BLOCKCHAIN
Bayern e.V.

Wir bringen Blockchain in Bayern voran.

Funktion der Blockchain erklärt

Ulrich Gallersdörfer, M.Sc.
Gründungsmitglied
Blockchain Bayern e.V.

Blockchain für den Mittelstand, 11.05.2021

www.blockchain-bayern.de

Ulrich Gallersdörfer

BLOCKCHAIN Bayern e.V.

Background

- Informatiker, Doktorand @ TU München
- Blockchain Bayern Gründungsmitglied
- Koordinator Blockchain Research Cluster

Forschung

- ***Identity Management*** *in Blockchains: Smart Contract Authentifizierung*
- ***Ökologische Auswirkungen von*** *Kryptowährungen*

Lehre

- **Vorlesung** *Blockchain-based Systems Engineering (>1000 Studierende, SoSe)*
- **Zertifikatsprogramm** *Certified Blockchain & Distributed Ledger Technology Manager TUM Institute for LifeLong Learning*

Sebis Chair
Faculty of Informatics
Boltzmannstraße 3
85748 Garching
ulrich.gallersdoerfer@tum.de
+49 89 289 17137
UliG.io
@UliGall

Um was geht es heute?

BLOCKCHAIN Bayern e.V.

1. Woher weiß ich, wie viele Coins ich habe? Wie lese ich die Blockchain?
2. Wie sende ich meine Coins und warum bin ich nicht anonym?
3. Wie einigt sich das Netzwerk auf einen Zustand?
4. Warum verbraucht der Bitcoin und andere Kryptowährungen so viel Strom und warum ist es so sicher?

Um was geht es heute?

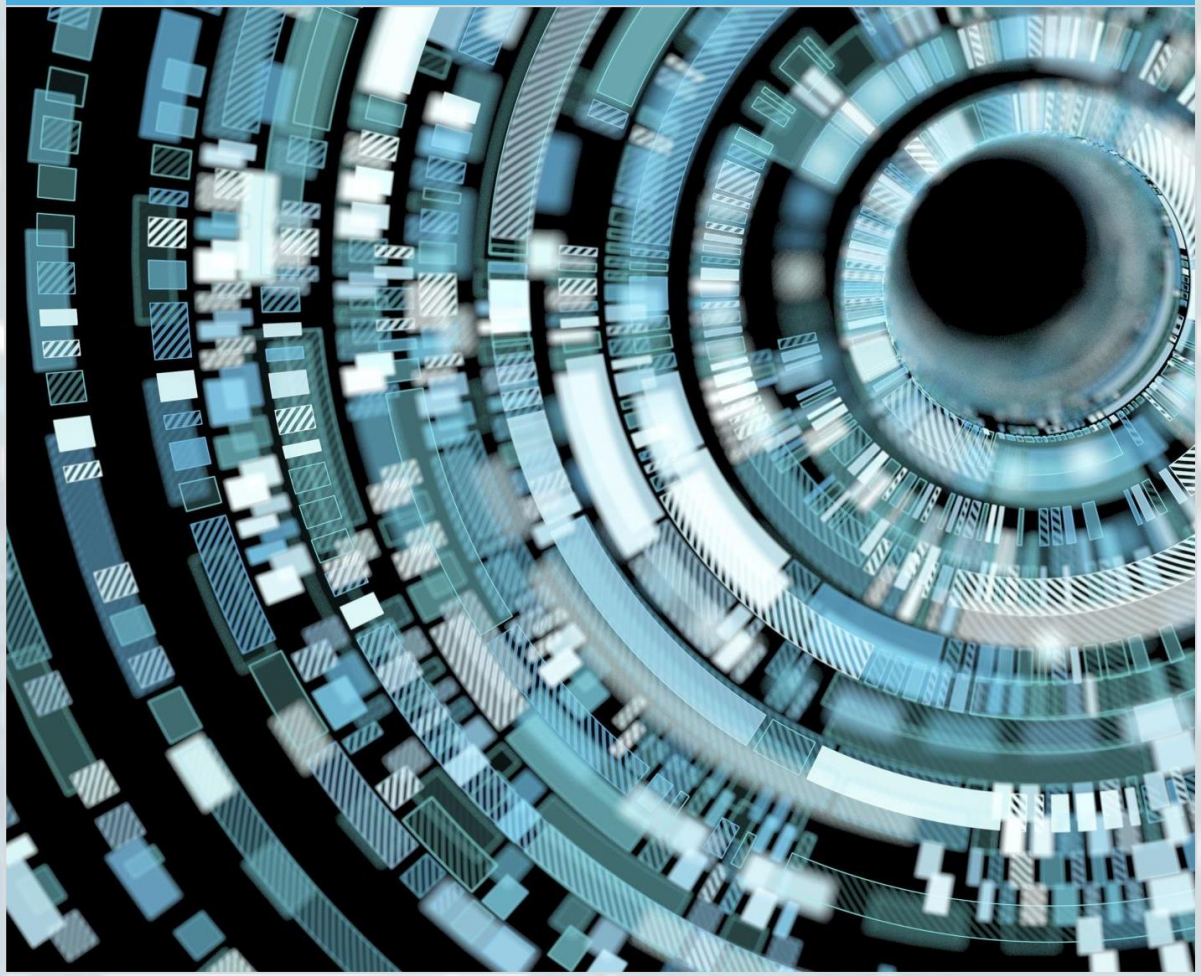
BLOCKCHAIN Bayern e.V.

1. Woher weiß ich, wie viele Coins ich habe? Wie lese ich die Blockchain?

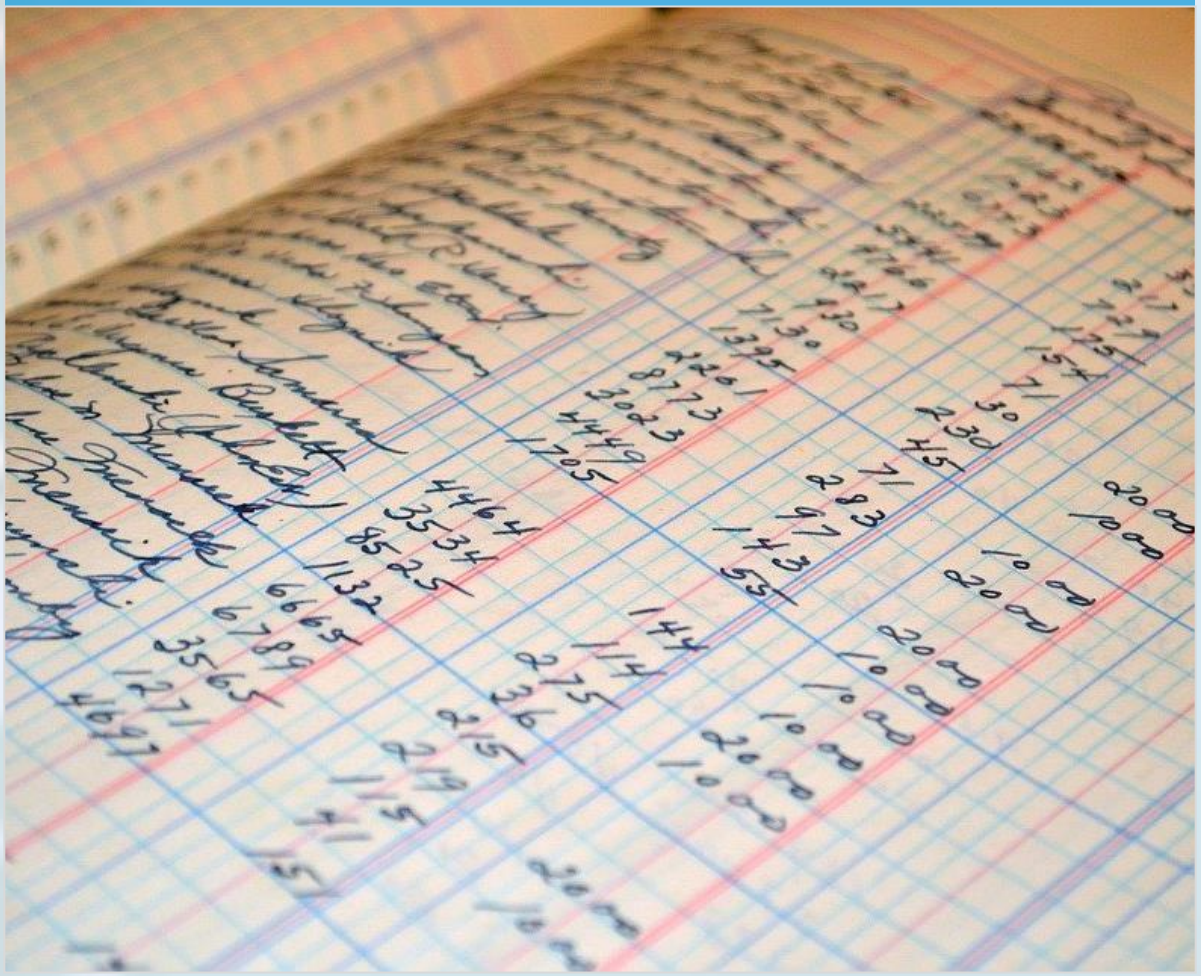
Was ist eine „Blockchain“?

BLOCKCHAIN Bayern e.V.

Eine dezentrale Datenbank



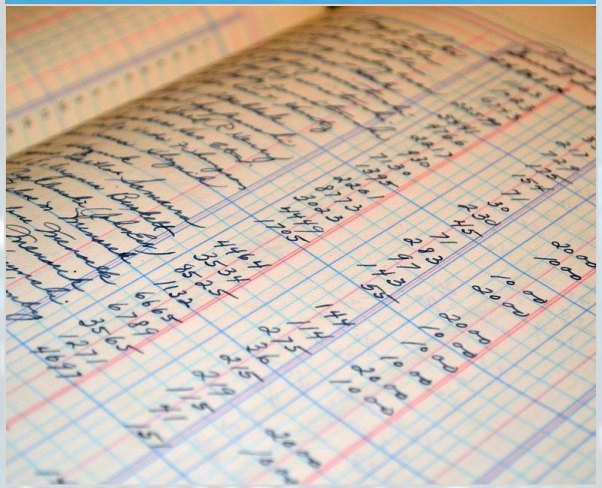
Ein dezentrales Register / Kassenbuch



Was ist eine „Blockchain“?

BLOCKCHAIN Bayern e.V.

Ein dezentrales Register



Teilt sich auf in Blöcke und Transaktionen

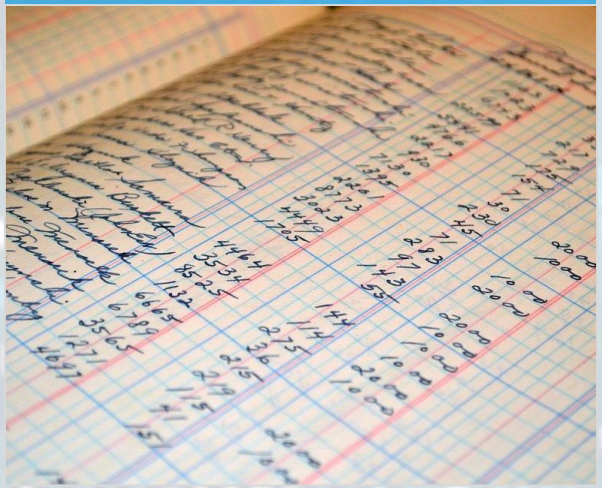
Transaktion 1
Von Person A
An Person B

Block

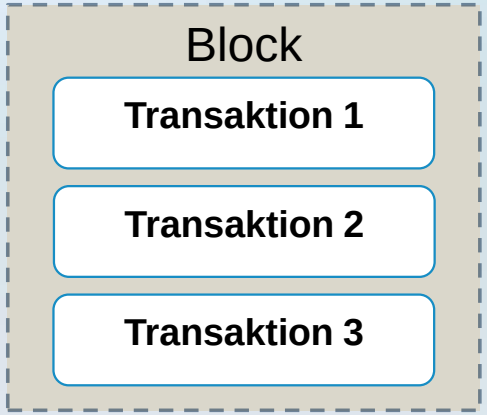
Was ist eine „Blockchain“?

BLOCKCHAIN Bayern e.V.

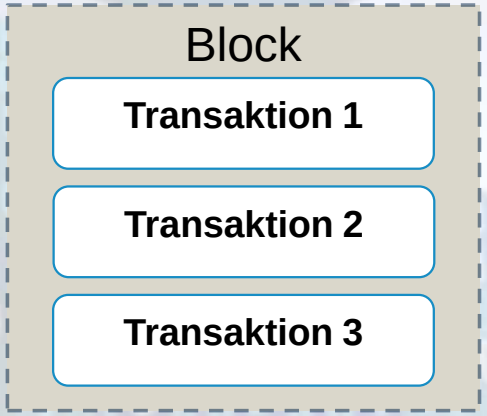
Ein dezentrales Register



Teilt sich auf in Blöcke und Transaktionen



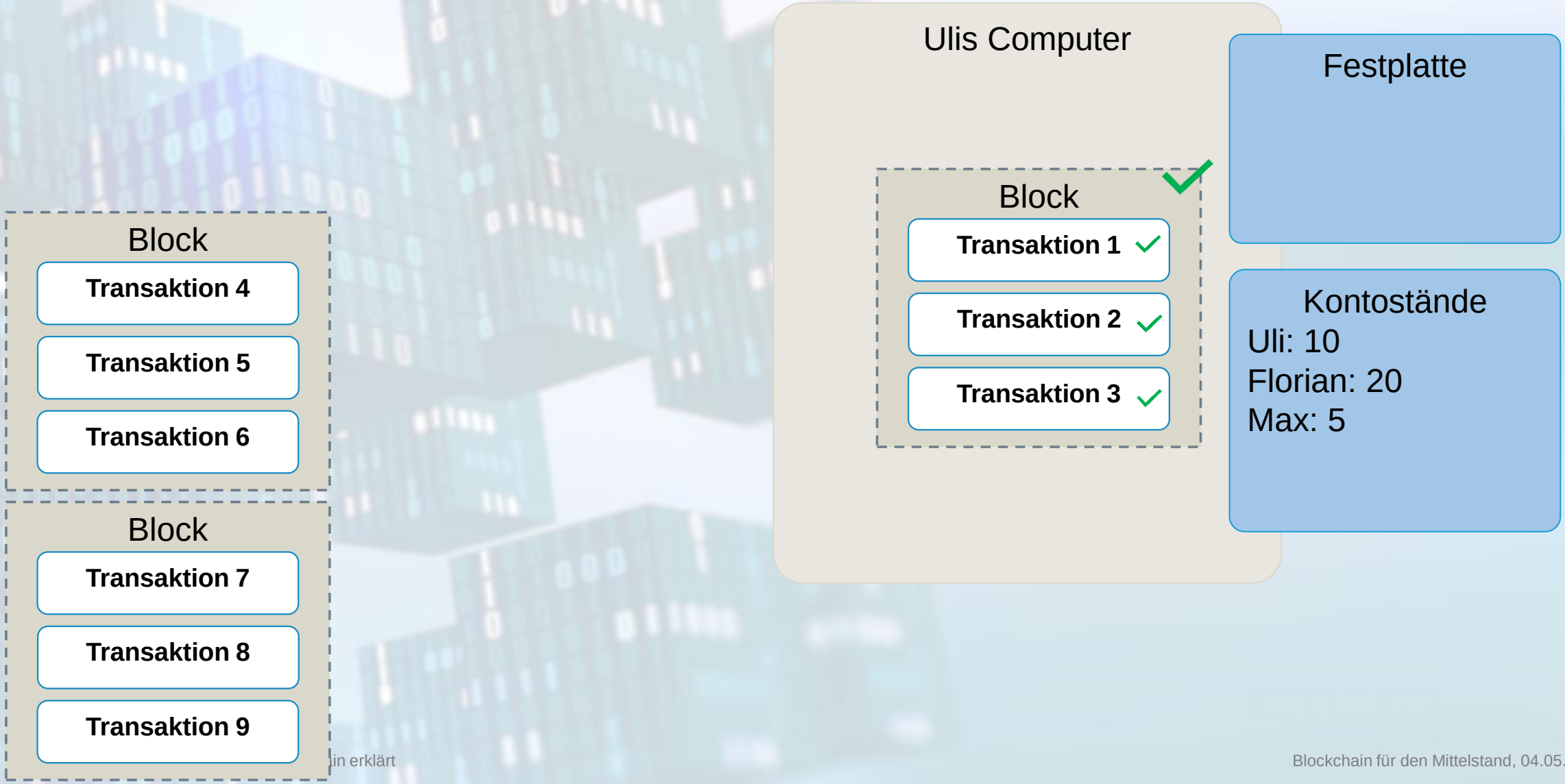
Was ist eine „Blockchain“?



Was ist eine „Blockchain“?

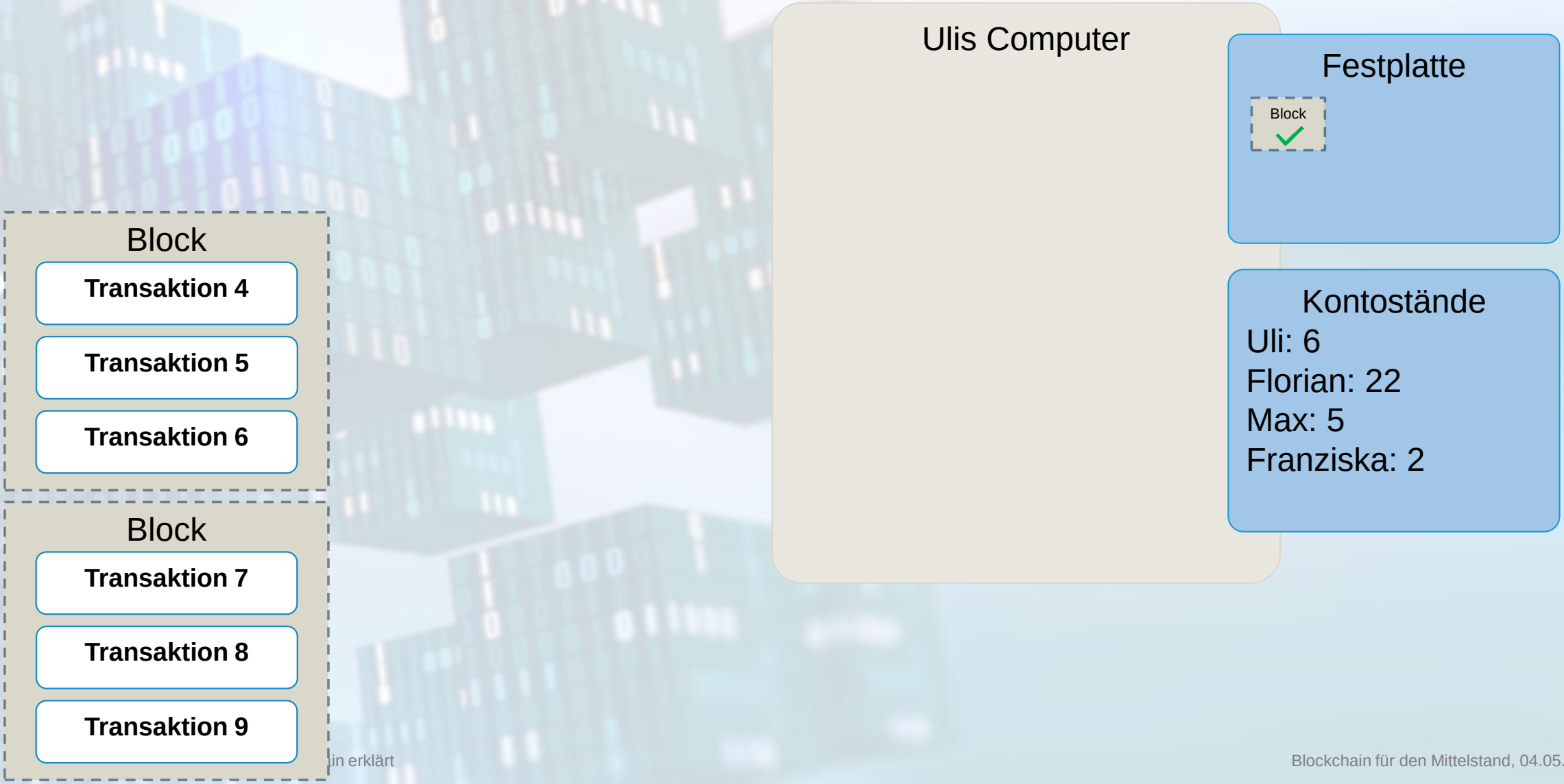
Was ist eine „Blockchain“?

BLOCKCHAIN Bayern e.V.



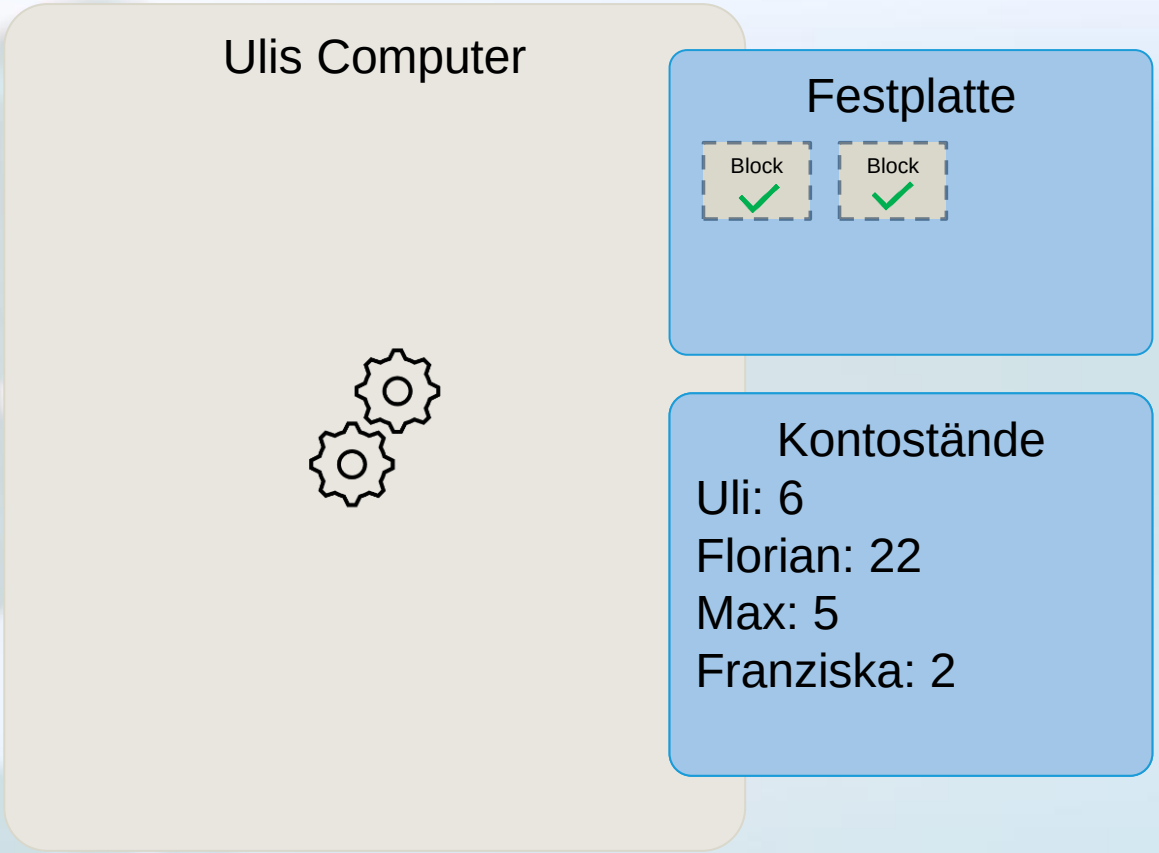
Was ist eine „Blockchain“?

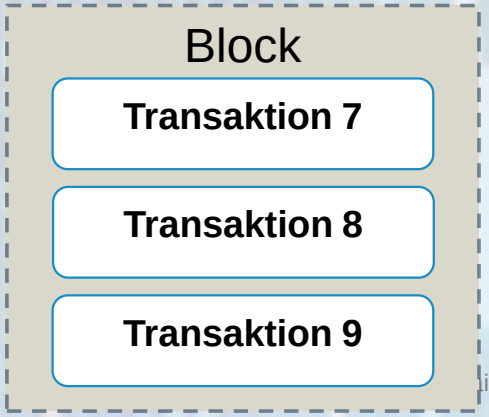
BLOCKCHAIN Bayern e.V.



Was ist eine „Blockchain“?

BLOCKCHAIN Bayern e.V.



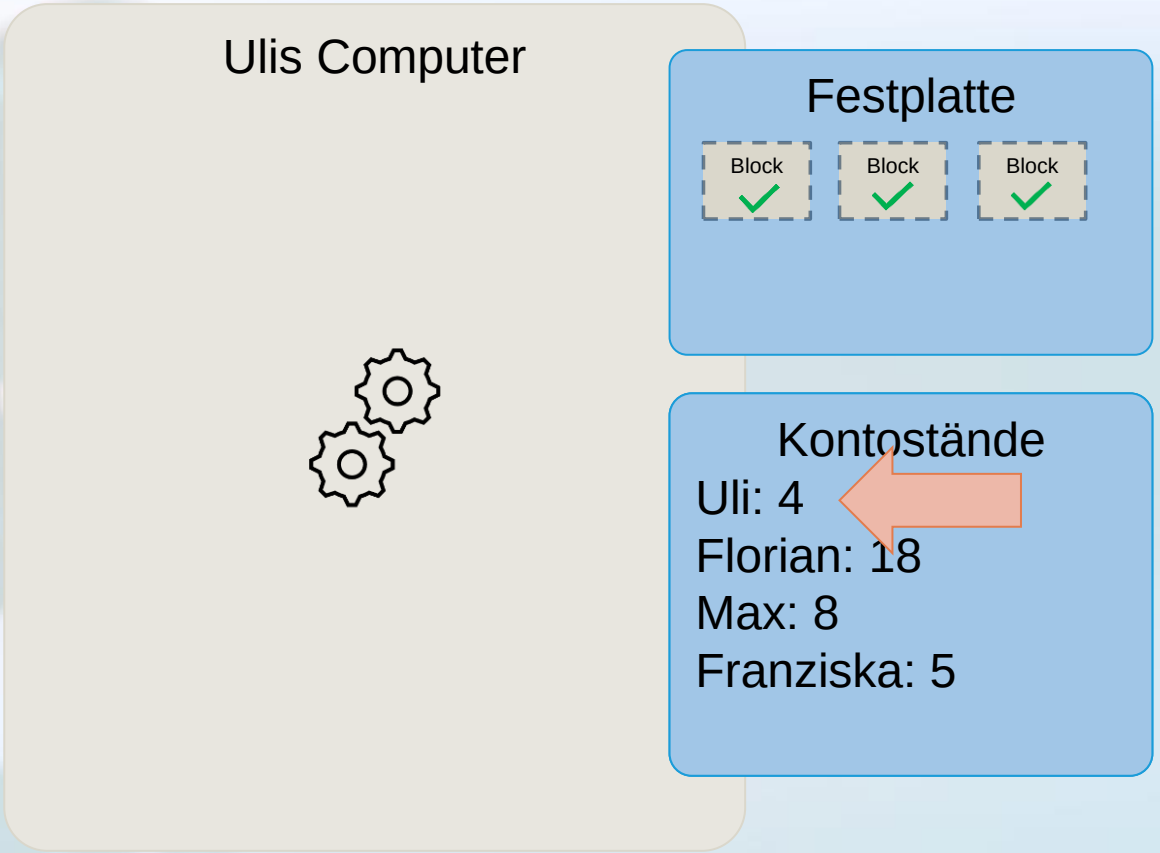


Was ist eine „Blockchain“?

BLOCKCHAIN Bayern e.V.

Zusammenfassung:

- Die Blockchain ist ein Logbuch von Transaktionen
- Jeder muss für sich lokal die Kontostände, bzw. Die Zustände ausrechnen
- Blöcke sind ein “Vehikel”, um Transaktionen zu bündeln
- Man muss immer auf den neusten “Stand” (und damit Block) sein, sonst weiß man nicht was los ist



Um was geht es heute?

BLOCKCHAIN Bayern e.V.

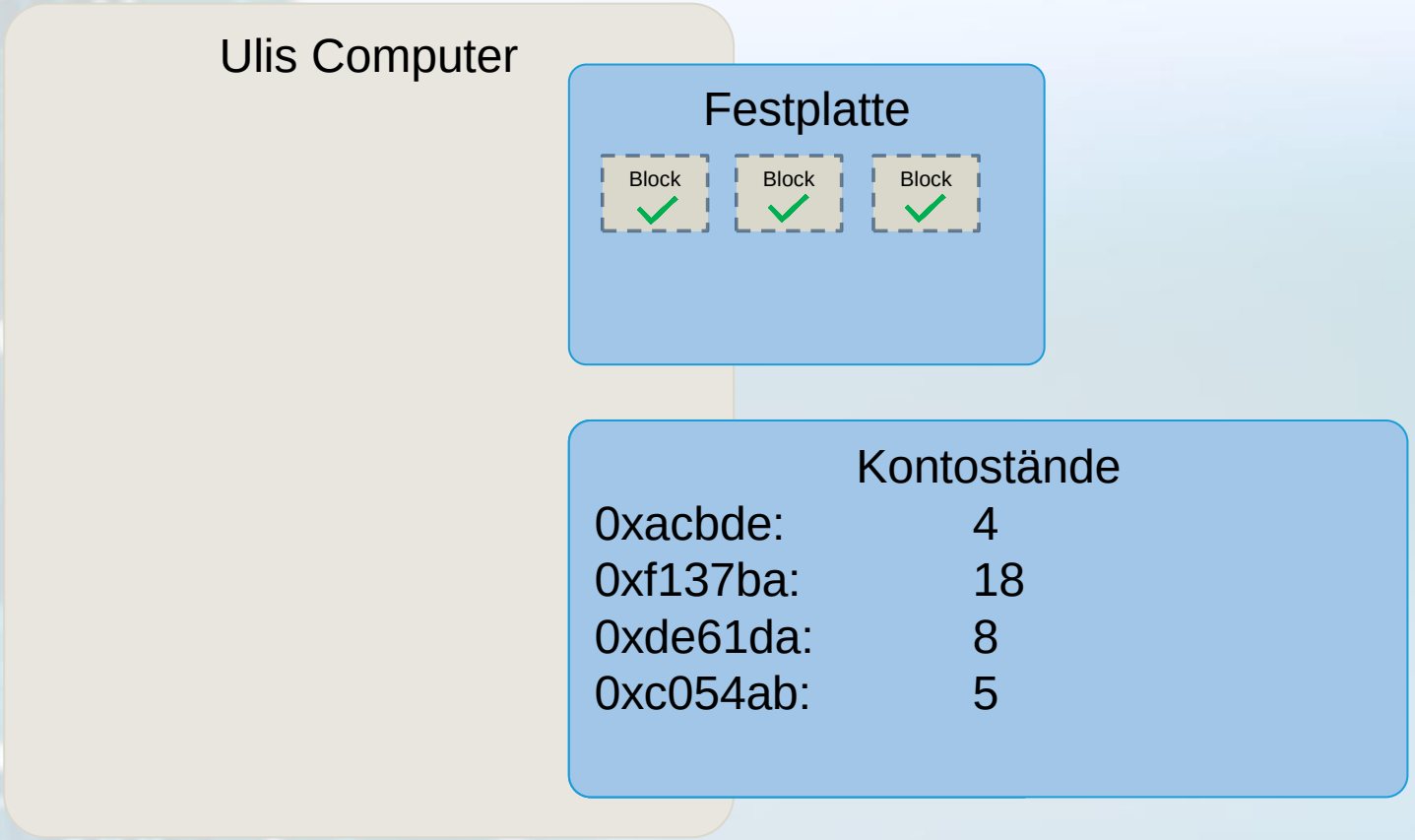
1. Woher weiß ich, wie viele Coins ich habe? Wie lese ich die Blockchain?
2. Wie sende ich meine Coins und warum bin ich nicht anonym?
3. Wie einigt sich das Netzwerk auf einen Zustand?
4. Warum verbraucht der Bitcoin und andere Kryptowährungen so viel Strom und warum ist es so sicher?

Um was geht es heute?

BLOCKCHAIN Bayern e.V.

2. Wie sende ich Coins und warum bin ich nicht anonym?

Wie sende ich Coins?



Wie sende ich Coins?

BLOCKCHAIN Bayern e.V.

Ulis Computer

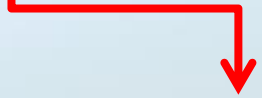
Kontostände	
0xacbde:	4
0xf137ba:	18
0xde61da:	8
0xc054ab:	5

Wie sende ich Coins?

Ulis Computer

Kontostände

0xacbde: 4



Wir haben bereits herausgefunden, wie wir feststellen, wie viel Geld ein Konto hat.

Wie sende ich Coins?

Ulis Computer

Kontostände

0xacbde: 4

Jetzt möchten wir verstehen, was die Kontonummer ausmacht.

Wie sende ich Coins?

Ulis Computer

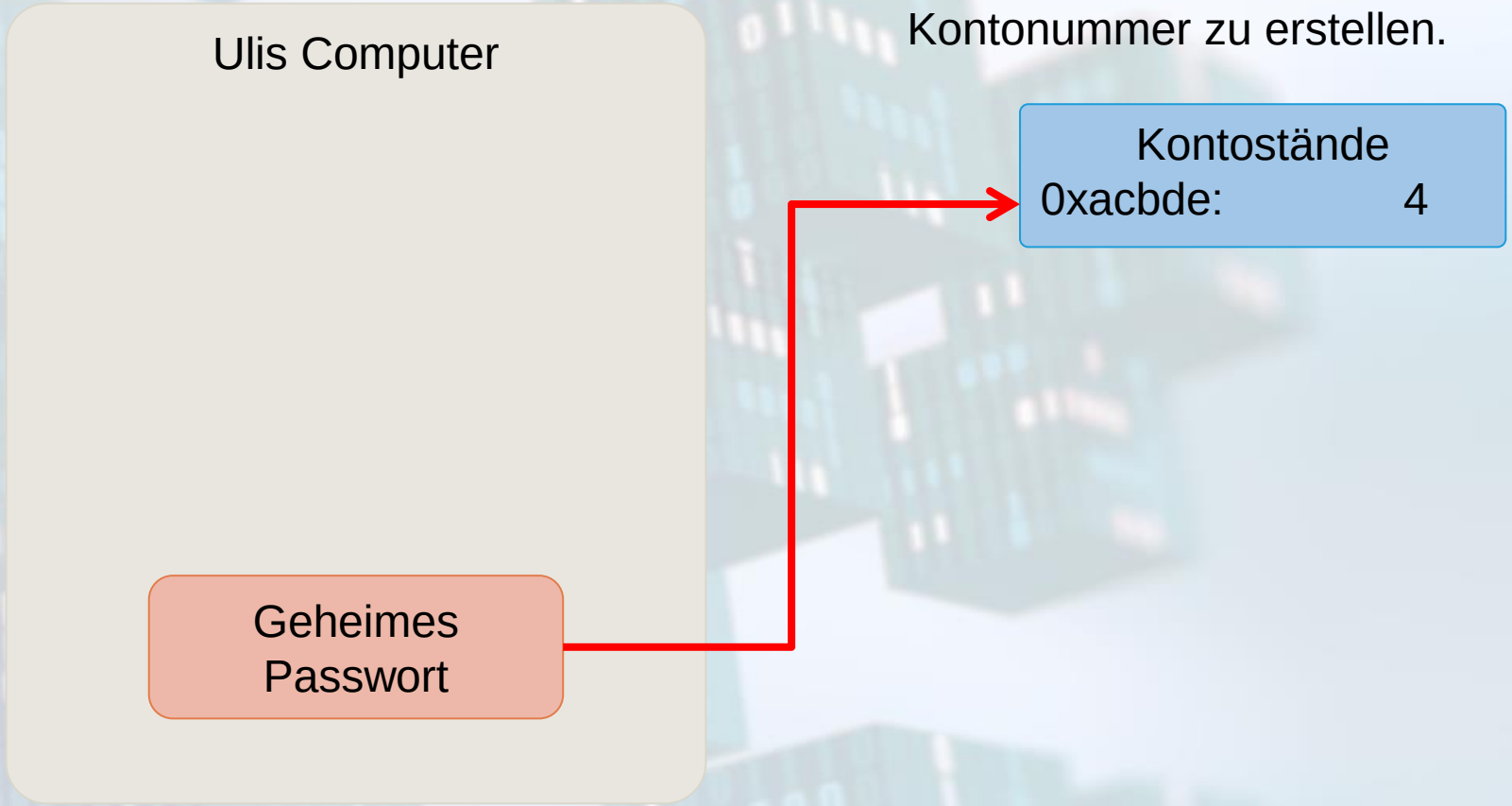
Kontostände
0xacbde: 4

Die Kontonummer funktioniert ähnlich zum Onlinebanking:

- Wer die Nummer weiß, kann dort hinüberweisen
- Zunächst weiß nur der Kontoinhaber die Nummer des Kontos (dazu gleich mehr)
- Nur berechtigte Personen können Überweisungen von der Kontonummer ausführen

Wie sende ich Coins?

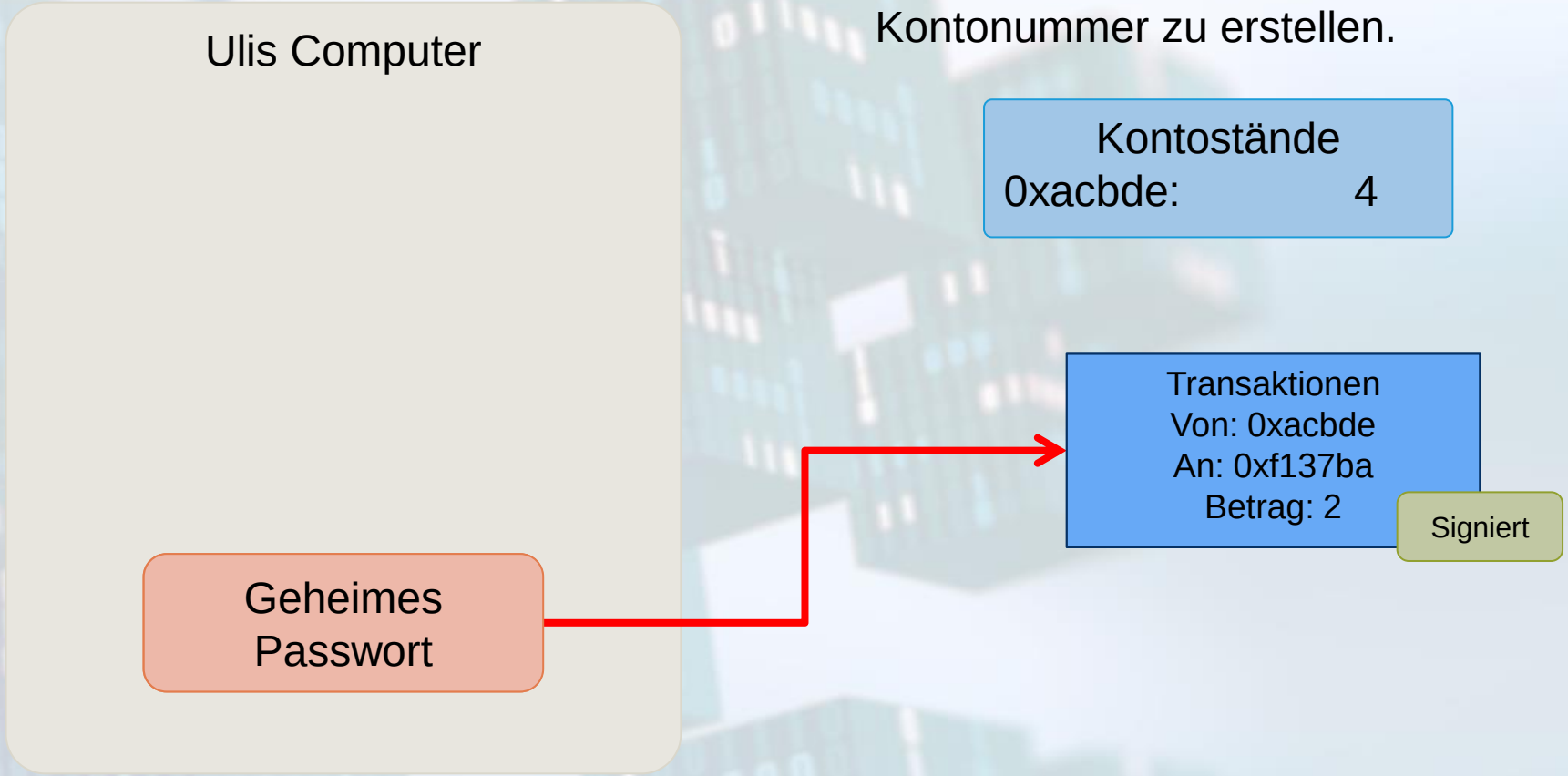
Ein geheimes Passwort erlaubt Transaktionen für die Kontonummer zu erstellen.



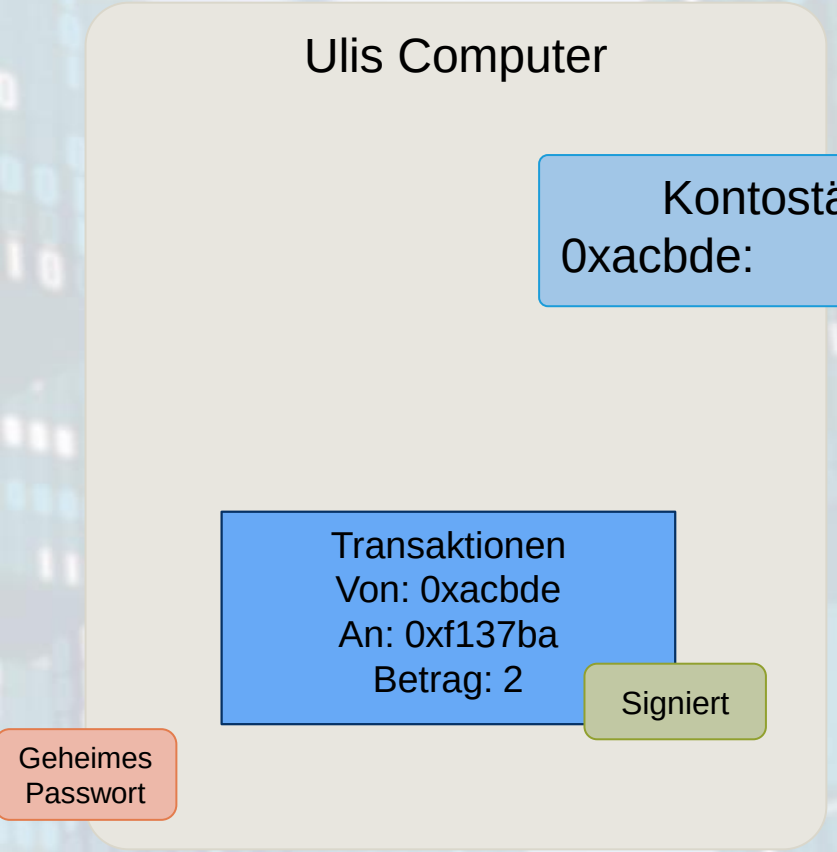
Wie sende ich Coins?

BLOCKCHAIN Bayern e.V.

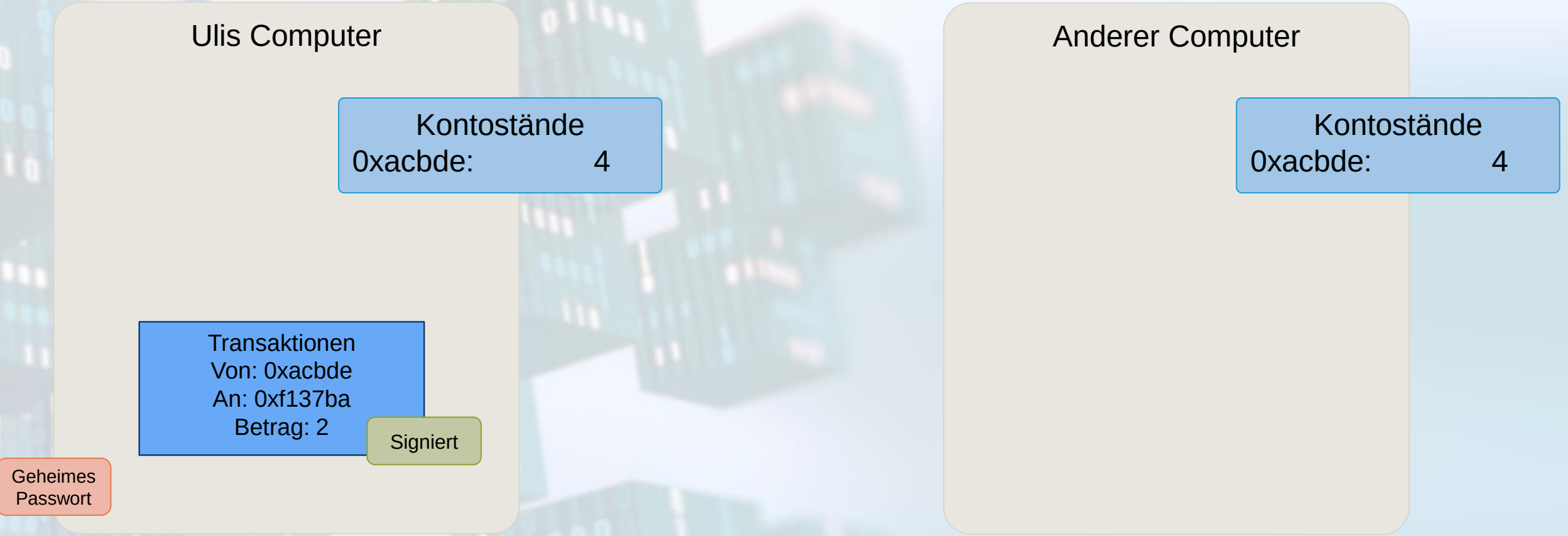
Ein geheimes Passwort erlaubt Transaktionen für die Kontonummer zu erstellen.



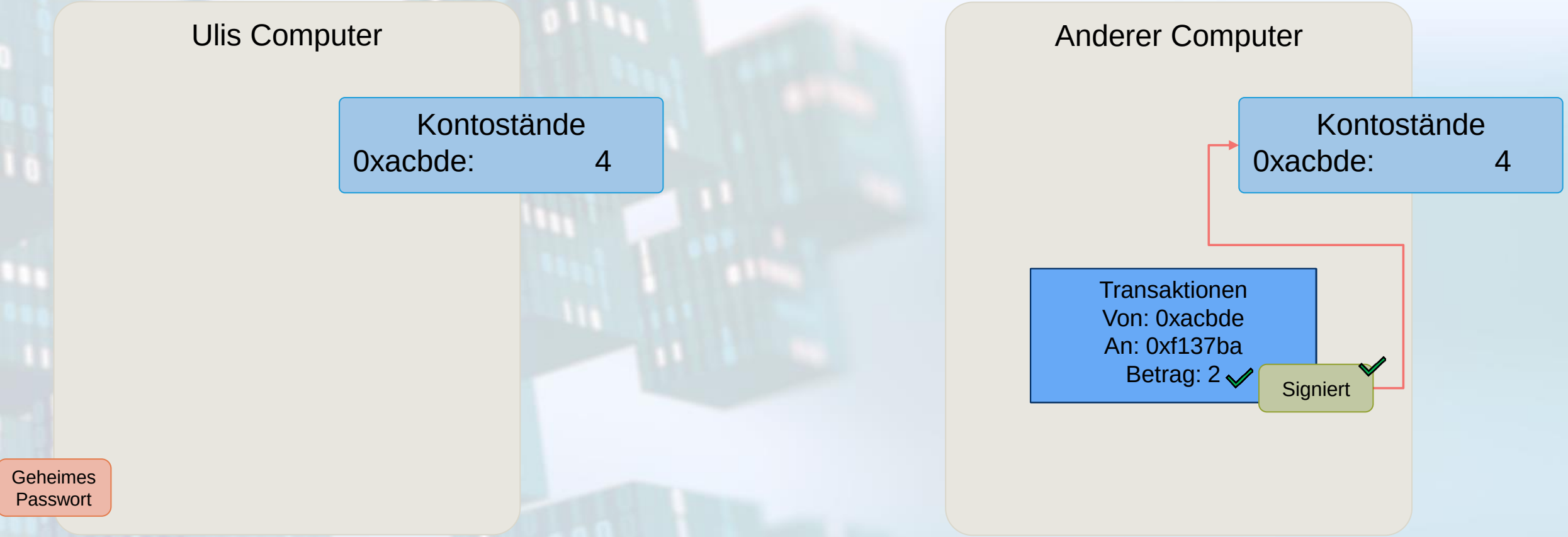
Wie sende ich Coins?



Wie sende ich Coins?



Wie sende ich Coins?



Wie sende ich Coins?

BLOCKCHAIN Bayern e.V.

Ulis Computer

Kontostände
0xacbde: 4

Geheimes Passwort

Anderer Computer

Kontostände
0xacbde: 4

Transaktion…

PCX

PCY

PCZ

Wie sende ich Coins?

BLOCKCHAIN Bayern e.V.

Ulis Computer

Kontostände
0xacbde: 4

Geheimes Passwort

Anderer Computer

Kontostände
0xacbde: 4

Dies sind Standardverfahren. Sie nutzen Sie tausendfach jeden Tag, hier im Onlinemeeting, beim Internetsurfen oder Onlinebanken.
Digitale Signaturen!

PCX
Transaktion…

PCY
Transaktion…

PCZ
Transaktion…

Warum bin ich nicht anonym?

- Ihre Kontonummern sind grundsätzlich pseudonym:
  - Jede Überweisung ist einer Kontonummer zuordenbar
  - Alle Kontonummern sind transparent
  - Sie können sich beliebig viele Kontonummern anlegen

- Grundsätzlich lassen sich aber ihre Aktivitäten Ihnen oder persönlichen Merkmalen zuordnen:
  - Sie bekommen z.B. Bitcoins von ihrer Börse. Die kennt sie genau.
  - Shops, in denen Sie mit Bitcoins bezahlen, sehen, woher das Geld kommt und auch z.B. wie viel sie haben
  - Services, die Informationen aufbereiten, speichern Ihre IP-Adressen und die Kontonummern, nach denen Sie gesucht haben

Insb. Strafverfolgung profitiert stark von der Transparenz

EHEMALIGER CIA-VIZE

Bitcoin ist ein "Segen für die Überwachung"

Illegales finde sich bei Bitcoin nicht mehr als im klassischen Bankensystem, meint ein ehemaliger CIA-Vizechef. Dafür sei alles besser verfolgbar.

15. April 2021, 11:21 Uhr, Moritz Tremmel

(Bild: Gerd Altmann/Pixabay)

Bitcoin-Transaktionen lassen sich auf der Blockchain leicht nachvollziehen - für alle.

Der ehemalige CIA-Vize-Chef Michael Morell will Bitcoin aus der Schmuddelecke holen. Die Digitalwährung werde zu viel mit kriminellen Aktivitäten in Verbindung gebracht. Dabei sei die Blockchain-Analyse ein hocheffektives Werkzeug zur Verbrechensbekämpfung, heißt es in einem elfseitigen Papier.

https://www.golem.de/news/ehemaliger-cia-vize-bitcoin-ist-ein-segen-fuer-die-ueberwachung-2104-155756.html

Um was geht es heute?

BLOCKCHAIN Bayern e.V.

1. Woher weiß ich, wie viele Coins ich habe? Wie lese ich die Blockchain?
2. Wie sende ich Coins und warum bin ich nicht anonym?
3. Wie einigt sich das Netzwerk auf einen Zustand?
4. Warum verbraucht der Bitcoin und andere Kryptowährungen so viel Strom und warum ist es so sicher?

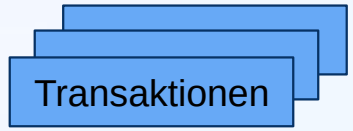
Um was geht es heute?

BLOCKCHAIN Bayern e.V.

3. Wie einigt sich das Netzwerk auf einen Zustand?

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.



Wallet Owner

- Hat Zugang für ein Blockchain Konto mit Geldbörse (**Wallet**)
- Besitzt die zugeordneten Einheiten (**Tokens**)
- Tätigt **Transaktionen** mit Tokens

Full Node

- **Verwaltet** und **speichert** die komplette Blockchain
- **Validiert** jede **Transaktion** und jeden Block
- Leitet alle neuen, validen **Transaktionen** an Miner weiter

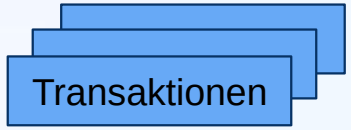
Miner

- Verhält sich wie Full Node
- **Erzeugt** aus mehreren Transaktionen einen **Block**
- Versucht, das **Mining-Puzzle** für Blöcke zu lösen
- Erhält **Belohnungen** (in **Tokens**) für neue **Blöcke** der Blockchain

Blockchain „eine Kette von Blöcken“

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.



Transaktion X
Kontonummer
Transaktionsdaten
Datum etc.
Signatur

senden

Blockchain „eine Kette von Blöcken“

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.

Transaktion X
Kontonummer ✓
Transaktionsdaten ✓
Datum etc. ✓
Signatur ✓

Überprüfen mit Blockchain

senden

Blockchain

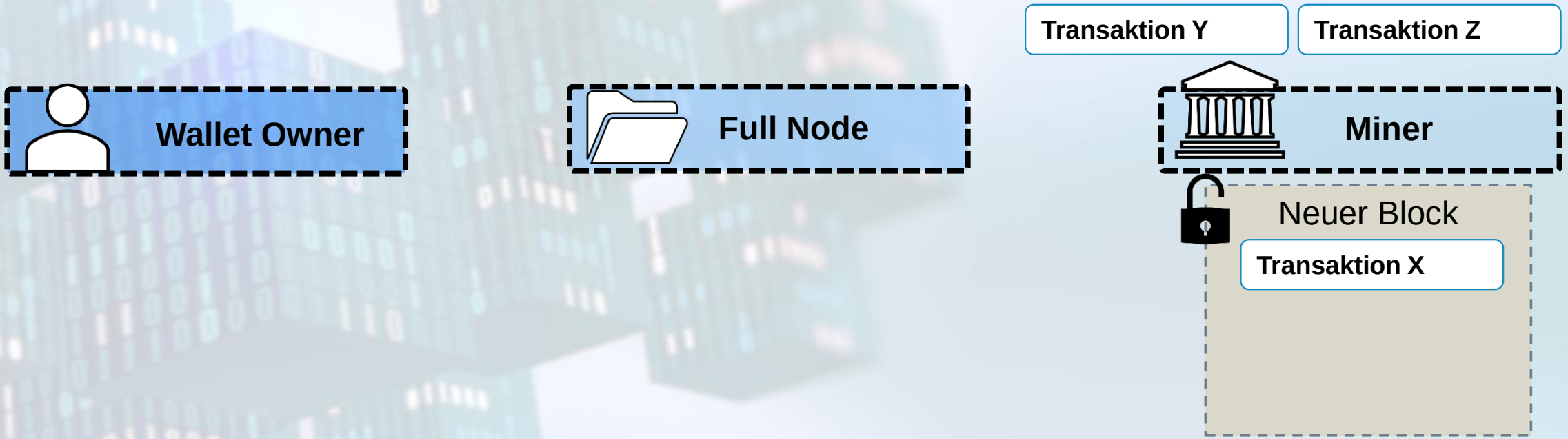
Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.

Transaktion X
Kontonummer ✓
Transaktionsdaten ✓
Datum etc. ✓
Signatur ✓

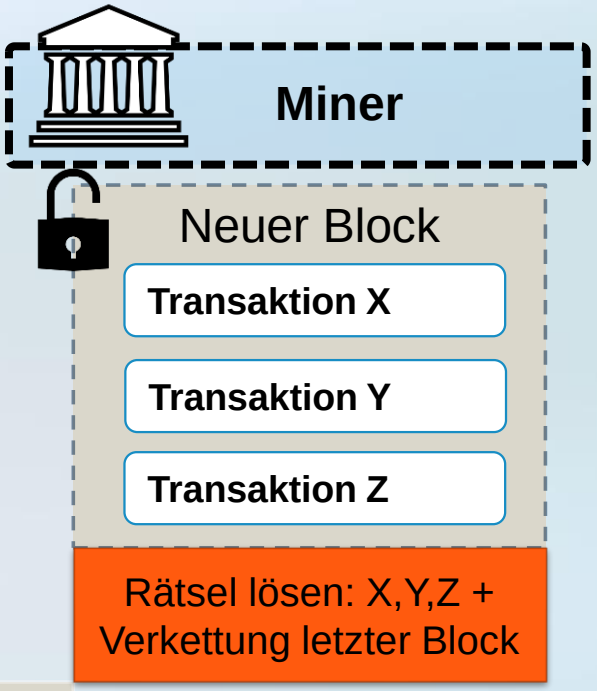
Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?



Wie funktionieren Transaktionen bei einer Blockchain?

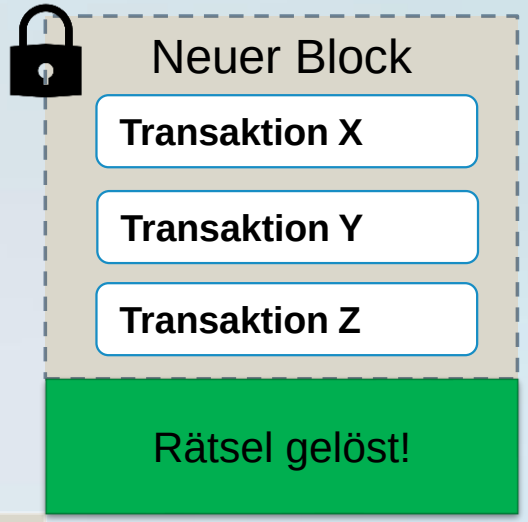
BLOCKCHAIN Bayern e.V.



Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.



Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?

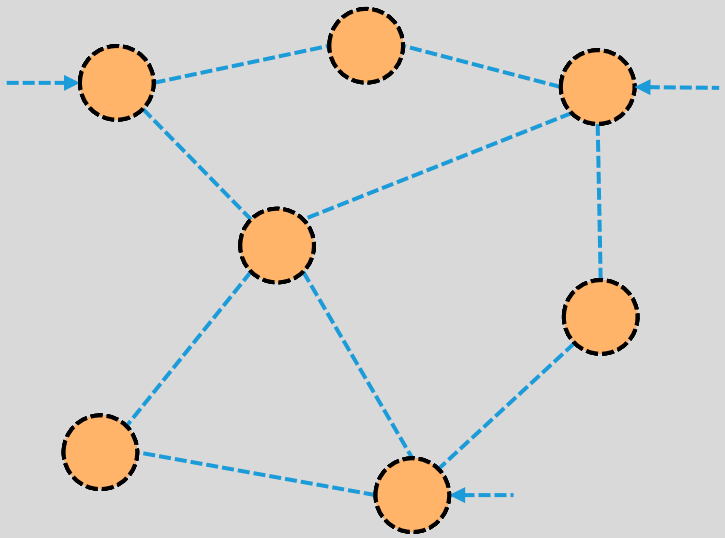
BLOCKCHAIN Bayern e.V.

Blockchain

Wie einigt sich das Netzwerk auf einen Zustand?

BLOCKCHAIN Bayern e.V.

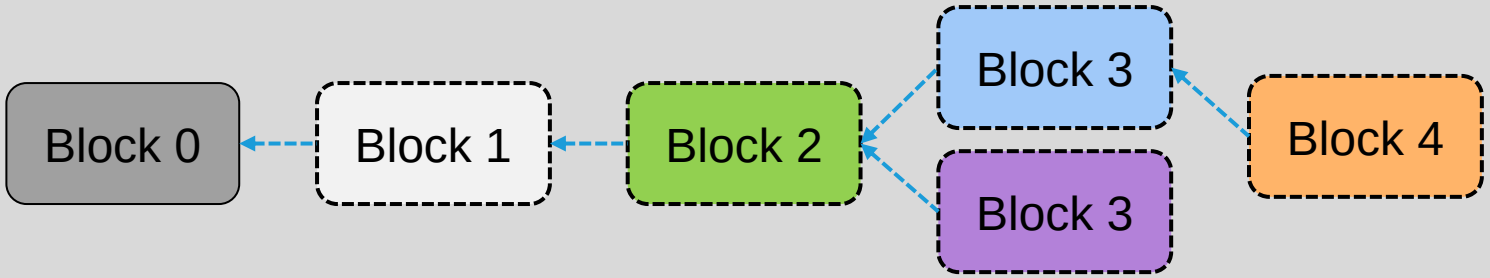
Netzwerk



1. Nur **valide Blöcke** werden aufgenommen.
2. Die **längste Kette** gewinnt.
3. Jeder baut auf dem Block auf, von dem er **zuerst gehört** hat.

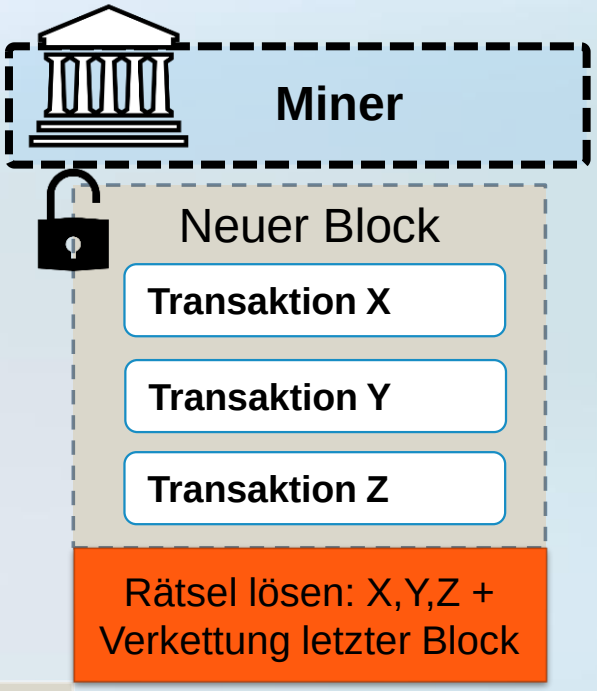
Regeln

Blockchain



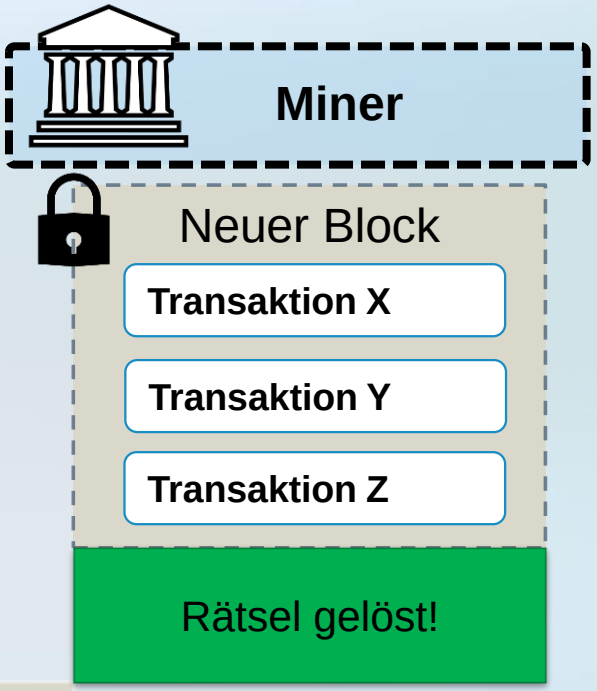
Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.



Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?

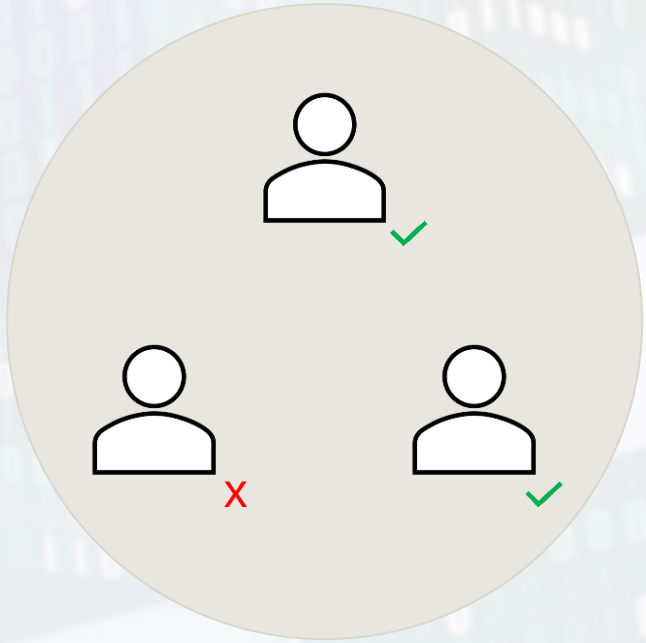


Warum brauchen wir ein solches Rätsel?

BLOCKCHAIN Bayern e.V.

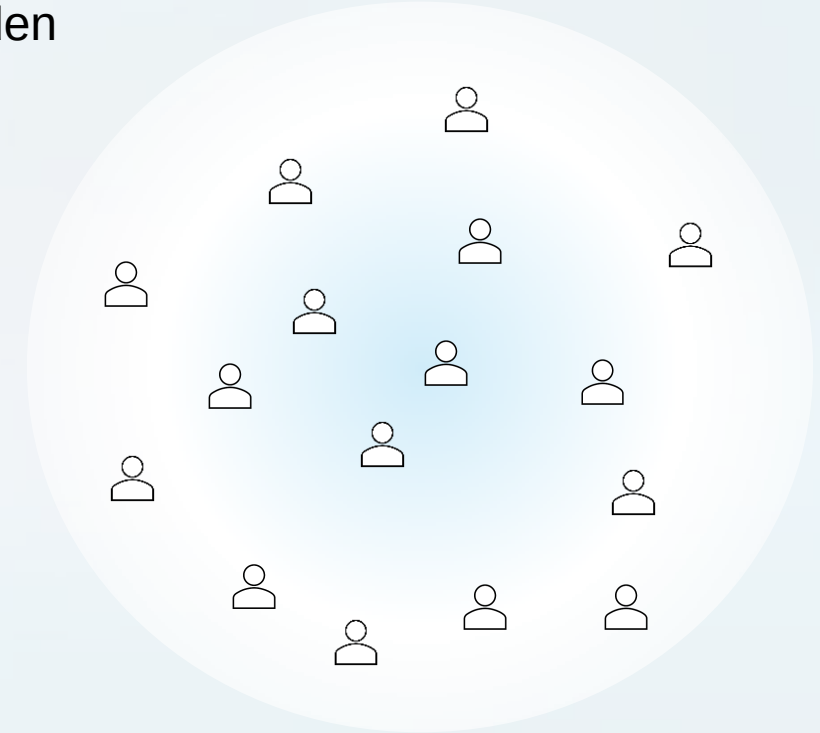
Zentralisiertes System

- Anzahl der Entitäten ist klar
- Einfache Form der Abstimmung darüber, welcher Block der nächste ist



Dezentralisiertes System

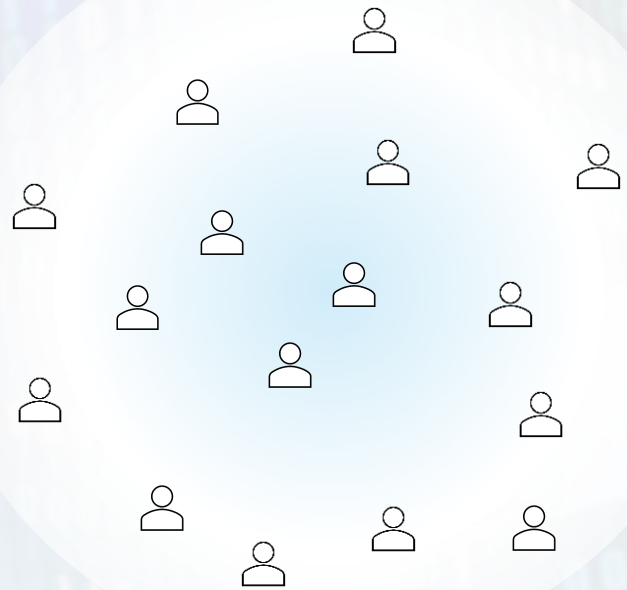
- Anzahl der Teilnehmer komplett unklar
- Teilnehmer kommen und gehen ständig
- “Teilnehmeridentitäten” können beliebig erstellt werden



Warum brauchen wir ein solches Rätsel?

BLOCKCHAIN Bayern e.V.

Dezentralisiertes System

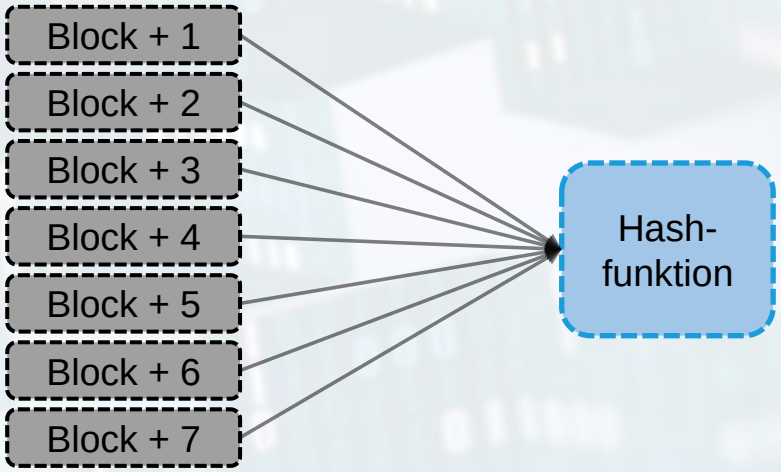


- Wir brauchen eine “Abstimmungsmöglichkeit”, bei der sich Stimmen nicht beliebig kopieren lassen
- Die Lösung von mathematischen Rätseln erfordert Rechenkraft und lässt sich nicht beliebig kopieren

- Wie funktioniert so ein Rätsel?

Wir bauen uns ein Rätsel!

1. Wir definieren einen Ausgaberaum.
2. Wir definieren einen Bereich, der, wenn er erreicht wird, als richtig anerkannt wird.
3. Wir definieren eine Funktion, die wir für das Rätsel nutzen[1]. Wir nutzen dafür eine Hashfunktion.
4. Wir probieren solange alle Möglichkeiten aus, bis wir ein Ergebnis im Zielbereich haben.

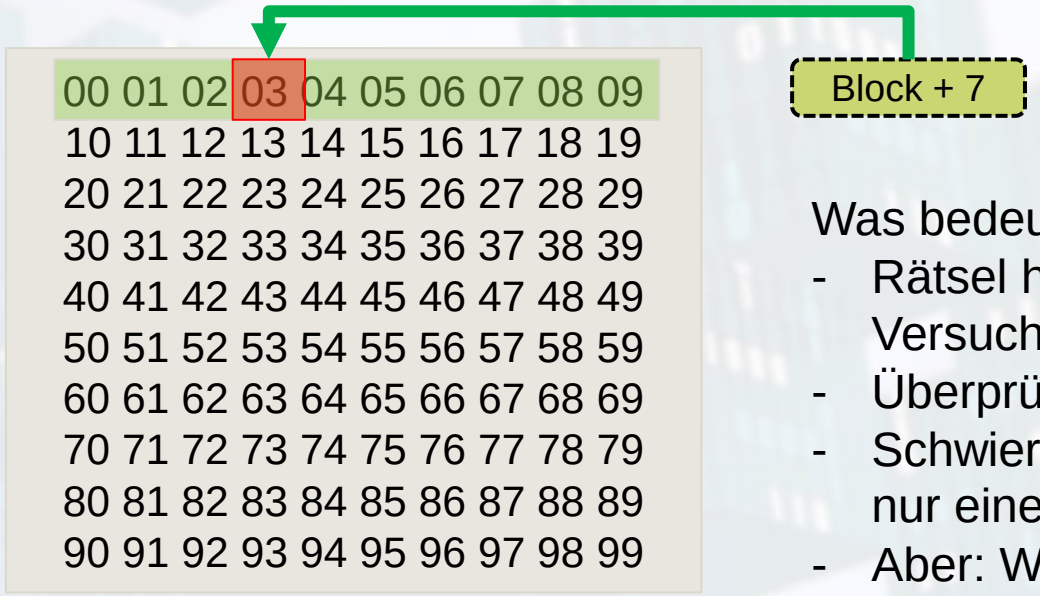


00 01 02 03 04 05 06 07 08 09
10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29
30 31 32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47 48 49
50 51 52 53 54 55 56 57 58 59
60 61 62 63 64 65 66 67 68 69
70 71 72 73 74 75 76 77 78 79
80 81 82 83 84 85 86 87 88 89
90 91 92 93 94 95 96 97 98 99

Alle 2-stelligen Zahlenkombinationen

[1]Diese Funktion sollte alle Ausgabewerte gleich wahrscheinlich ausgeben.

Wir bauen uns ein Rätsel!



Alle 2-stelligen Zahlenkombinationen

Was bedeutet das?

- Rätsel hat 7 Versuche benötigt (im Durchschnitt 10 Versuche)
- Überprüfung des Rätsels benötigt immer nur einen Versuch
- Schwierigkeit lässt sich beliebig anpassen (Grüner Bereich nur eine Zahl Knapp 100 Versuche für eine Lösung)
- Aber: Wenn alle versuchen, diese Rätsel zu lösen, wird es einer als erstes schaffen

Löst jeder das selbe Rätsel?

- Jeder hat die selbe Rätselschwierigkeit, aber nicht das selbe Rätsel. Das liegt daran, dass die Belohnung für das Rätsellösen an die eigene Adresse gezahlt wird und die ist immer unterschiedlich.

[1]Diese Funktion sollte alle Ausgabewerte gleich wahrscheinlich ausgeben.

Um was geht es heute?

BLOCKCHAIN Bayern e.V.

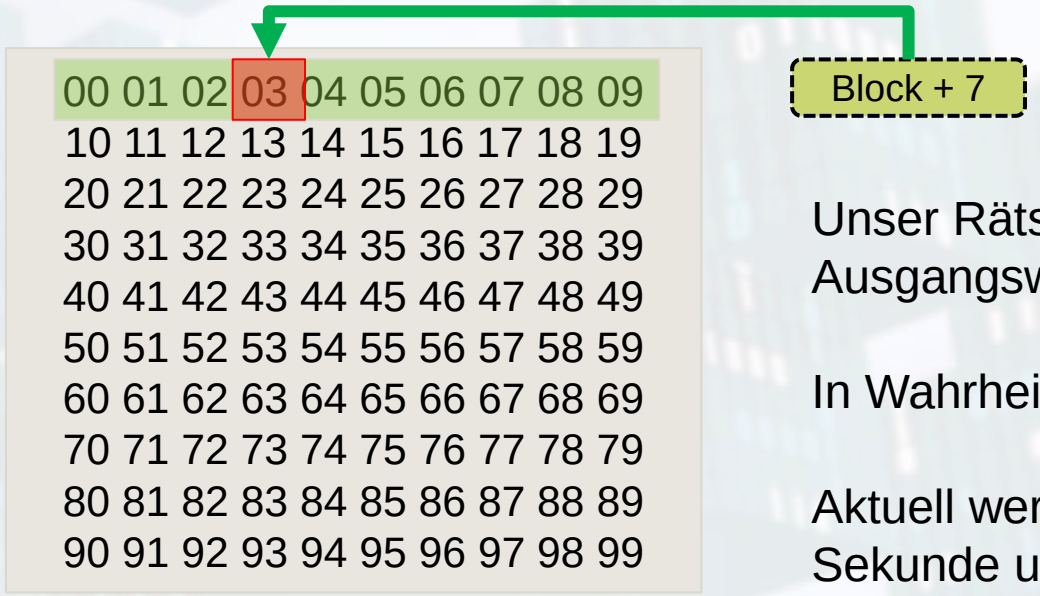
1. Woher weiß ich, wie viele Coins ich habe? Wie lese ich die Blockchain?
2. Wie sende ich Coins und warum bin ich nicht anonym?
3. Wie einigt sich das Netzwerk auf einen Zustand?
4. Warum verbraucht der Bitcoin und andere Kryptowährungen so viel Strom und warum ist es so sicher?

Um was geht es heute?

BLOCKCHAIN Bayern e.V.

4. Warum verbraucht der Bitcoin und andere Kryptowährungen so viel Strom und warum ist es so sicher?

Rätsel und der Energieverbrauch



Alle 2-stelligen Zahlenkombinationen

Unser Rätsel ist stark vereinfacht. Wir haben nur 100 mögliche Ausgangswerte, 10% dieser sind als Lösung zugelassen.

In Wahrheit gibt es 2^{256} Ausgangswerte. Unfassbar viel!

Aktuell werden 177 Millionen Billionen (10^{18}) Versuche pro Sekunde unternommen, um alle 10 Minuten eine neue Lösung zu finden. *Der Lösungsbereich ist unfassbar klein.*

Das macht das Netzwerk extrem sicher. Ein Angreifer müsste so viel Rechenleistung wie das gesamte Netzwerk aufbringen, um es erfolgreich zu attackieren.

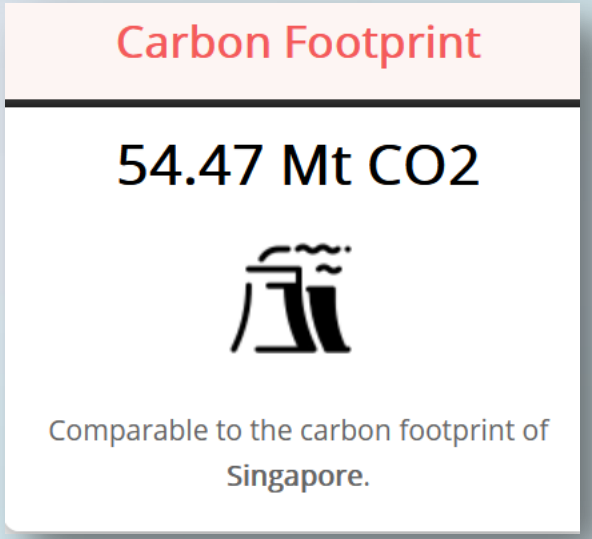
Aktueller Energieverbrauch: 148 TWh

Cambridge Bitcoin Electricity Consumption Index, https://cbeci.org/

Einordnung des Energieverbrauchs

- Stromverbrauch ist die eine Sache, CO^2-Ausstoß die andere.
- Der Stromverbrauch von Bitcoin hängt nicht von den Transaktionen ab, sondern von den Aufwänden für das Puzzle.
- Keine andere Kryptowährung oder Blockchain-Technologie verbraucht so viel Strom wie der Bitcoin.
- Viele andere Konsensmechanismen verbrauchen ähnlich viel Strom wie normale verteilte Datenbanken (~meist irrelevant wenig).
- Stromverbrauch / CO2-Ausstoß hochkomplexes Thema, das leider oft missverstanden wird.

Cambridge Bitcoin Electricity Consumption Index, https://cbeci.org/



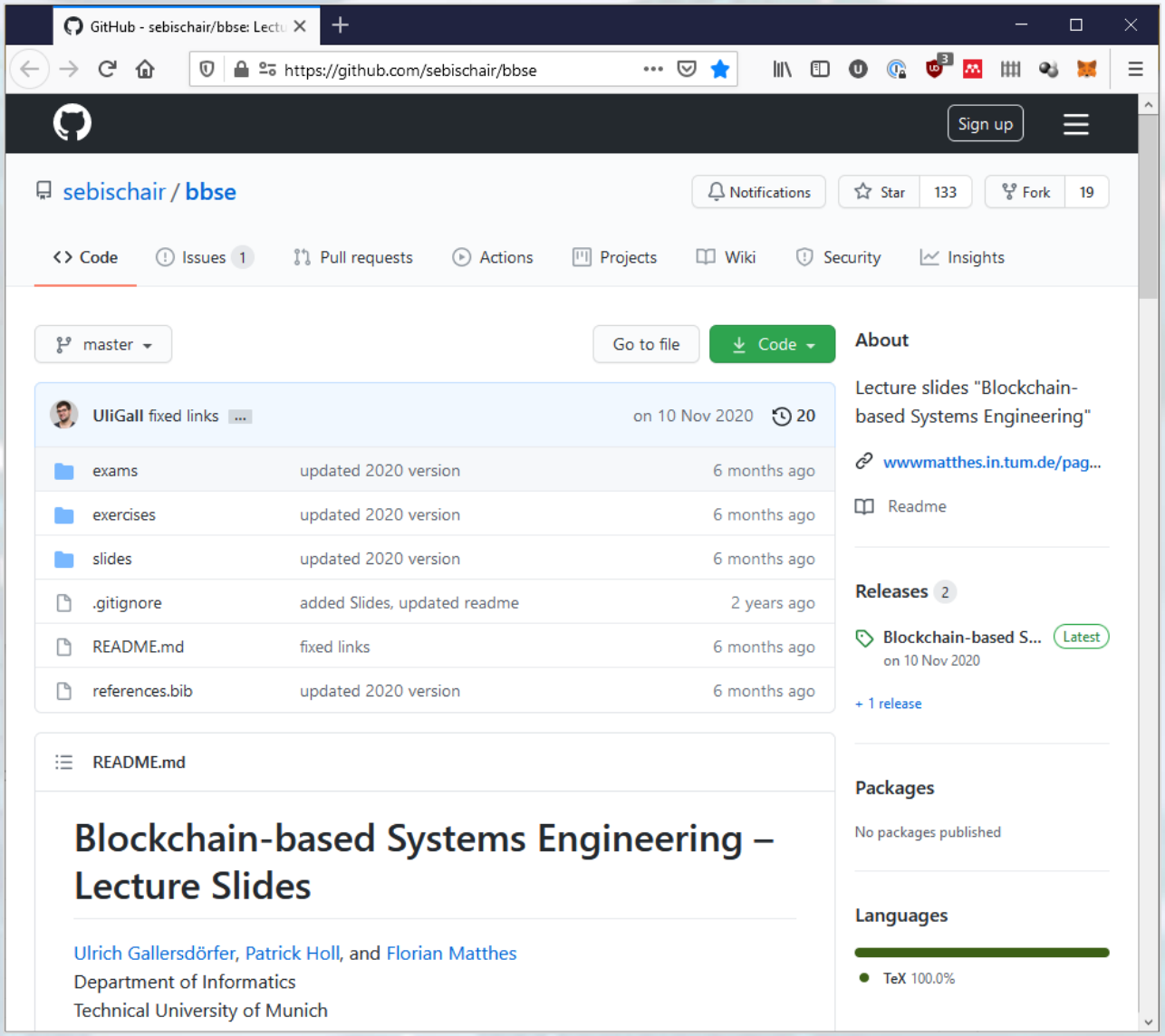
https://digiconomist.net/bitcoin-energy-consumption

Um was geht es heute?

BLOCKCHAIN Bayern e.V.

1. Woher weiß ich, wie viele Coins ich habe? Wie lese ich die Blockchain?
2. Wie sende ich Coins und warum bin ich nicht anonym?
3. Wie einigt sich das Netzwerk auf einen Zustand und warum ist es so sicher?
4. Warum verbraucht der Bitcoin und andere Kryptowährungen so viel Strom?

Sollten Sie noch nicht genug haben…



Unter folgendem Link finden Sie unsere Vorlesung:
https://github.com/sebischair/bbse

BLOCKCHAIN
Bayern e.V.

Wir bringen Blockchain in Bayern voran.

Vielen Dank.

Ihre Fragen an:
kontakt@blockchain-bayern.de

www.blockchain-bayern.de

Smart Contracts – Kurz erklärt

BLOCKCHAIN Bayern e.V.

Ulis Computer

Kontostände

0xacbde:	4
0xf137ba:	18
0xde61da:	8
0xc054ab:	5
0x12345:	12

Smart Contract

- Wird durch eine Transaktion erstellt (Code als “Beigabe”)
- Wird wie ein normales Konto behandelt
- Sobald installiert, reagiert er gemäß seines Codes
- Code unveränderlich, daher Bugs schlecht fixbar