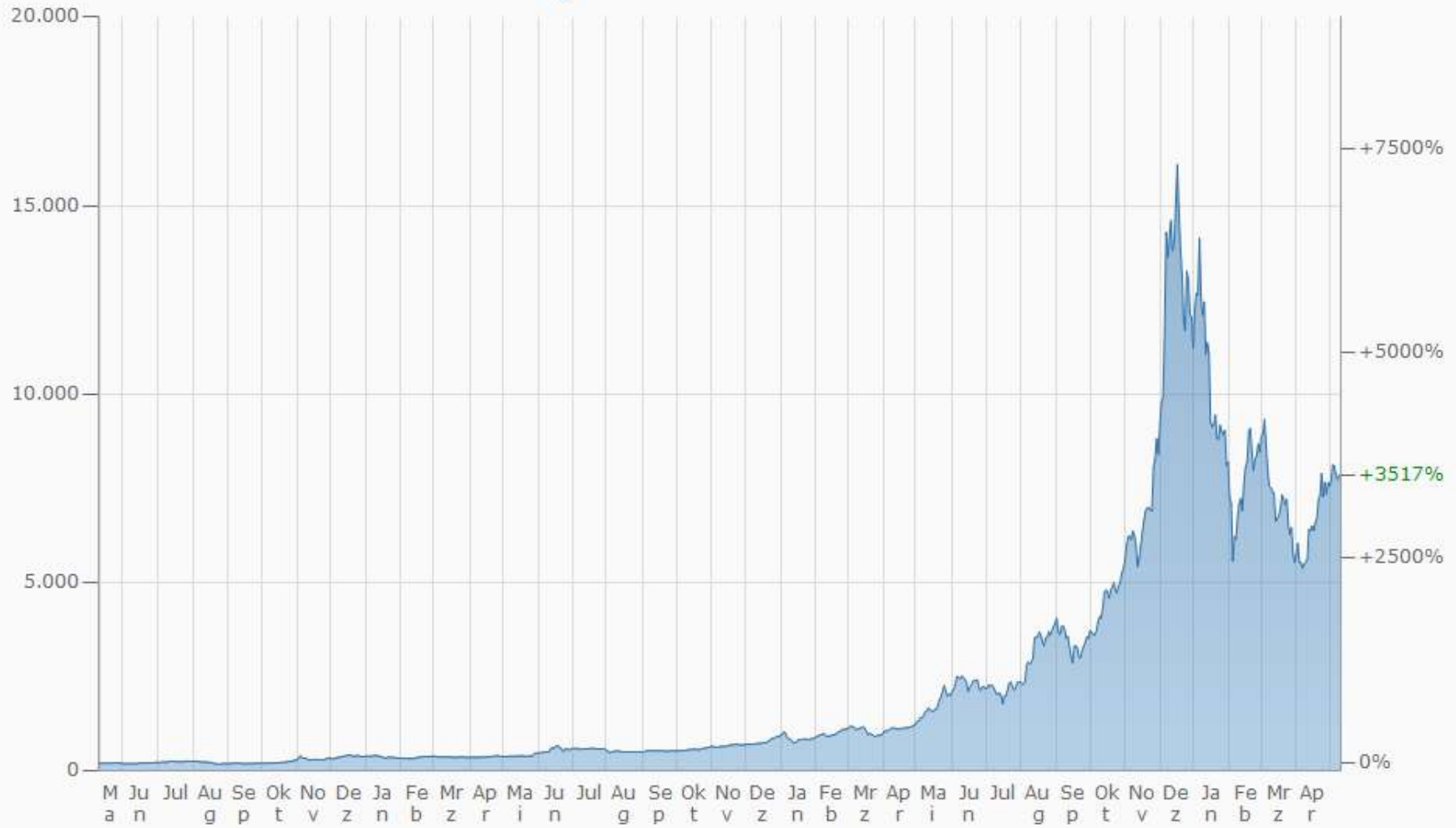


Blockchain im Unterricht

Wie funktionieren eigentlich Bitcoin
& Co.?

BITCOIN - EURO (BTC - EUR) CHART - 3 JAHRE

Intraday 1 Woche 1 Mon. 6 Mon. 1 Jahr 3 Jahre 5 Jahre Max



bitcoin

Alle

News

Bilder

Videos

Shopping

Mehr

Ungefähr 86.600.000 Ergebnisse (0,43 Sekunden)

bitcoin

Alle

News

Ungefähr 86.600.0



Bitcoin

Währung

Bitcoin ist eine digitale Währung, gleichzeitig auch der Name des weltweit verwendbaren dezentralen Buchungssystems sowie die vereinfachende Bezeichnung einer kryptografisch legitimierten Zuordnung von Arbeits- oder Rechenaufwand. [Wikipedia](#)

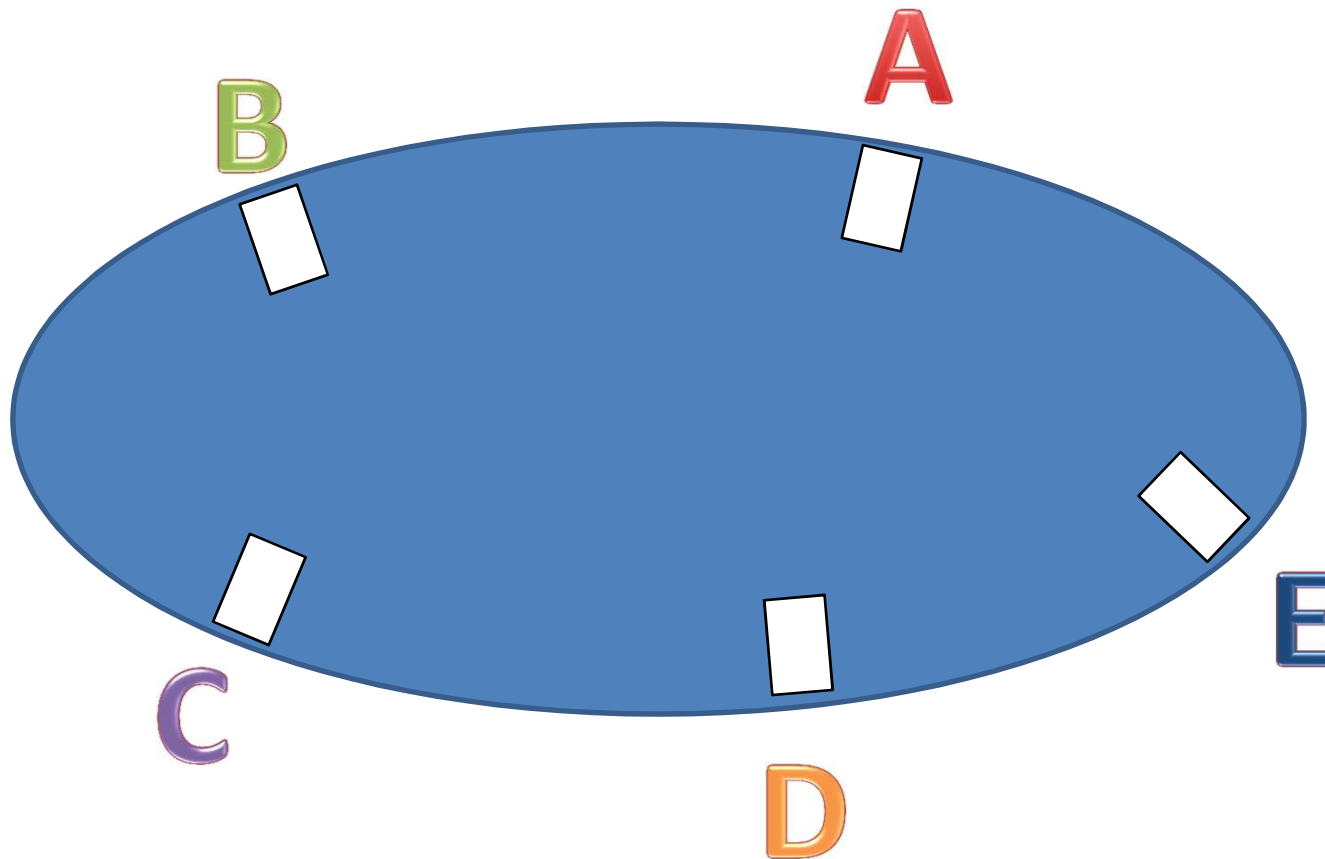
Mining: SHA-256

Blockchain: 160 GB (Stand 03/2018)

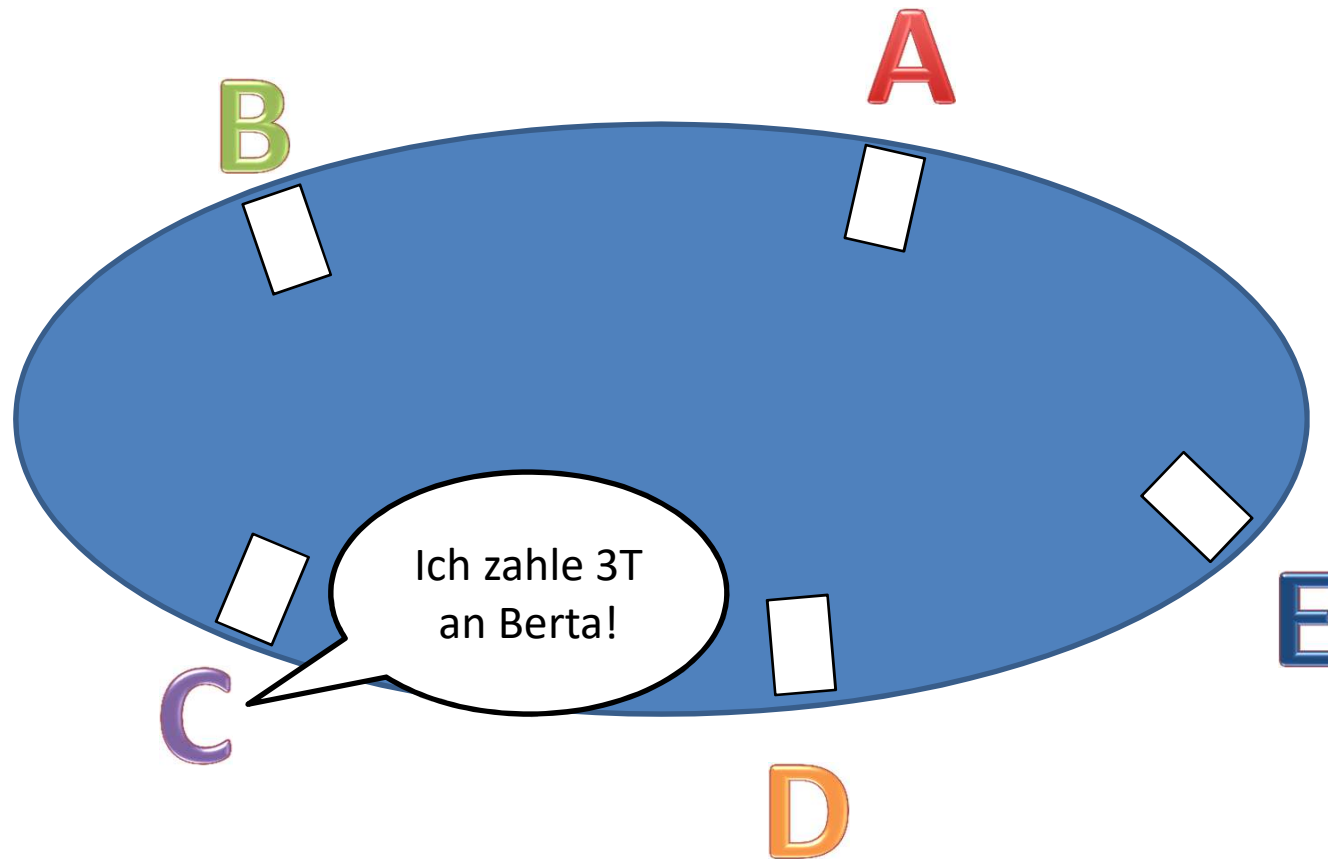
Erscheinungsjahr: 2009

Programmiersprache: C++

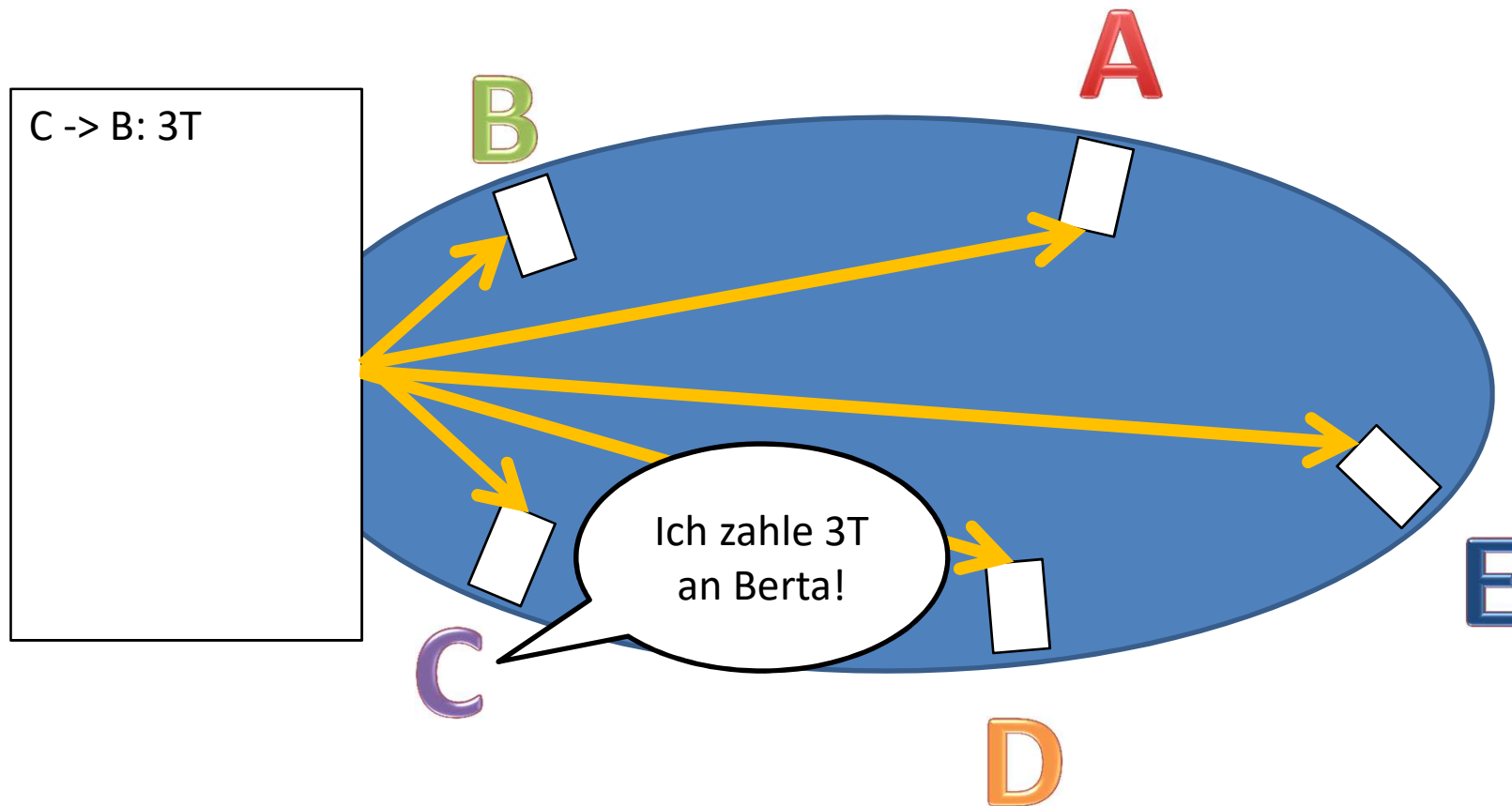
Kryptowährung verstehen ohne Programmierkenntnisse



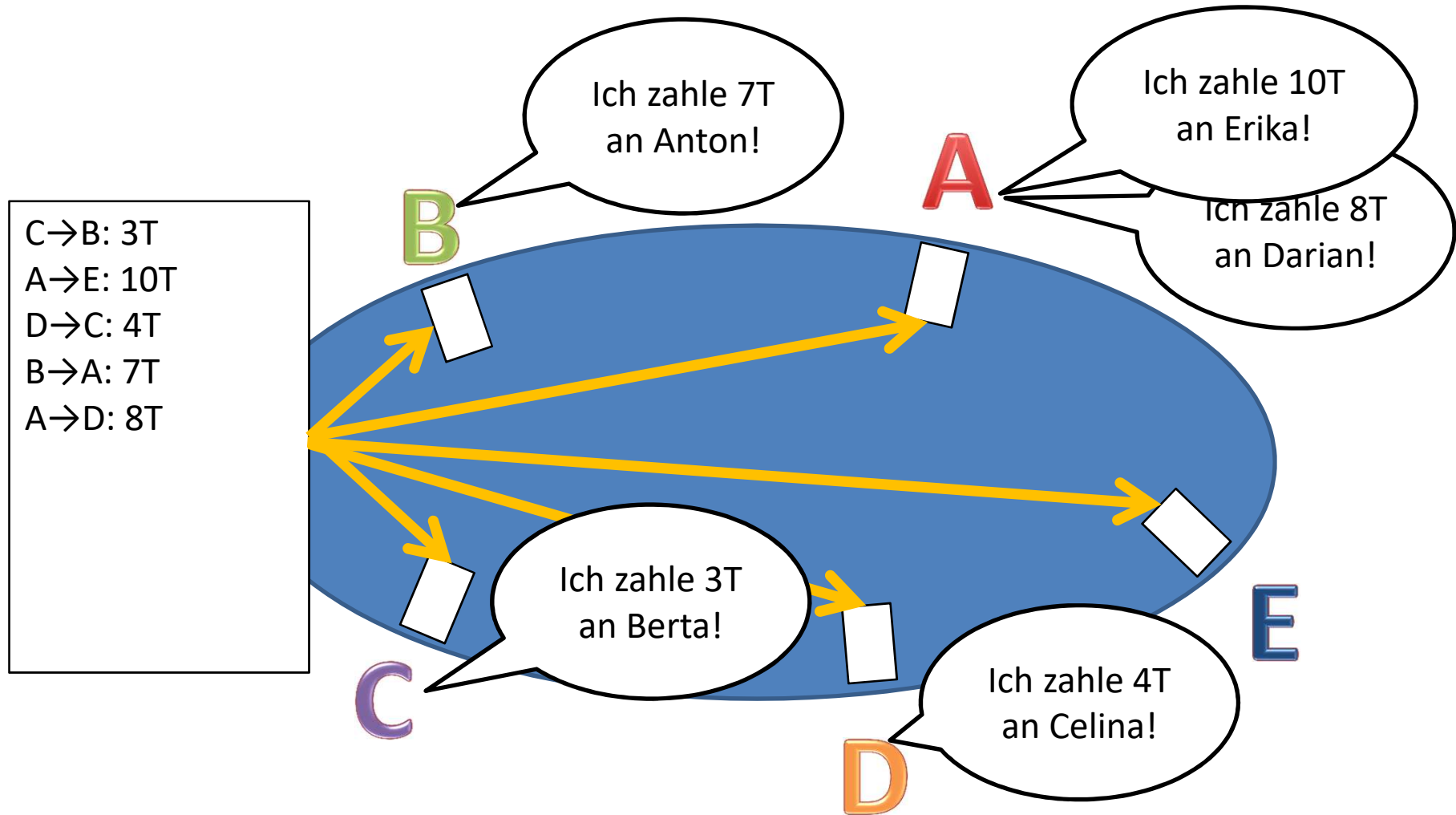
Kryptowährung verstehen ohne Programmierkenntnisse



Kryptowährung verstehen ohne Programmierkenntnisse



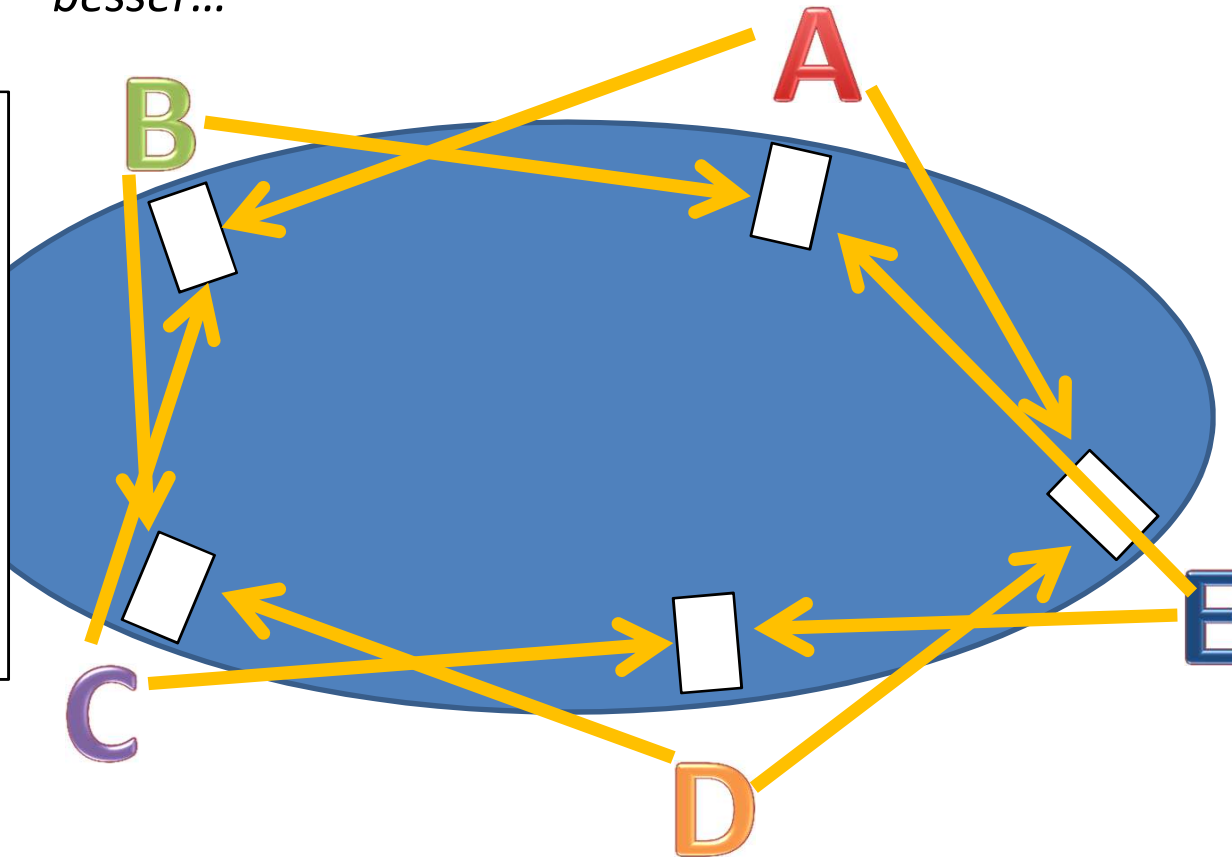
Kryptowährung verstehen ohne Programmierkenntnisse



Kryptowährung verstehen ohne Programmierkenntnisse

Vertrauen ist gut, Kontrolle ist besser...

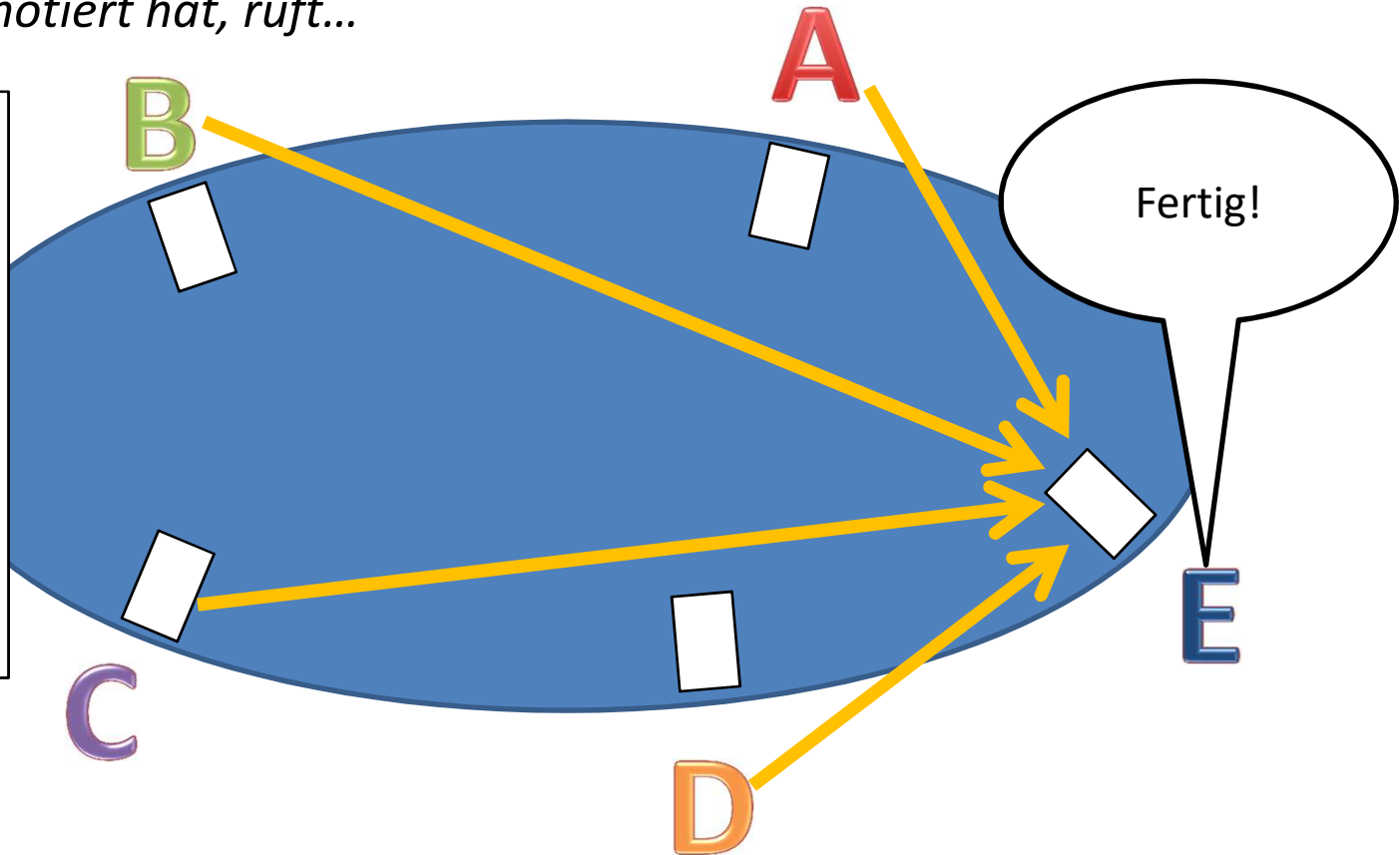
C → B: 3T
A → E: 10T
D → C: 4T
B → A: 7T
A → D: 8T



Kryptowährung verstehen ohne Programmierkenntnisse

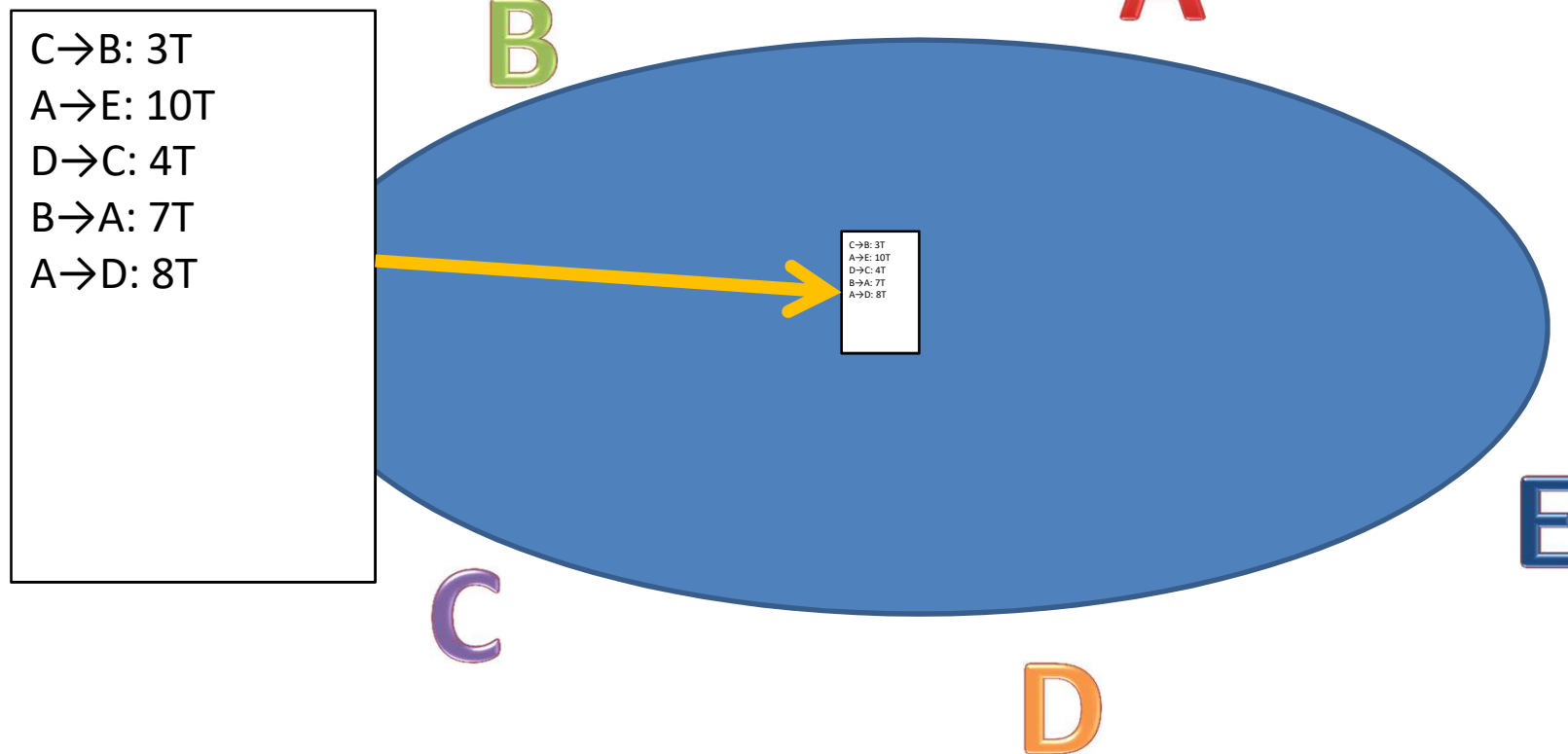
Alle 10 Minuten: Zettel abgeben
Wer als Erstes alle Transaktionen
notiert hat, ruft...

- C → B: 3T
- A → E: 10T
- D → C: 4T
- B → A: 7T
- A → D: 8T



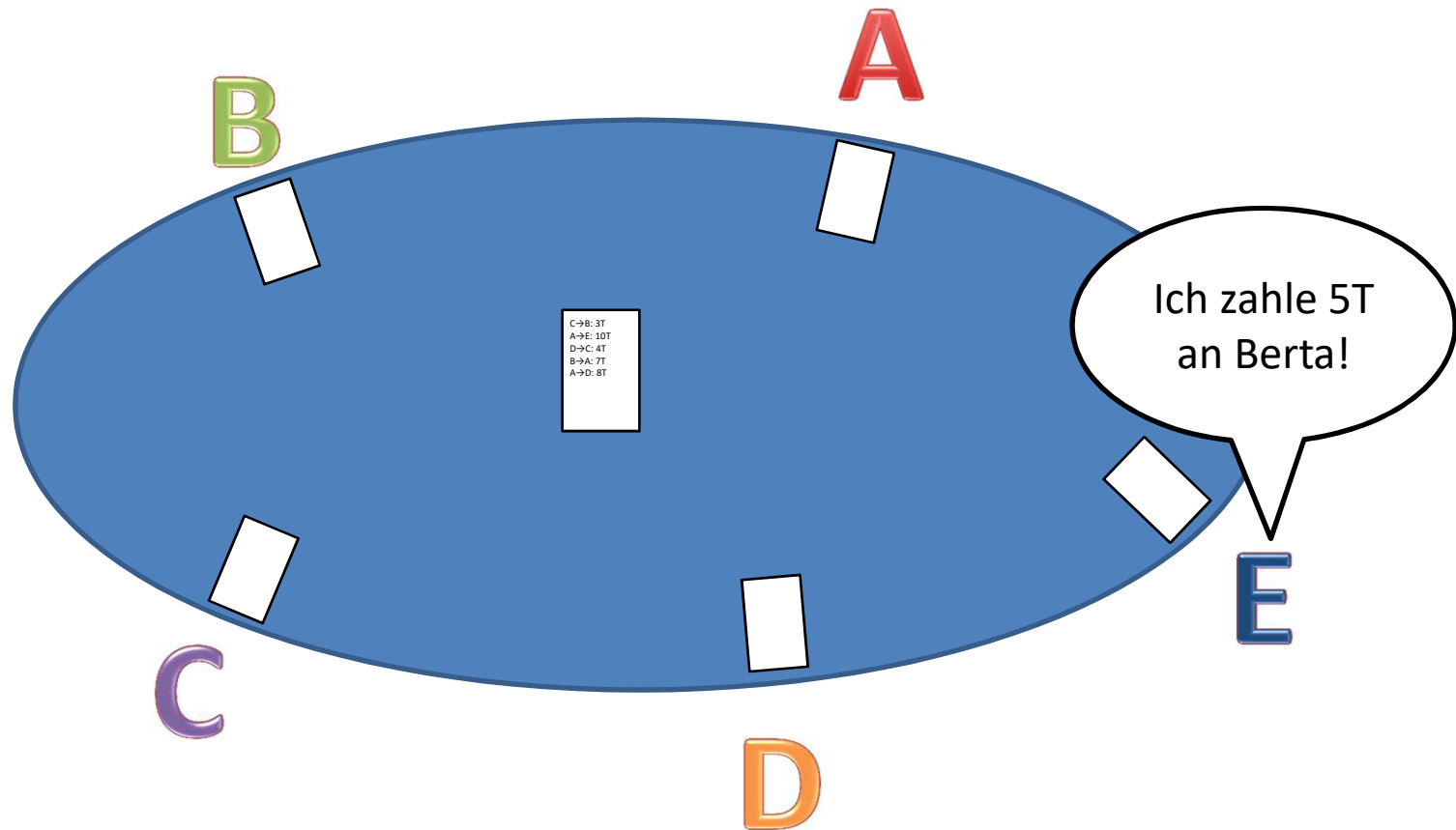
Kryptowährung verstehen ohne Programmierkenntnisse

Alle geben ihren Zettel ab, der bestätigte Zettel kommt als neue Seite ins Transaktionsbuch...

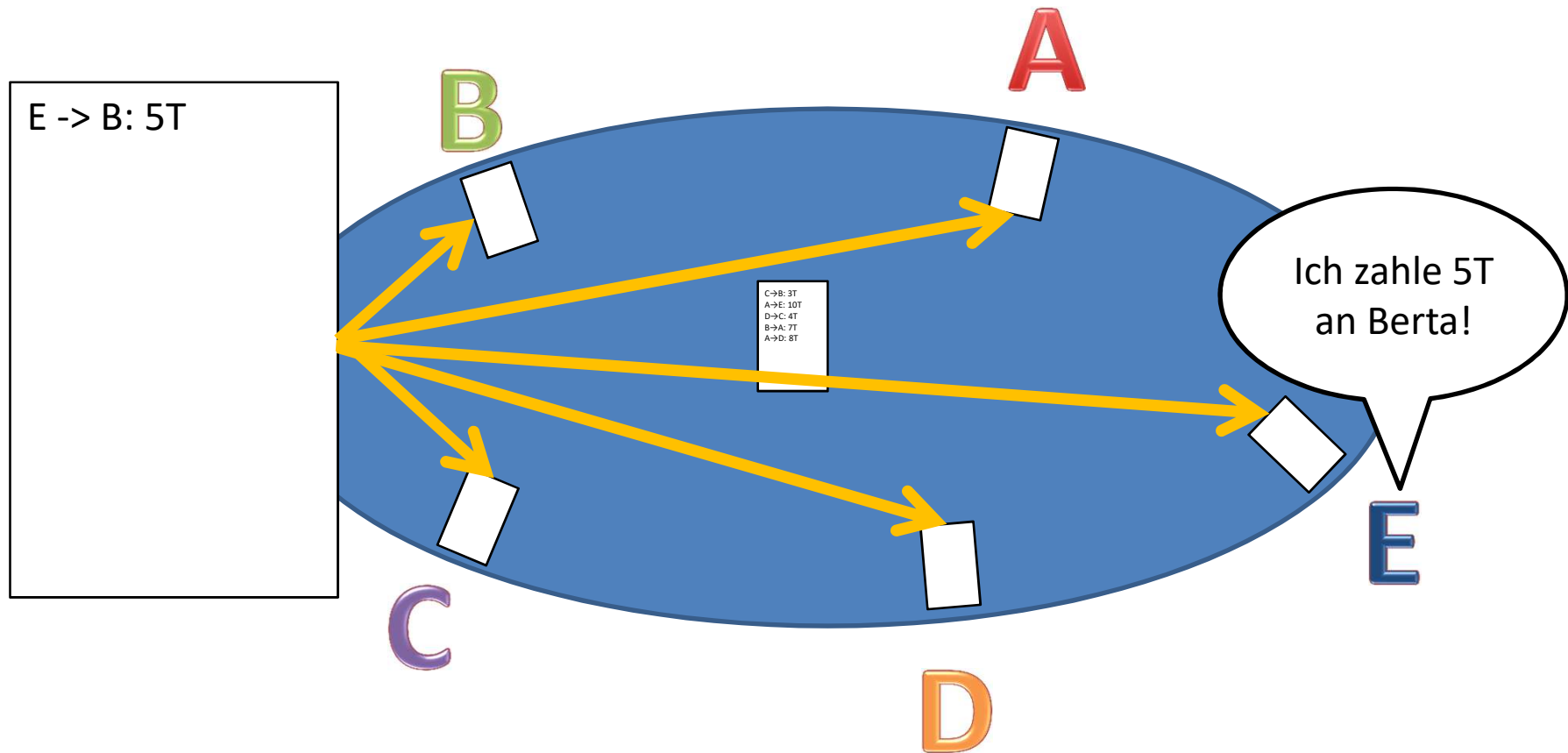


Kryptowährung verstehen ohne Programmierkenntnisse

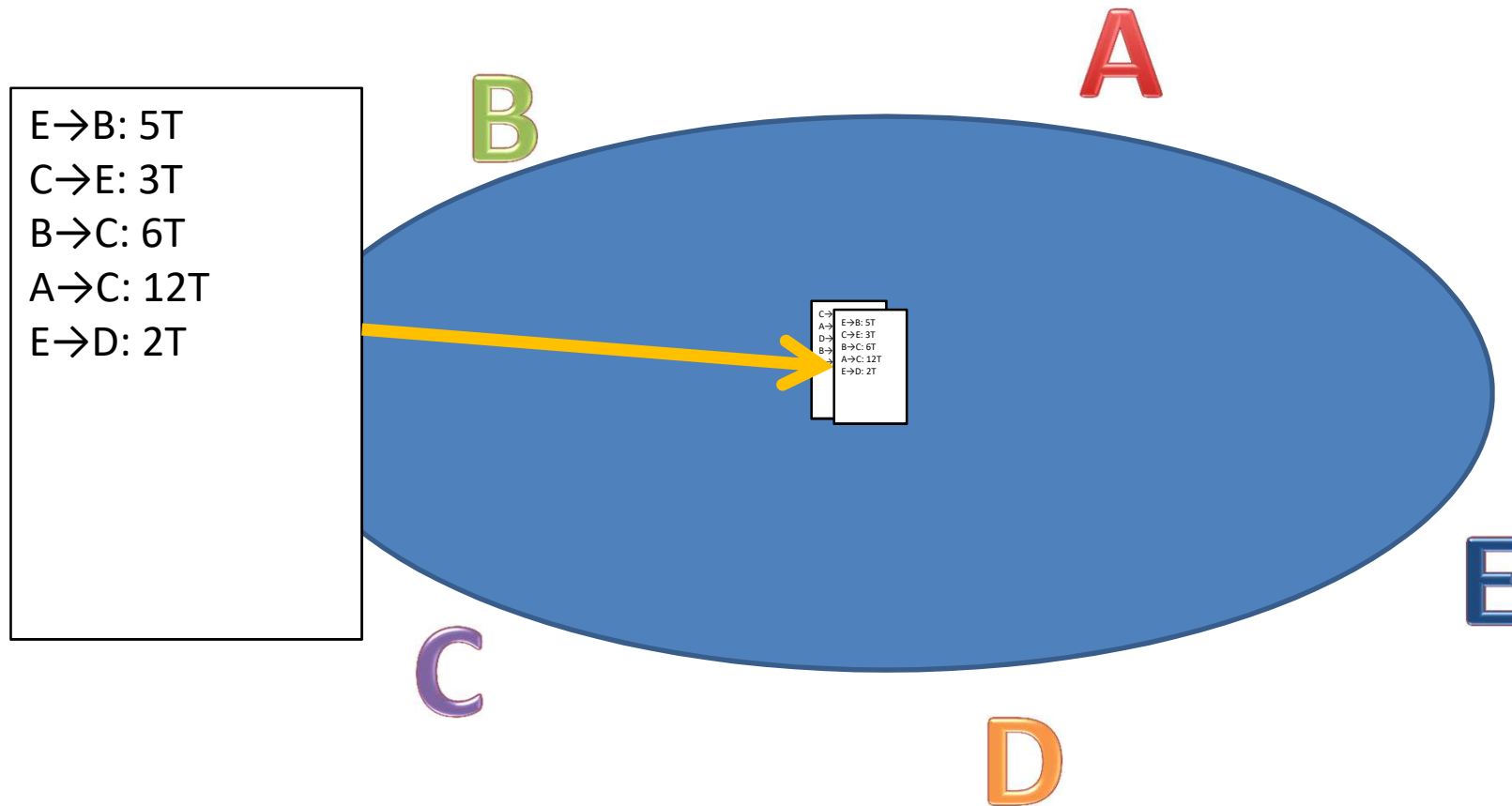
...und es geht wieder von vorne los...



Kryptowährung verstehen ohne Programmierkenntnisse

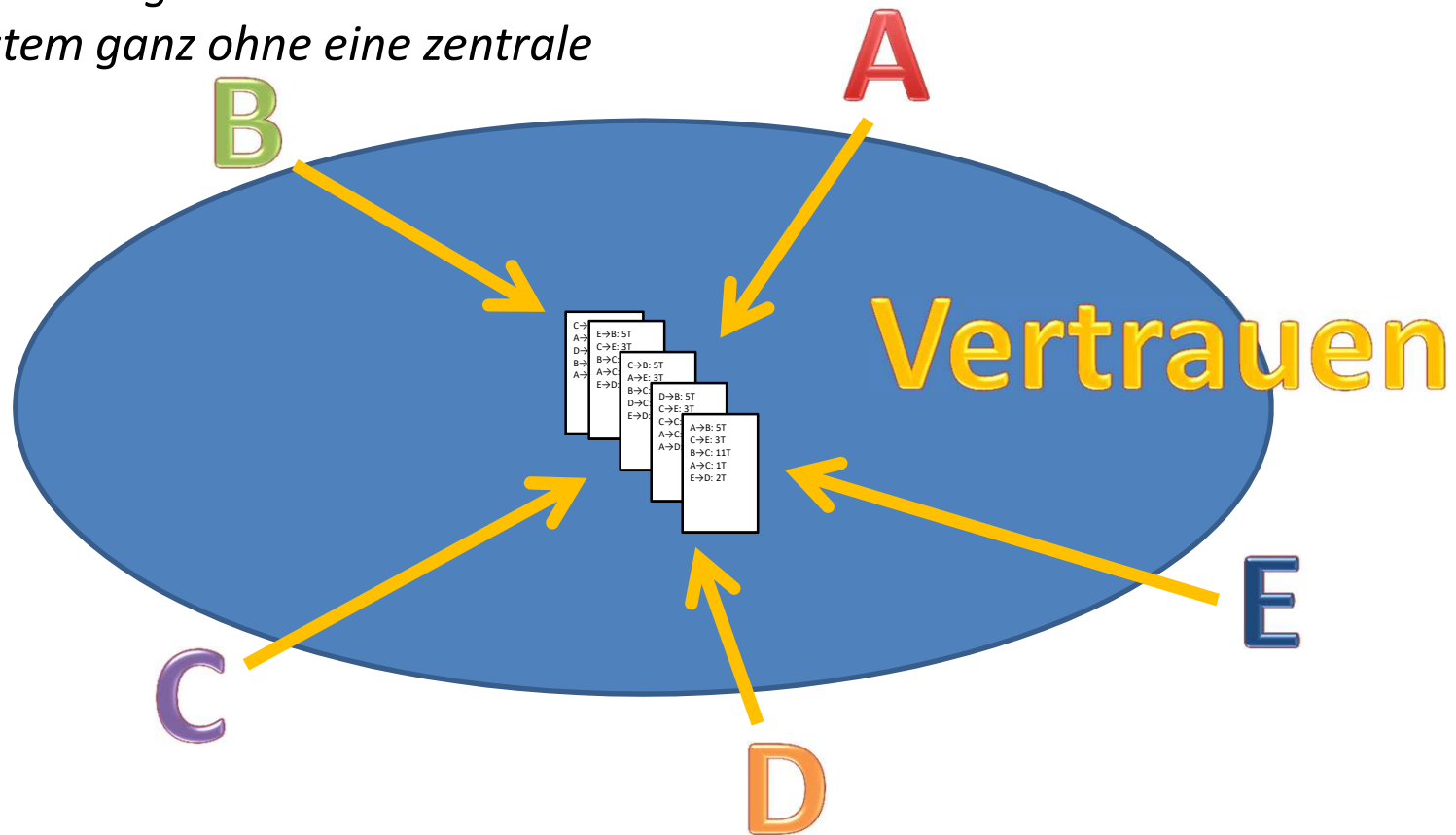


Kryptowährung verstehen ohne Programmierkenntnisse



Kryptowährung verstehen ohne Programmierkenntnisse

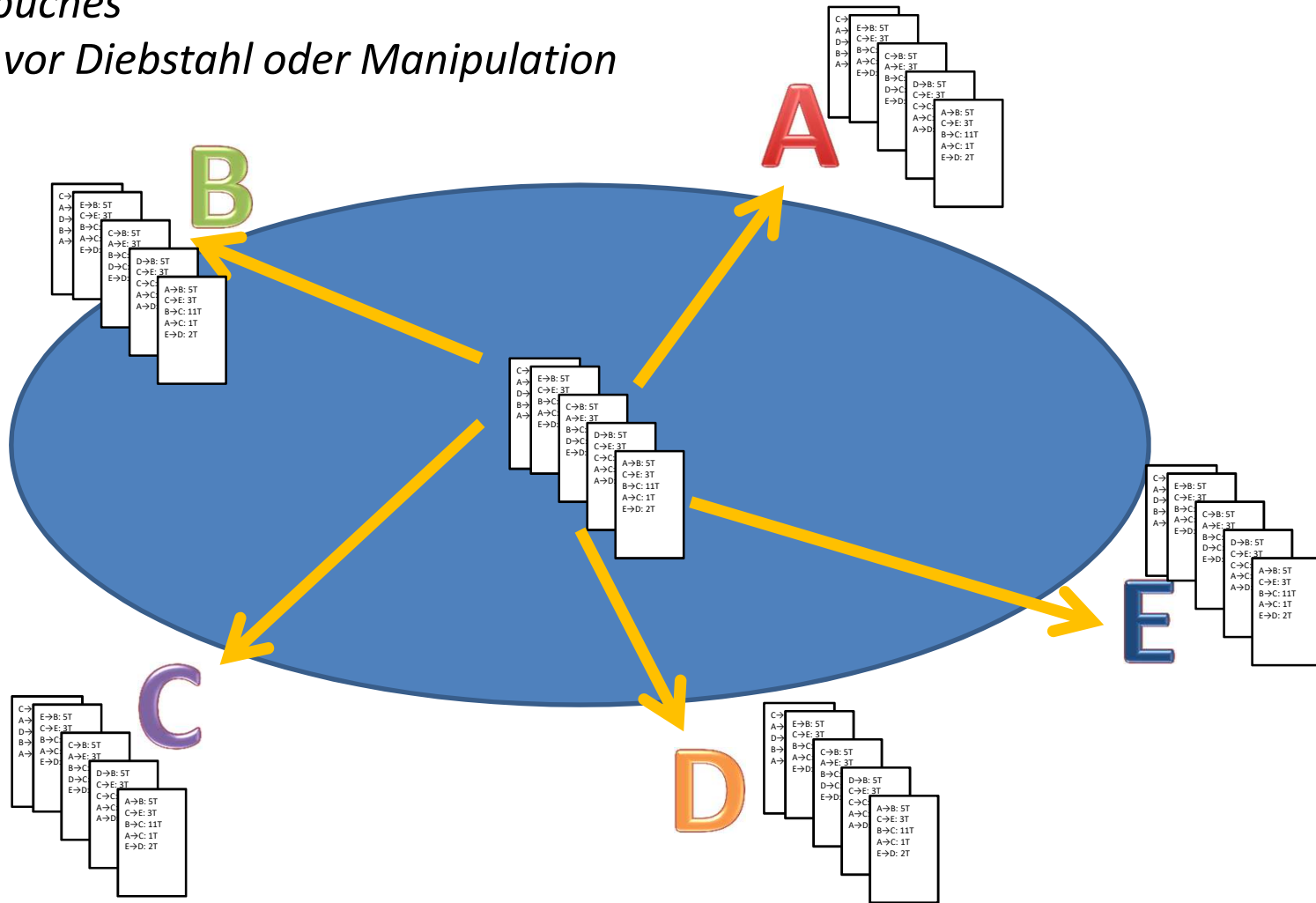
*In der Mitte liegt ein Transaktionsbuch dessen Korrektheit alle Teilnehmer bestätigen können
=> Vertrauen in das gemeinsame Währungssystem ganz ohne eine zentrale Institution*



Kryptowährung verstehen ohne Programmierkenntnisse

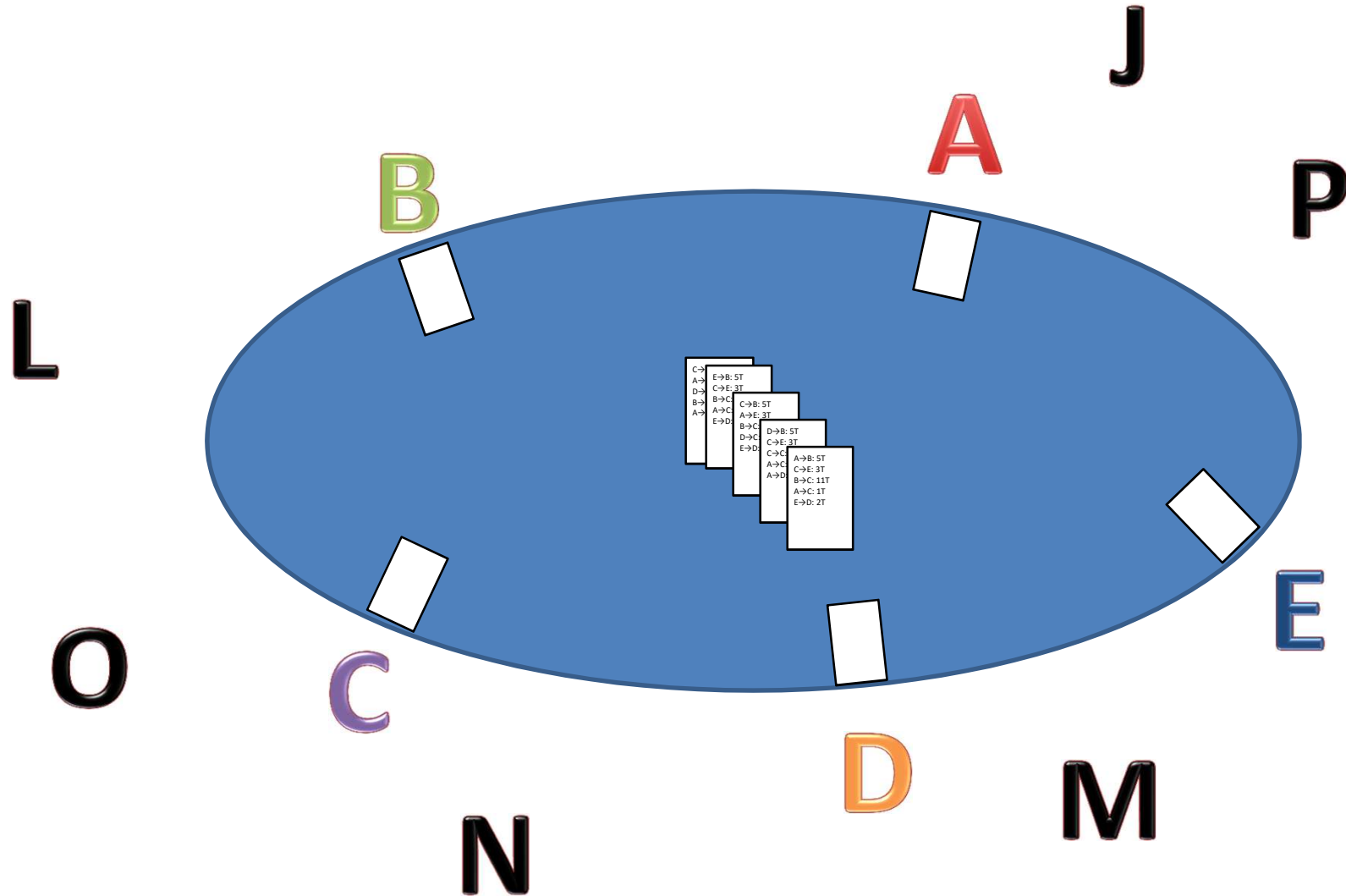
Jeder Teilnehmer hat eine Kopie des Transaktionsbuches

=> Sicherheit vor Diebstahl oder Manipulation



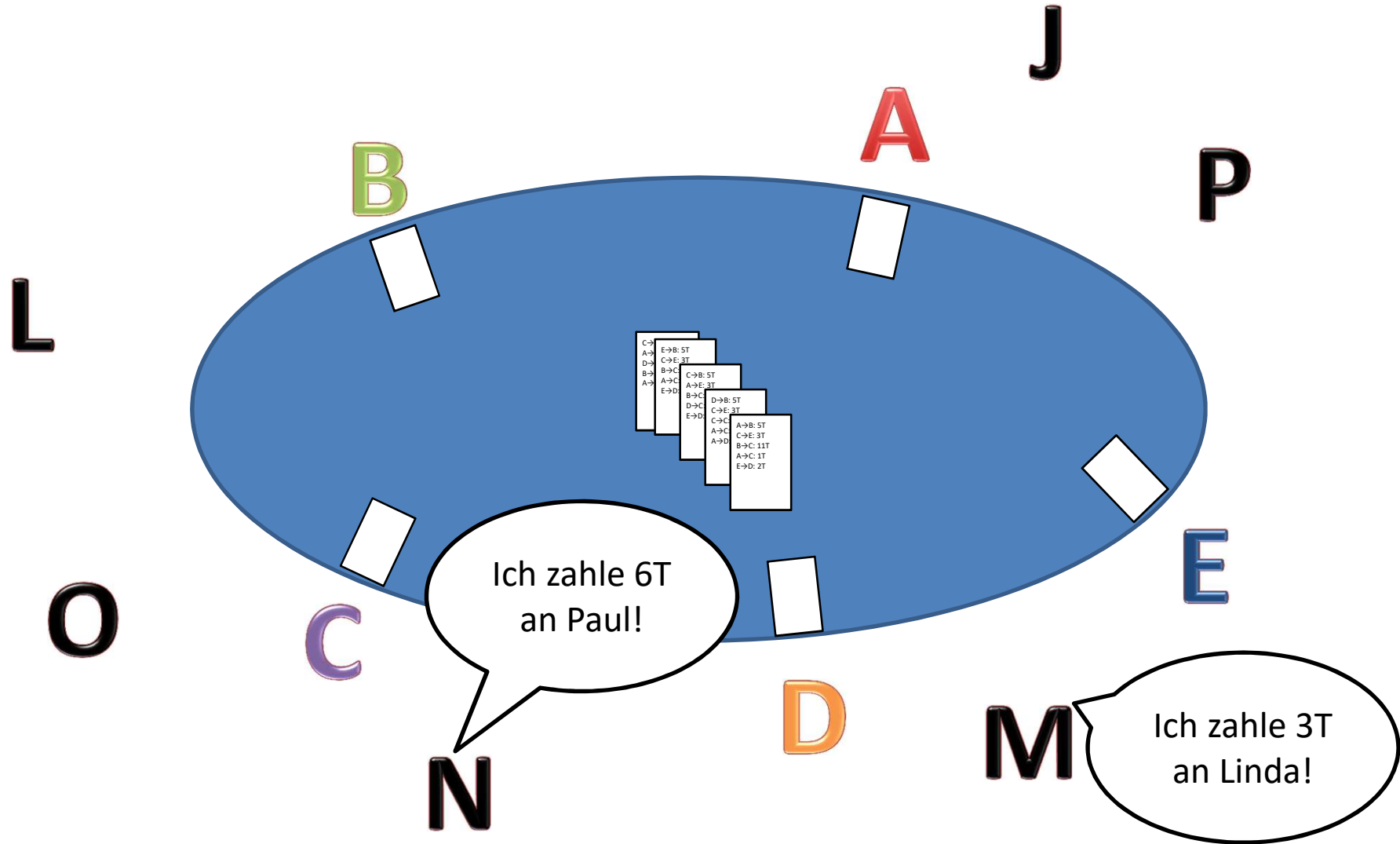
Kryptowährung verstehen ohne Programmierkenntnisse

Passive Nutzer kommen hinzu...



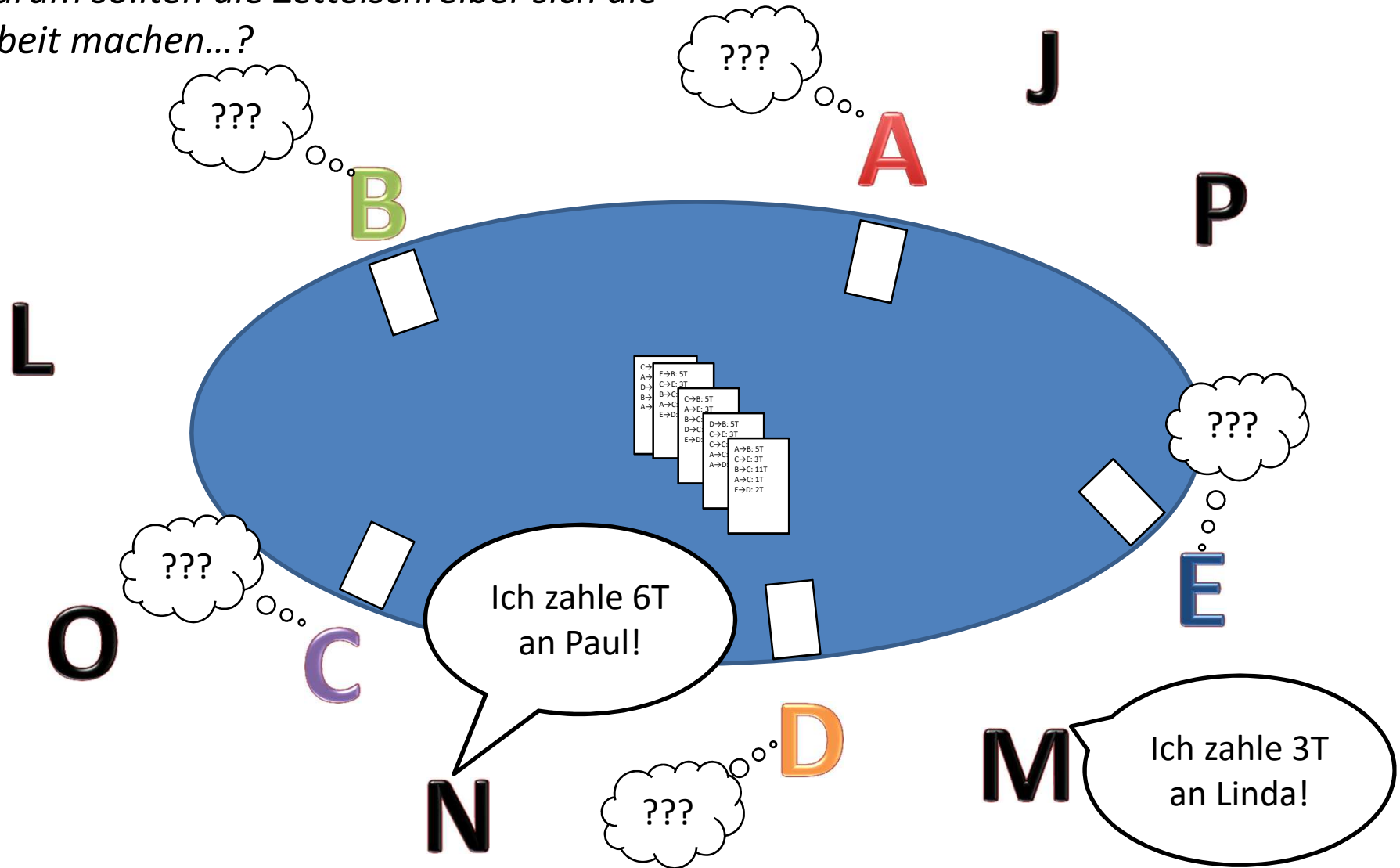
Kryptowährung verstehen ohne Programmierkenntnisse

Passive Nutzer kommen hinzu...



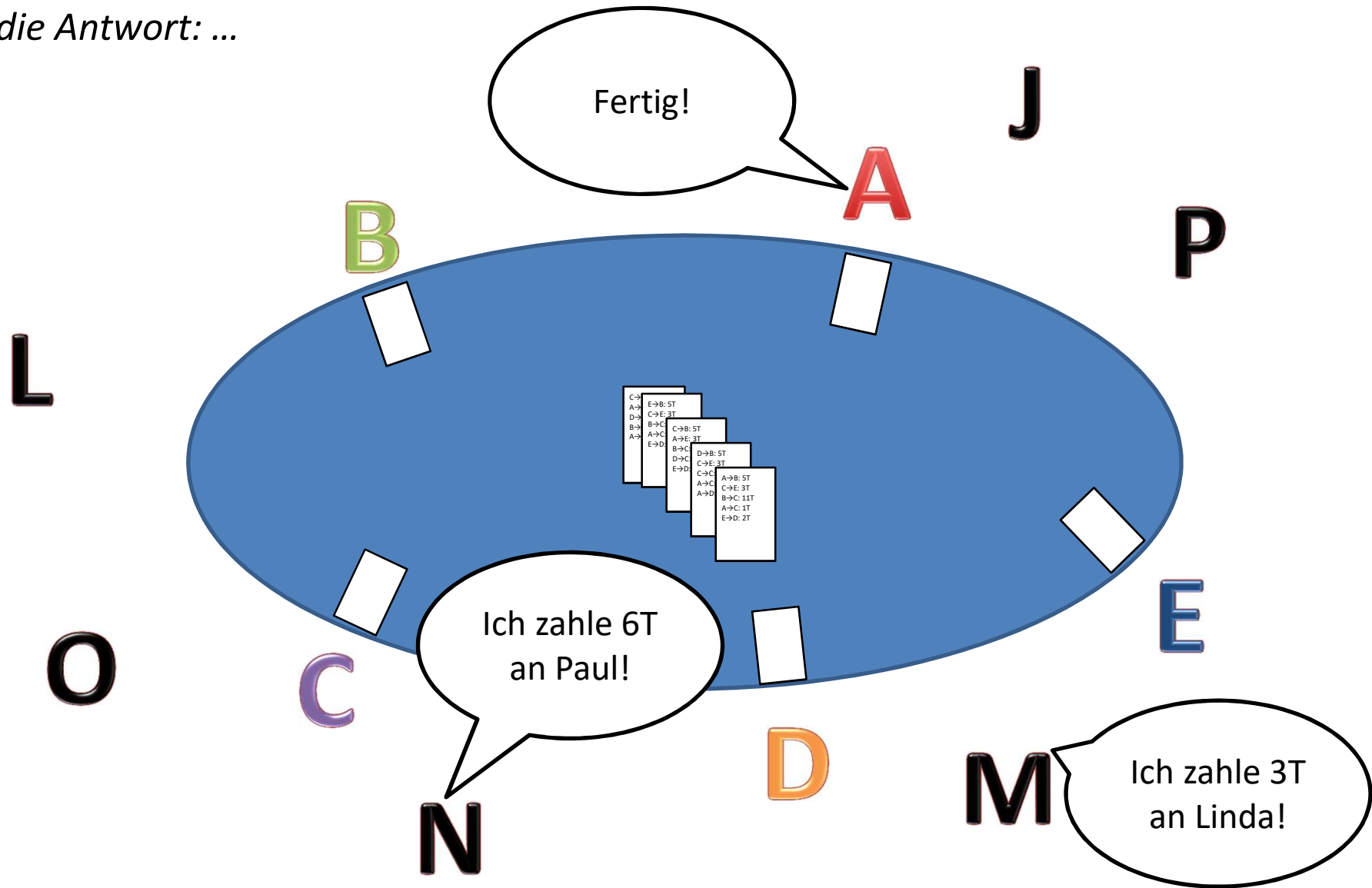
Kryptowährung verstehen ohne Programmierkenntnisse

Warum sollten die Zettelschreiber sich die Arbeit machen...?



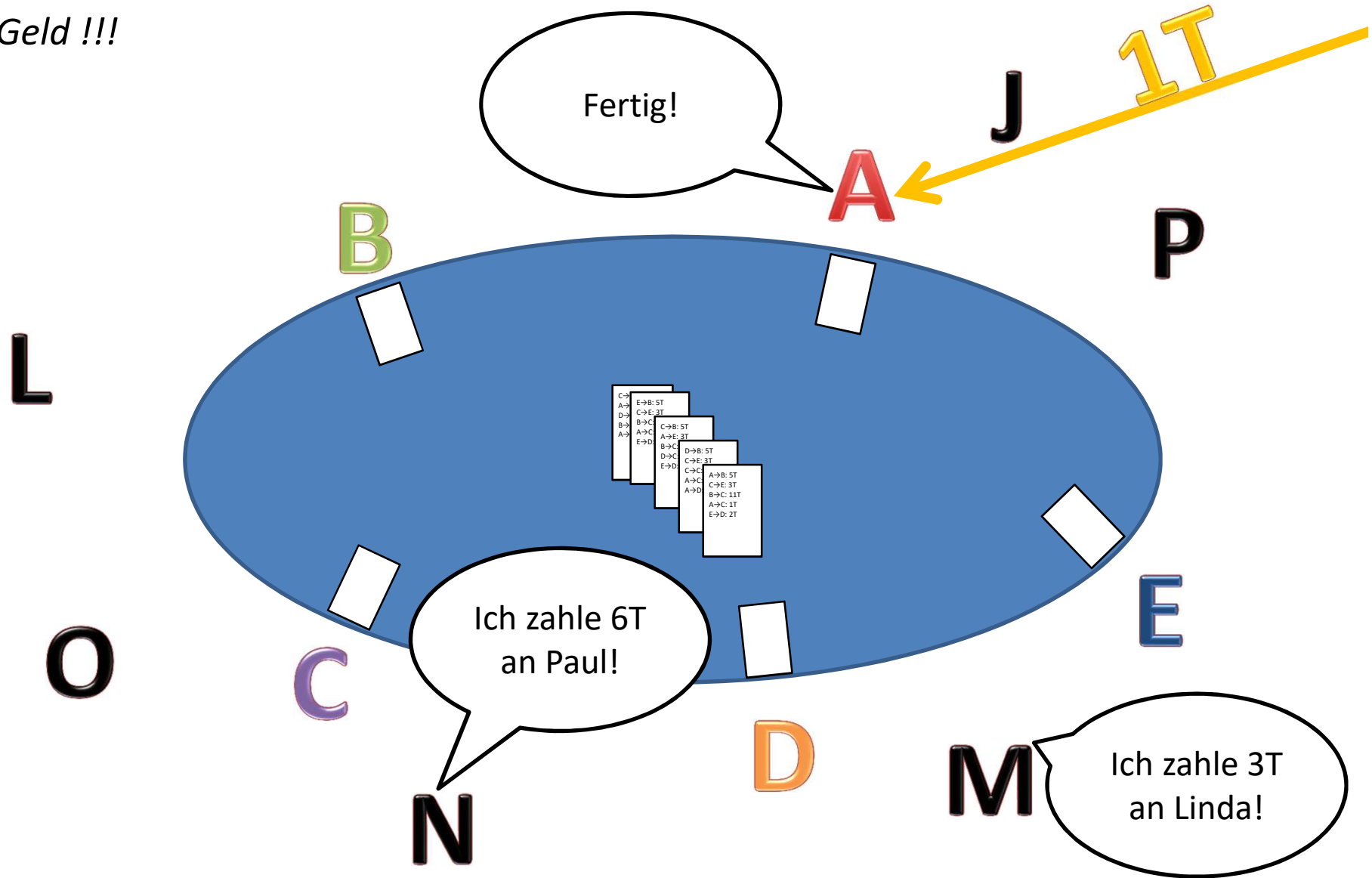
Kryptowährung verstehen ohne Programmierkenntnisse

... die Antwort: ...



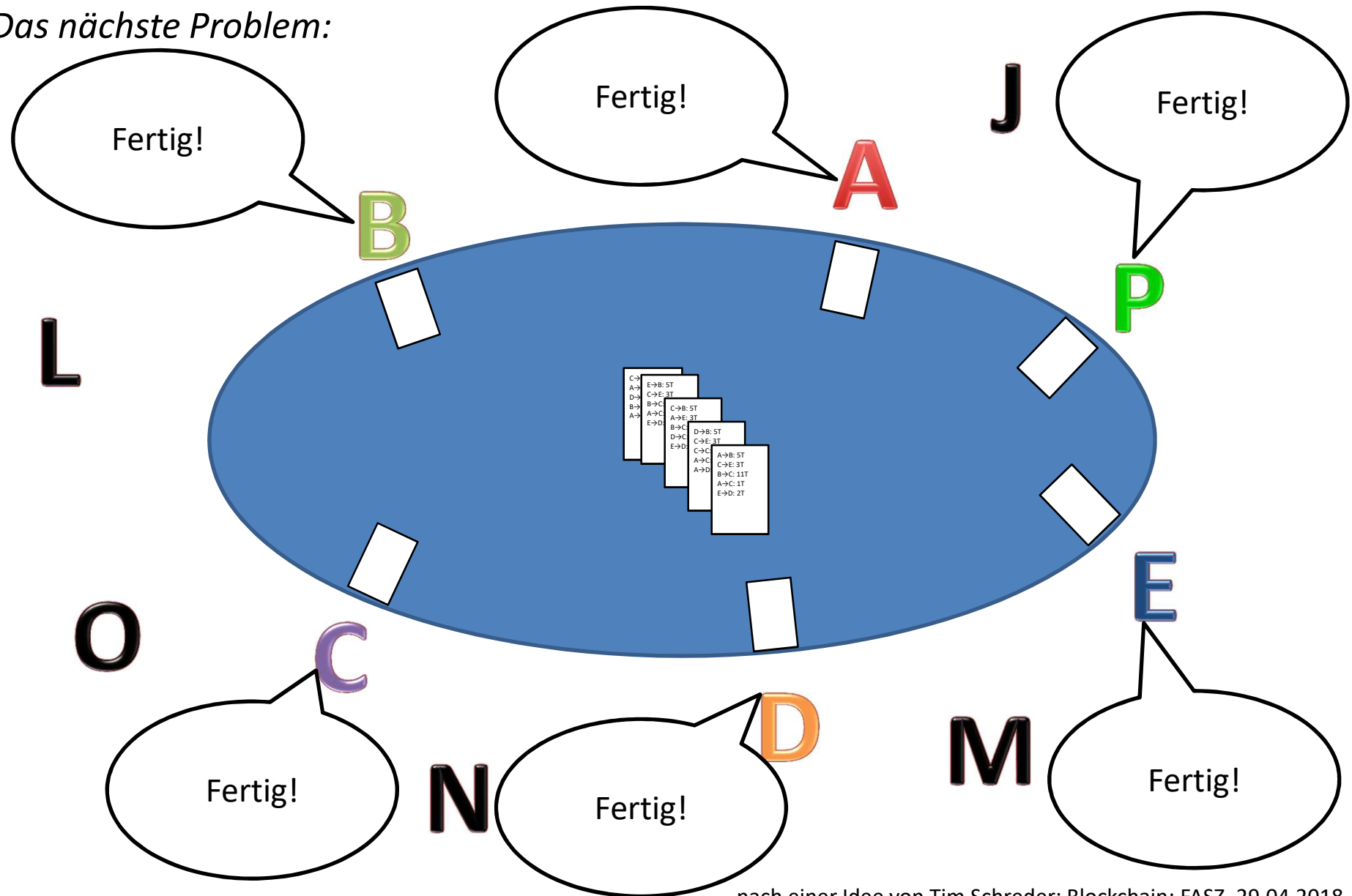
Kryptowährung verstehen ohne Programmierkenntnisse

... Geld !!!



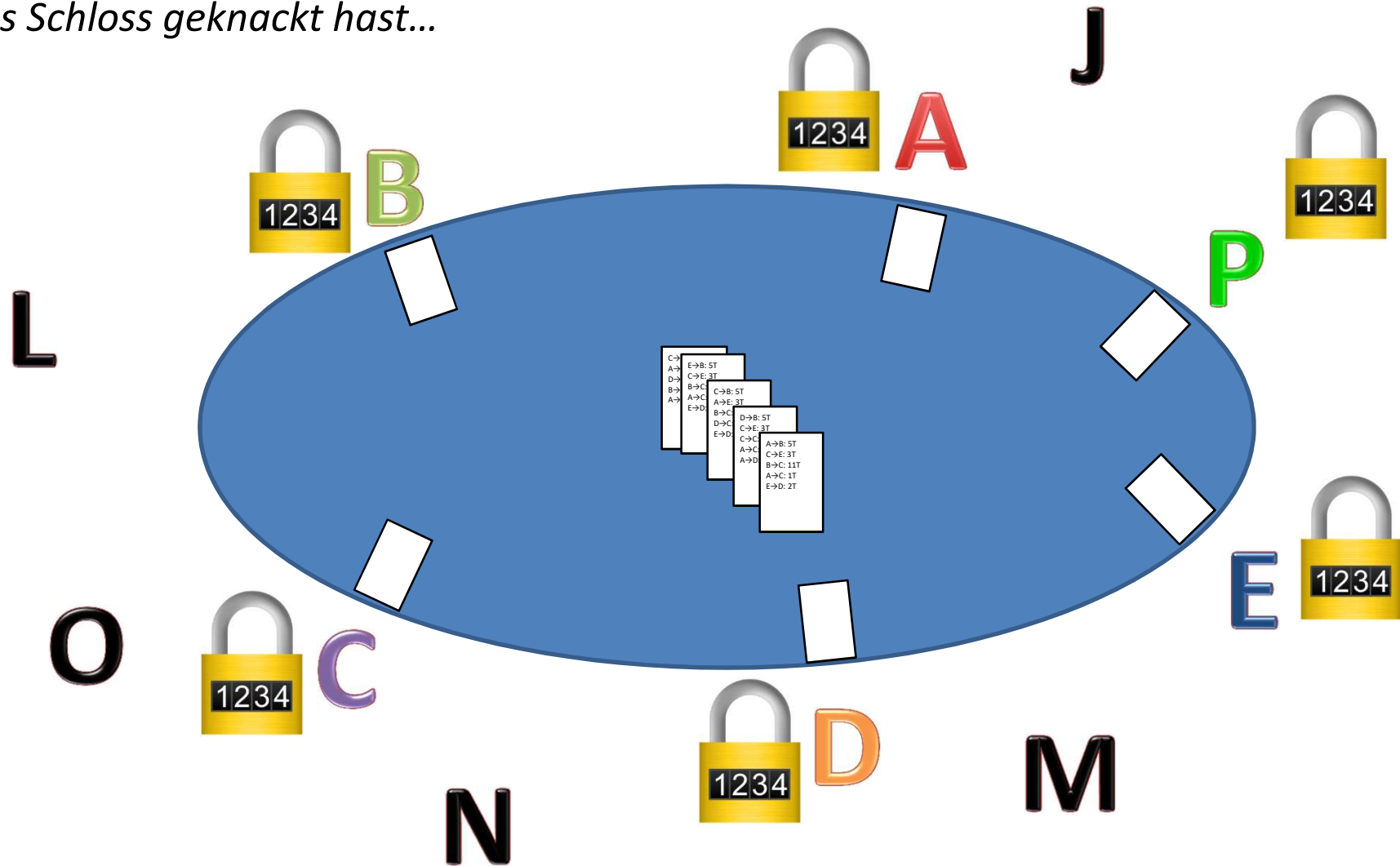
Kryptowährung verstehen ohne Programmierkenntnisse

Das nächste Problem:



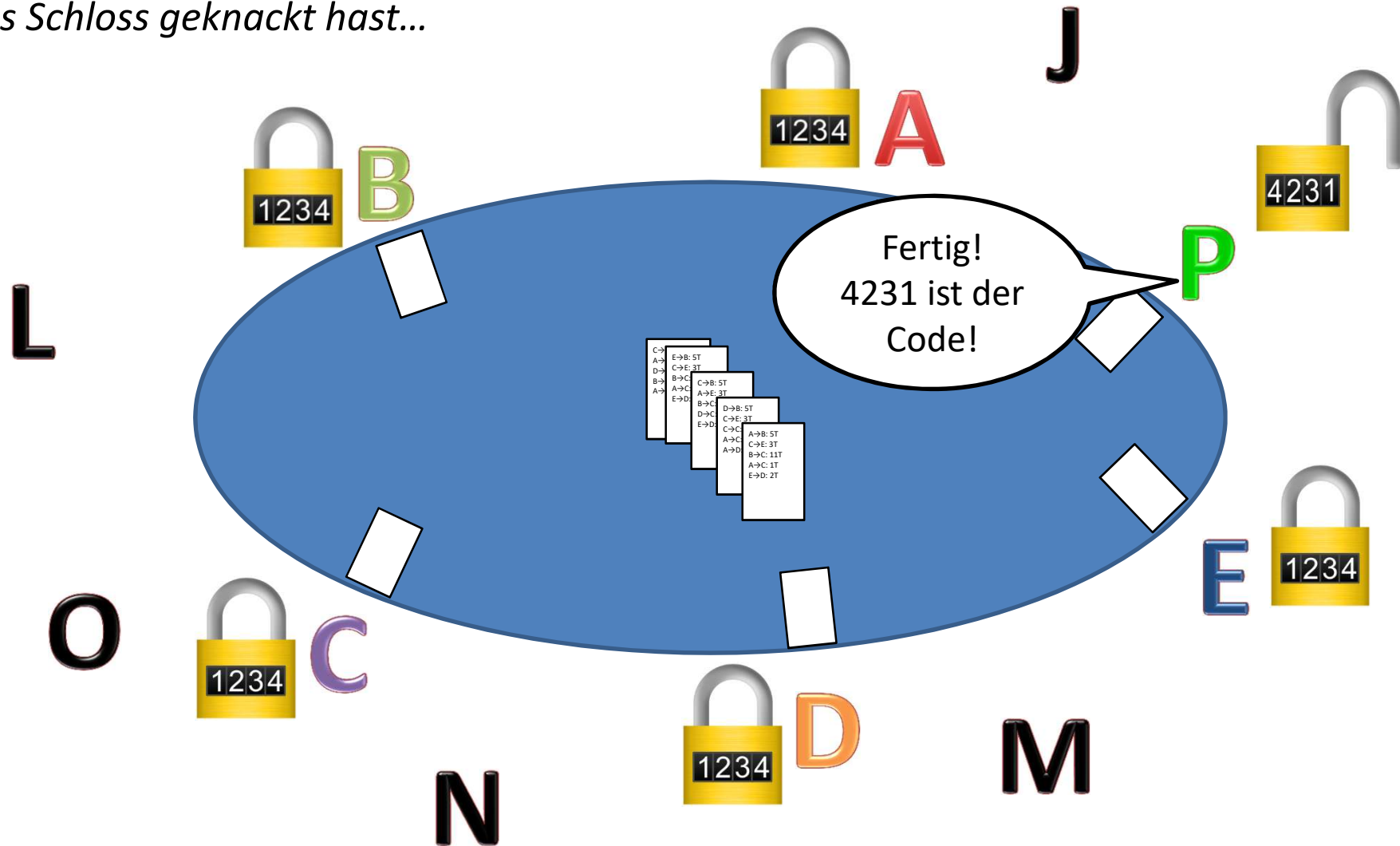
Kryptowährung verstehen ohne Programmierkenntnisse

Lösung: Du bist erst fertig, wenn du zusätzlich das Schloss geknackt hast...



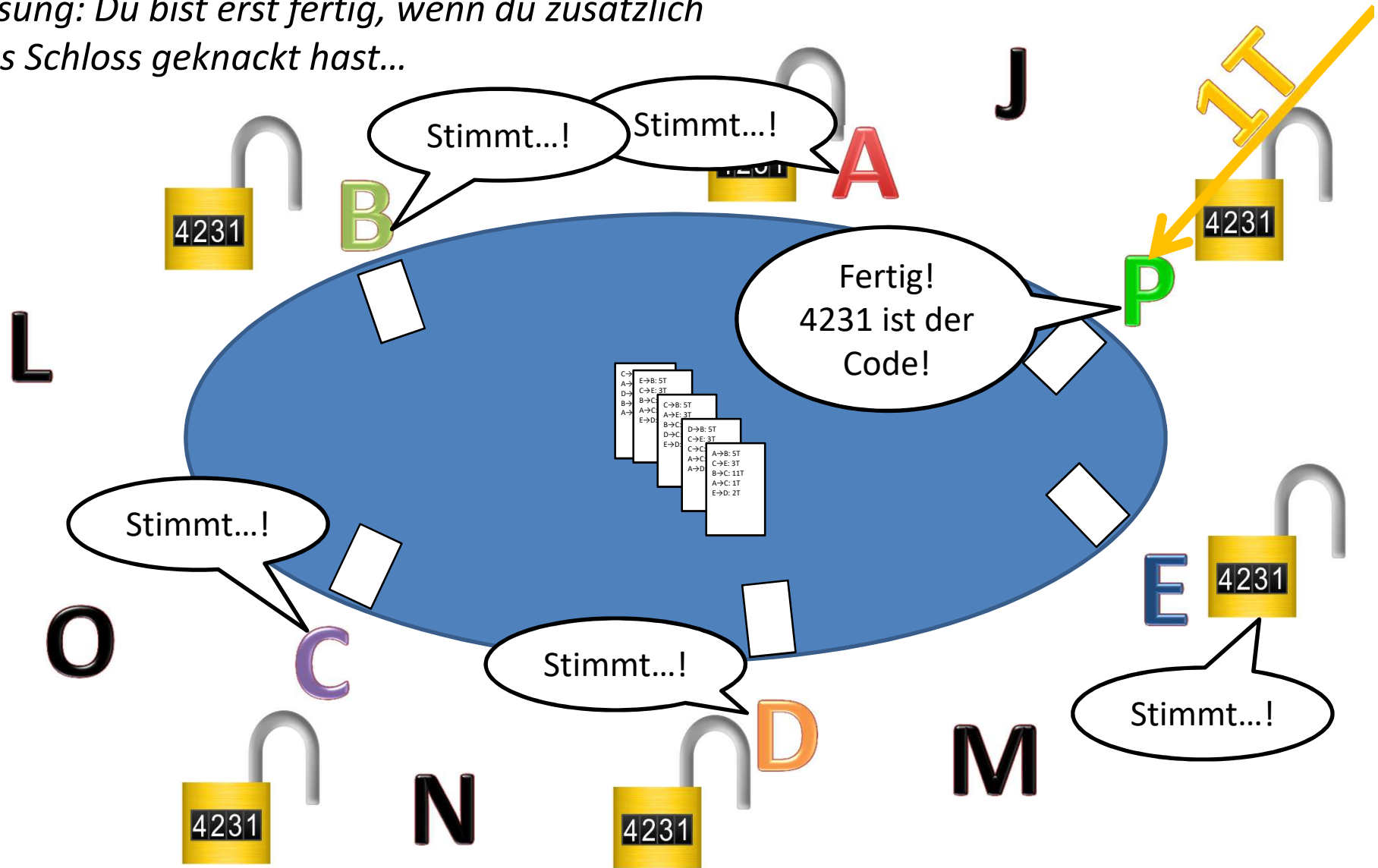
Kryptowährung verstehen ohne Programmierkenntnisse

Lösung: Du bist erst fertig, wenn du zusätzlich das Schloss geknackt hast...



Kryptowährung verstehen ohne Programmierkenntnisse

Lösung: Du bist erst fertig, wenn du zusätzlich das Schloss geknackt hast...



Zusammenhang zu Bitcoin

- Blockchain: Transaktionsbuch ([168GB](#))
- Miner: Aktive Nutzer
- Mining: „Schloss knacken“
- 10 Minuten: 10 Minuten
- Kryptowährung / digitale Währung:

Bitcoin, Ethereum, Ripple, Bitcoin Cash, EOS, Litecoin, Cardano, Stellar, Iota, Tron

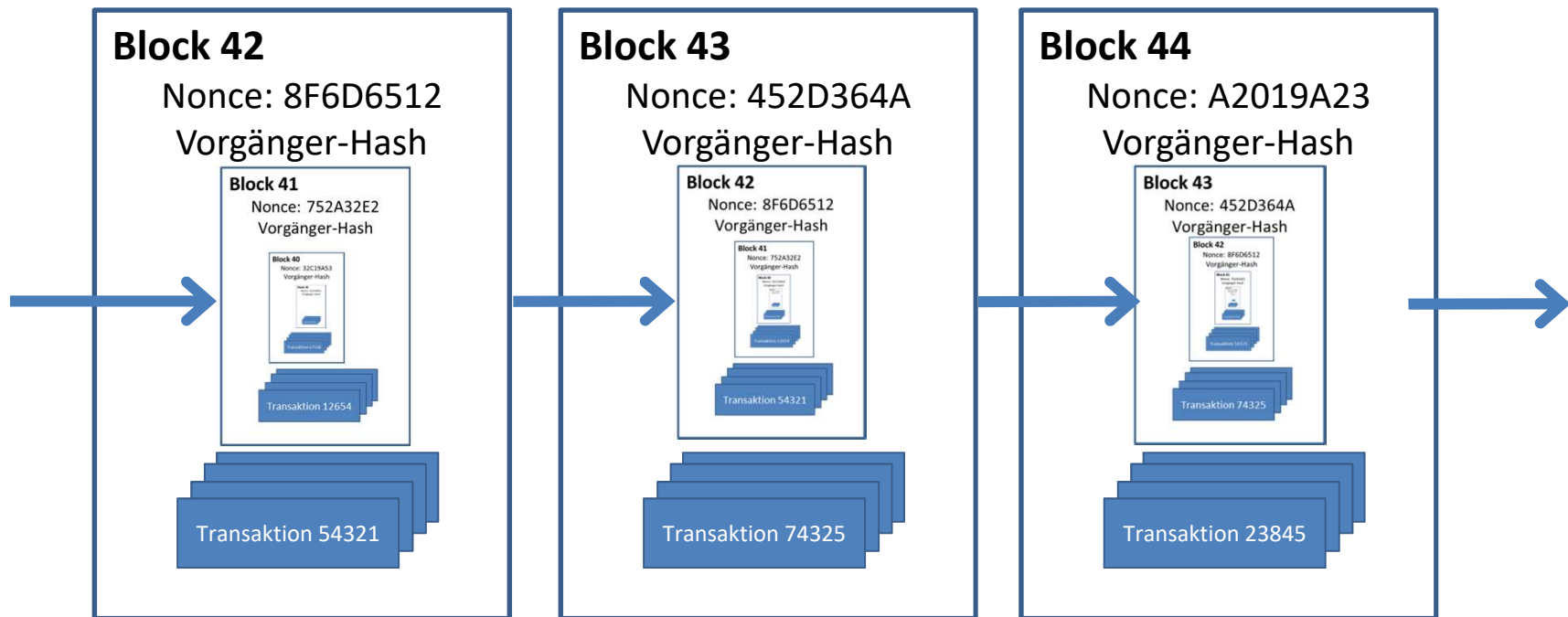
Blockchain

- chain: Kette
- Eine kontinuierlich erweiterbare Liste von Datensätzen, wobei jedes Kettenglied mit allen anderen vorher verknüpft ist.
- Unterschied zu herkömmlichen Datenbanken:
Die Änderung eines Kettenglieds macht die Änderung aller folgenden Kettenglieder notwendig => Manipulationssicherheit

Blockchain-Grundlagen

- kryptografische Hashfunktion
z.B. SHA-256
 - kollisionsresistente Streuwertfunktion, d.h. es ist praktisch unmöglich zwei unterschiedliche (beliebig große) Eingabewerte zu finden, die den gleichen Ausgabewert fester Länge (Hashwert) erzeugen (vgl. Fingerabdruck)
=> minimale Änderung des Eingabewerts erzeugt maximale Änderung des Ausgabewerts (ca. 50% der Bits)
- Nonce („Number used once“): Proof of Work: Zahl, die so lange geändert wird, bis der Hash nicht größer als eine bestimmte Obergrenze ist. (vgl. „Schloss knacken“)

Blockchain – Wie funktioniert die Verkettung?



Blockchain-Demo

z.B. <https://anders.com/blockchain/blockchain.html>

The image illustrates a sequence of five blockchain blocks. Each block is shown in a separate panel with the following fields:

- Block #:** 1, 2, 3, 4, 5
- Nonce:** 2661, 26219, 4105, 47949, 56265
- Data:** Transactions (e.g., C→B: 3T, A→E: 10T, etc.)
- Prev:** Previous block's hash
- Hash:** Mined hash of the current block
- Mine:** Button to mine the block

Arrows indicate the link from the 'Hash' of one block to the 'Prev' of the next block. The final block (Block # 5) is highlighted with a red background, indicating it is the most recent mined block.

Block #	Nonce	Prev Hash	Hash
1	2661	000000000000000000000000	0000d5893be3489d6621
2	26219	0000d5893be3489d6621	00004eb9c65f081a53f1
3	4105	00004eb9c65f081a53f1	0000bc1ef2d5454a9e61
4	47949	0000bc1ef2d5454a9e61	0000e4becbf6788dc91
5	56265	0000e4becbf6788dc91	c8bdac81c8fc15e7e0b7

Blockchain-Demo

z.B. <https://anders.com/blockchain/blockchain.html>

The image shows five blocks in a blockchain sequence. Each block contains the following fields:

- Block: #**: 1, 2, 3, 4, 5
- Nonce**: 2661, 26219, 4105, 47949, 56265
- Data**: Transactions (e.g., C→B: 3T, A→E: 10T, D→C: 4T, B→A: 7T, A→D: 8T)
- Prev:**: Previous block's hash (e.g., 00)
- Hash:**: Current block's hash (e.g., 0000d5893be3489d662f081a53f081a53f081a53f081a53f081a53f081a53f081a53f)
- Mine**: Button to mine the block

The fifth block is highlighted in pink and has a red arrow pointing to its 'Mine' button, indicating it is the current block being mined.

Blockchain-Demo

z.B. <https://anders.com/blockchain/blockchain.html>

The image displays five blocks of a blockchain, numbered 1 to 5. Each block contains a set of data, a previous hash, and a new hash. The fifth block is highlighted in red, and a red arrow points to its 'Mine' button. The 'Nonce' value for the fifth block is circled in red.

Block #	Nonce	Prev Hash	Hash
1	2661	000000000000000000000000	0000d5893be3489d6621
2	26219	0000d5893be3489d6621	00004eb9c65f081a53f1
3	4105	00004eb9c65f081a53f1	0000bc1ef2d5454a9e61
4	47949	0000bc1ef2d5454a9e61	0000e4becbf6788dc91
5	56265	0000e4becbf6788dc91	c8bdac81c8fc15e7e0b7

Block 1 Data: C→B: 3T, A→E: 10T, D→C: 4T, B→A: 7T, A→D: 8T

Block 2 Data: E→B: 5T, C→E: 3T, B→C: 6T, A→C: 12T, E→D: 2T

Block 3 Data: C→B: 5T, A→E: 3T, B→C: 6T, D→C: 12T, E→D: 2T

Block 4 Data: D→B: 5T, C→E: 3T, C→C: 6T, A→C: 12T, A→D: 2T

Block 5 Data: A→B: 5T, C→E: 3T, B→C: 11T, A→C: 1T, E→D: 2T

Blockchain-Demo

z.B. <https://anders.com/blockchain/blockchain.html>

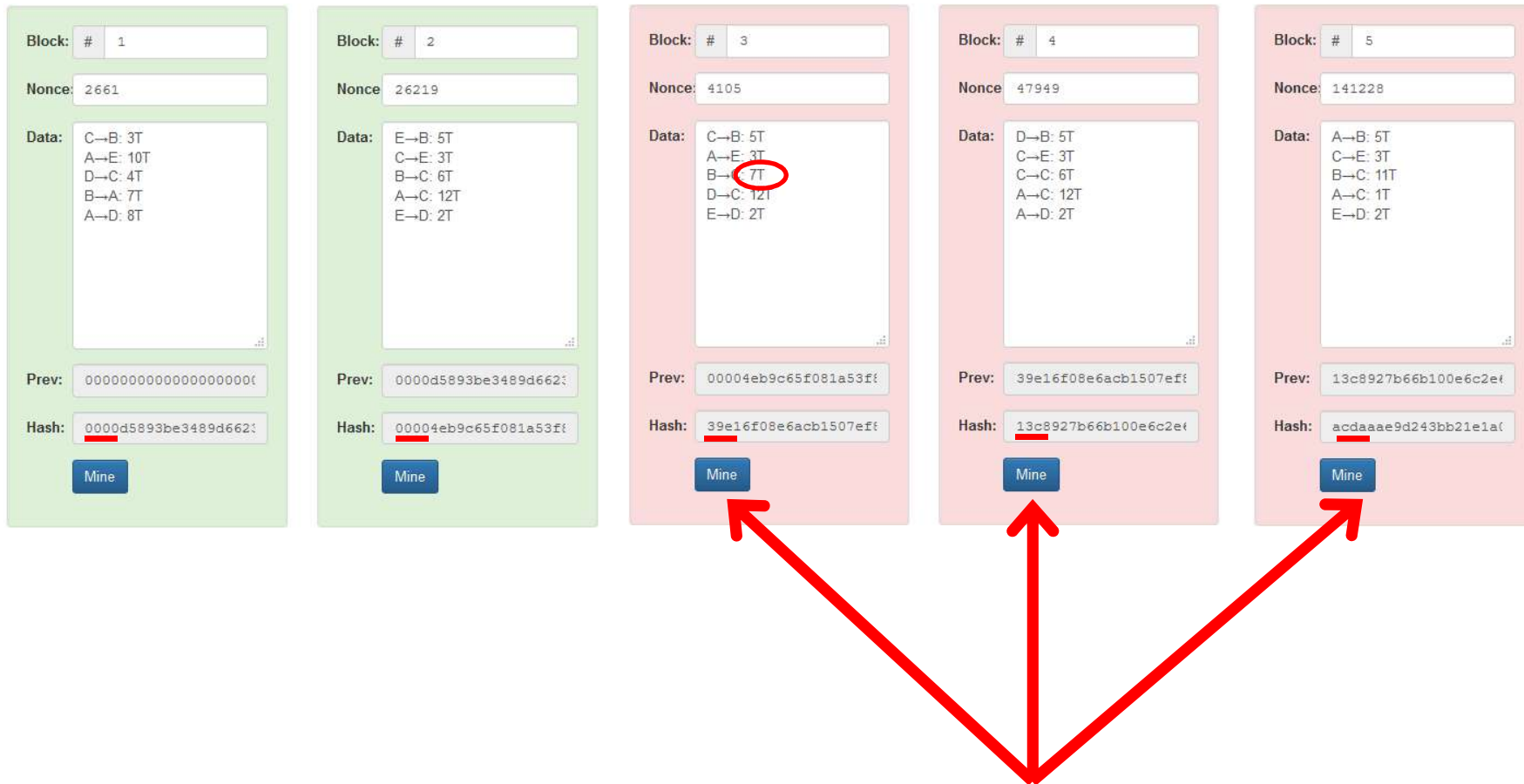
The image displays five sequential blocks in a blockchain demo. Each block is a light green rectangular panel containing the following fields:

- Block: #**: A text input field showing the block number (1, 2, 3, 4, 5).
- Nonce**: A text input field showing a unique value for each block (2661, 26219, 4105, 47949, 141228).
- Data**: A text area containing transaction data in the format 'Sender→Receiver: Amount'.
 - Block 1: C→B: 3T, A→E: 10T, D→C: 4T, B→A: 7T, A→D: 8T
 - Block 2: E→B: 5T, C→E: 3T, B→C: 6T, A→C: 12T, E→D: 2T
 - Block 3: C→B: 5T, A→E: 3T, B→C: 6T, D→C: 12T, E→D: 2T. The '6T' in 'B→C: 6T' is circled in red.
 - Block 4: D→B: 5T, C→E: 3T, C→C: 6T, A→C: 12T, A→D: 2T
 - Block 5: A→B: 5T, C→E: 3T, B→C: 11T, A→C: 1T, E→D: 2T
- Prev:**: A text input field showing the previous block's hash (e.g., 000000000000000000000000).
- Hash:**: A text input field showing the current block's hash. The first few characters are highlighted in red to show the leading zeros.
- Mine**: A blue button at the bottom of each block.

The progression shows how each new block's hash depends on the previous block's hash and its own data and nonce. The 'Prev' field of a block is the 'Hash' of the previous block.

Blockchain-Demo

z.B. <https://anders.com/blockchain/blockchain.html>



Nochmal zu Bitcoin...

- Peer-to-Peer-Netzwerk
- Mining-Belohnung + Gebühr: 12,5 Bitcoins = 90T€
- obere Grenze: 21 Mio. Bitcoin
- Ressourcen-Verbrauch: 1Gigawatt: 50T€/h; Spezialhardware mit geringem Lebenszyklus (s. Grafikkarten)
- 75% aller Bitcoins werden in China produziert (billiger Kohlestrom)
- Schätzung: Juli 2019: Mehr Strombedarf als USA
- Verästelung bei „gleichzeitigem“ Finden gültiger Blöcke

Alternative Anwendungen des Blockchain-Verfahrens

- Grundsätzlich: Alle Datensätze (Transaktionen), die im Nachhinein nicht mehr verändert werden sollen
- Aufzeichnung sicherheitskritischer Operationen von Softwareprozessen
- Elektronische Gesundheitsakte
- Elektronische Stimmabgabe
- Transportweg-Aufzeichnung, Herkunftsnachweis (s. [Hyperledger Fabric von IBM](#))
- Smart Contract (automatischer Ablauf von Transaktionen)

Alternative Anwendung und Nonce/Proof-of-Work

Hinweis: Diese Folie war in der ursprünglichen Fassung nicht vorhanden und wurde aufgrund der Diskussion auf der iMedia erstellt

- Empfehlenswerte Literatur (s.u.):
[FIT] Fraunhofer FIT: Blockchain: Grundlagen, Anwendungen und Potenziale – White Paper
https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf (frei downloadbar)
[\[CT\] c't 23/2017: Das macht Blockchain](#) (kostenpflichtig)
- In einem genehmigungsbasierten Blockchain-System ist ein „kostenintensiver PoW [Proof-of-Work] [...] hinfällig, weshalb effizientere Mechanismen zur Konsensfindung implementiert werden können“ ([FIT], S. 11)
- „Zudem können Systeme darin unterschieden werden, auf welche Weise ein Konsens über den Systemstatus erreicht wird. Neben dem im Bitcoin-System verwendeten Proof-of-Work existiert eine Vielzahl an Methoden.“ ([FIT], S. 12)
- Zusammenfassend lässt sich die Blockchain allgemein in jedem Bereich einsetzen, der die Erfassung, den Nachweis oder Transfer jeglicher Art von Kontrakt oder Objekt zum Gegenstand hat ([FIT], S.17)

Blockchain im Unterricht

- Rollenspiel
- Rechercheaufträge
- Hashfunktionen
- Kryptologie

Fragen?

