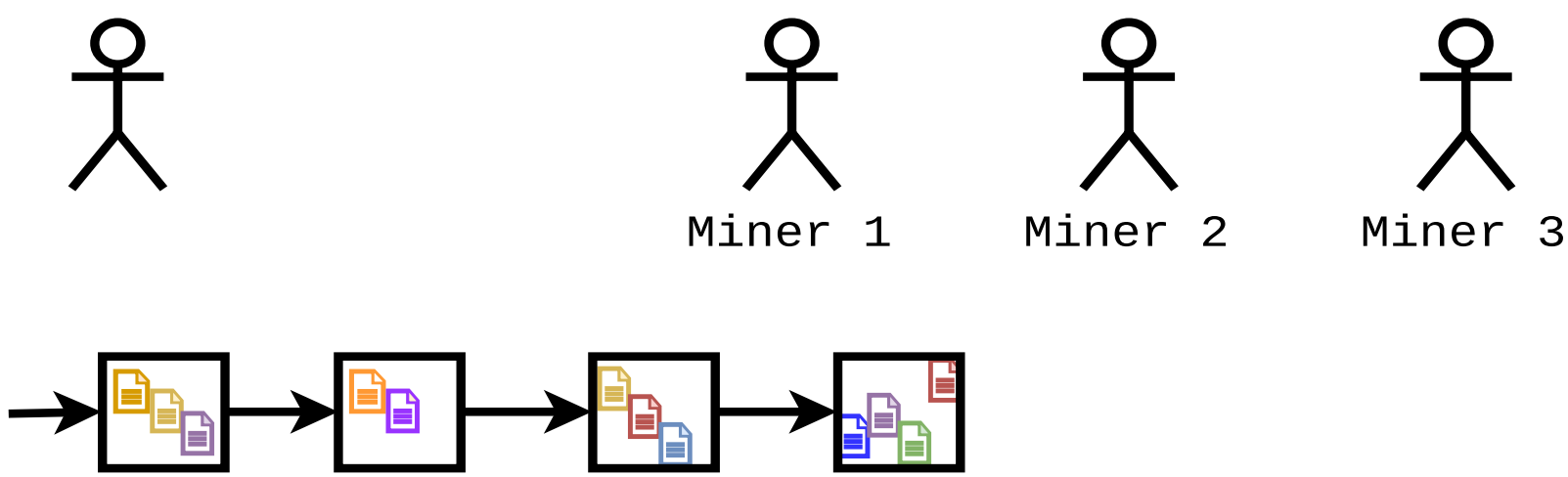
Blockchain: Funktionsweise





Blockchain: Funktionsweise

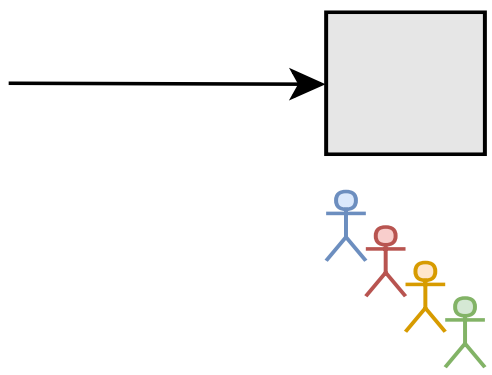




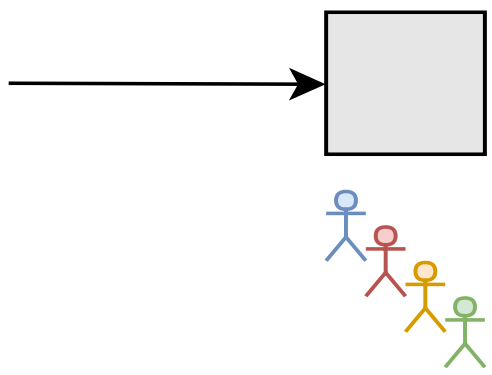
Double-Spending gelöst

- Der einzelne Miner kann Double-Spending verhindern:
  - nimmt nur gültige Transaktionen in den neuen Block
  - prüft jede Transaktion im neuen Block gegen die Blockchain
- Alle anderen Miner überprüfen dies auch
- Vollständige Induktion

Verzweigungen der Blockchain

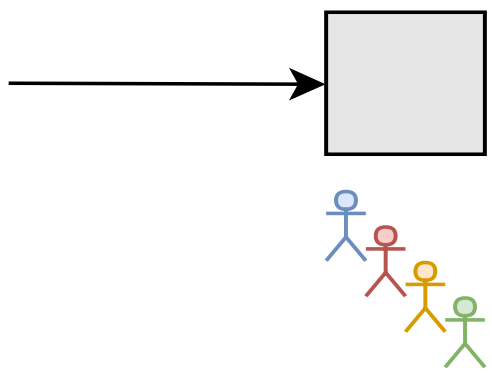


Verzweigungen der Blockchain



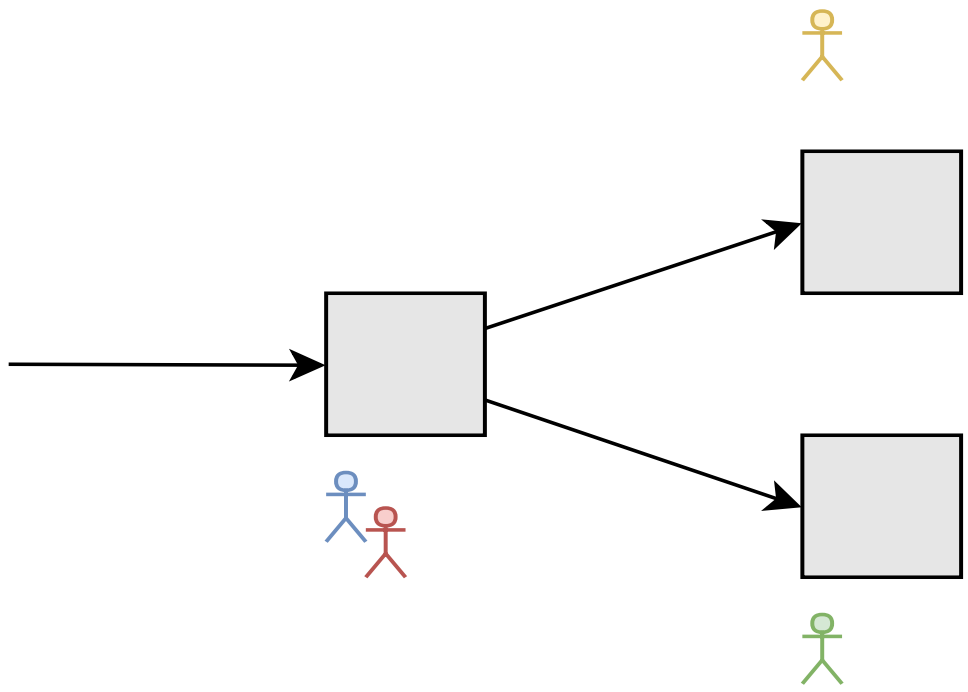
- Mehrere Miner finden zeitnah verschiedene Lösungen

Verzweigungen der Blockchain



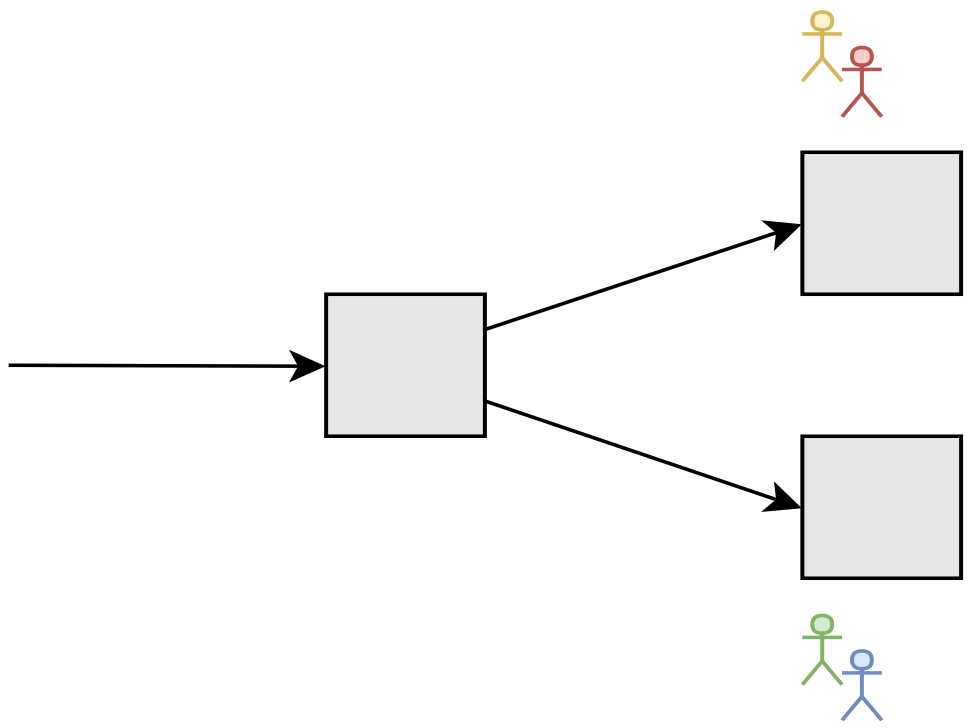
- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert

Verzweigungen der Blockchain



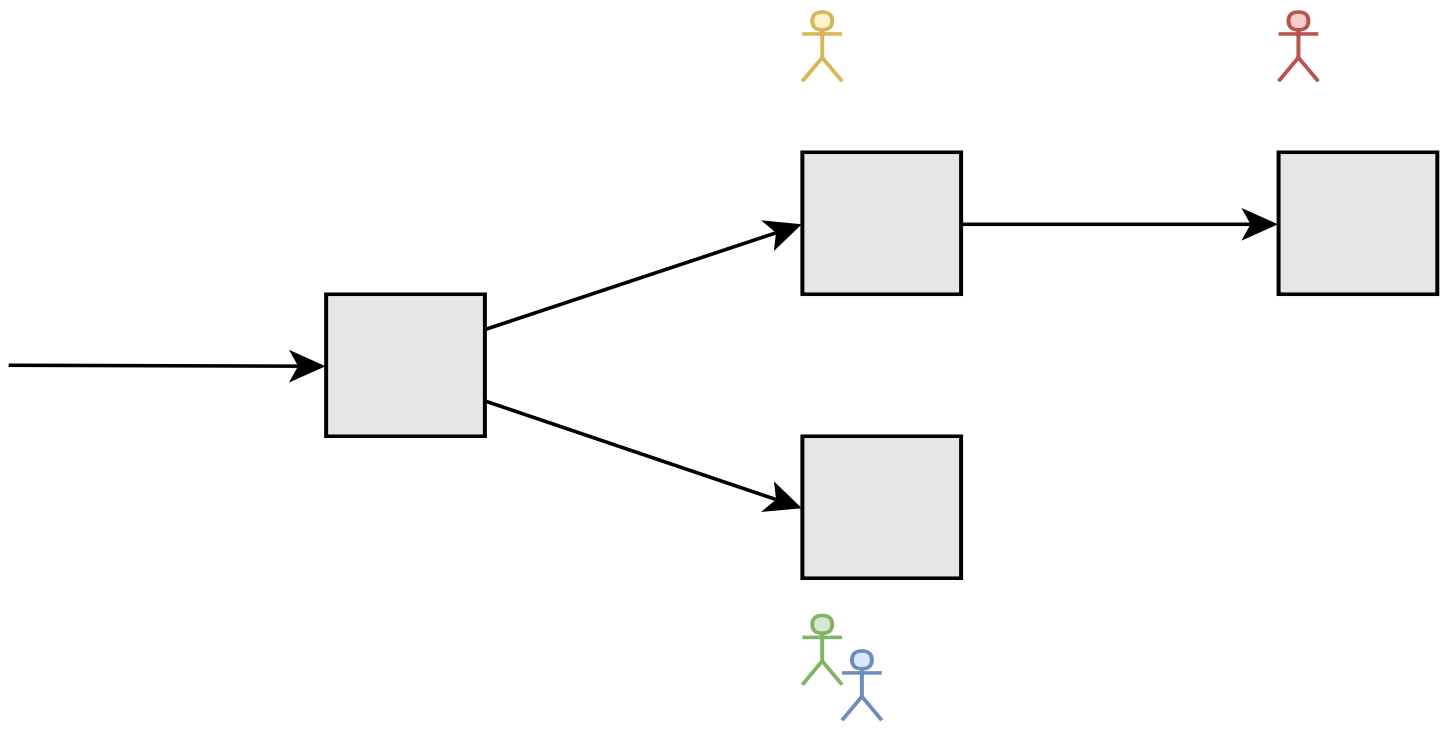
- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert

Verzweigungen der Blockchain



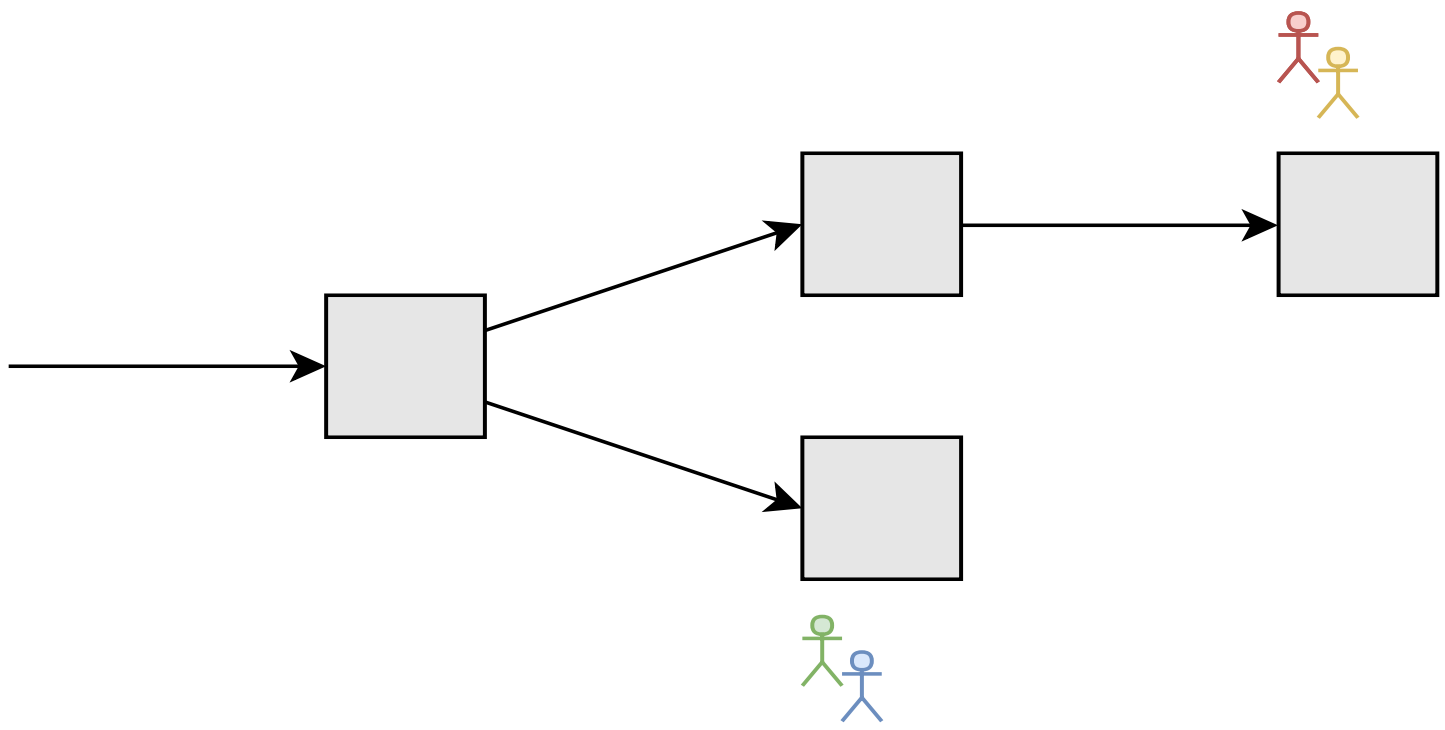
- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert

Verzweigungen der Blockchain



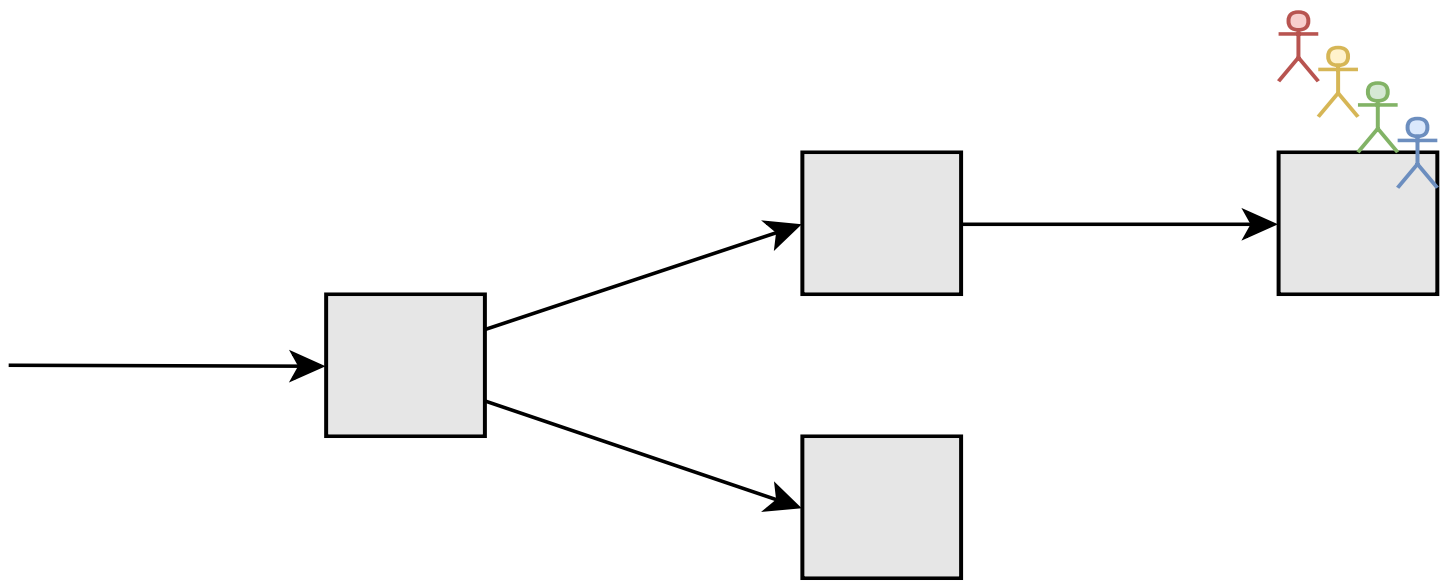
- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert

Verzweigungen der Blockchain



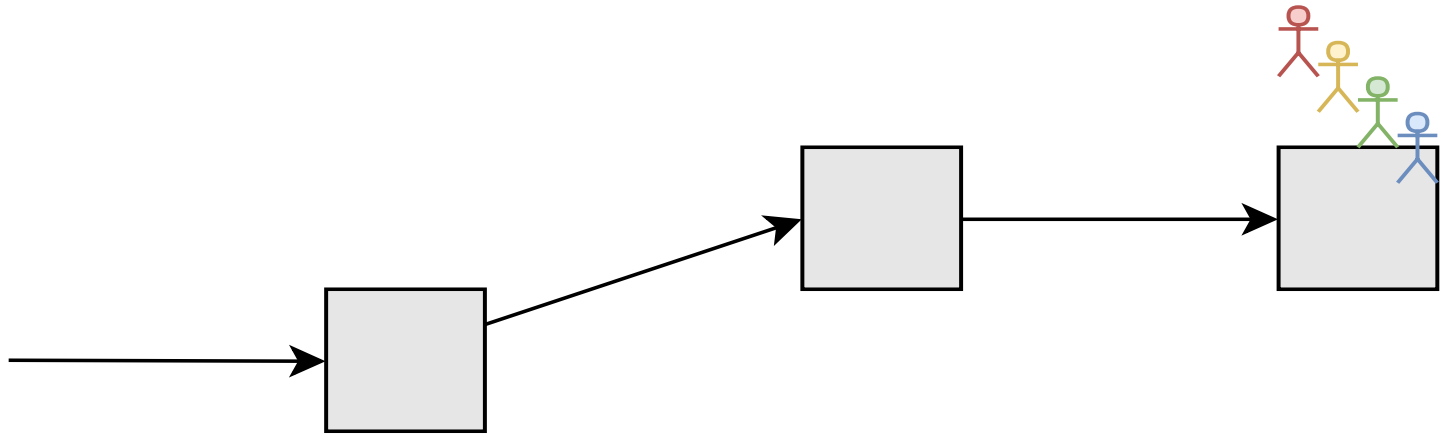
- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert

Verzweigungen der Blockchain



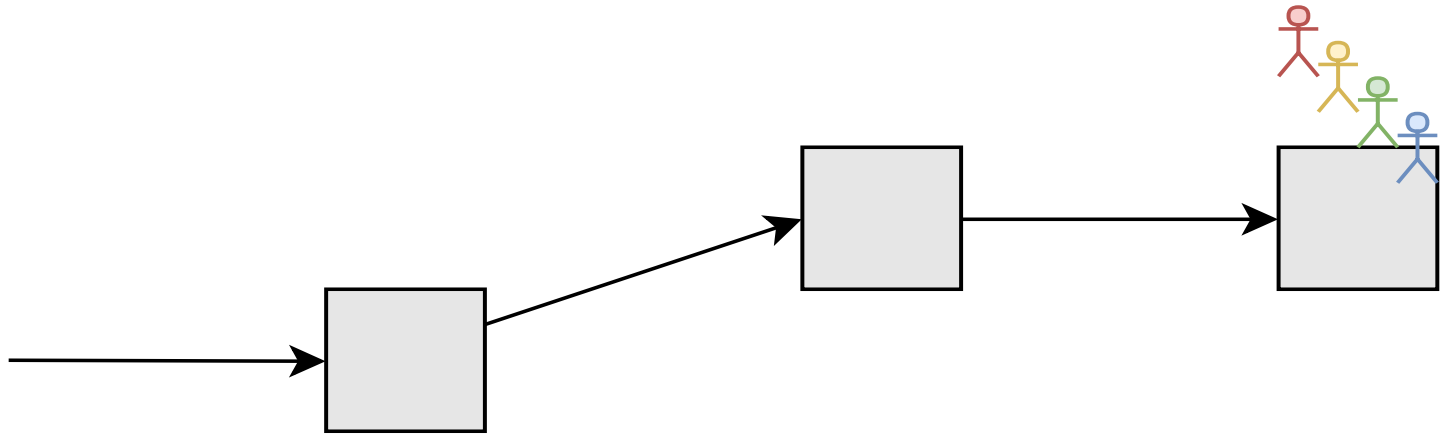
- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert

Verzweigungen der Blockchain



- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert

Verzweigungen der Blockchain



- Mehrere Miner finden zeitnah verschiedene Lösungen
- Zu jedem Zeitpunkt wird längste Kette als gültig definiert
- Wahrscheinlichkeit für gleichzeitige Funde muss gering sein.
- Innerhalb weniger Blöcke setzt sich dann ein Ast durch.

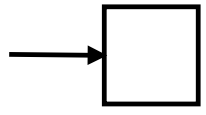
Mining mit Proof-of-Work

Mechanismus zur Beschränkung von Funden gültiger Blöcke:

- Alle Teilnehmer führen die Transaktionen lokal aus.
- Bestimmung, wessen Zustand tatsächlich ausgewählt wird:
  - Der neue Zustand ist mit einer Zahl zu versehen.
  - Diese ist nur sehr schwer zu finden.

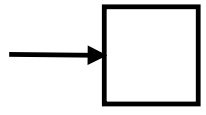
- Kryptographisches Hashing: nur Brute-Force-Suche möglich

Fork



Jetzt möchte man aber was ändern:

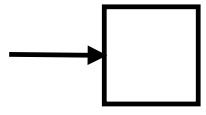
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.

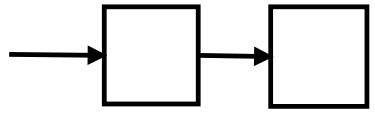
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.
- Es muss von einem gewissen Punkt weggeforkt werden.

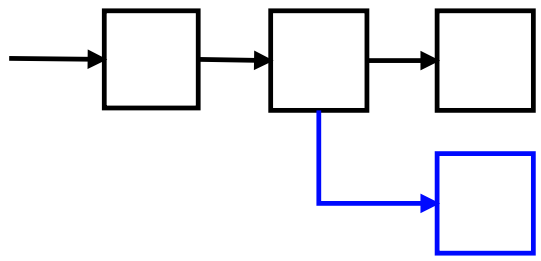
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.
- Es muss von einem gewissen Punkt weggeforkt werden.

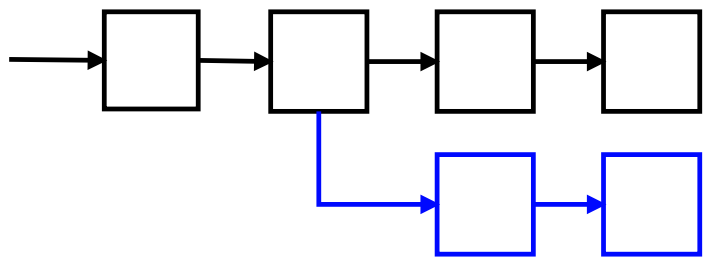
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.
- Es muss von einem gewissen Punkt weggeforkt werden.

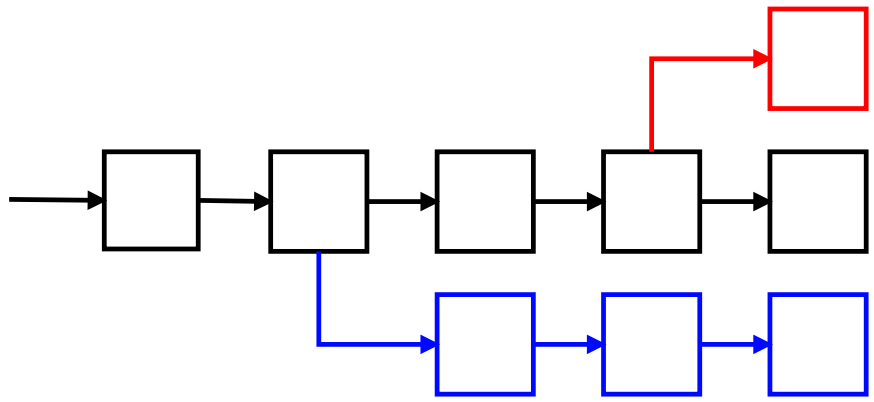
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.
- Es muss von einem gewissen Punkt weggeforkt werden.

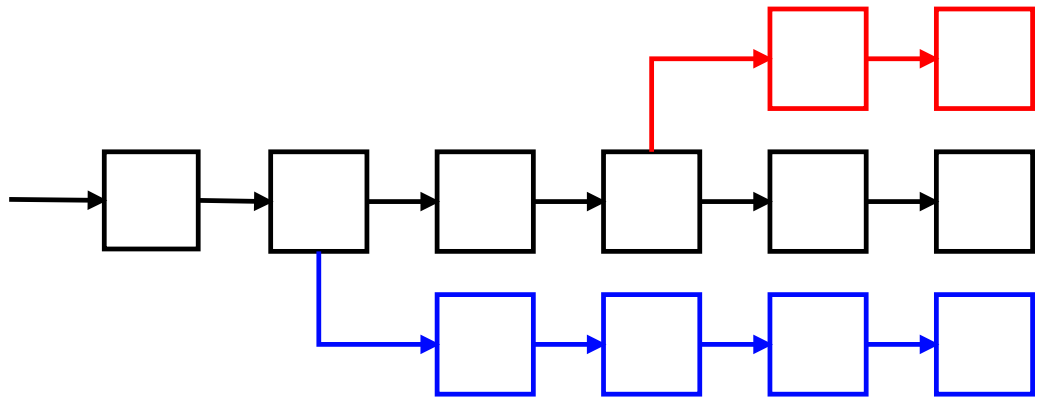
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.
- Es muss von einem gewissen Punkt weggeforkt werden.

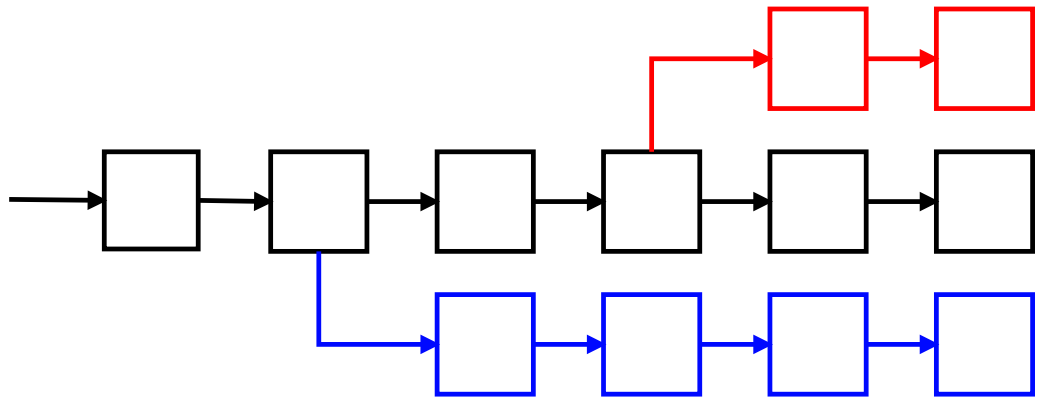
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.
- Es muss von einem gewissen Punkt weggeforkt werden.

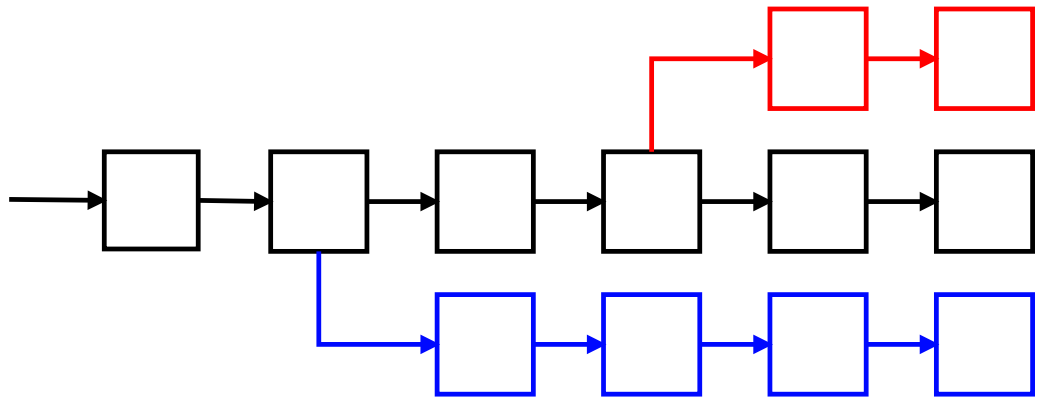
Fork



Jetzt möchte man aber was ändern:

- Das P2P-Netz kann nicht kontrolliert werden.
- Es muss von einem gewissen Punkt weggeforkt werden.
- Das P2P-Netz entscheidet, welche Stränge weiter exisitieren.

Fork



Beispiele:

- Bitcoin Cash: bei Block 478558, 1. August 2017
- Bitcoin Gold: bei Block 491407, 24. Oktober 2017

Übersicht

Geschichte
Vision
Grundlagen
Blockchain
Bitcoin
Entwicklung
Anwendungen

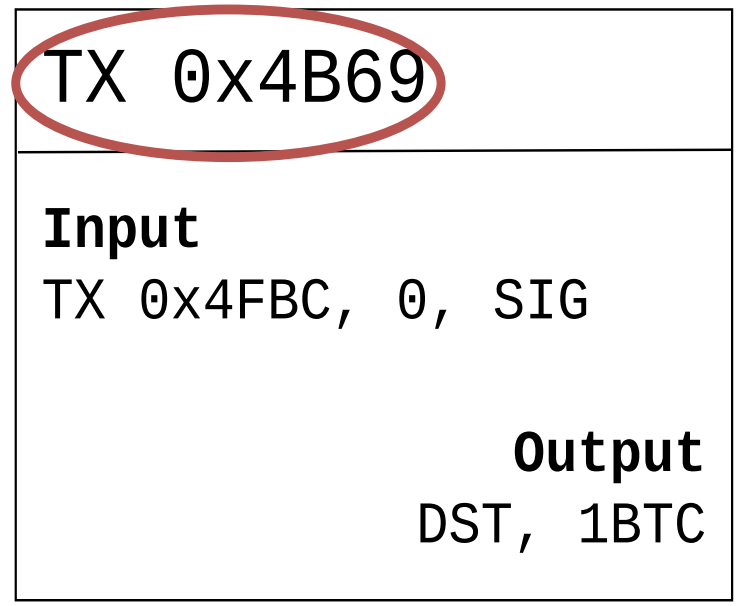
Bitcoin-Transaktion

TX 0x4B69

Input
TX 0x4FBC, 0, SIG

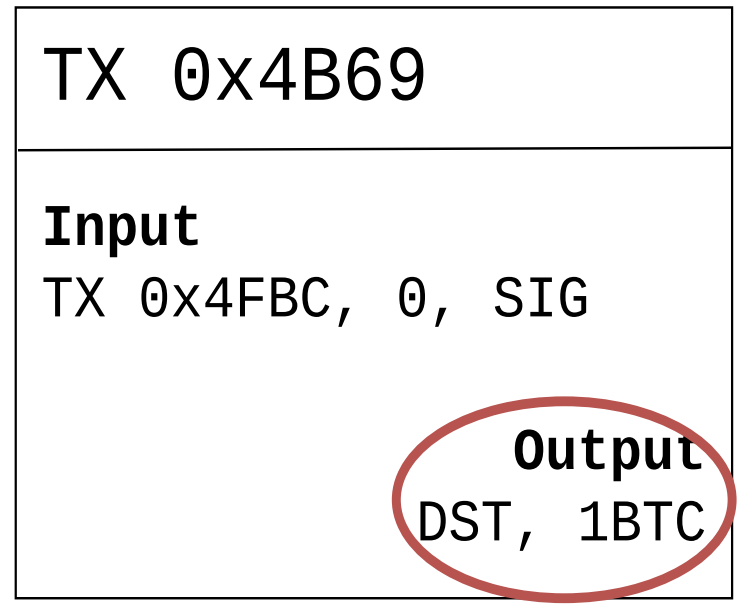
Output
DST, 1BTC

Bitcoin-Transaktion



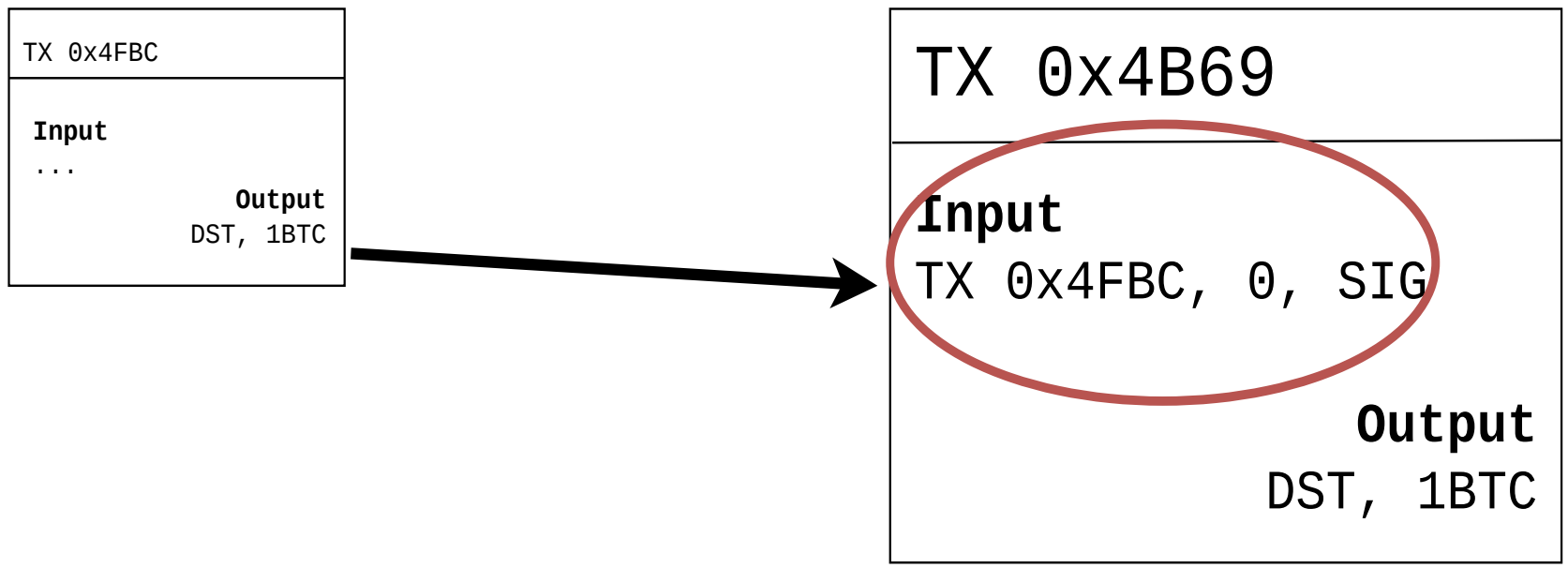
- Transaktionshash

Bitcoin-Transaktion



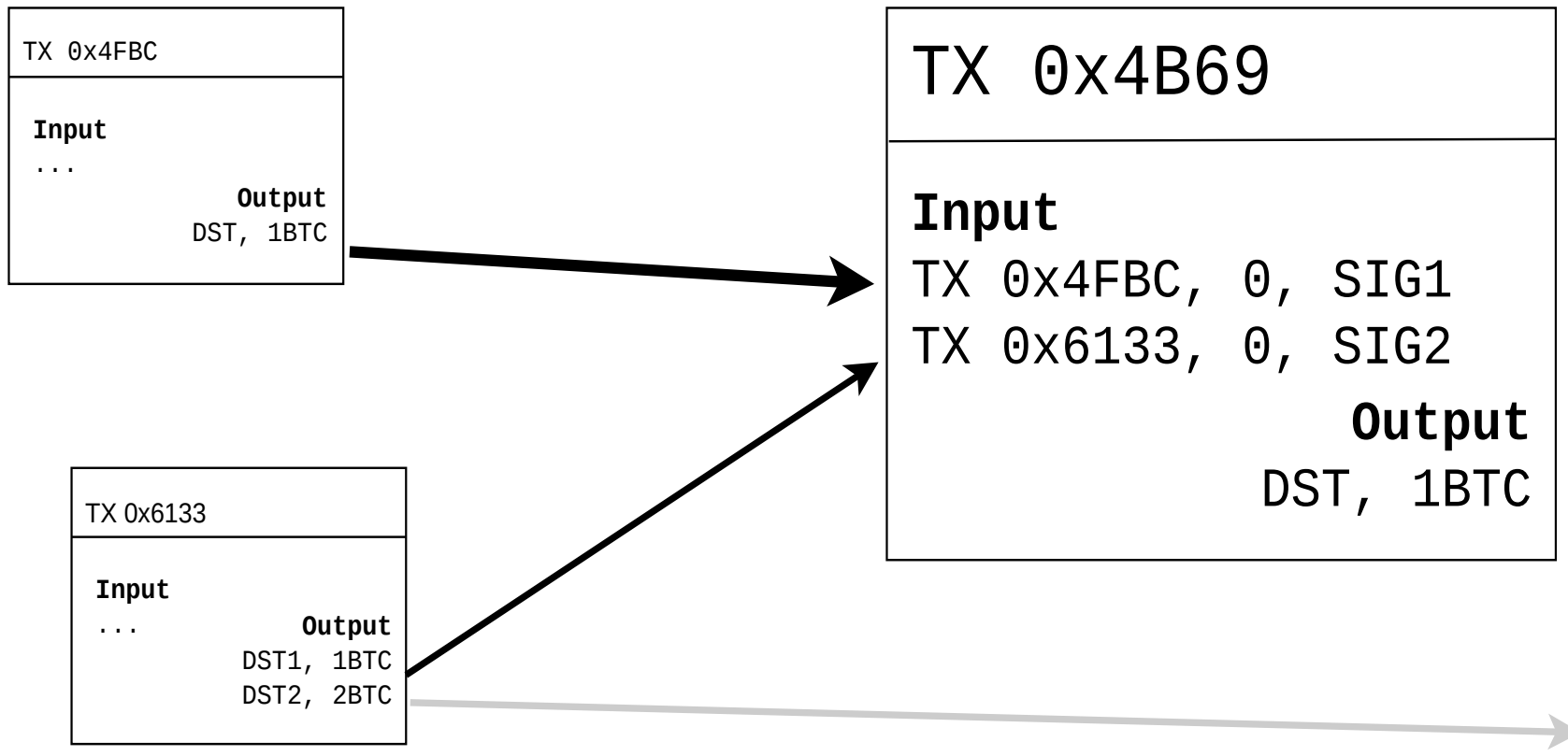
- Transaktionshash
- Output: Empfänger und Betrag

Bitcoin-Transaktion



- Transaktionshash
- Output: Empfänger und Betrag
- Input: Verweis auf Output, Nachweis der Legitimation des Verwenders

Bitcoin-Transaktion



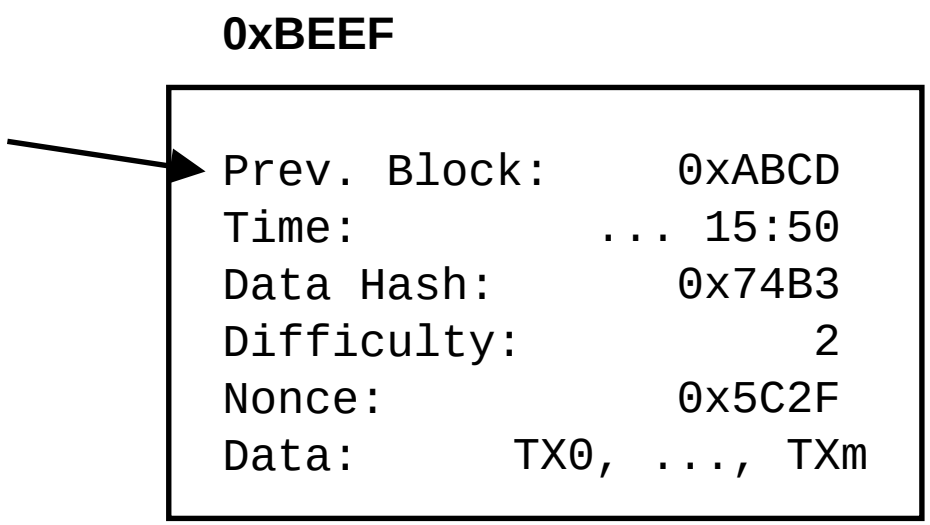
- Mehrere Eingaben und Ausgaben in einer Transaktion möglich
- Nachweis der Legitimität der Verwendung eines Outputs

Legitimität

- Output
  - Hash eines Public-Key
- Input
  - Referenz auf bisher nicht referenzierten Output
    - Damit Referenz auf Hash eines Public-Keys
  - Mit zugehörigem Public-Key
  - Signatur der Transaktion

- So wird gleichzeitig der Besitz des Outputs sowie die Echtheit der Transaktion nachgewiesen

Bitcoin-Mining



Bitcoin-Mining

0xBEEF

```
Prev. Block:     0xABCD
Time:         ... 15:50
Data Hash:       0x74B3
Difficulty:           2
Nonce:            0x5C2F
Data:      TX0, ..., TXm
```

0x1234

```
Prev. Block:     0xBEEF
Time:         ... 15:59
Data Hash:       0xC0DE
Difficulty:           2
Nonce:            ??????
Data:      TX0, ..., TXn
```

Bitcoin-Mining

0xBEEF

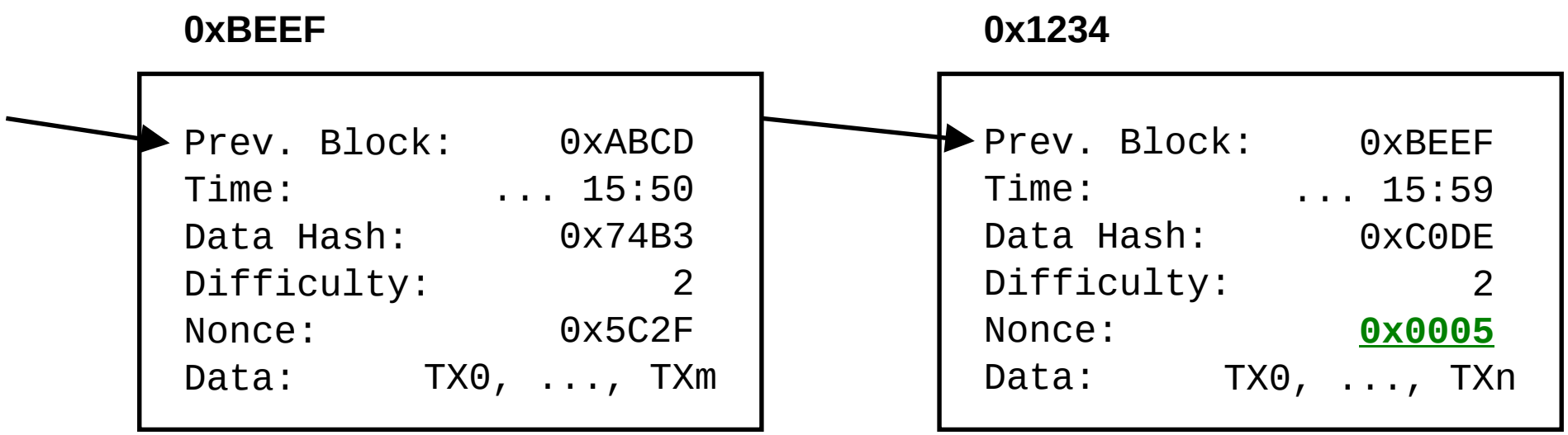
```
Prev. Block:      0xABCD
Time:          ... 15:50
Data Hash:        0x74B3
Difficulty:            2
Nonce:             0x5C2F
Data:       TX0, ..., TXm
```

0x1234

```
Prev. Block:      0xBEEF
Time:          ... 15:59
Data Hash:        0xC0DE
Difficulty:            2
Nonce:             ??????
Data:       TX0, ..., TXn
```

- hash(Block_{0x0000}) = 0x8F4B99...
- hash(Block_{0x0001}) = 0x037268...
- hash(Block_{0x0002}) = 0xA3FC56...
- hash(Block_{0x0003}) = 0xFBBADE...
- hash(Block_{0x0004}) = 0x223485...
- **hash(Block_{0x0005}) = 0x00FA33...**

Bitcoin-Mining



- hash(Block_{0x0000}) = 0x8F4B99...
- hash(Block_{0x0001}) = 0x037268...
- hash(Block_{0x0002}) = 0xA3FC56...
- hash(Block_{0x0003}) = 0xFBBADE...
- hash(Block_{0x0004}) = 0x223485...
- **hash(Block_{0x0005}) = 0x00FA33...**

Difficulty

- Selbstregulierung der Blockchain
- Alle 2016 Blöcke wird der Schwierigkeitsgrad neu berechnet
- Kann sowohl steigen als auch fallen
- Je schwerer, desto mehr führende Nullen im Hash
- Aktuell sind 70 führende Nullen im Hash nötig
- 7 Transaktionen pro Sekunde

Schöpfung von Bitcoins

- Belohnung am Anfang 50 BTC pro Block
  - Halbierung alle 210.000 Blöcke
  - Aktuell ist die Blockchain bei Block ~523.000
  - Belohnung aktuell 12.5 BTC pro Block
  - Bei Block 630.000 wird die Belohnung auf 6.25 BTC halbiert
  - Belohnung fällt bis ~2130 auf 0

Gebühren

- Anreiz für Miner, eine Transaktion in ihren Block aufzunehmen
- Steuerung durch Differenz von Inputs und Outputs

Wallet

- In der Wallet werden die eigenen Schlüssel gespeichert.
- Das eigene Vermögen entspricht also der Menge der mit den eigenen Schlüsseln lösbaren, noch nicht ausgegebenen Outputs.


TREZOR
Confirm sending
0.0469 BTC
to
1Nuu2753n7h32nCQJ
CT2HVKTFfQjhpXhcw
Cancel
Confirm

Load & Verify

Bitcoin Address

1DFevETMVpNTynxD9gBsKziVyFfCB2opzf

bitcoin bitcoin bitcoin bitcoin bitcoin bitcoin bitcoin bitcoin bit

bitcoin

Amount:

Private Key

KwusAKEHPJBQZBvLaNYVVvfaG2Nb5t9F4DuUMU6BNGXGXmXB8fnJ

Spend

Übersicht

Geschichte

Vision

Grundlagen

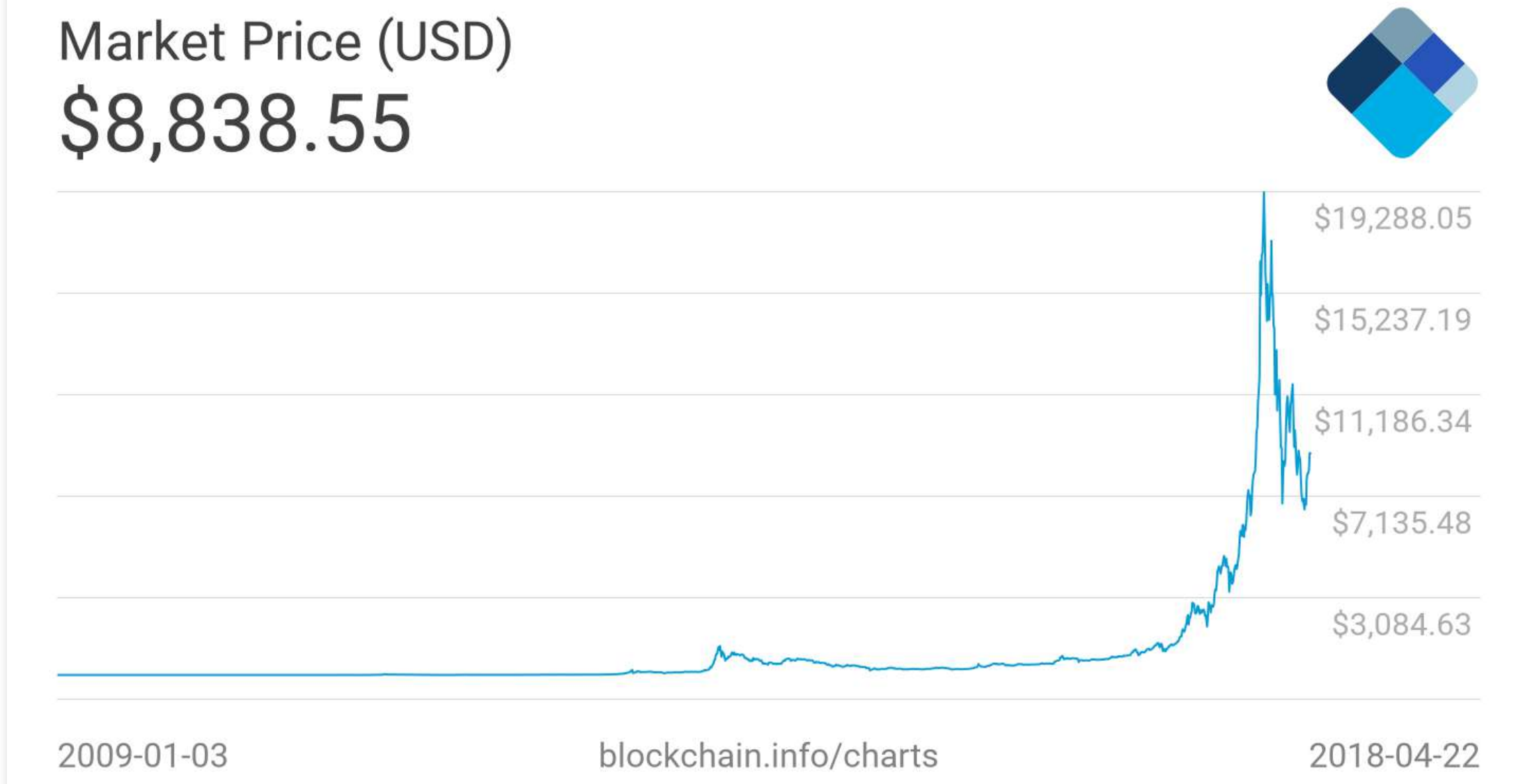
Blockchain

Bitcoin

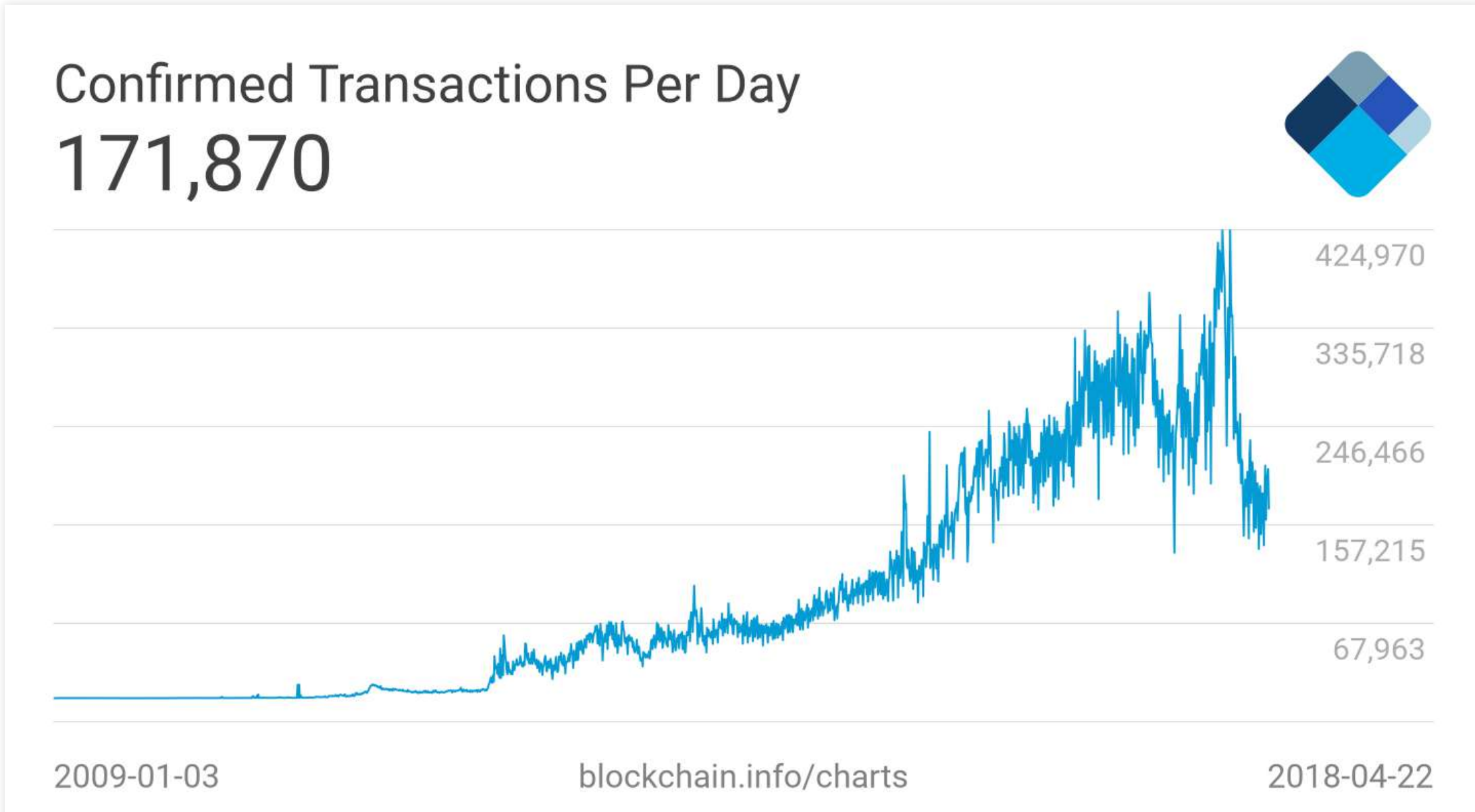
Entwicklung

Anwendungen

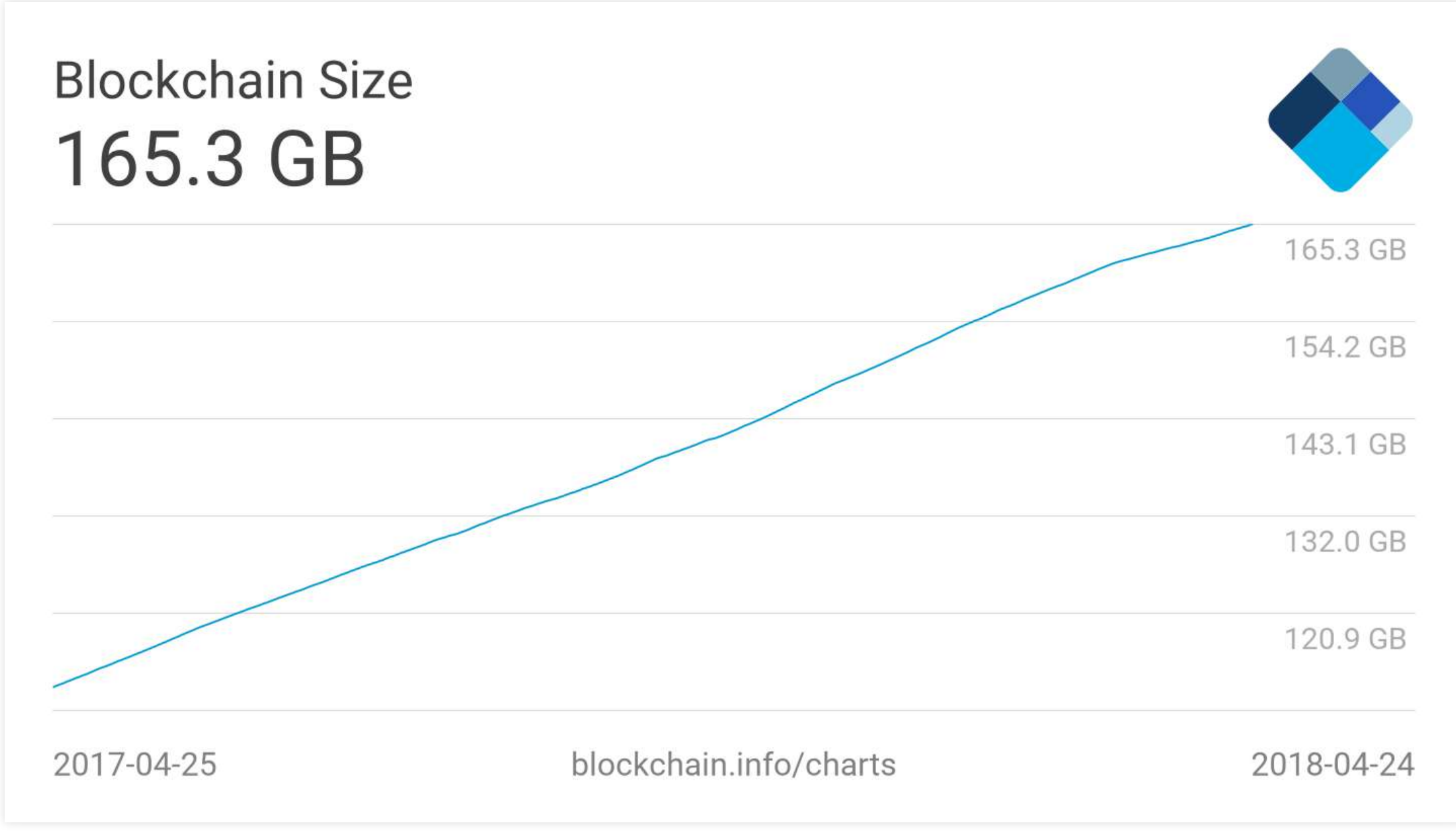
Kurs


Market Price (USD)
$8,838.55
$19,288.05
$15,237.19
$11,186.34
$7,135.48
$3,084.63
2009-01-03
blockchain.info/charts
2018-04-22

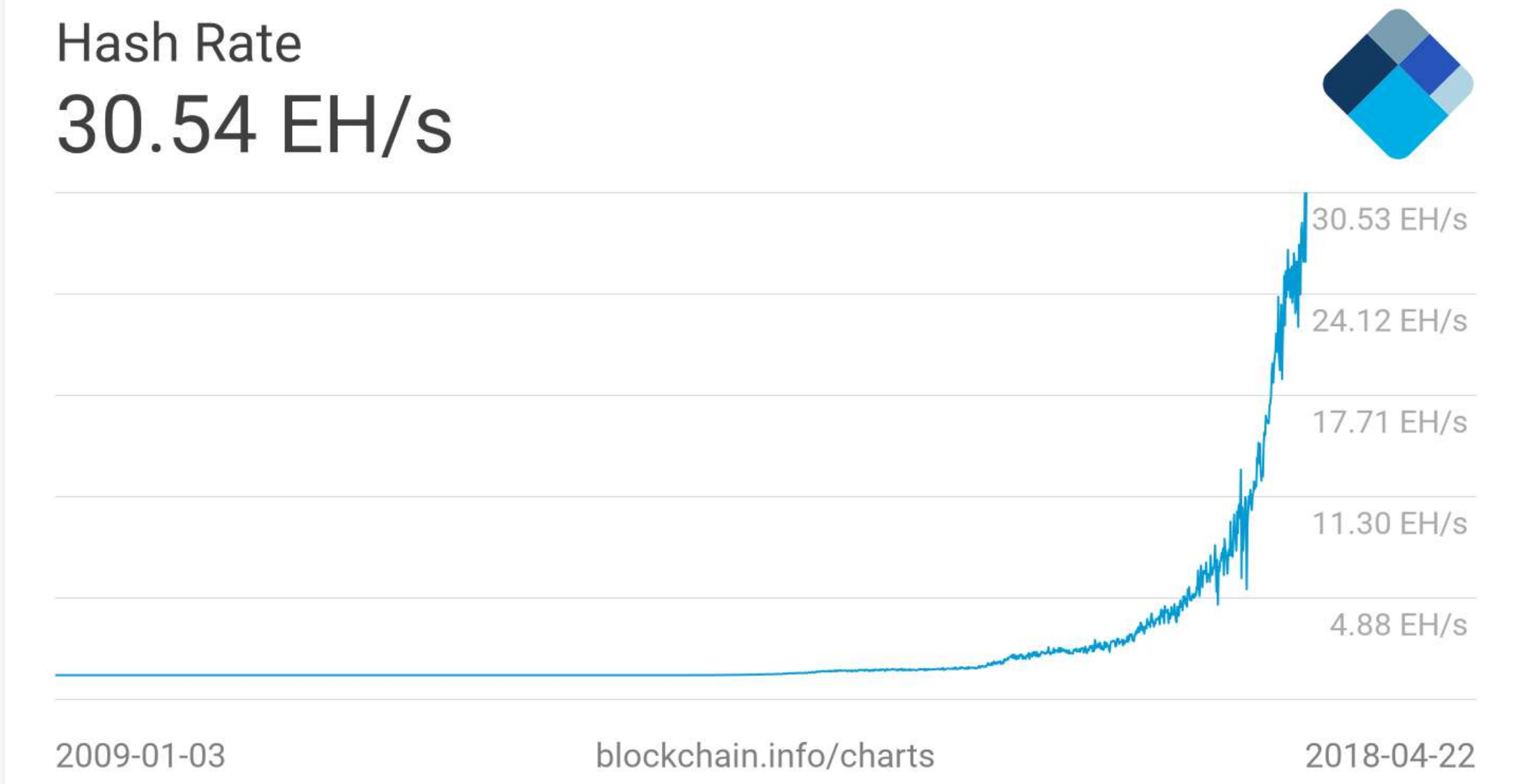
Transaktionen



Größe der Blockchain



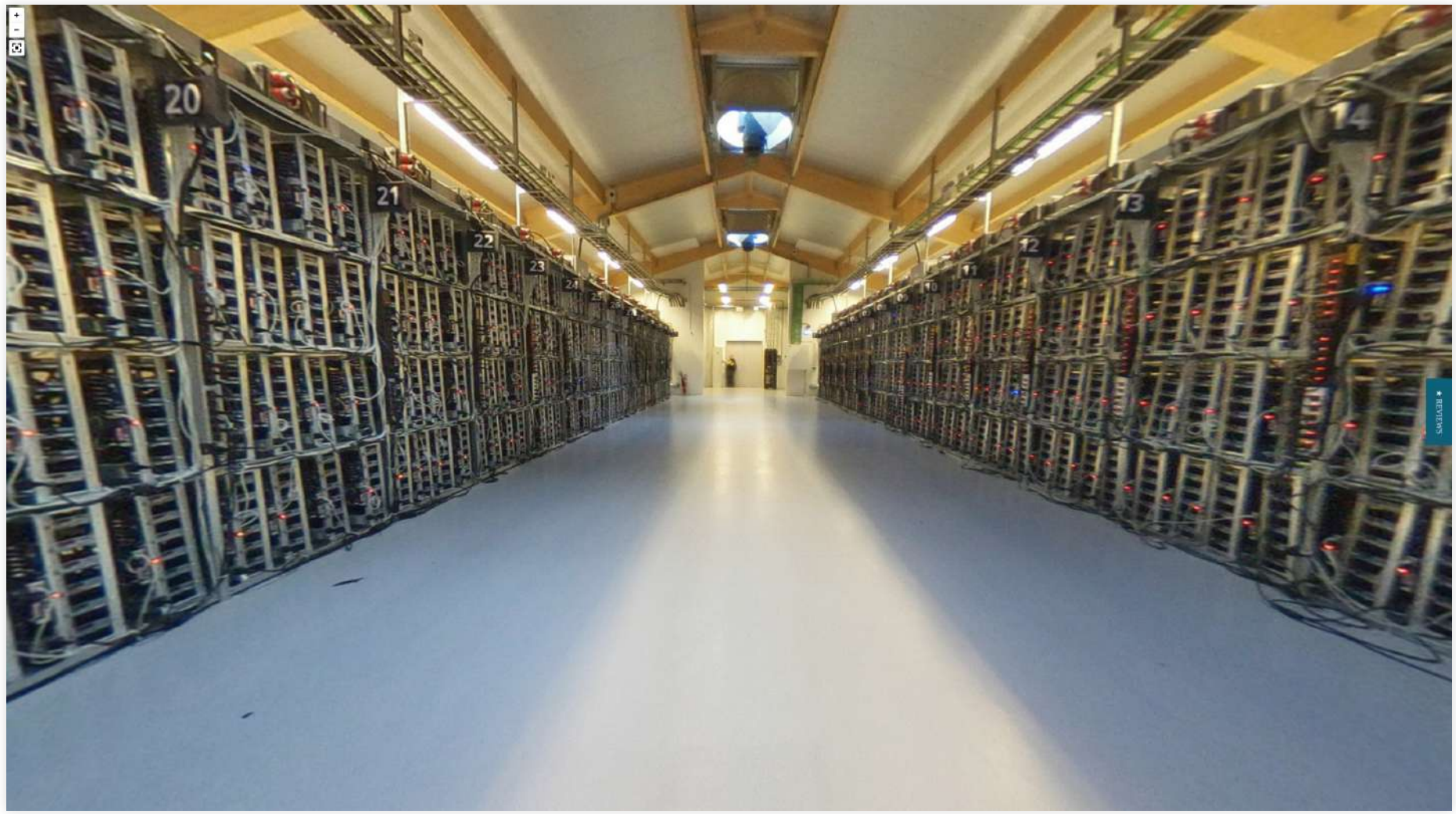
Hashrate


Hash Rate
30.54 EH/s
30.53 EH/s
24.12 EH/s
17.71 EH/s
11.30 EH/s
4.88 EH/s
2009-01-03
blockchain.info/charts
2018-04-22

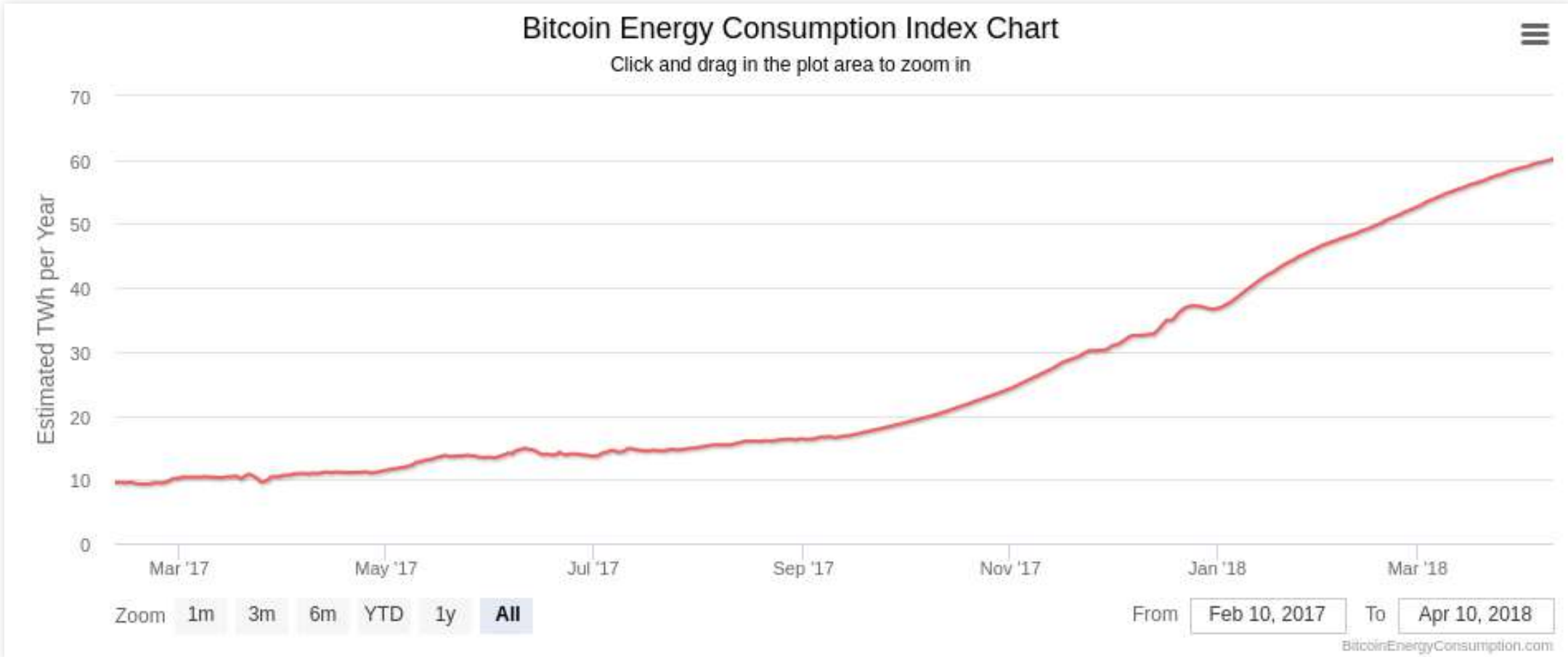
Hardware

CPU → GPU → FPGA → ASIC

Hardware



Geschätzter Stromverbrauch

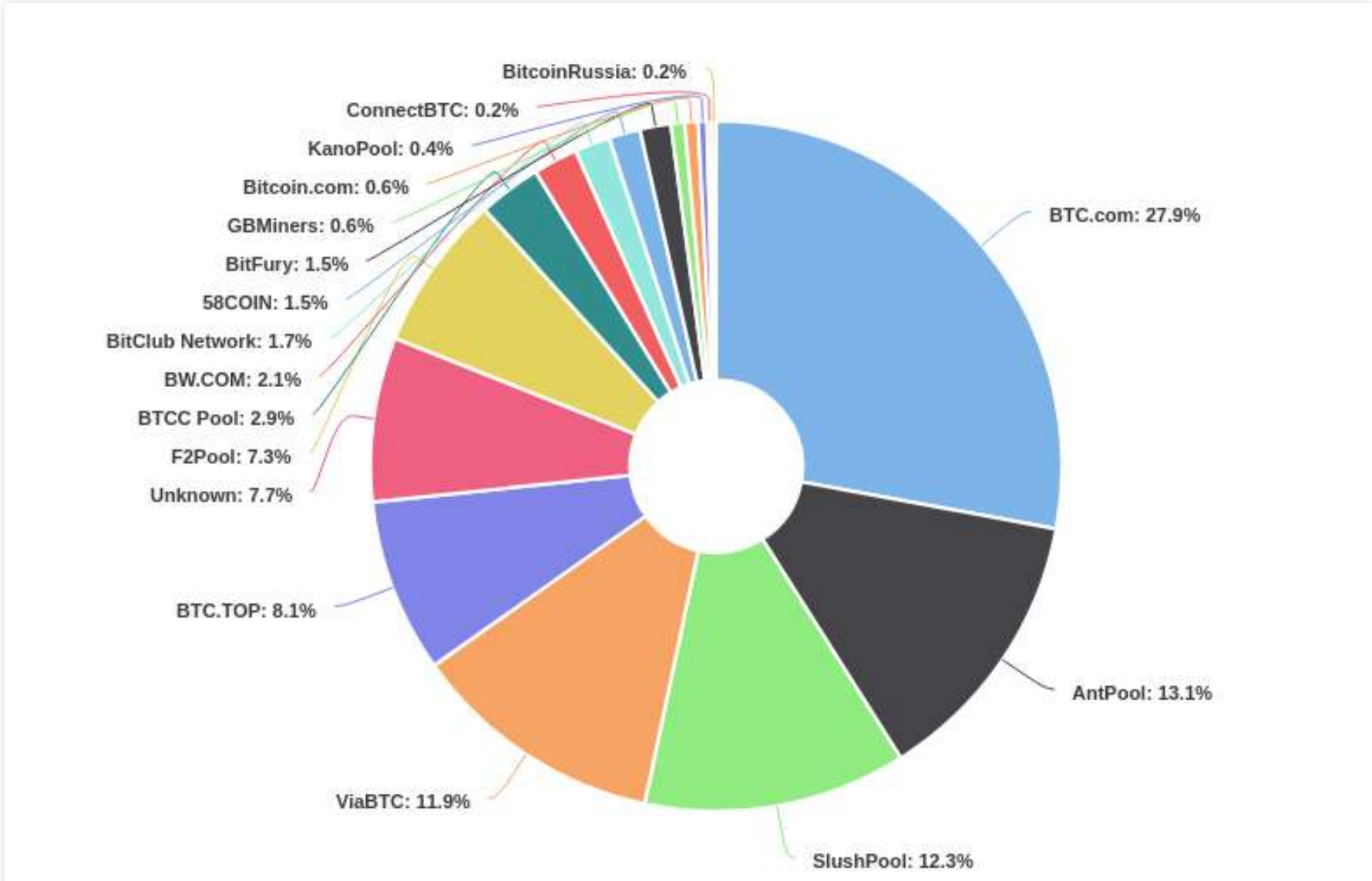


~5,7 Atomkraftwerke

Mining: Kosten je BTC

South Korea	$26,170
Niue	$17,566
Bahrain	$16,773
Solomon Island	$16,209
Cook Islands	$15,861
...	
Germany	$14,275
...	
Myanmar	$1,983
Ukraine	$1,852
Uzbekistan	$1,788
Trinidad and Tobago	$1,190
Venezuela	$531

Schätzung der Verteilung der Hashleistung



Übersicht

Geschichte

Vision

Grundlagen

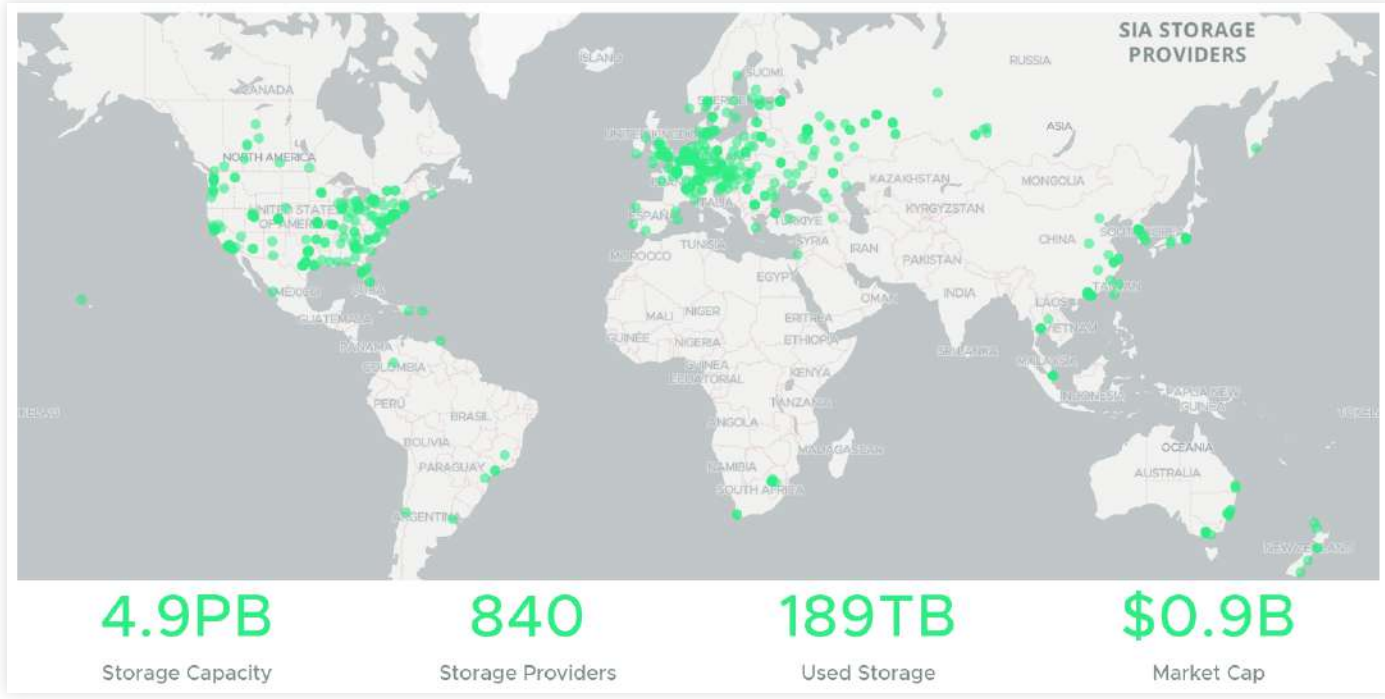
Blockchain

Bitcoin

Entwicklung

Anwendungen

Cloud Storage



(www.sia.tech)

- Verschlüsselte Dateifragmente werden von beliebigen Anbietern gespeichert
- Redundante Speicherung, für den Fall, dass Anbieter ausfallen
- Proof-of-Storage anforderbar

Schweden nutzt jetzt offiziell die Blockchain für Grundbucheintragungen

7. Juli 2017 | Sven Wagenknecht

BLOCKCHAIN

512 13 3 0 4 6 8 0 115

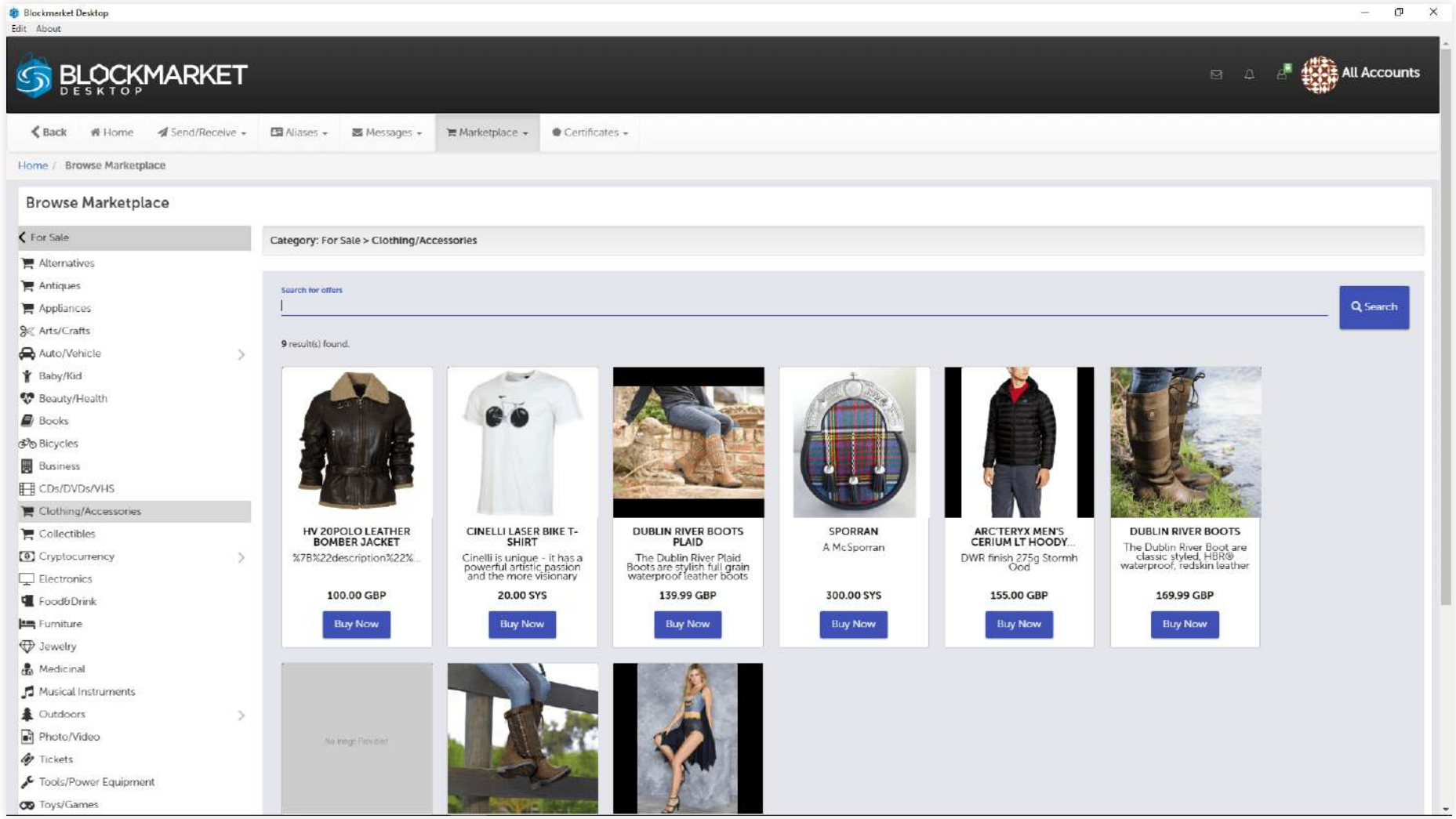
Wie berichtet wurde, hat in Schweden das Grundbuchamt Lantmäteriet seit kurzem angefangen Grundstücke und Eigentümer über eine Blockchain einzutragen.

Schon seit 2016 ist bekannt, dass Schweden an einer Blockchain-Lösung diesbezüglich forscht. Ende Mai wurde dann die letzte Testphase erfolgreich abgeschlossen. Trotz der fortschrittlichen Digitalisierung des Grundbuchamtes, soll die Blockchain zu deutlichen Effizienzsteigerungen führen.

Konkret sollen so um die 100 Millionen Euro eingespart werden können, die für Bürokratie und Betrugsfälle jedes Jahr fällig werden. Das es tatsächlich zu so hohen Einsparungen kommt, bleibt jedoch zu bezweifeln. Darüber hinaus haben aber auch die Banken Interesse an dem Projekt, da sich so in der Zukunft auch Hypothekengeschäfte über eine Blockchain darstellen lassen. Entsprechend wundert es auch nicht, dass zwei schwedische Banken bei dem Projekt involviert sind.

(https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragungen)

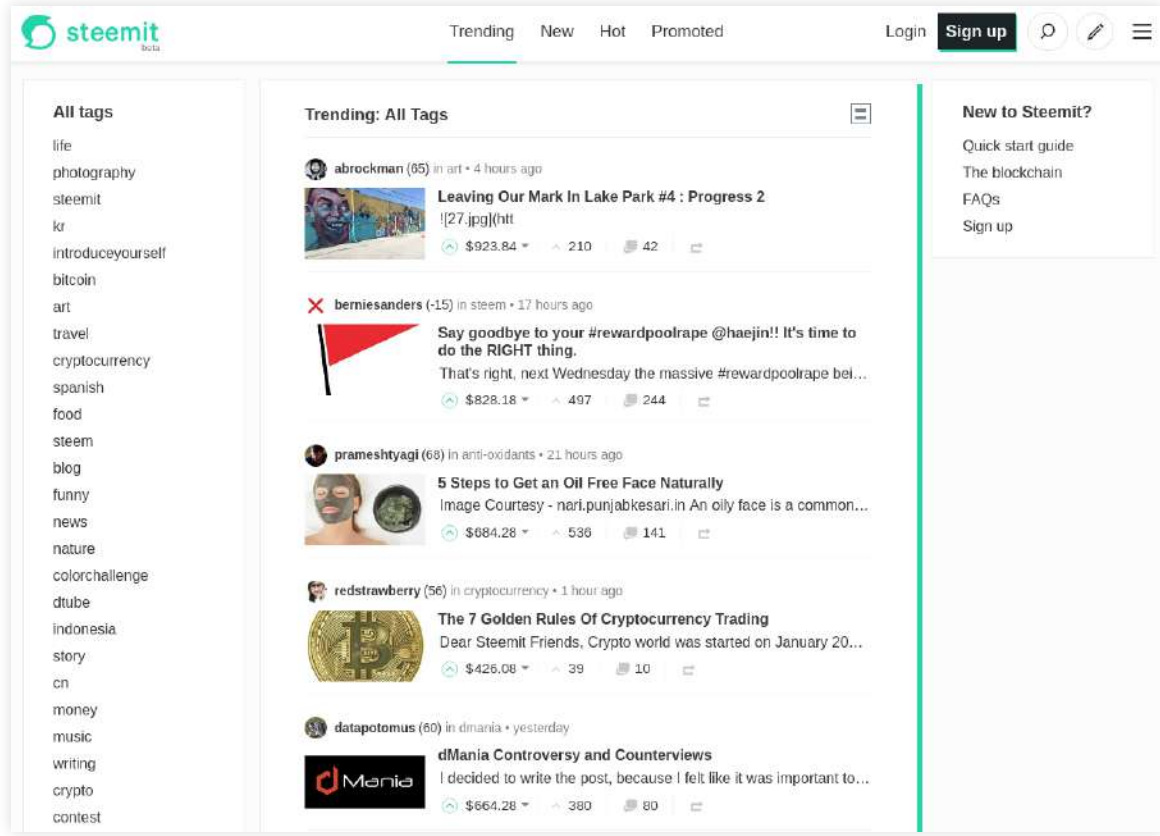
Marktplatz



(https://www.syscoin.org/)

- Dezentralisierter Marktplatz

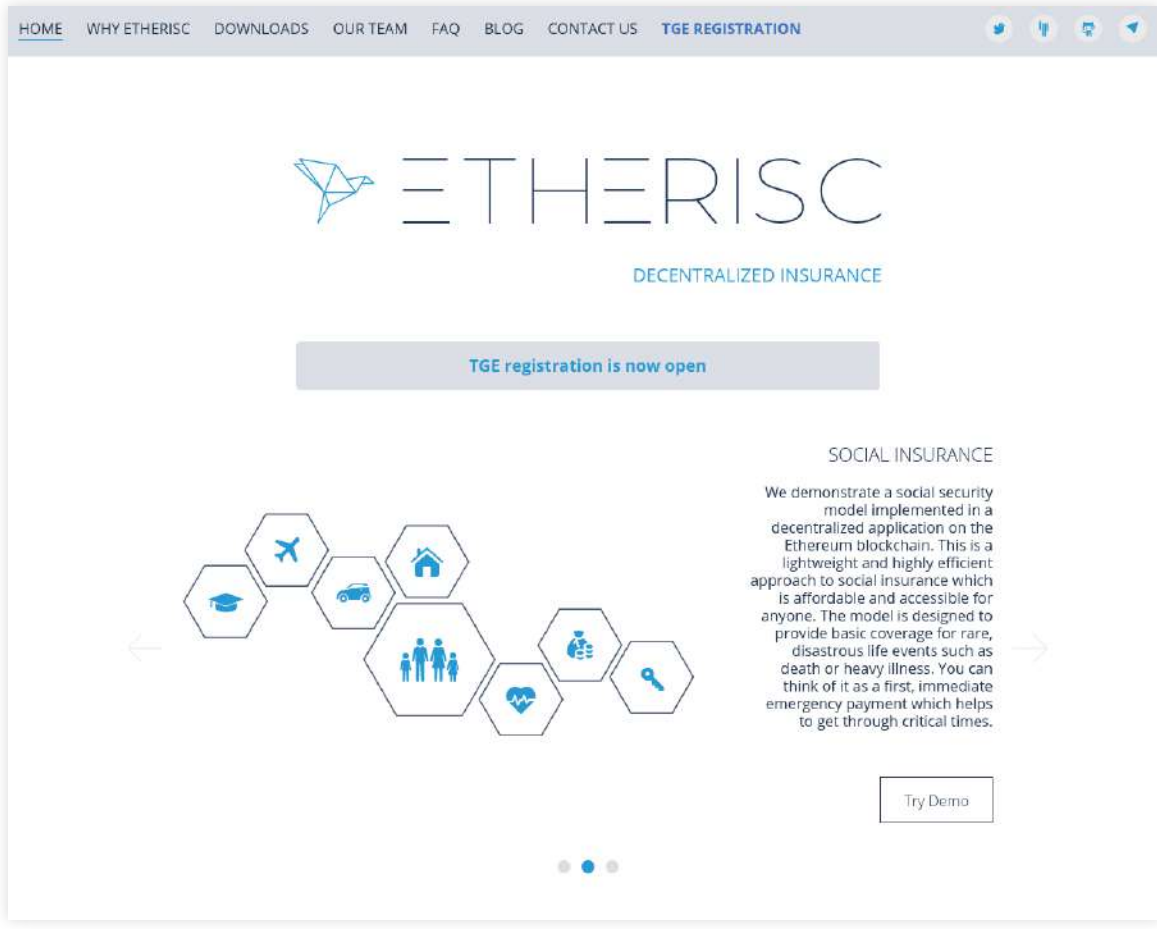
Social Media



(https://steemit.com/)

- Alle Inhalte werden in einer Blockchain gespeichert.
- Belohnung der Verfasser erfolgt entsprechend der Popularität ihrer Inhalte.

Versicherung



(https://etherisc.com/)

- Gemeinsame Register für firmenübergreifende Daten
- Einblick in Daten nur für beteiligte Parteien
- Abbildung der Prozesse mit Smart Contracts

Fragen?

Quellen

- https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/FhG-Positionspapier-Blockchain.pdf
- https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf
- https://bitcoin.org/bitcoin.pdf
- https://bitcoin.org/en/developer-reference
- https://blockchain.info/charts/market-price?timespan=all
- https://digiconomist.net/bitcoin-energy-consumption
- https://blockchain.info/de/pools
- https://www.genesis-mining.com/enigma
- https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm
- https://blockchain.info/charts/hash-rate
- https://blockchain.info/charts/n-transactions?timespan=all
- https://blockchain.info/charts/blocks-size
- https://blockze.ro/
- https://bitcoin.org/de/wallets/hardware/trezor/
- http://fortune.com/2018/03/07/bitcoin-mining-costs-global-south-korea-venezuela/
- https://www.openbazaar.org/
- https://steemit.com/
- https://etherisc.com/
- https://sia.tech/
- http://www.coin-blog.de/blog/paper-wallet-anleitung
- https://de.wikipedia.org/wiki/Bitcoin_Core