Blockchain im Unterricht

Wie funktionieren eigentlich Bitcoin & Co.?

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

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

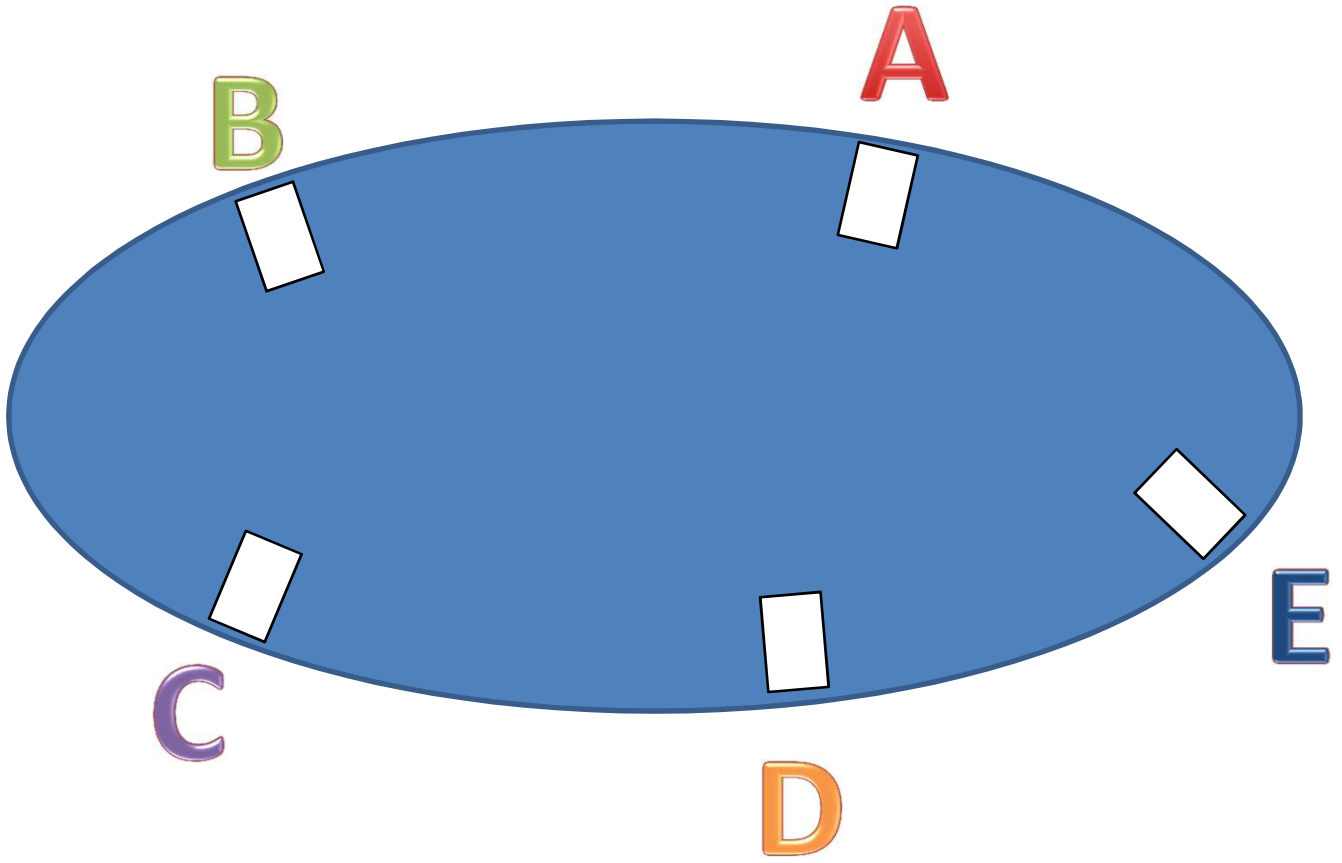
Mining: SHA-256

Blockchain: 160 GB (Stand 03/2018)

Erscheinungsjahr: 2009

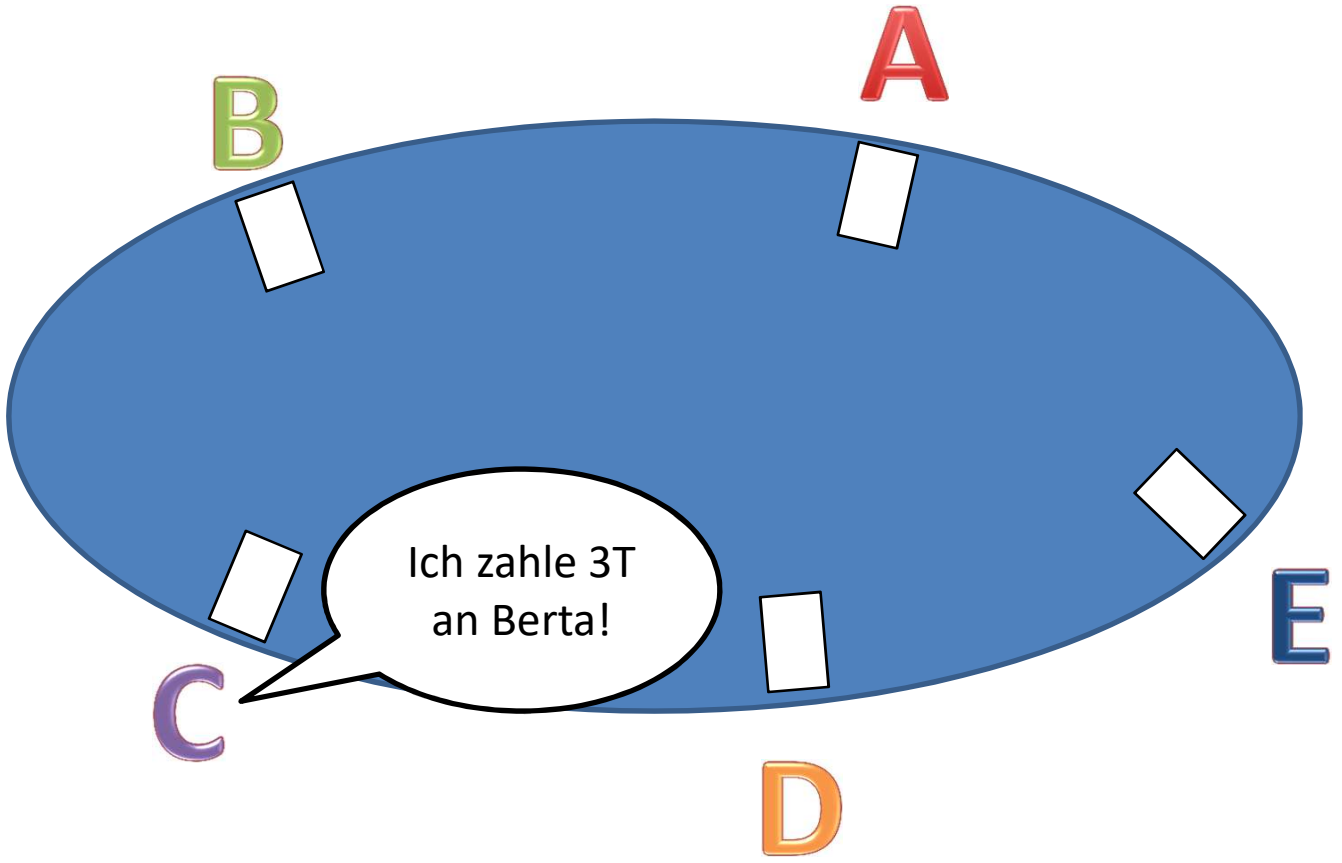
Programmiersprache: C++

Kryptowährung verstehen ohne Programmierkenntnisse



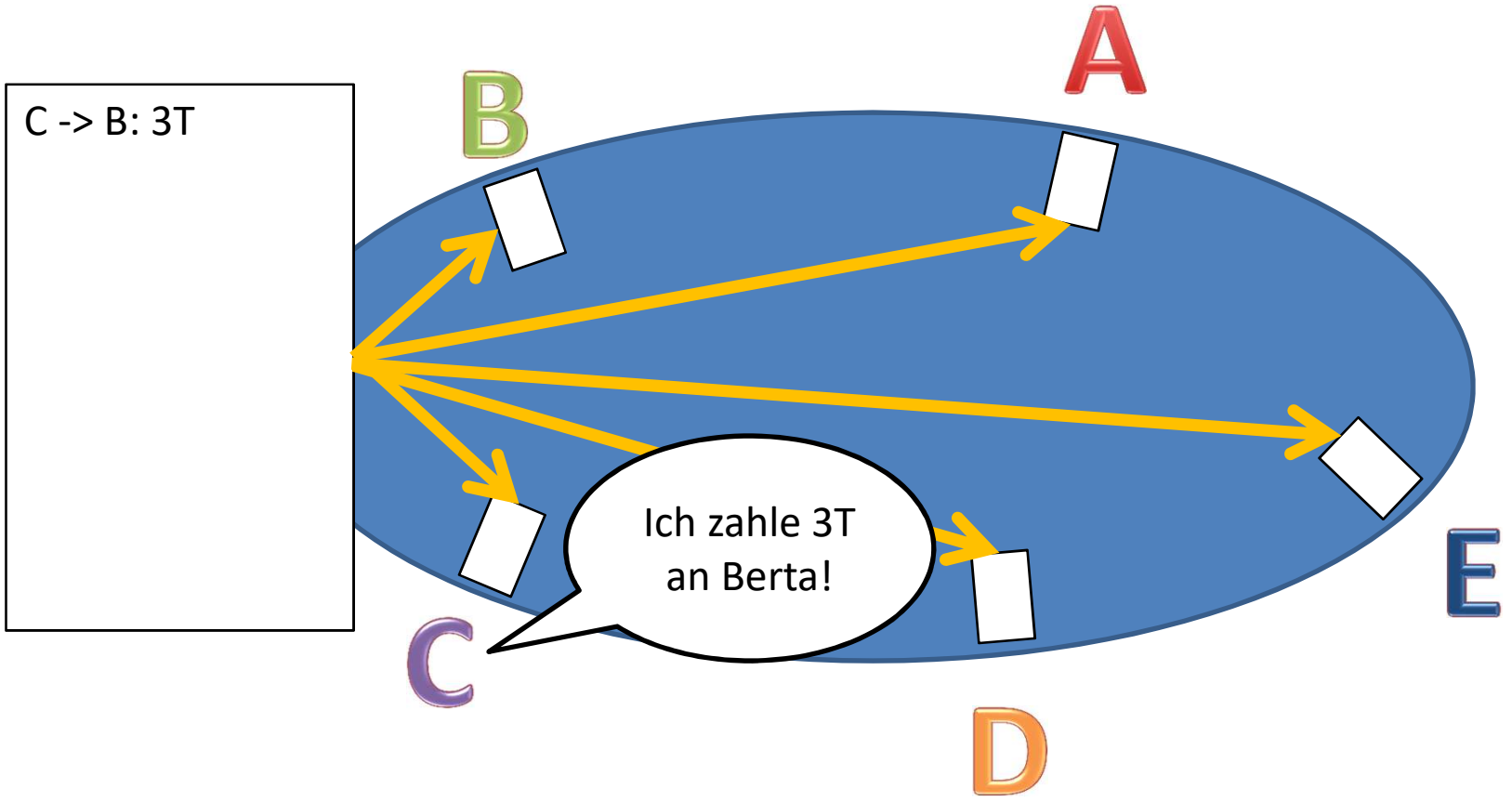
nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse



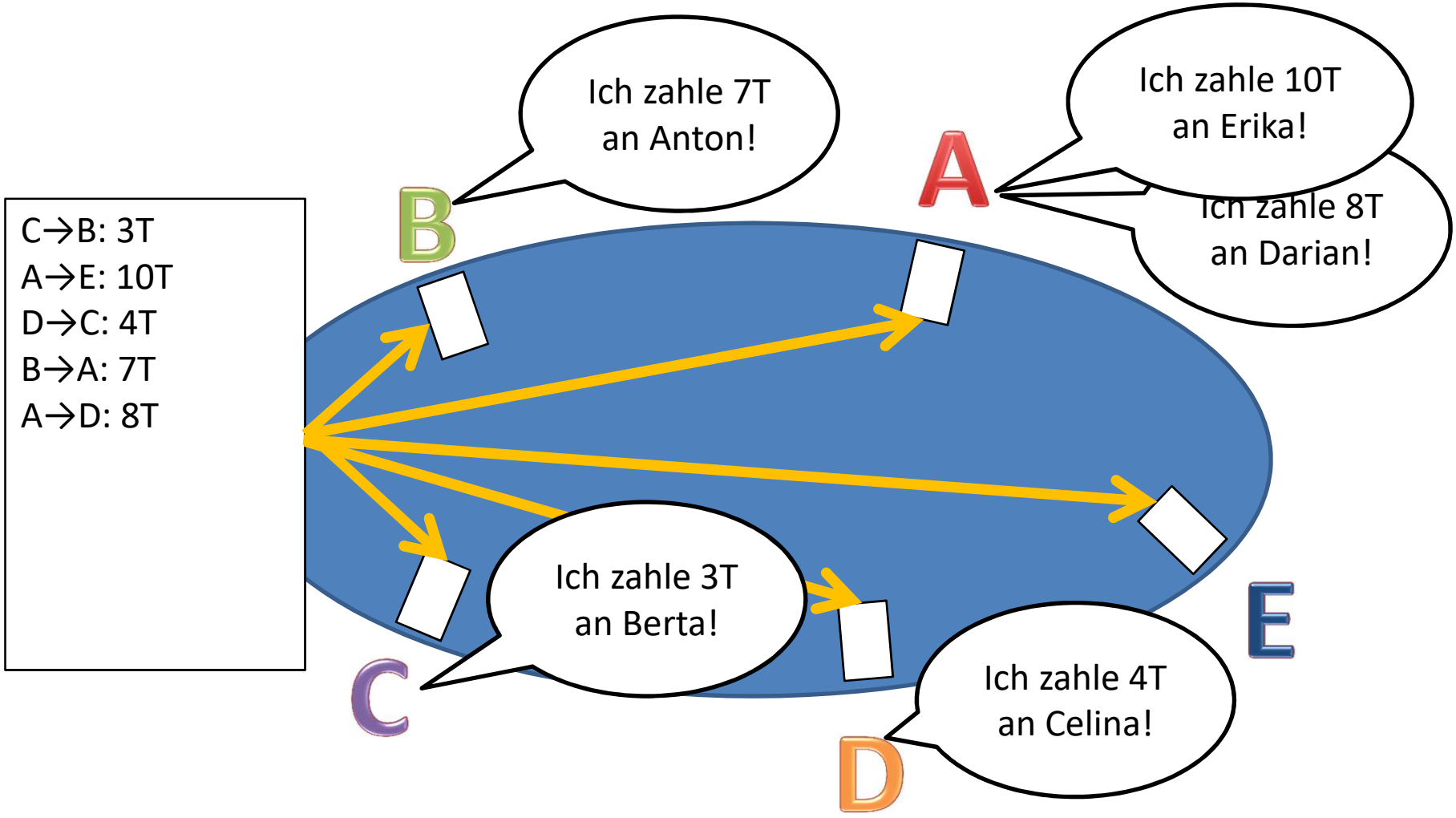
nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

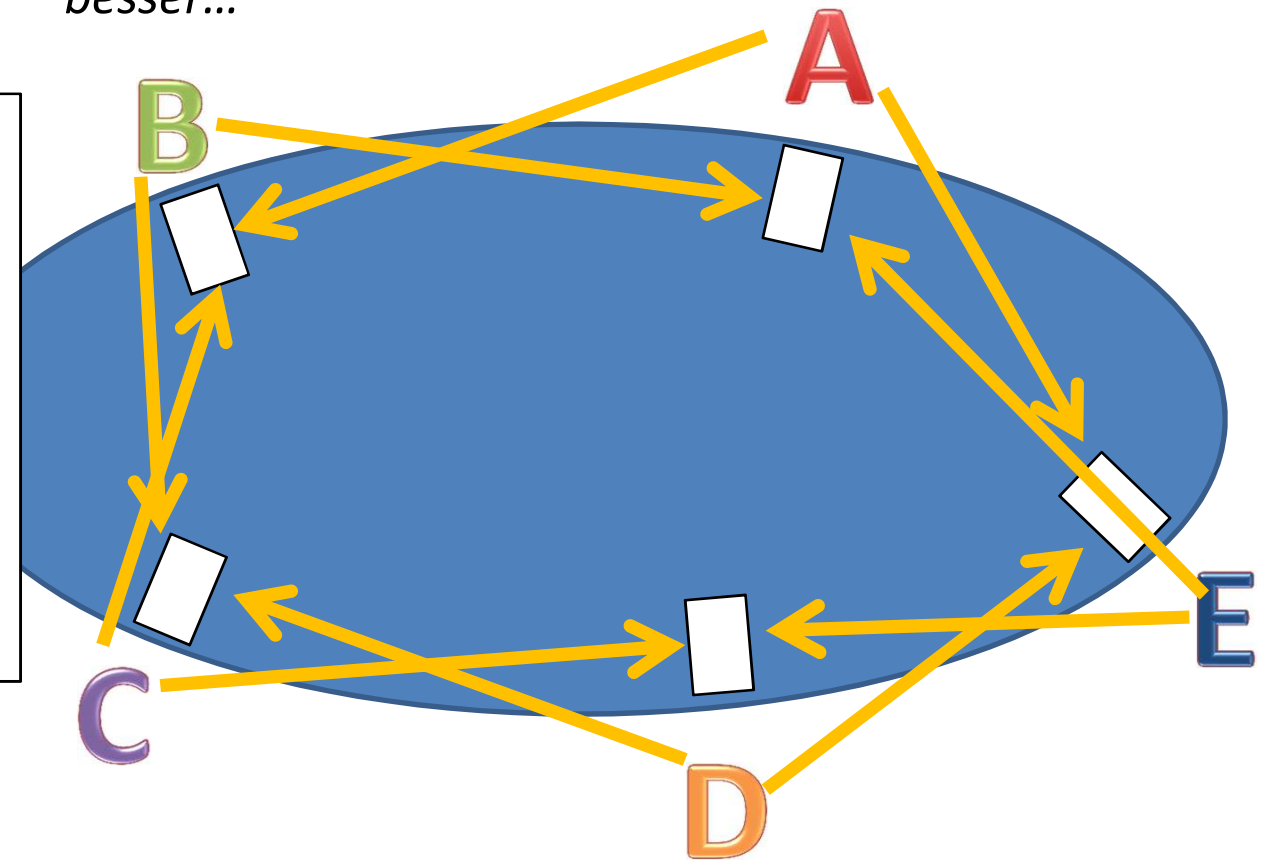


nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

Vertrauen ist gut, Kontrolle ist besser…

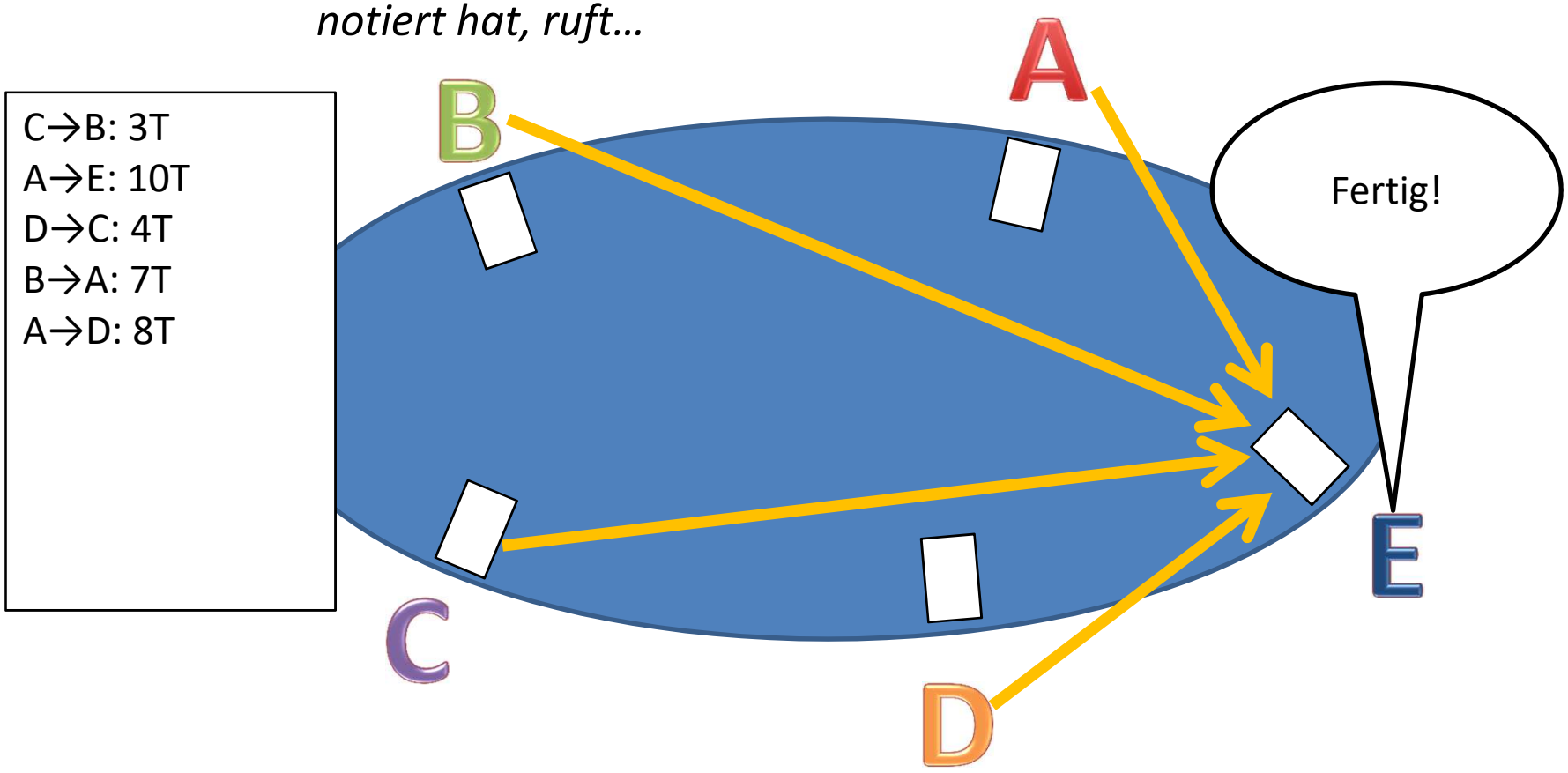
C→B: 3T
A→E: 10T
D→C: 4T
B→A: 7T
A→D: 8T



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

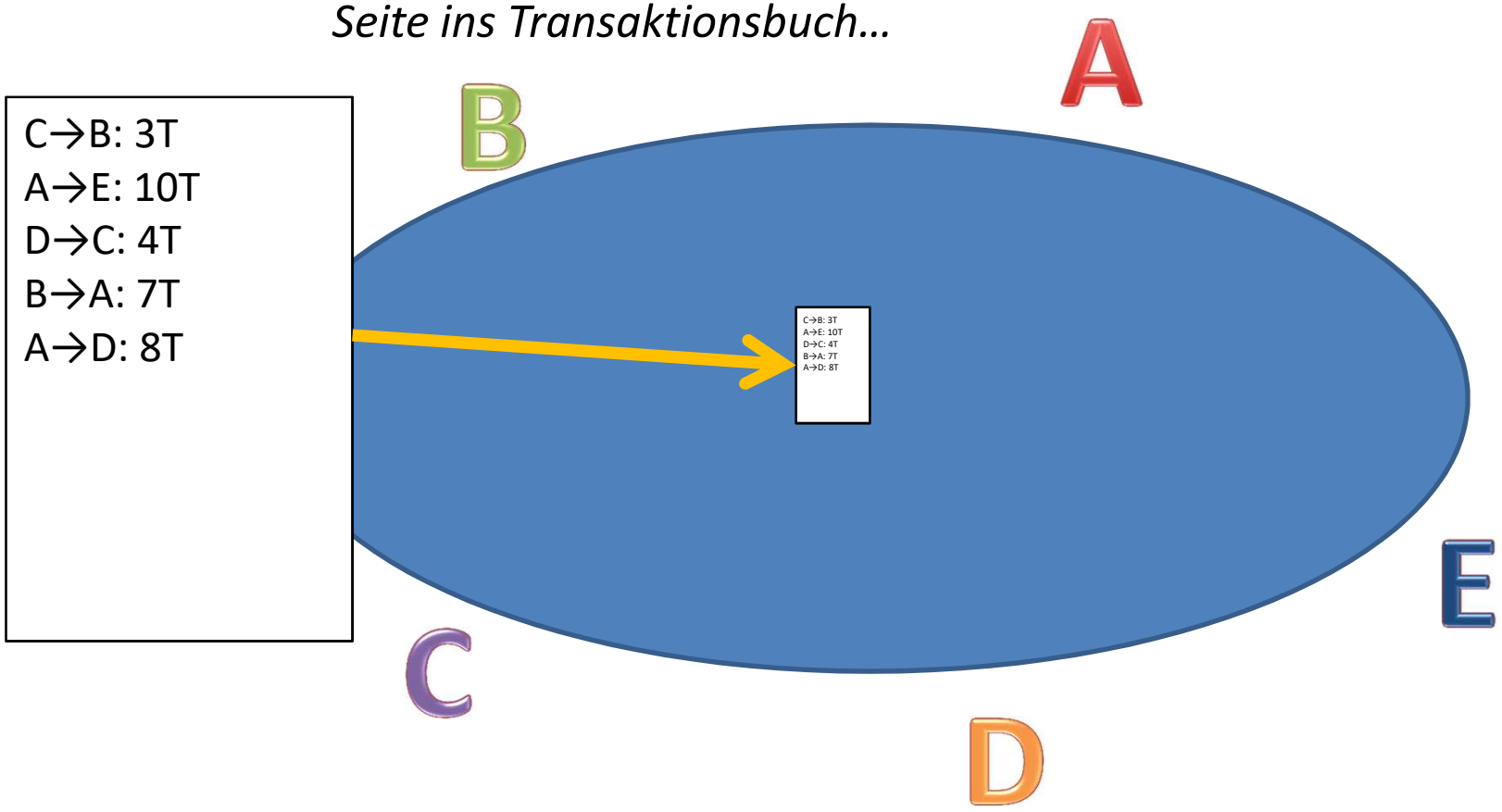
Alle 10 Minuten: Zettel abgeben
Wer als Erstes alle Transaktionen notiert hat, ruft…



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

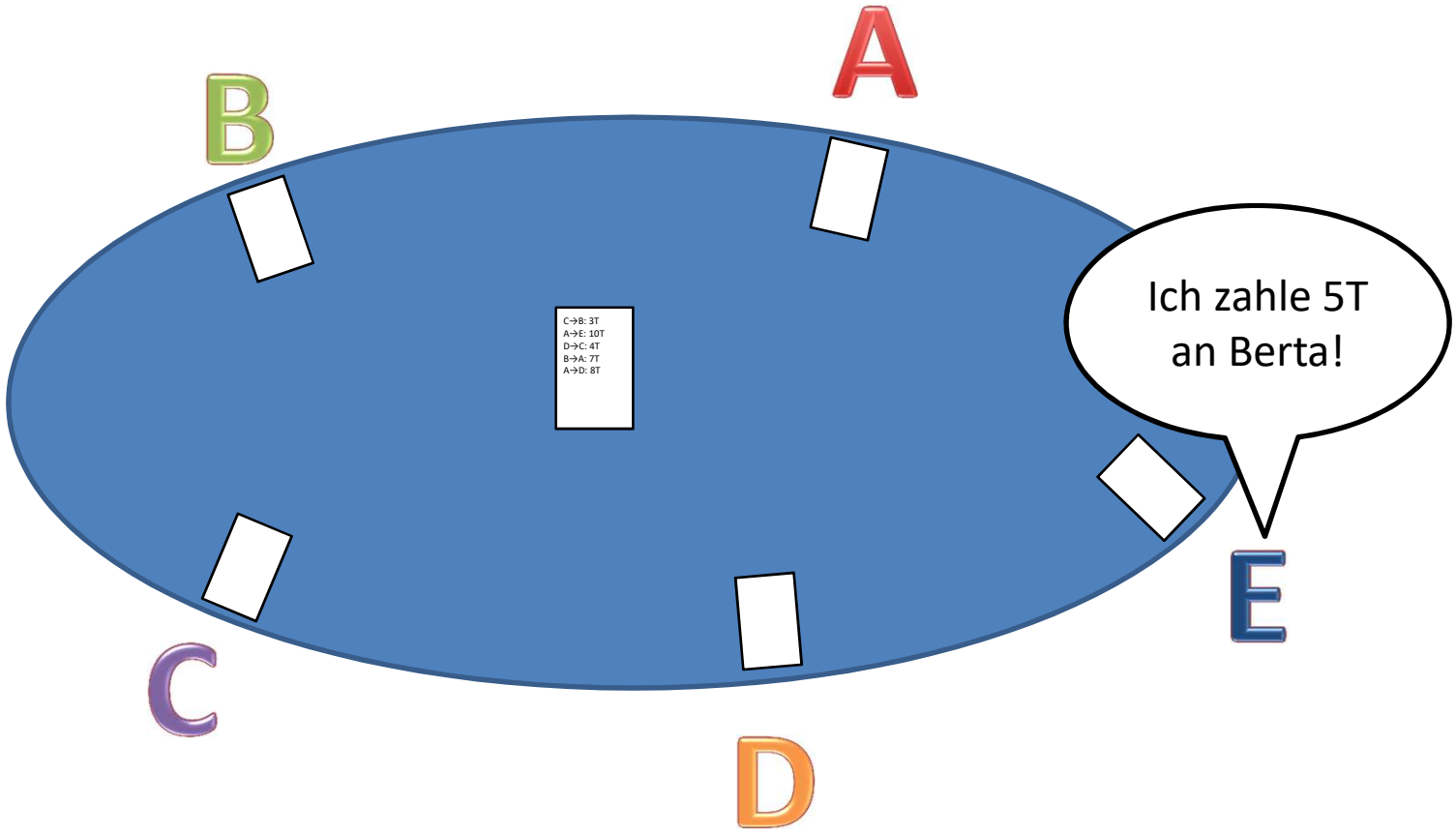
Alle geben ihren Zettel ab, der bestätigte Zettel kommt als neue Seite ins Transaktionsbuch…



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

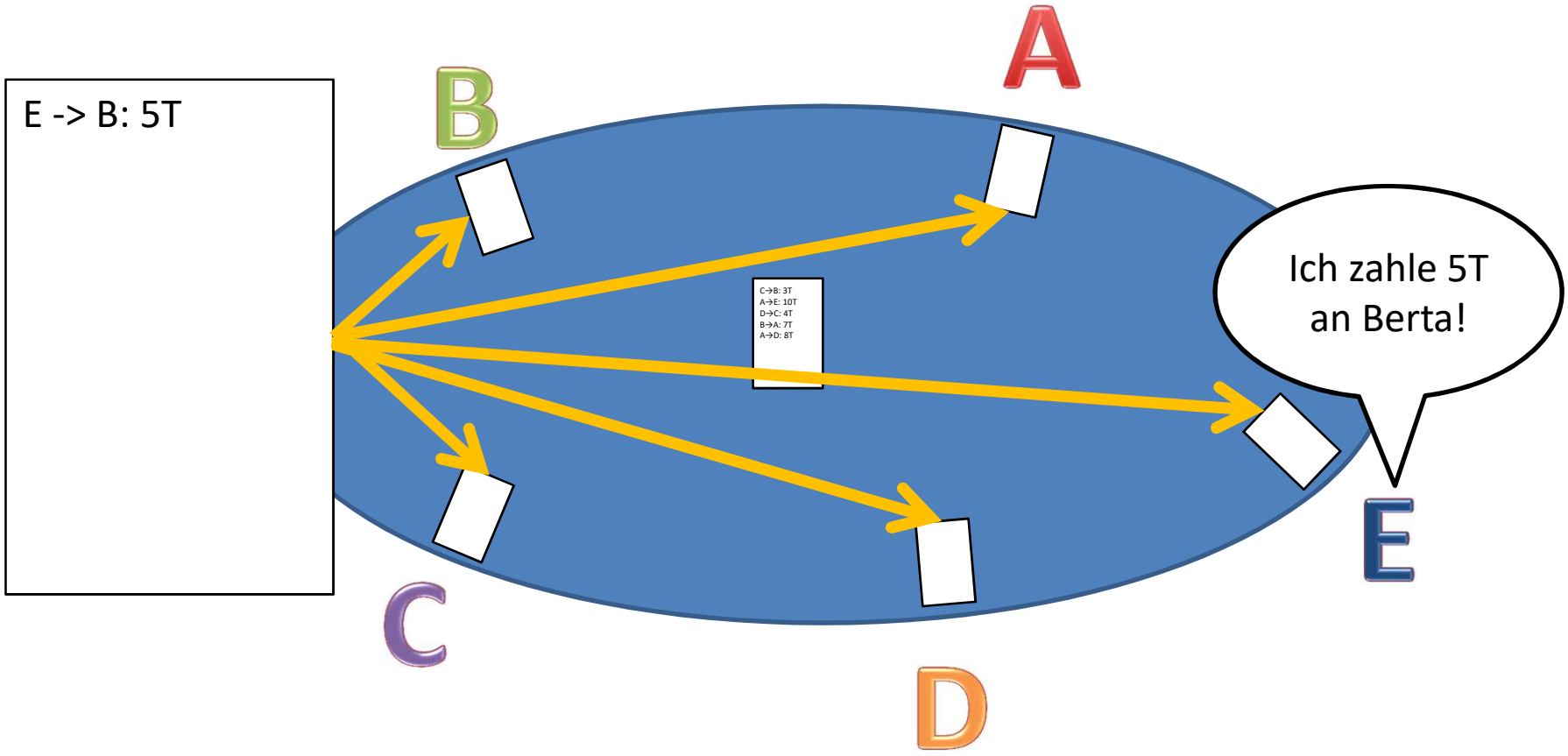
Kryptowährung verstehen ohne Programmierkenntnisse

…und es geht wieder von vorne los…



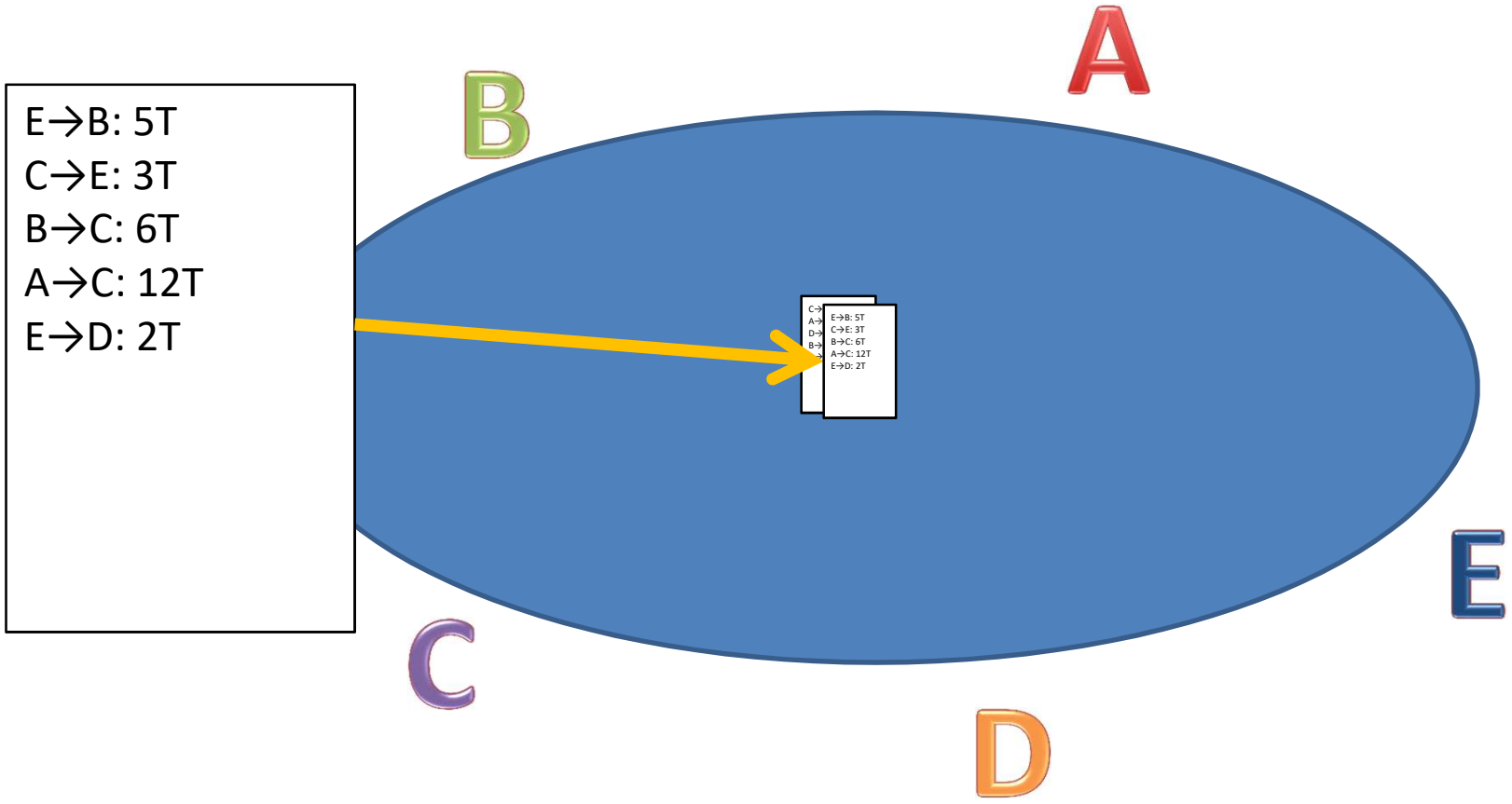
nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

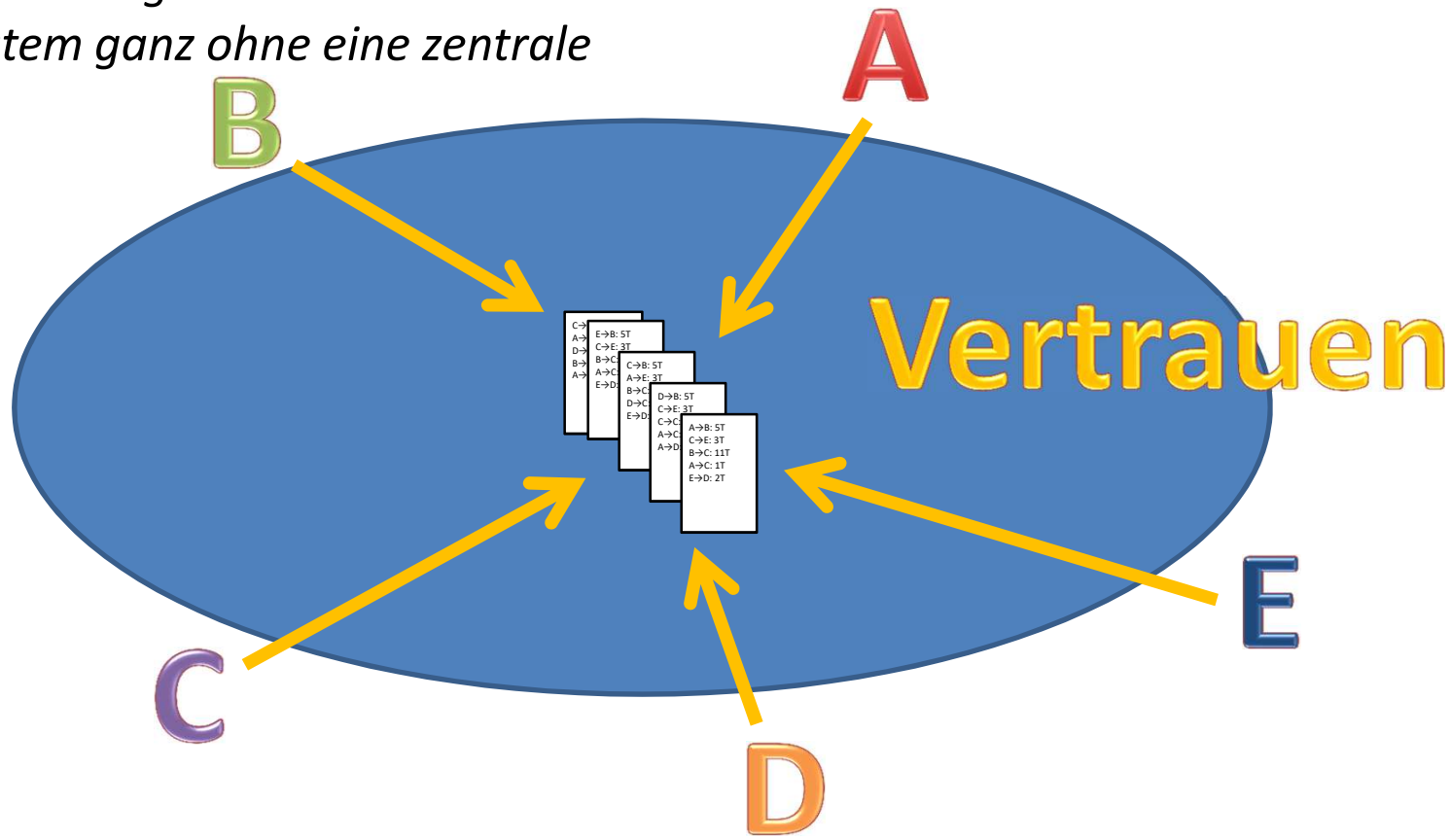
Kryptowährung verstehen ohne Programmierkenntnisse



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

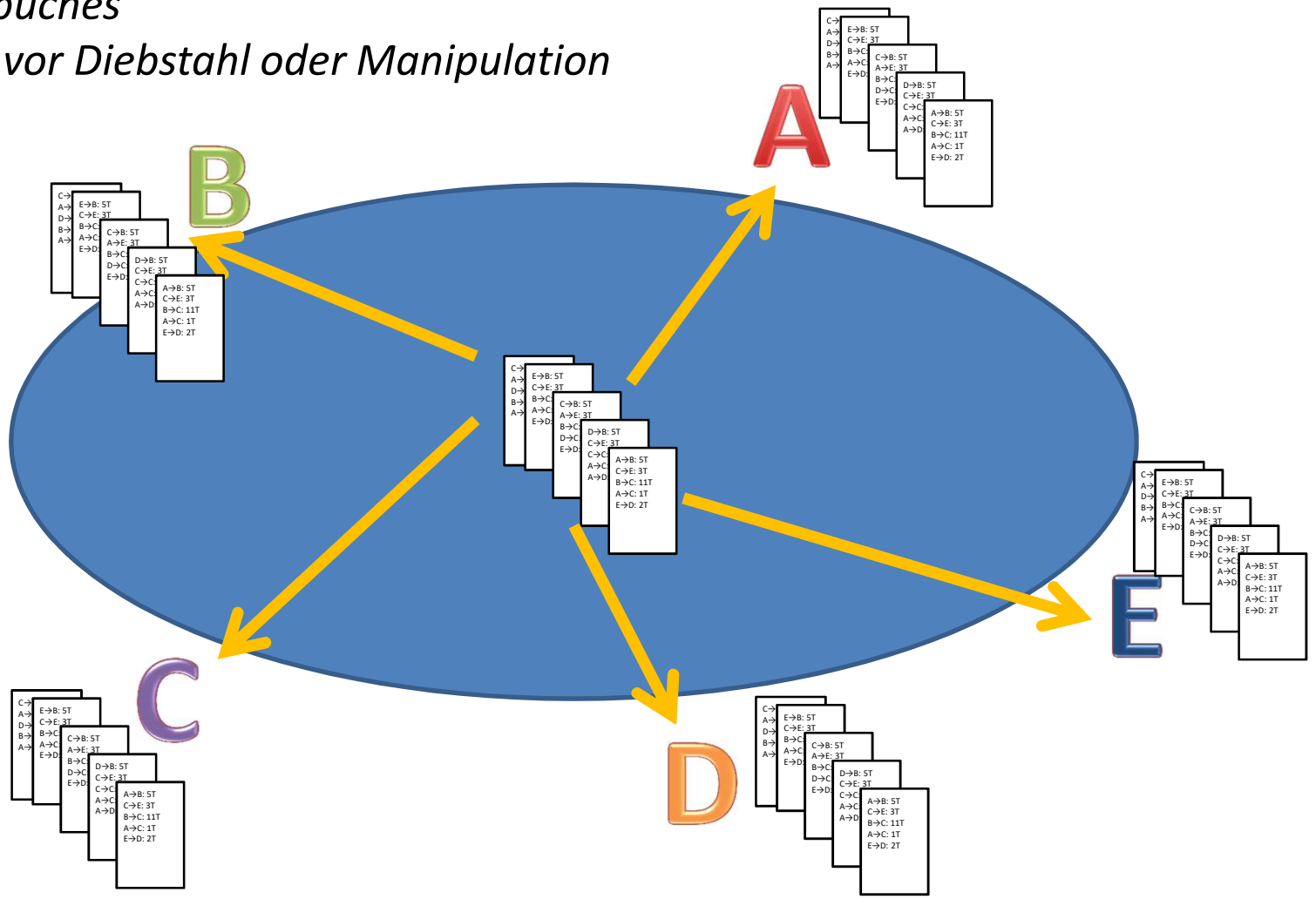
In der Mitte liegt ein Transaktionsbuch dessen Korrektheit alle Teilnehmer bestätigen können => Vertrauen in das gemeinsame Währungssystem ganz ohne eine zentrale Institution



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

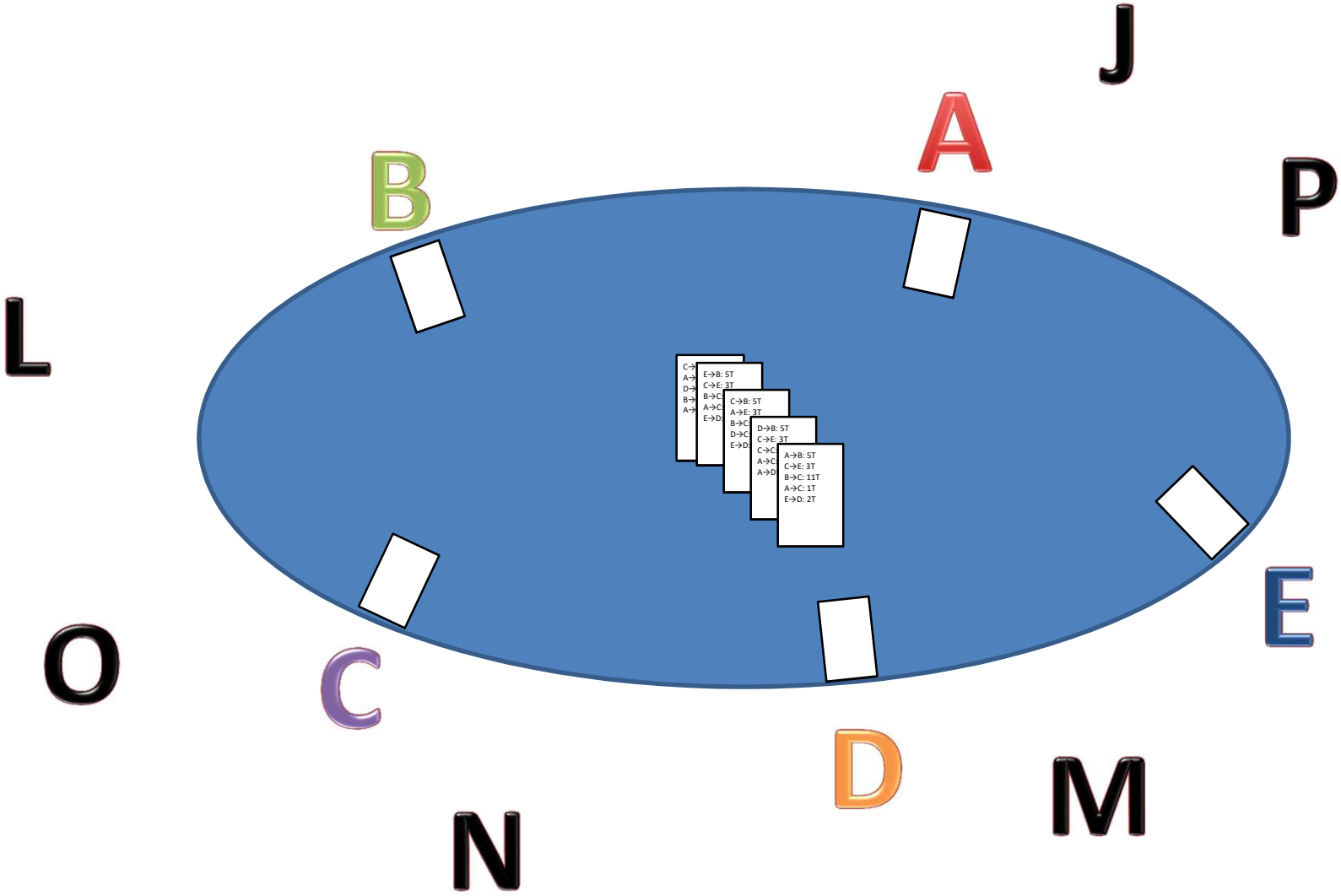
Jeder Teilnehmer hat eine Kopie des Transaktionsbuches
=> Sicherheit vor Diebstahl oder Manipulation



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

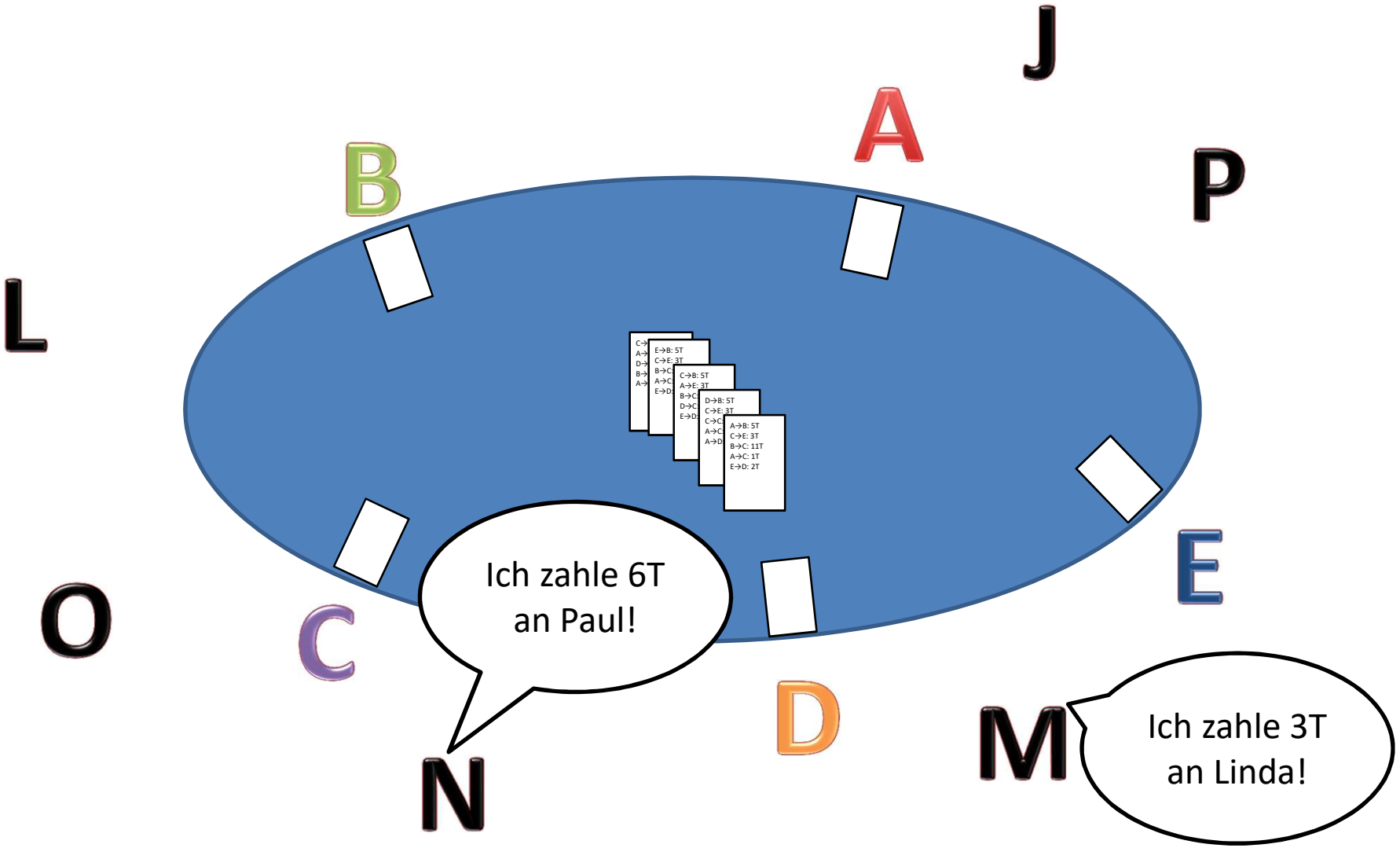
Passive Nutzer kommen hinzu…



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

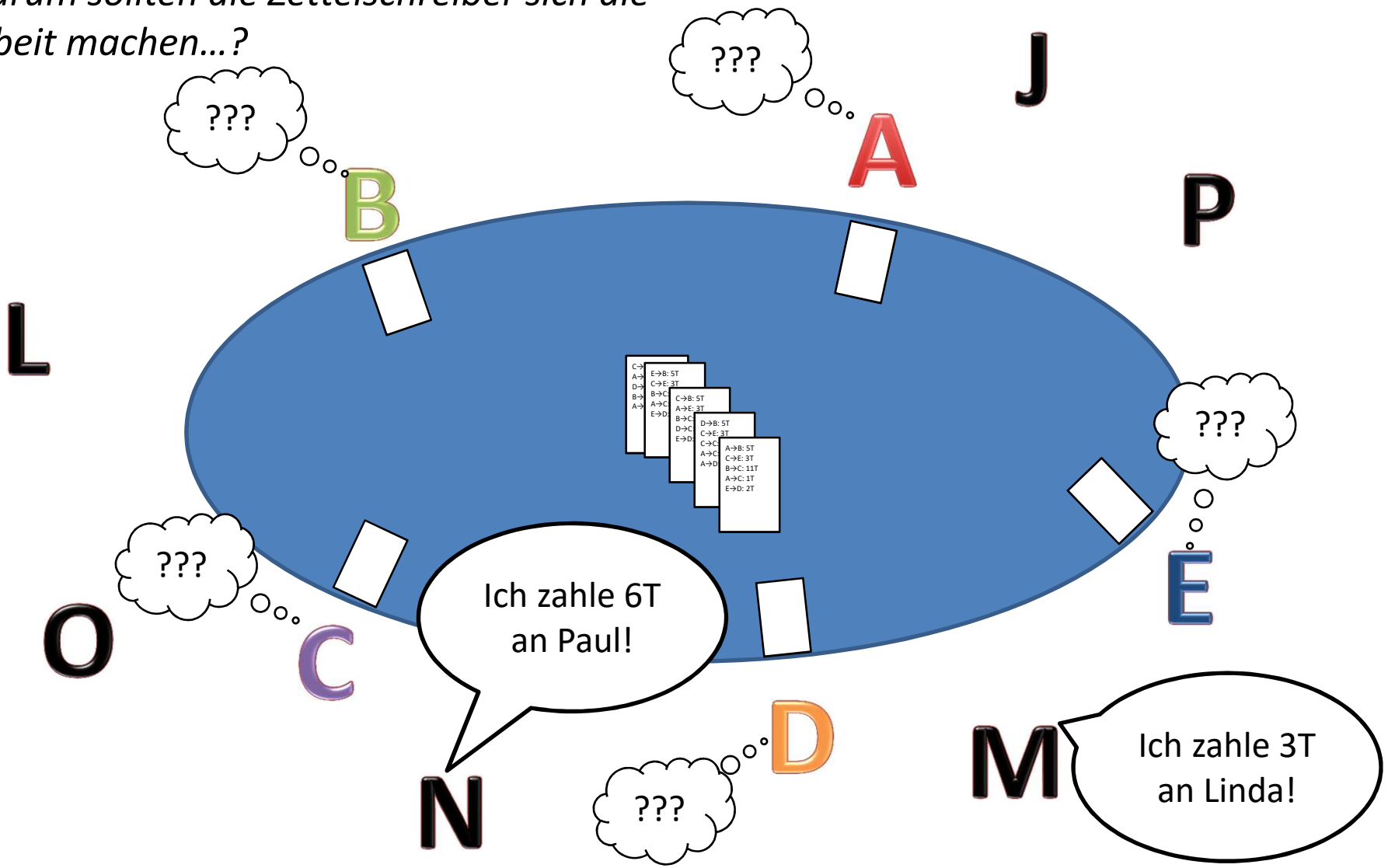
Passive Nutzer kommen hinzu…



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

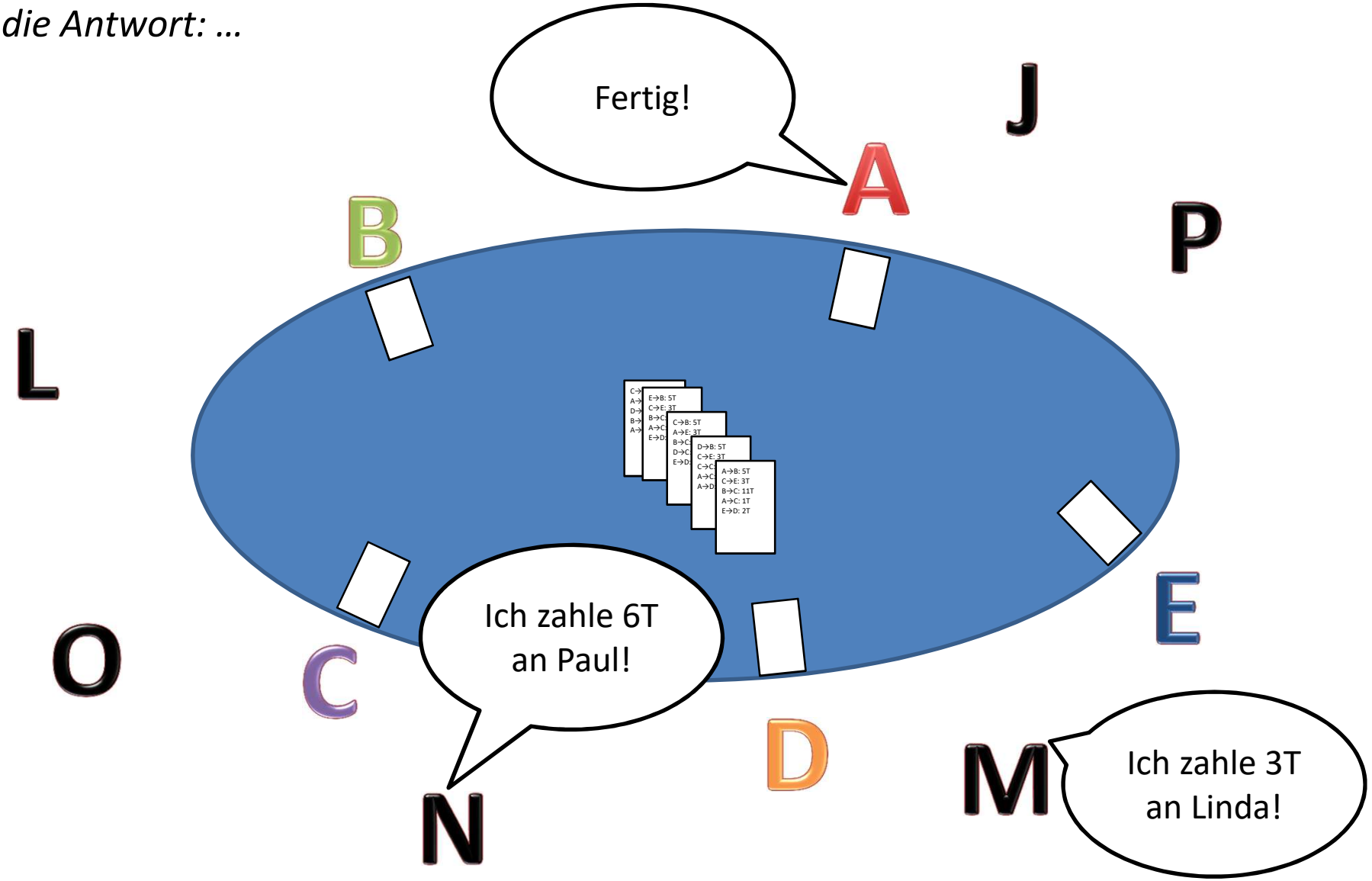
Warum sollten die Zettelschreiber sich die Arbeit machen…?



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

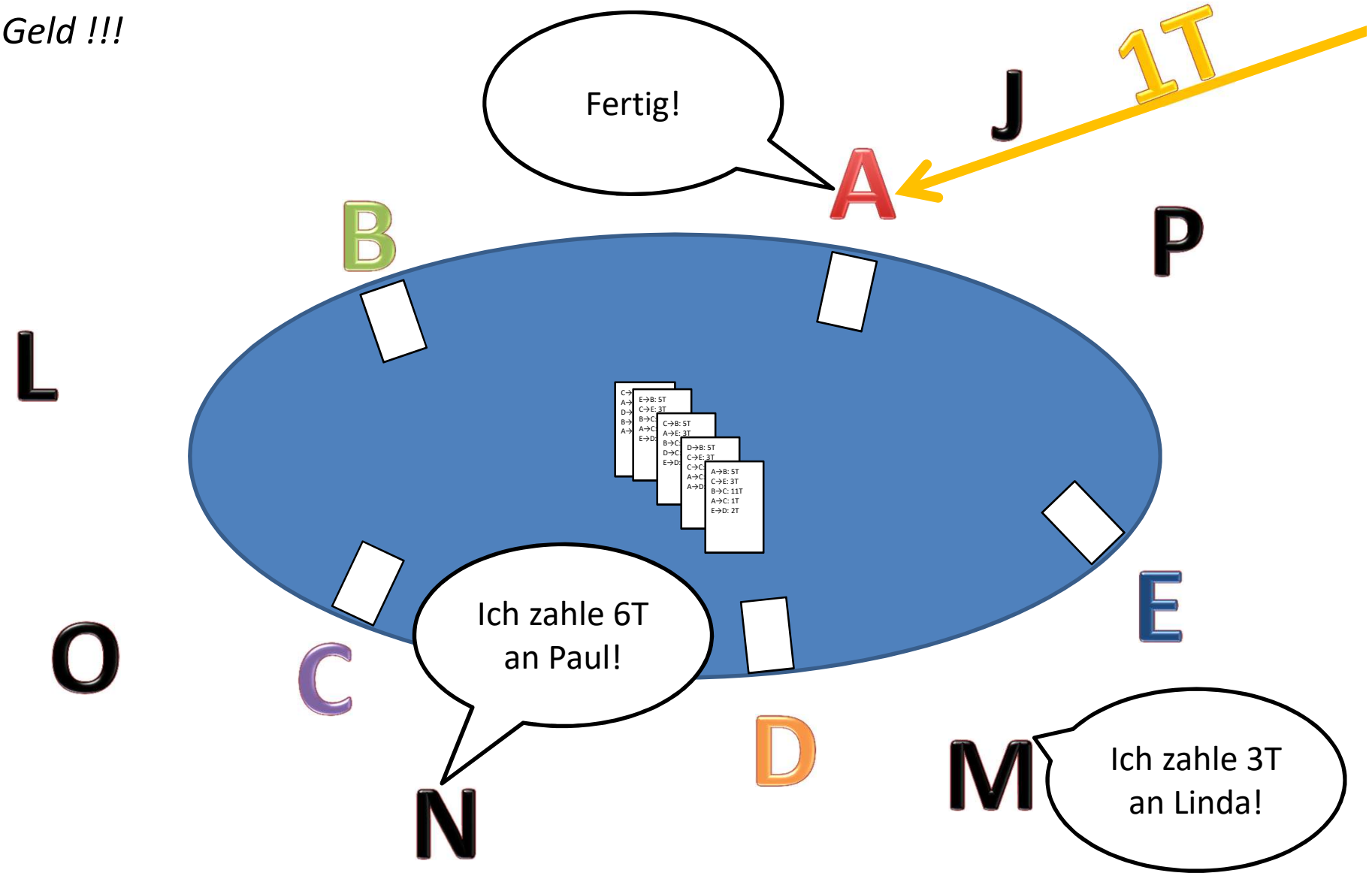
… die Antwort: …



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

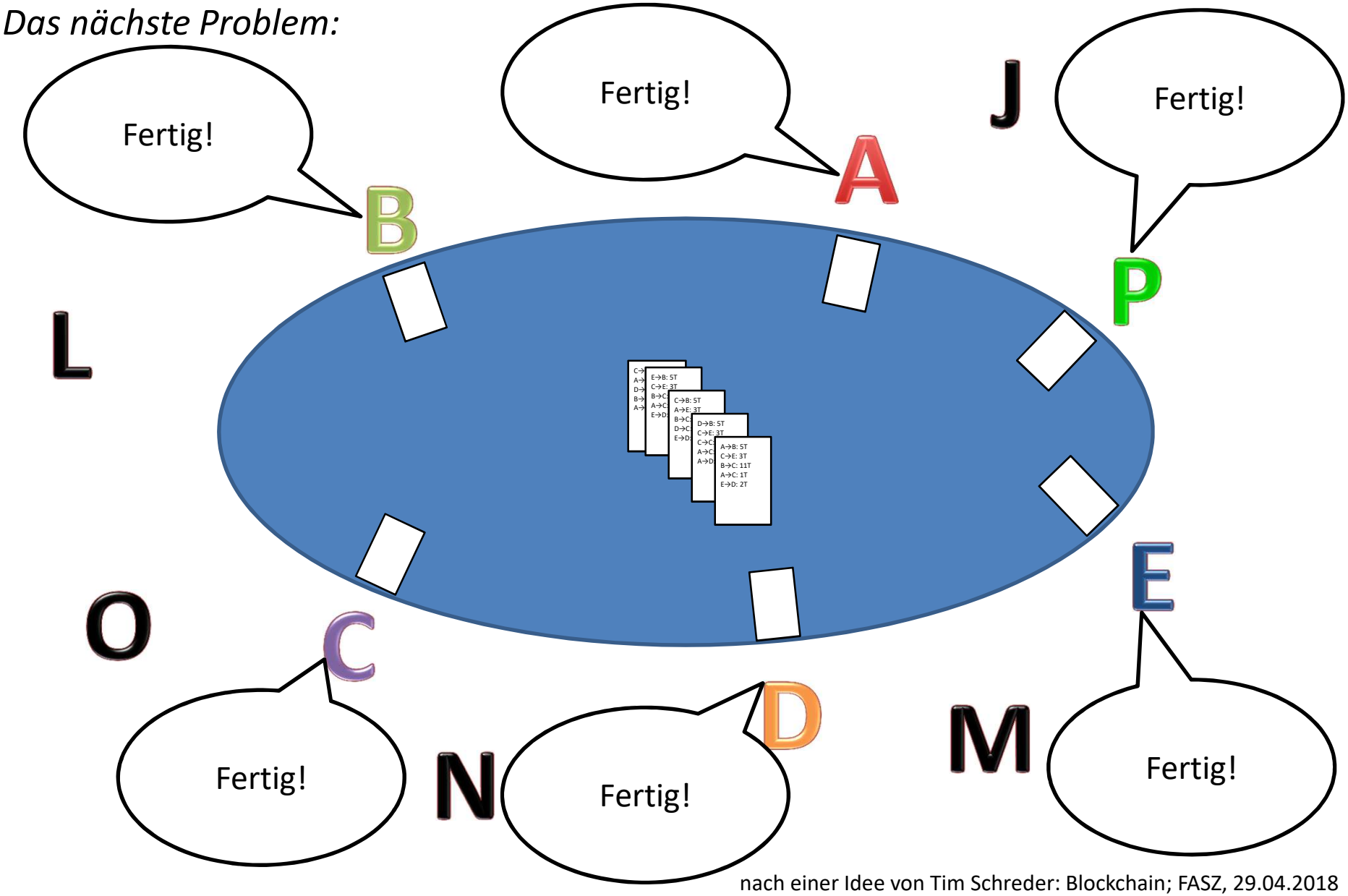
… Geld !!!



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

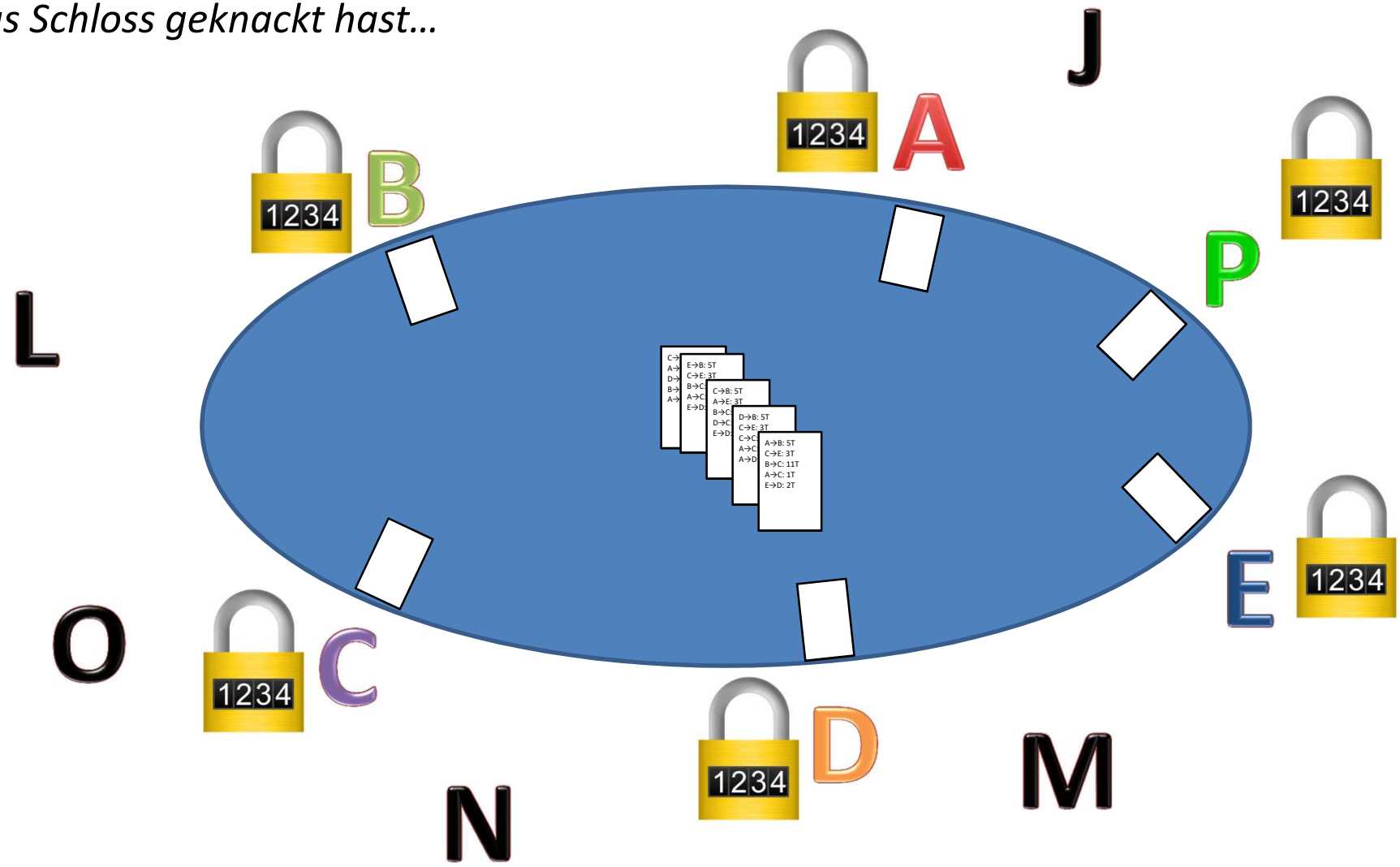
Das nächste Problem:



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

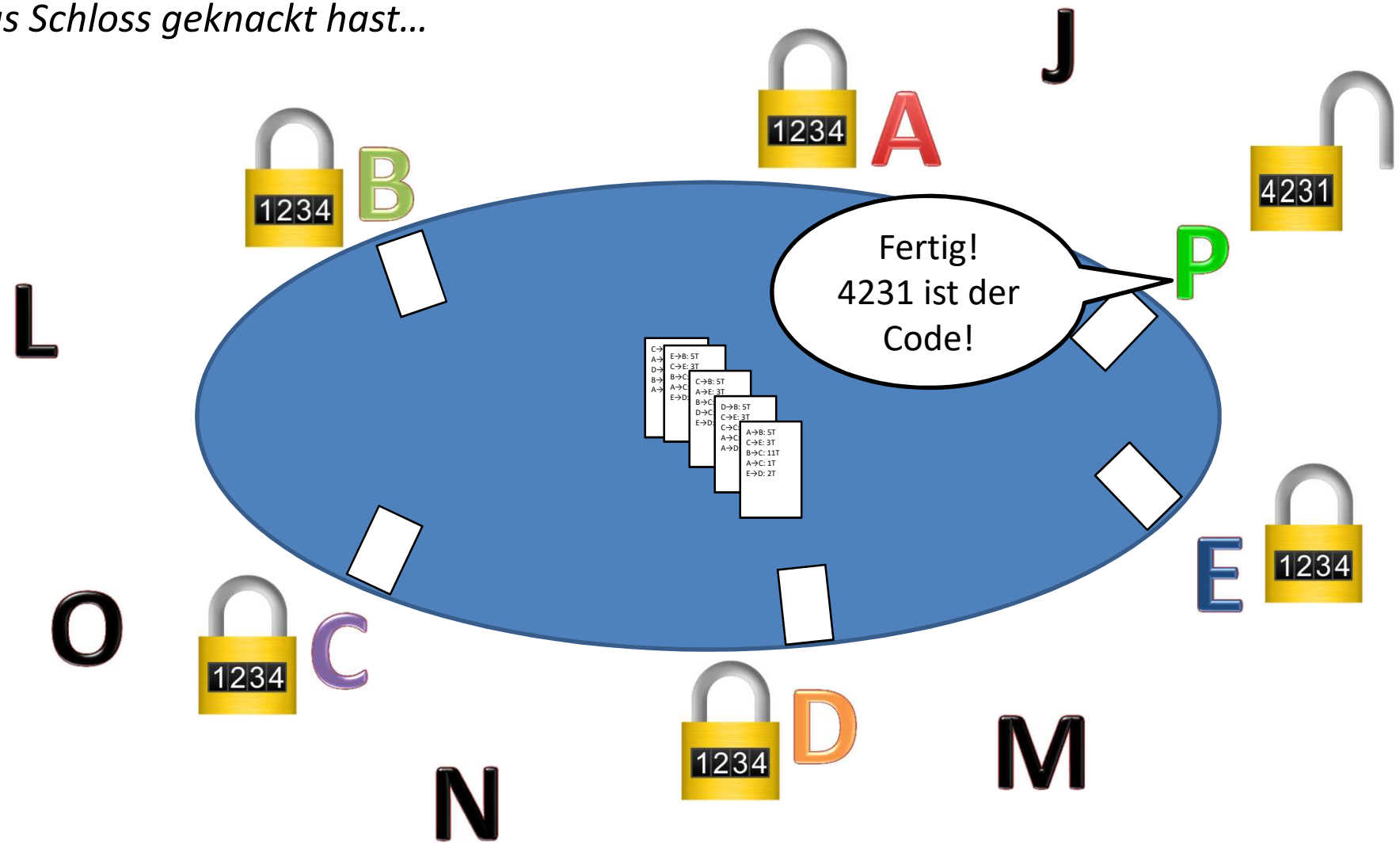
Lösung: Du bist erst fertig, wenn du zusätzlich das Schloss geknackt hast…



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

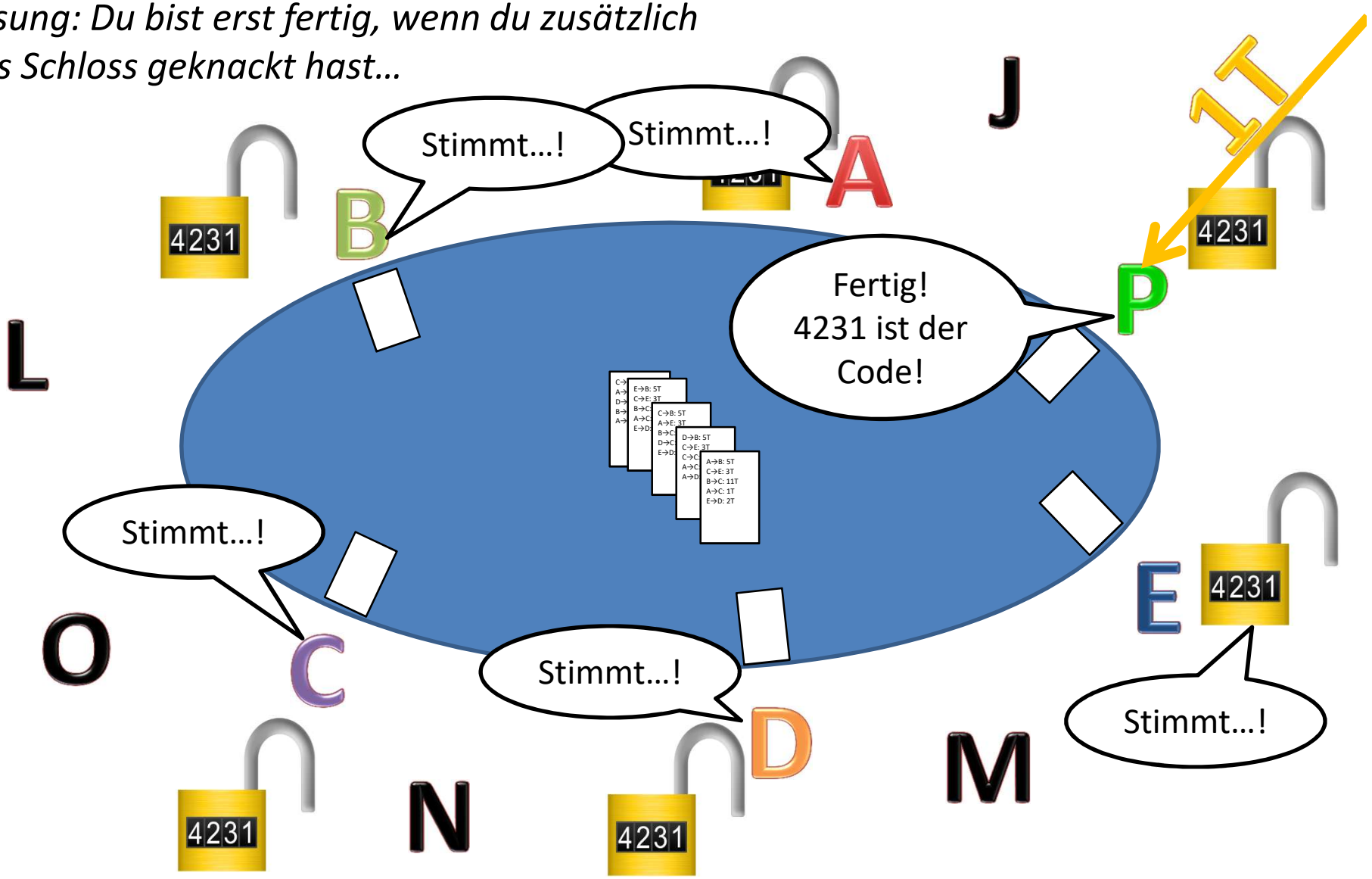
Lösung: Du bist erst fertig, wenn du zusätzlich das Schloss geknackt hast…



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

Kryptowährung verstehen ohne Programmierkenntnisse

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



nach einer Idee von Tim Schreder: Blockchain; FASZ, 29.04.2018

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

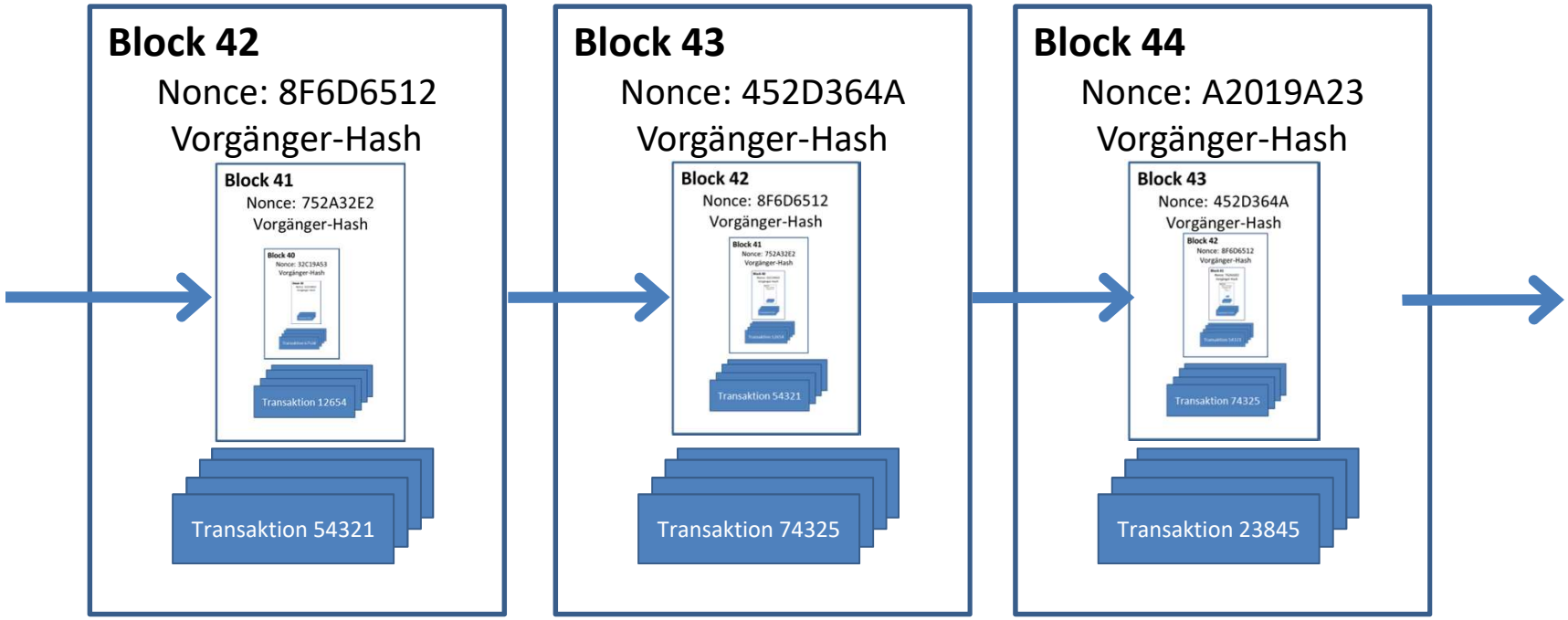
Blockchain

- 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 das 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“)

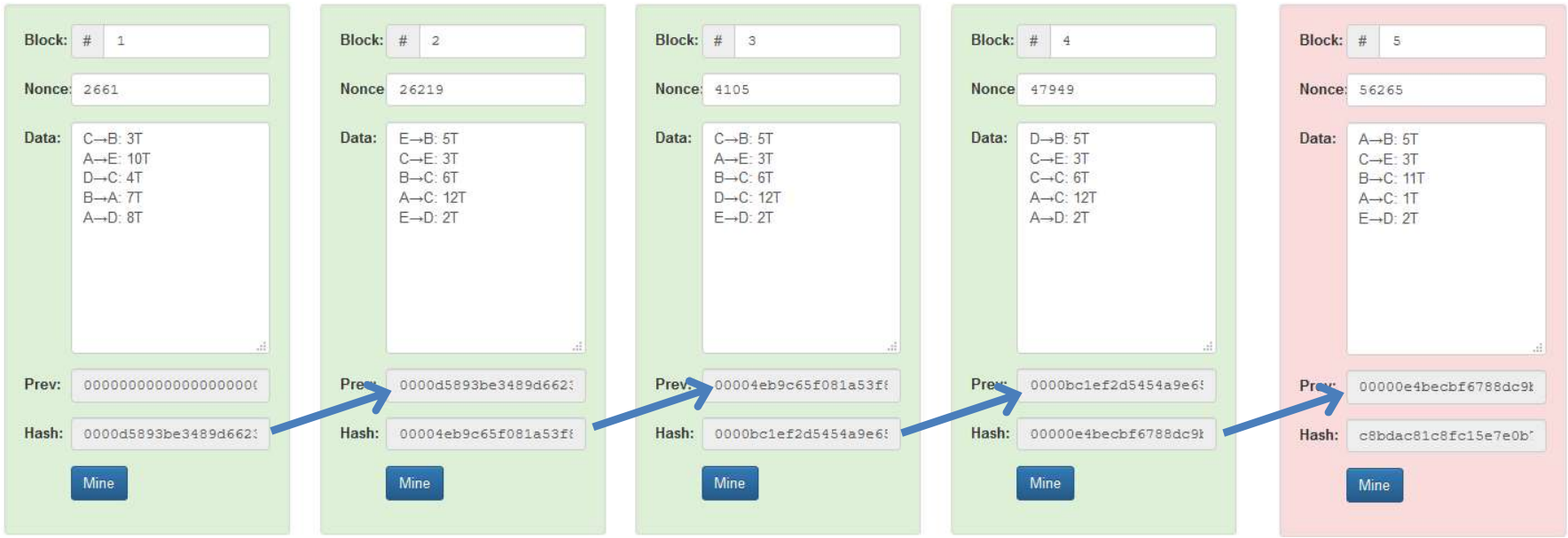
Blockchain – Wie funktioniert die Verkettung?



s. c't 23/2017

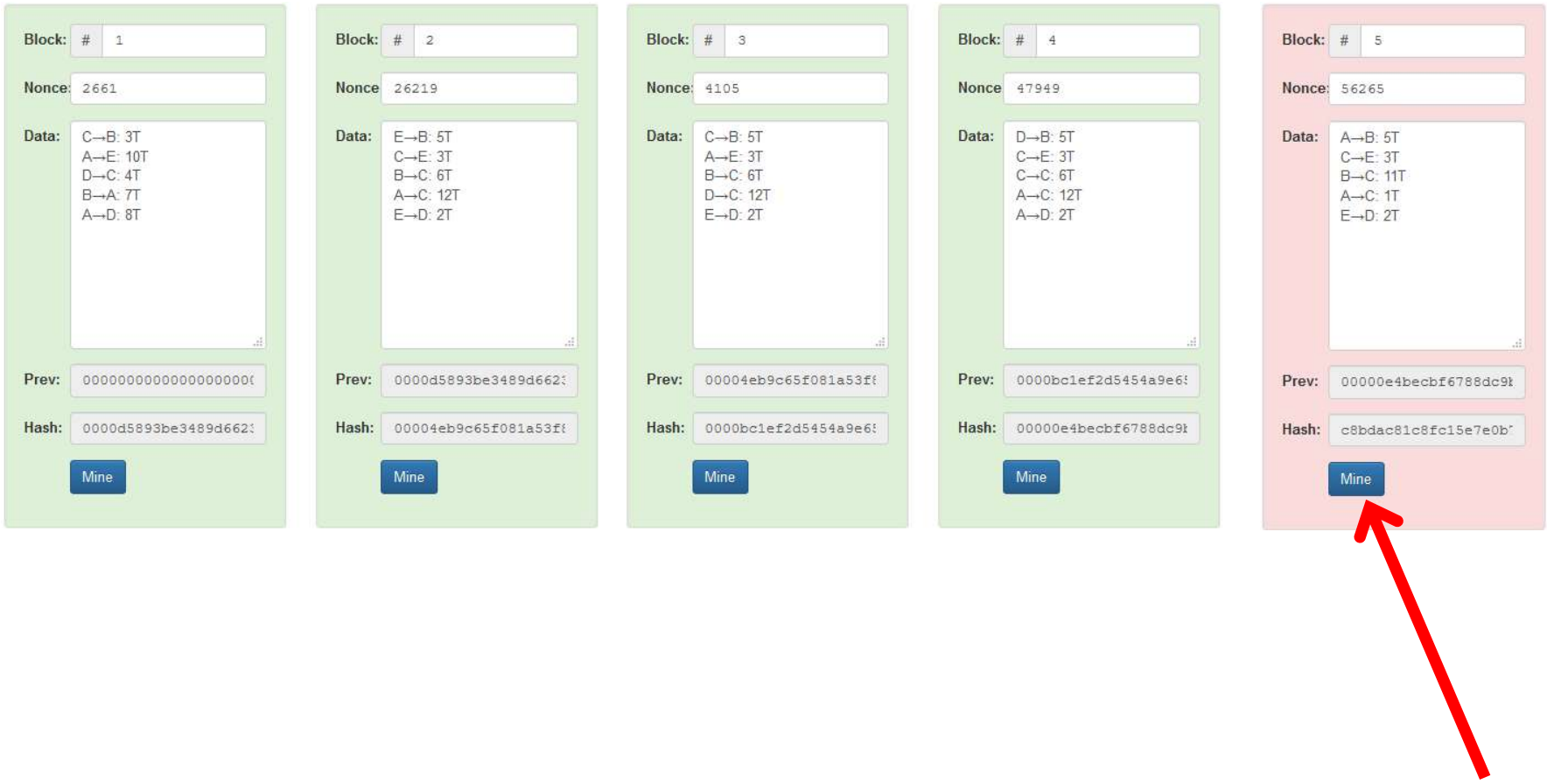
Blockchain-Demo

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



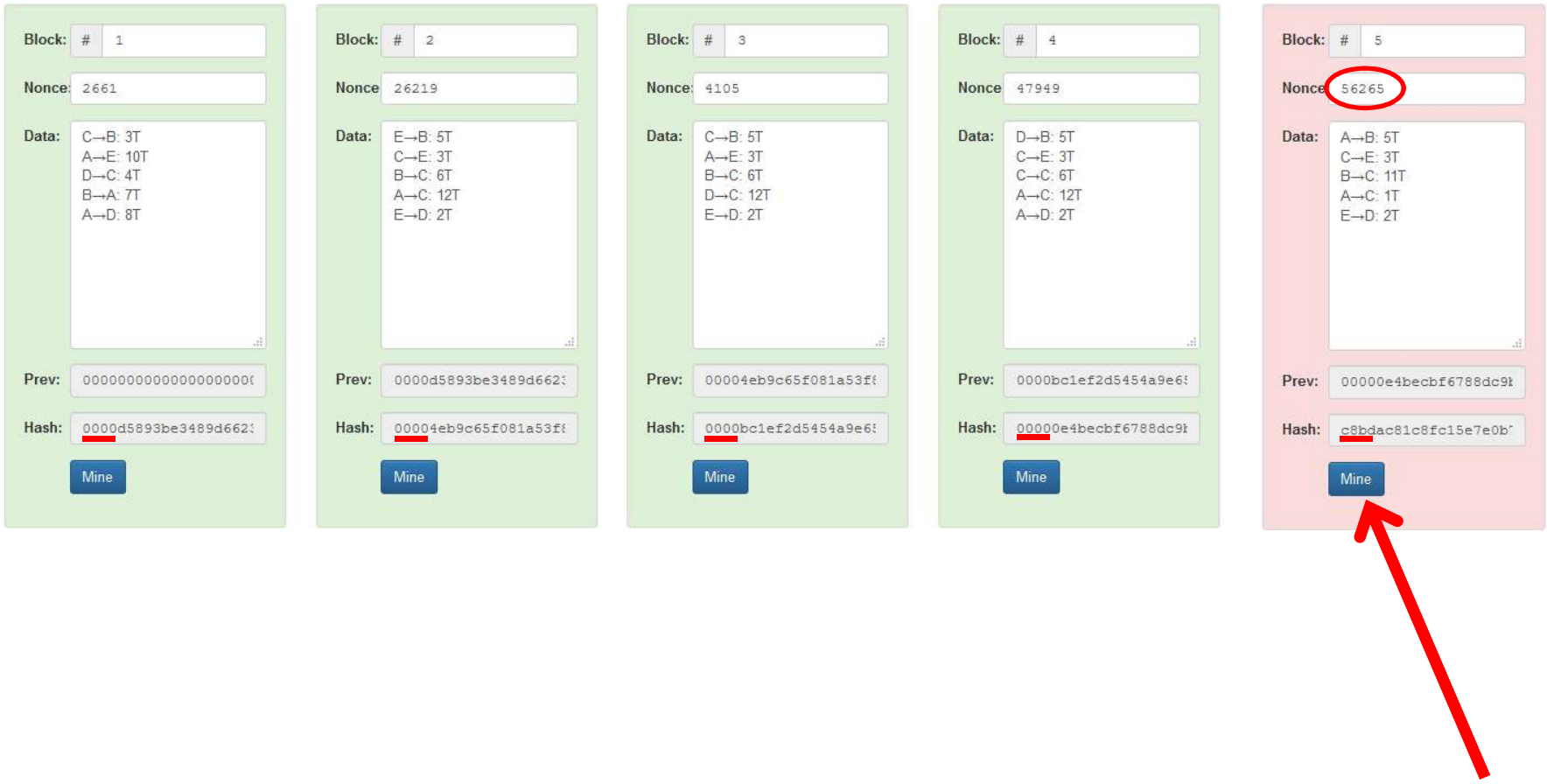
Blockchain-Demo

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



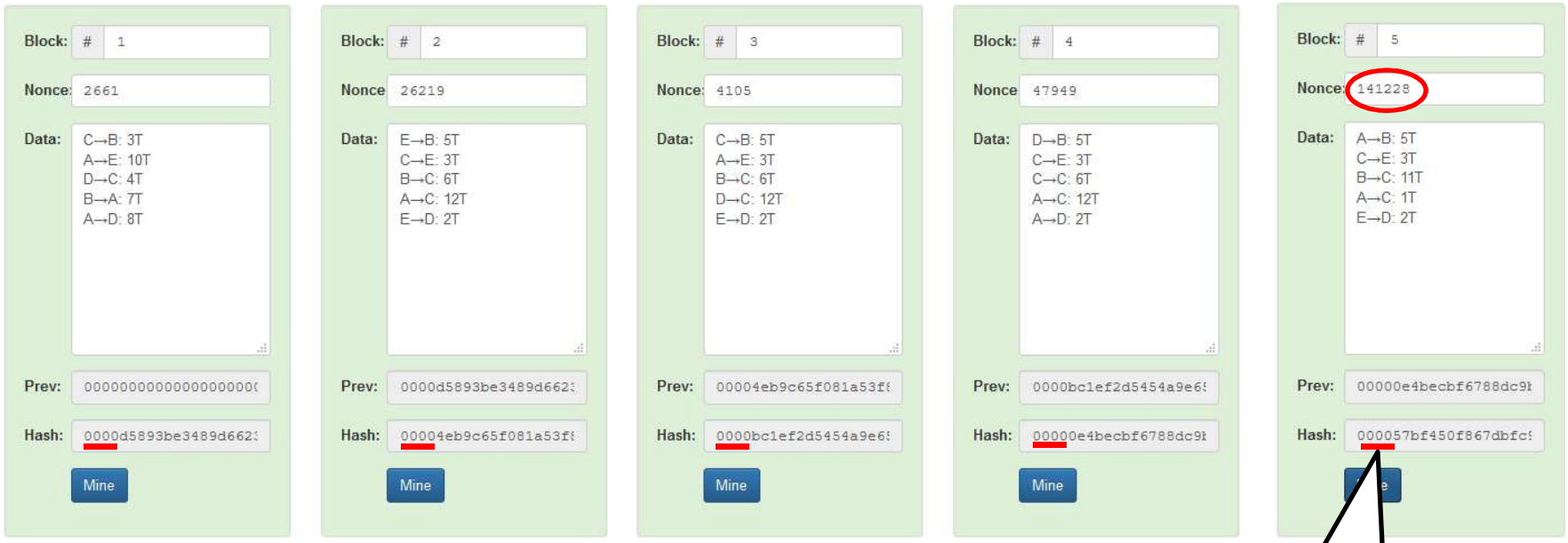
Blockchain-Demo

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



Blockchain-Demo

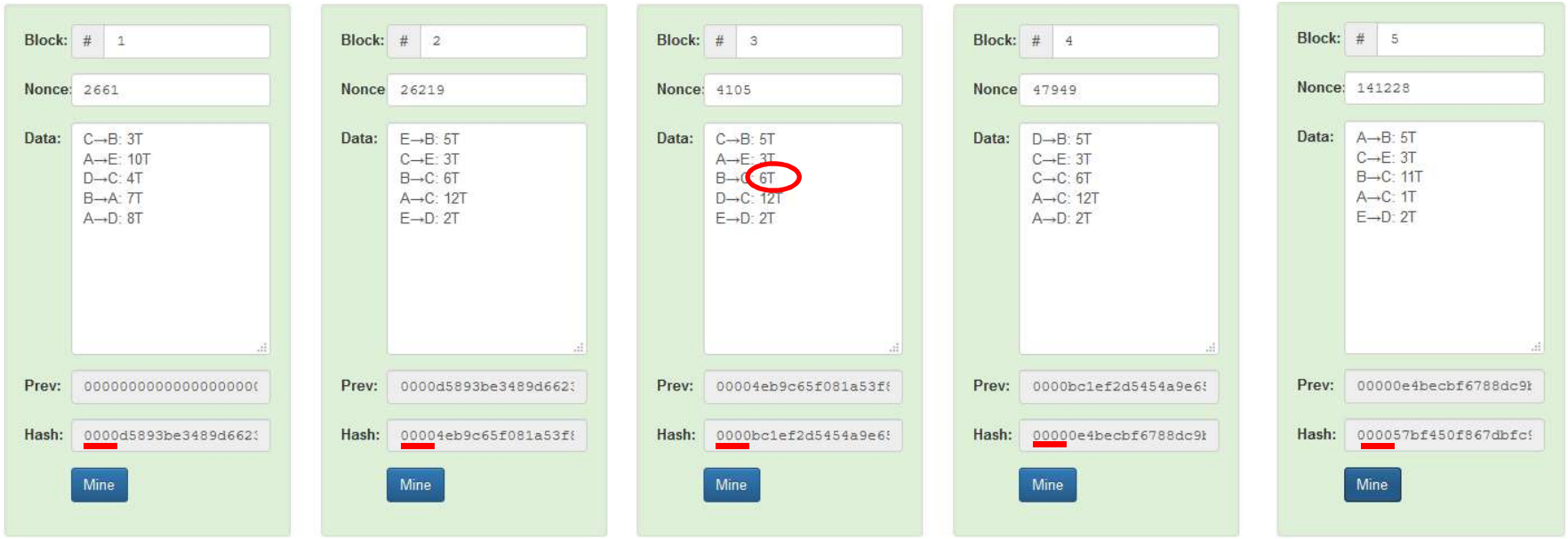
z.B. https://anders.com/blockchain/blockchain.html



Tatsächlich! Das „Schloss“ lässt sich damit öffnen!

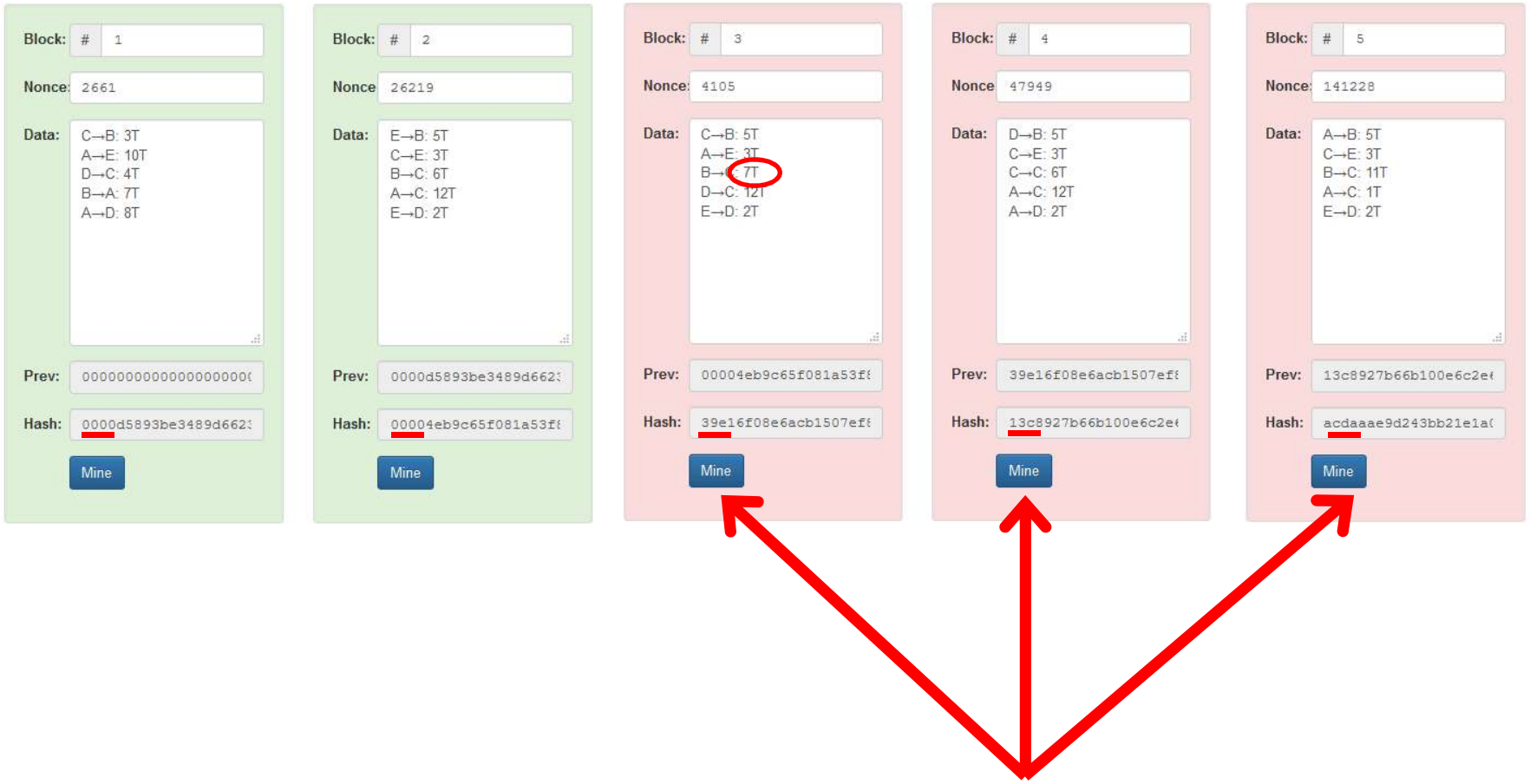
Blockchain-Demo

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



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

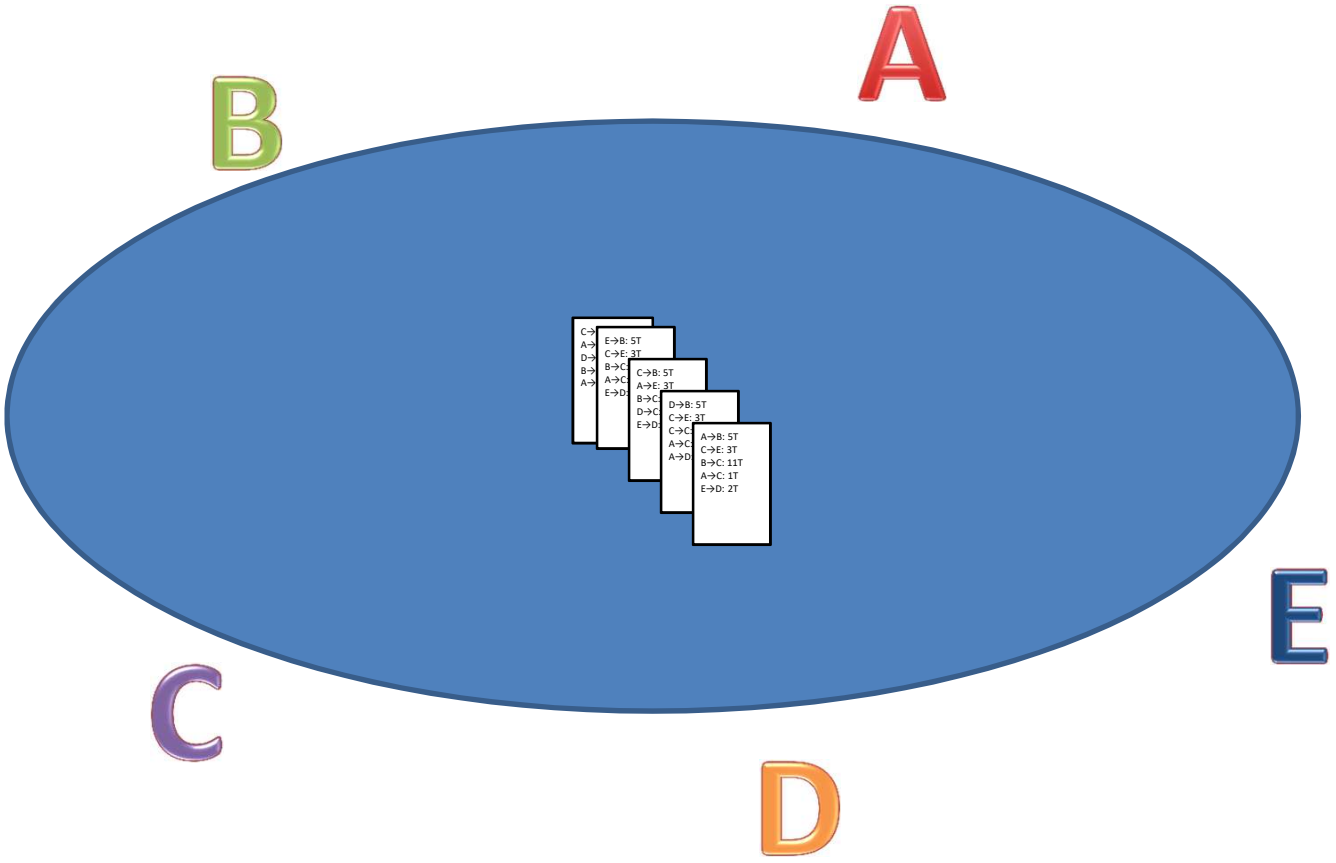
Hinweis: Diese Folie war in der ursprünglichen Fassung nicht vorhanden und wurde aufgrund der Diskussion auf der iMedia erstellt

- 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?


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