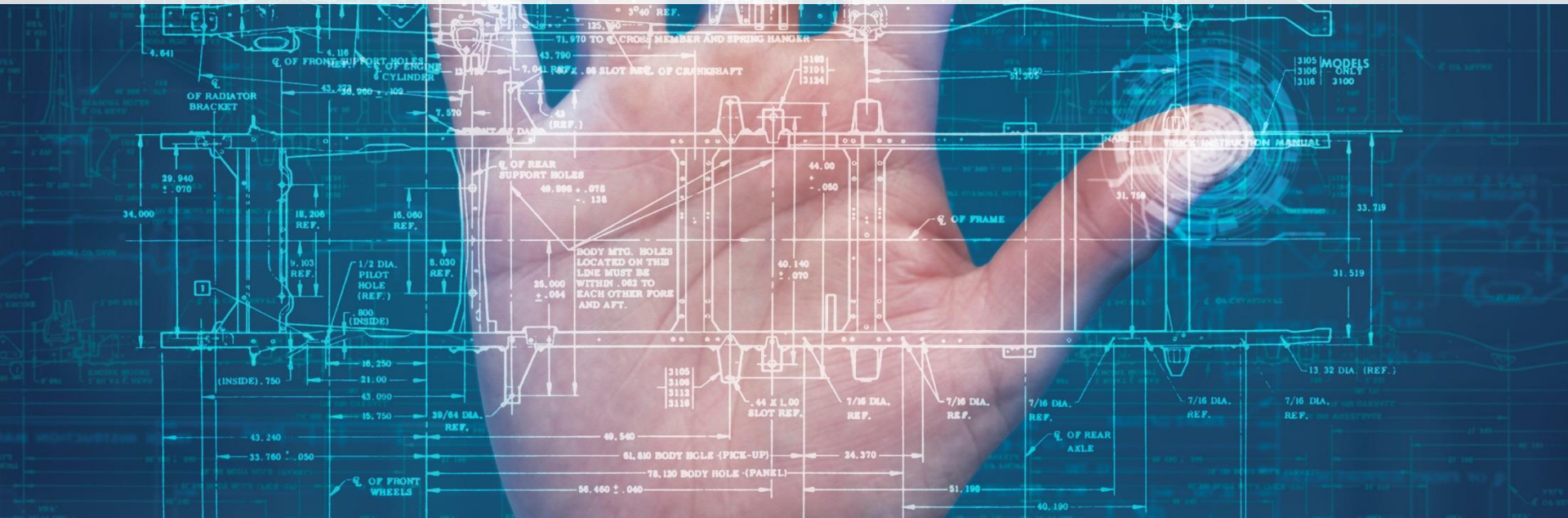
Blockchain am Beispiel von Kryptowährungen

Informationstagung Fachkommission Haft des SVV, 12. Mai 2019

Dr. Philipp Hurni, Cyber Model Lead, Swiss Re Cyber Centre of Competence



Agenda

- Public vs. Private Blockchains
- Blockchain-Prinzipien am Beispiel von Kryptowährungen
  - Wie funktioniert ein Kryptowährungssystem?
  - Wie funktioniert eine Transaktion?
  - Übersicht über Kryptowährungen
- Smart Contracts – die nächste Anwendung der Blockchain

Public vs. Private Blockchains

- Die Publikation des Bitcoin-Konzeptes in 2008 hat eine rasante Entwicklung losgetreten
- Eine Vielzahl von unterschiedlichen Blockchain-Konzepten sind in der Zwischenzeit entstanden.

  ⇨ Blockchain ≠ Bitcoin
- Eines der wichtigsten Unterscheidungskriterien ist die Frage, ob die Blockchain allen möglichen Teilnehmenden zugänglich ist, oder ob der Kreis der Partizipierenden eingeschränkt ist.

Public Blockchain
Permissionless

- Jeder kann dem Netz beitreten und lesen, schreiben, teilnehmen (z.b. “minen”)
- Teilnehmer sind anonym
- Niemand hat Kontrolle über das Netz. Transaktionen können nicht mehr verändert werden sobald validiert.
- Konsens via “Proof of Work” oder “Proof of Stake” (Mining)

Bitcoin (BTC)

Ethereum (ETH)

Private Blockchain
Permissioned

- Einschränkungen bezüglich der Teilnehmenden
- Identität der Teilnehmenden ist bekannt
- Einige Akteure können per Design mehr Rechte haben als andere
- Konsens via “Voting”

HYPERLEDGER

ripple

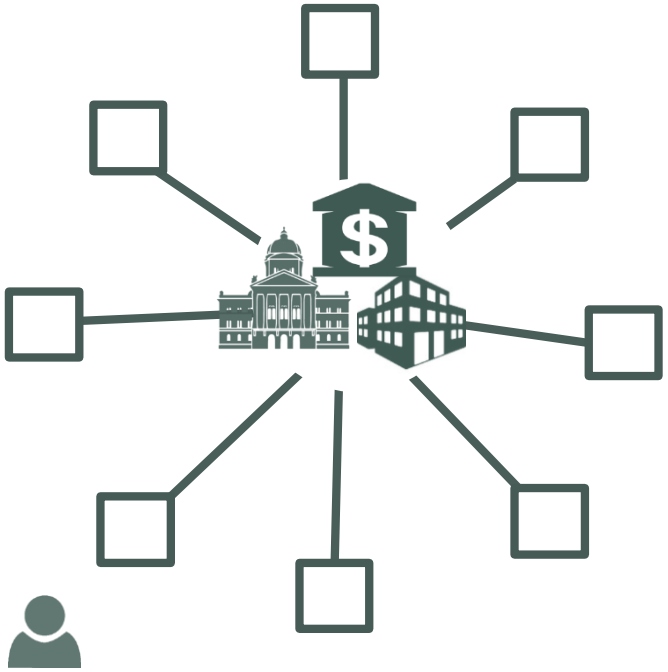
B3i

corda

- Blockchain ≠ Bitcoin
- Kryptowährung Bitcoin = die erste public permissionless Blockchain

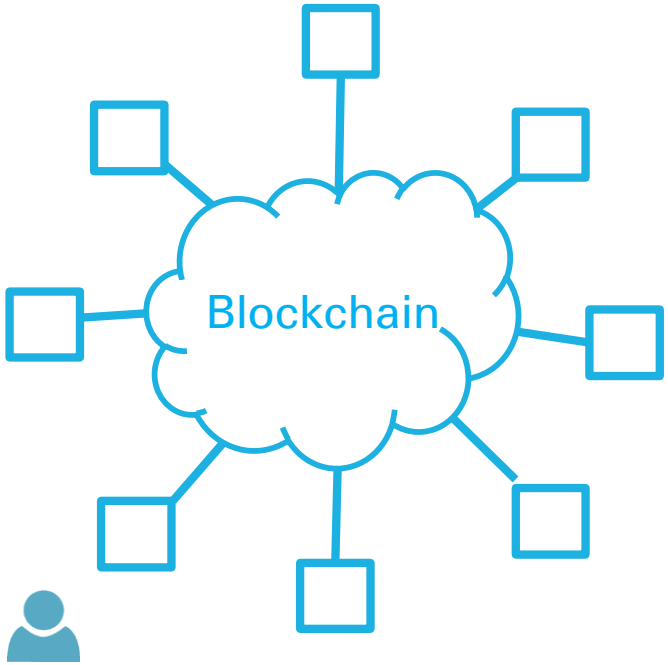
Wie funktioniert ein Kryptowährungssystem?
Fiatgeld vs. Kryptowährungen

Fiatgeld



- System zentraler Intermediäre (Nationalbanken, Geschäftsbanken)
- Vertrauen durch Staat, Regulierung, (offizielles Zahlungsmittel)

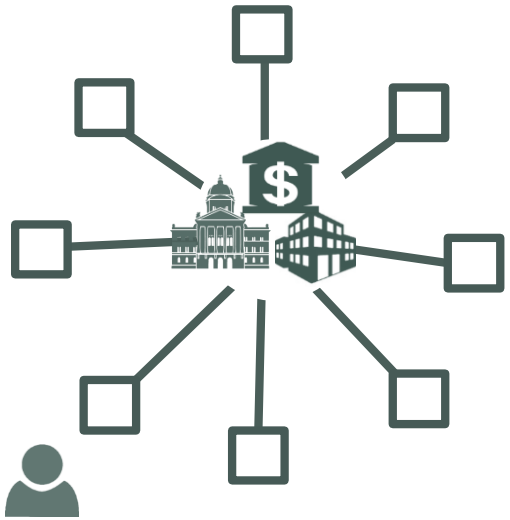
Kryptowährung



- Verteiltes System von gleichberechtigten Akteuren
- Vertrauen durch Kryptografie/Sicherheit der Algorithmen

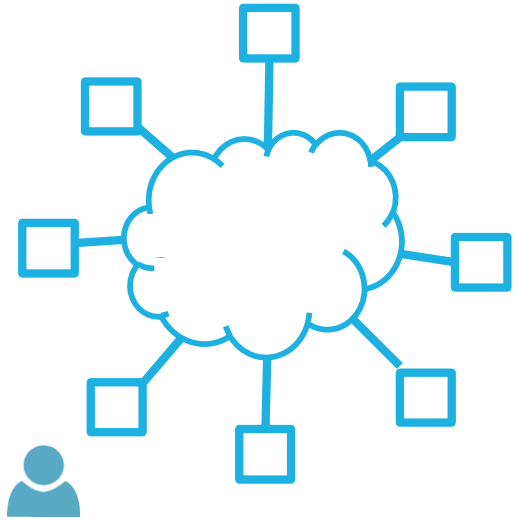
Wer (er)schafft Geld?

Fiatgeld



Nationalbank und Geschäftsbanken schaffen Geld und kontrollieren die Geldmenge

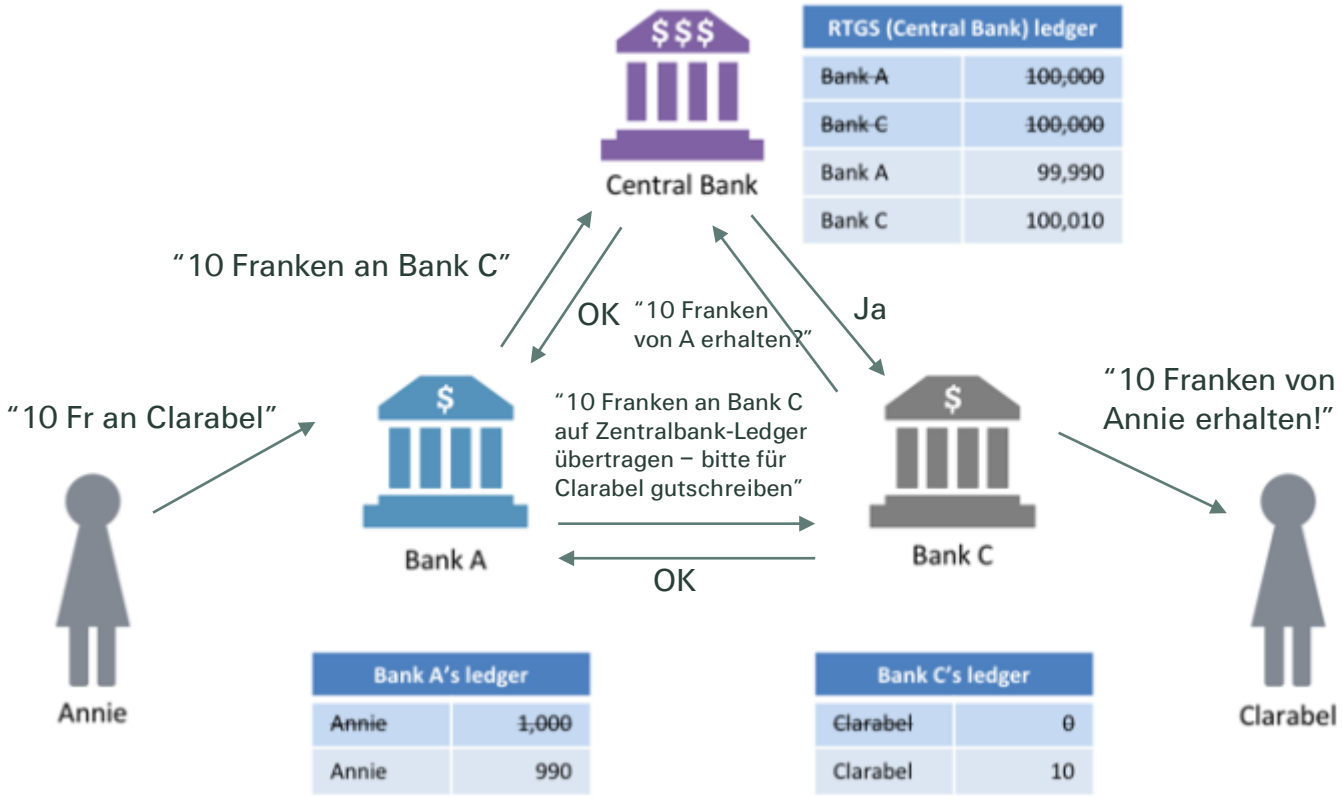
Kryptowährung



- Kryptowährungssystem (Algorithmus) definiert die Rate von neu produzierter Währung
- Jeder Akteur kann durch Mining an der Geldschöpfung teilnehmen, und ermöglicht damit gleichzeitig die Kernprozesse der Währung (Transaktionen)

Wie funktioniert eine Transaktion?

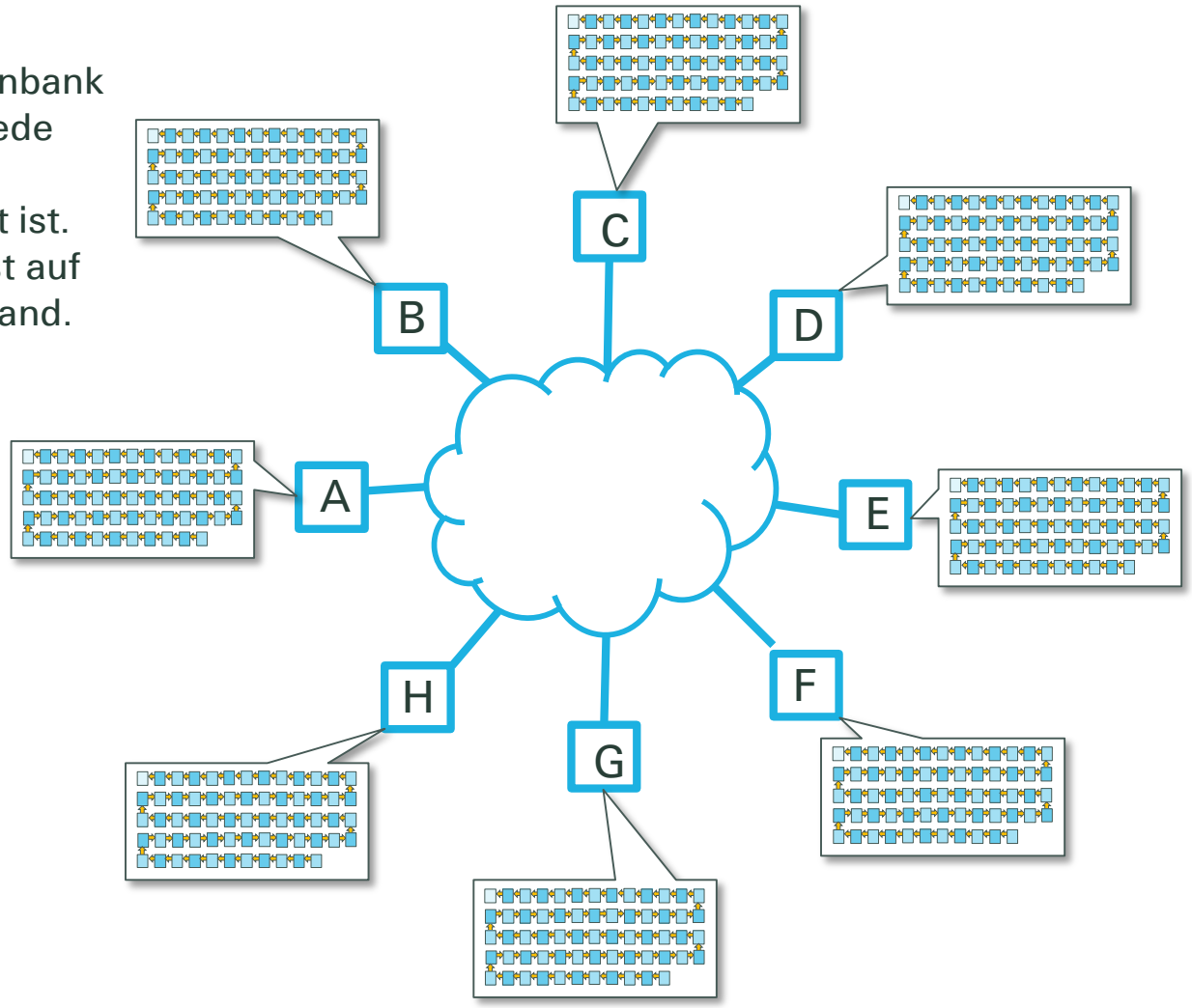
Fiatgeld



Wie funktioniert eine Transaktion?

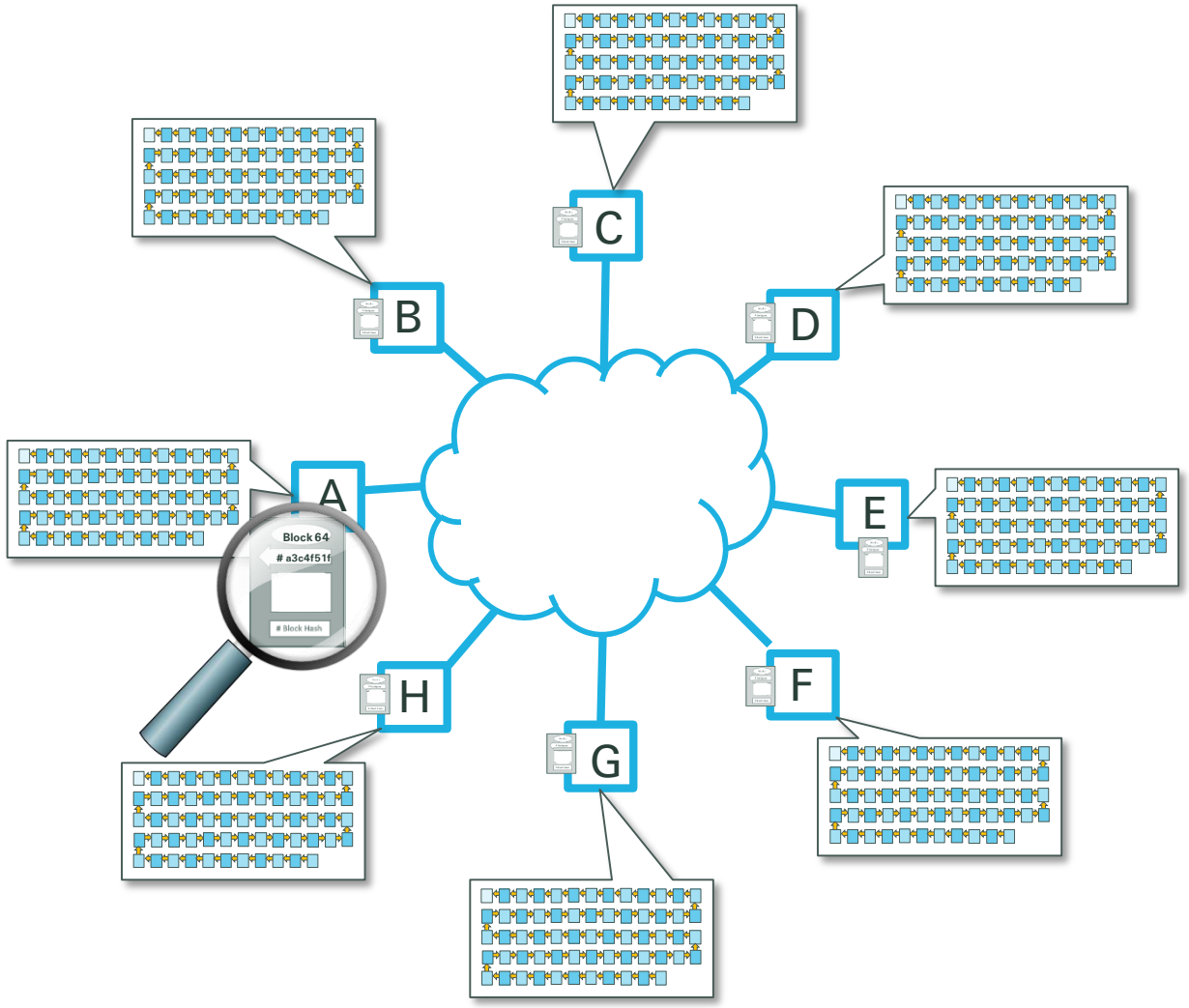
Jeder Rechner hält jederzeit eine Kopie der vollständigen Blockchain lokal.

Blockchain:
verteilte Datenbank auf welcher jede Transaktion aufgezeichnet ist. Jeder Node ist auf demselben stand.



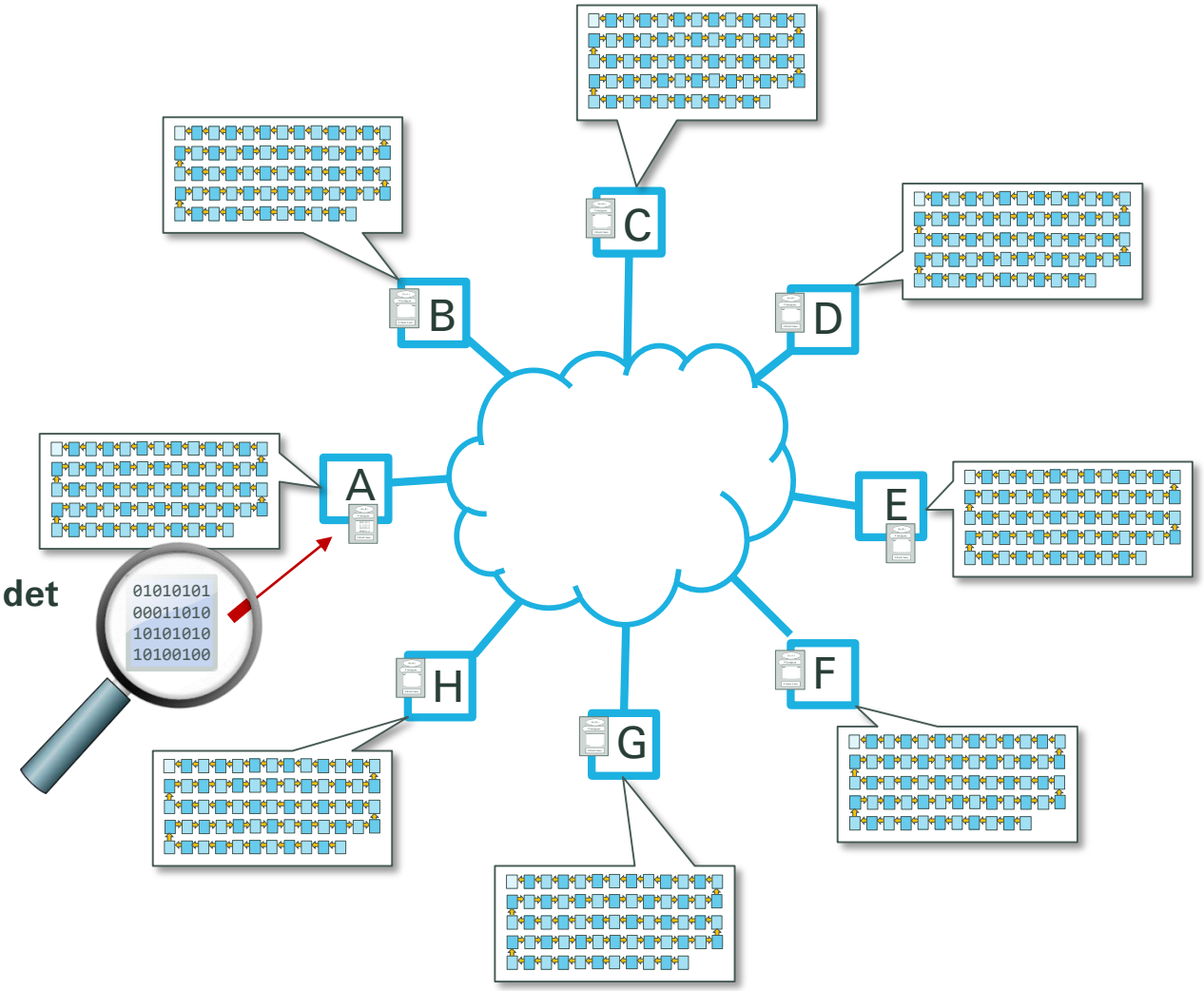
Wie funktioniert eine Transaktion?

Jeder Rechner hält einen neuen Block bereit für neue Daten.



Wie funktioniert eine Transaktion?

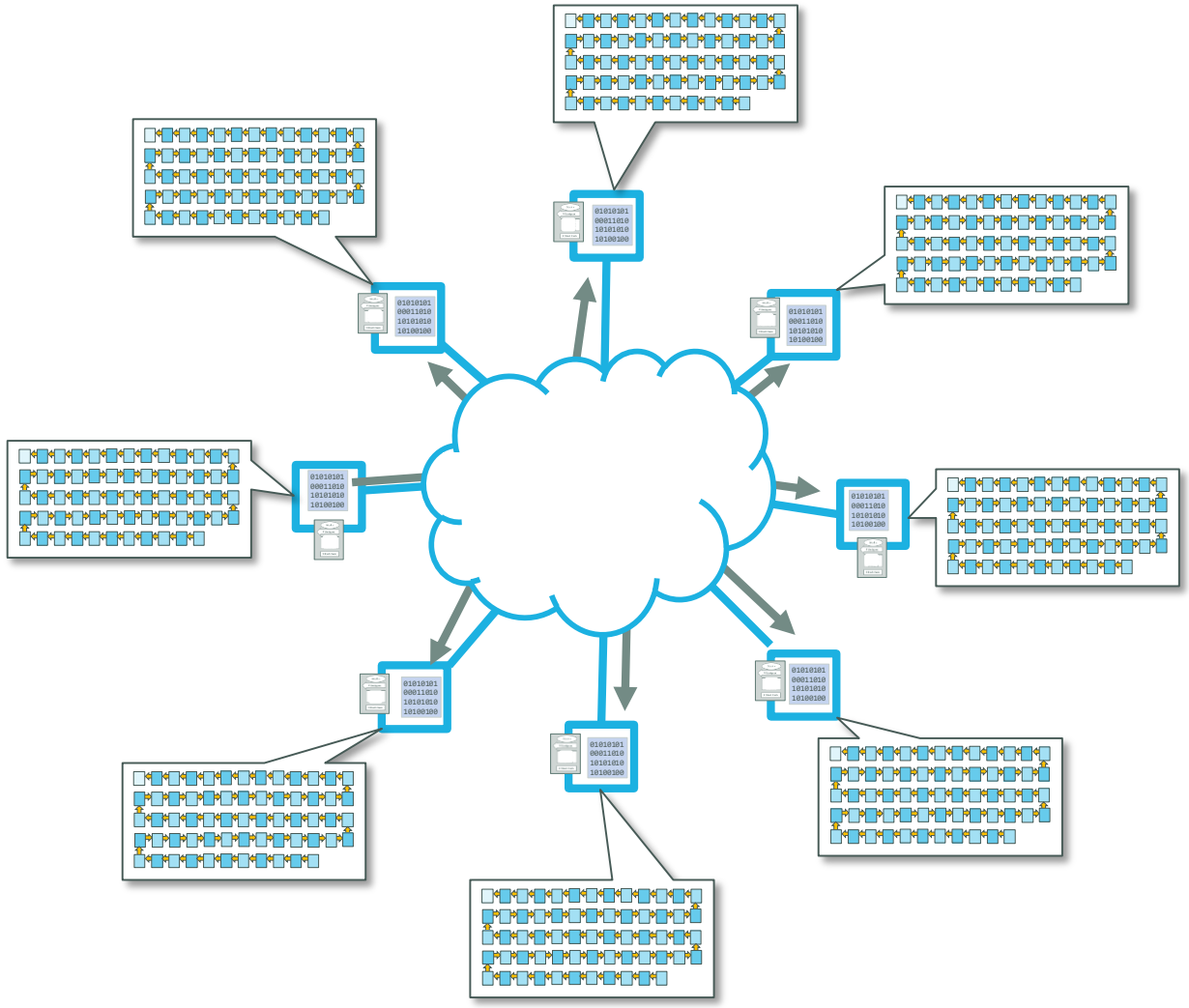
Eine neue Transaktion wird beim Rechner A erfasst



Beispiel: A sendet 1 Bitcoin zu B

Wie funktioniert eine Transaktion?

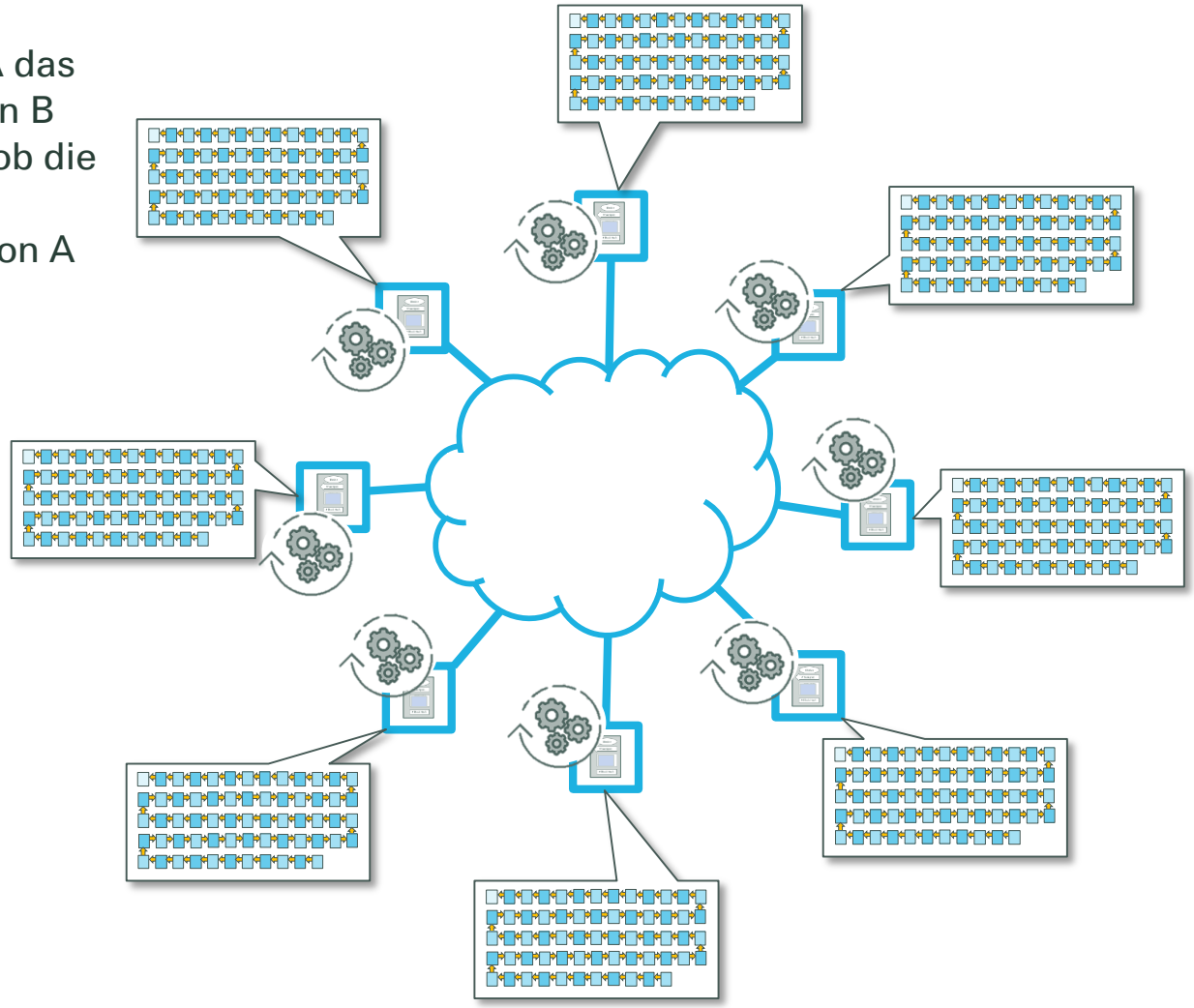
Die neue Transaktion wird sofort an alle Rechner gesendet – Netzwerkweiter Broadcast



Wie funktioniert eine Transaktion?

Jeder Rechner validiert nun den Block (verschiedene Methoden je Anwendung)

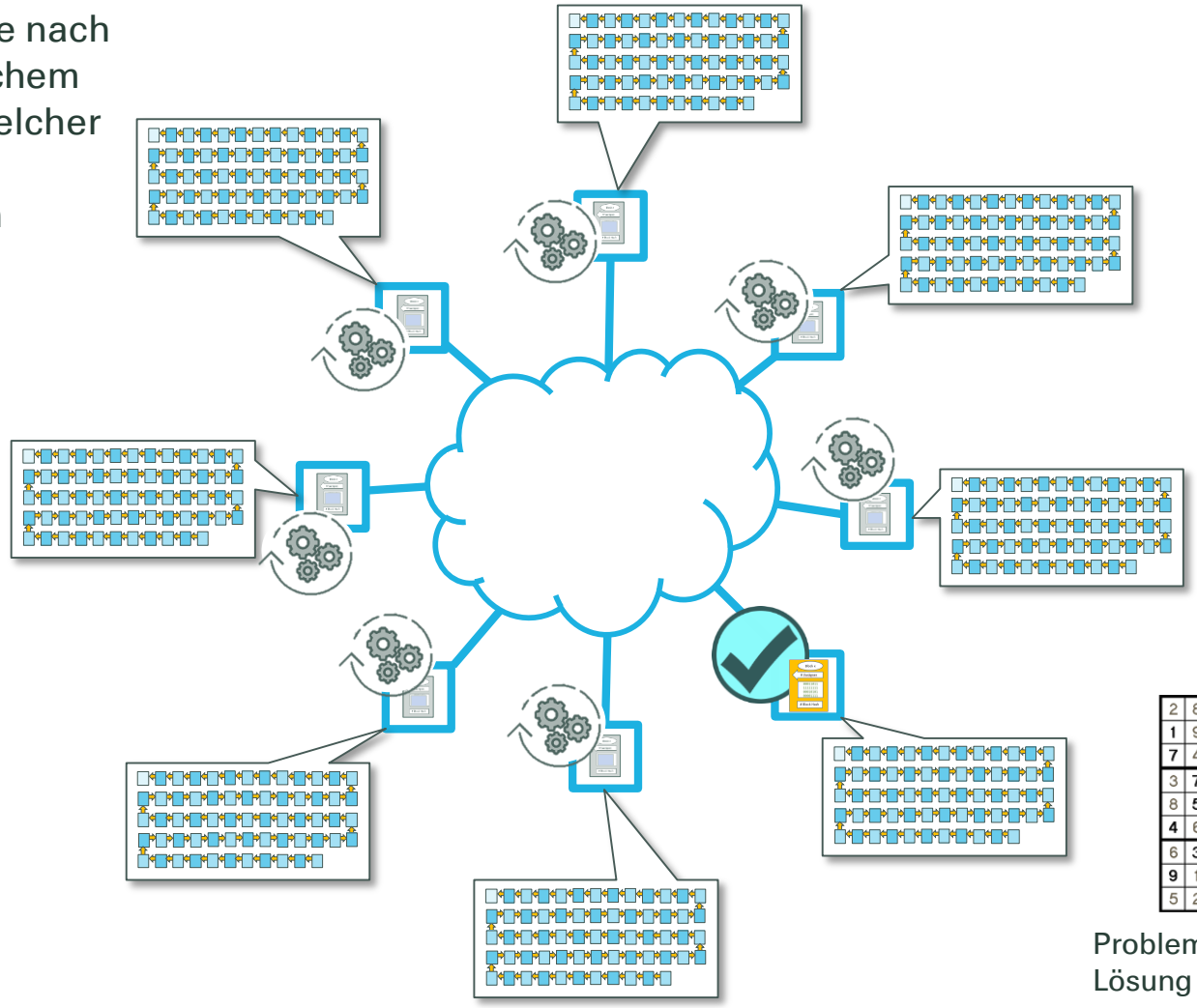
Validierung:
Prüfung ob A das Guthaben von B besitzt, und ob die Transaktion tatsächlich von A kommt



Wie funktioniert eine Transaktion?

Jeder Rechner validiert nun den Block (verschiedene Methoden je Anwendung)

Mining: suche nach Kryptografischem Hashwert, welcher bestimmte Bedingungen erfüllt.

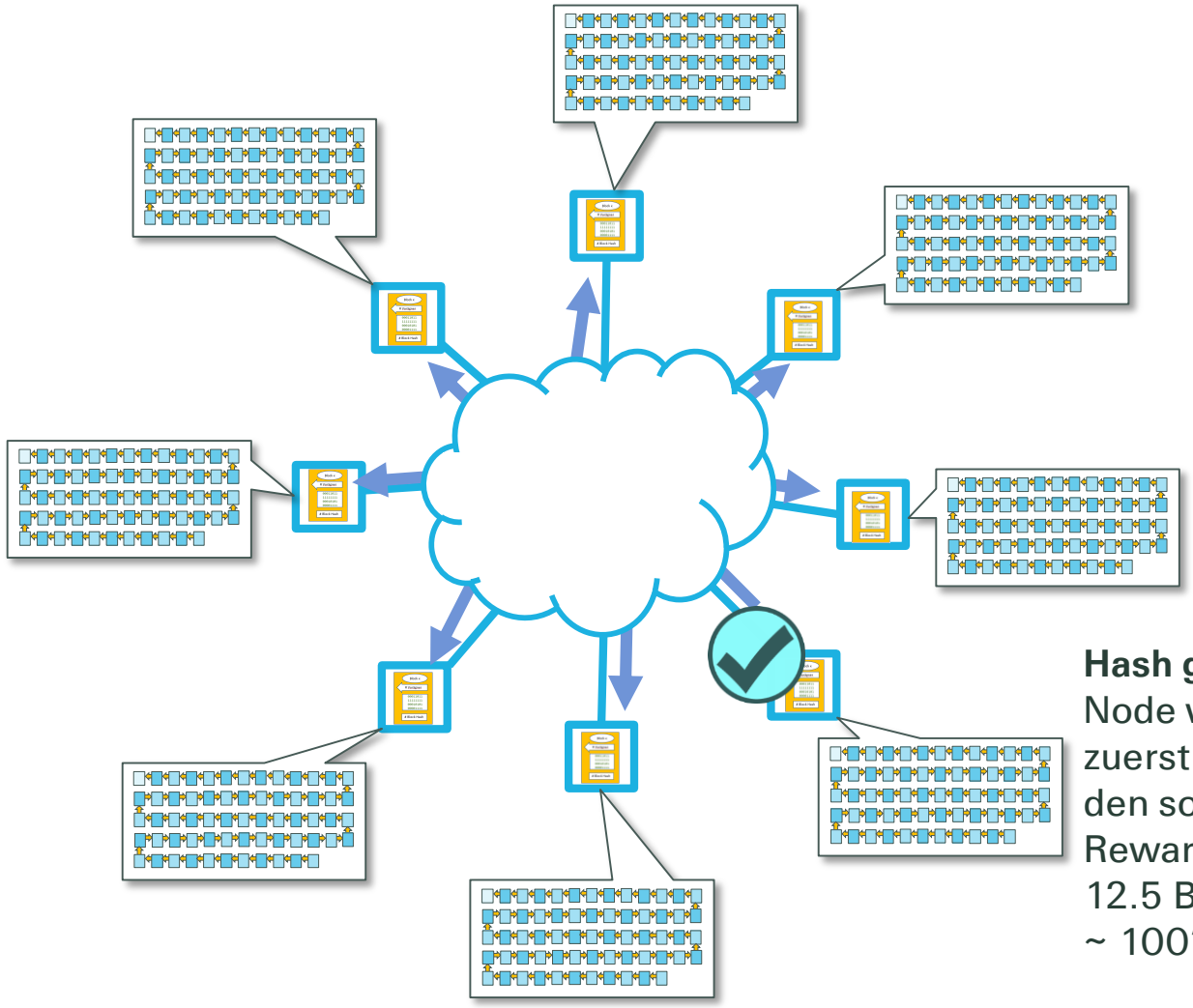


2	8	6	1	5	4	9	7	3
1	9	5	7	6	3	8	4	2
7	4	3	2	8	9	5	1	6
3	7	9	6	2	5	4	8	1
8	5	1	3	4	7	6	2	9
4	6	2	9	1	8	7	3	5
6	3	4	5	7	2	1	9	8
9	1	7	8	3	6	2	5	4
5	2	8	4	9	1	3	6	7

Problem lösen: schwierig
Lösung validieren: einfach!

Wie funktioniert eine Transaktion?

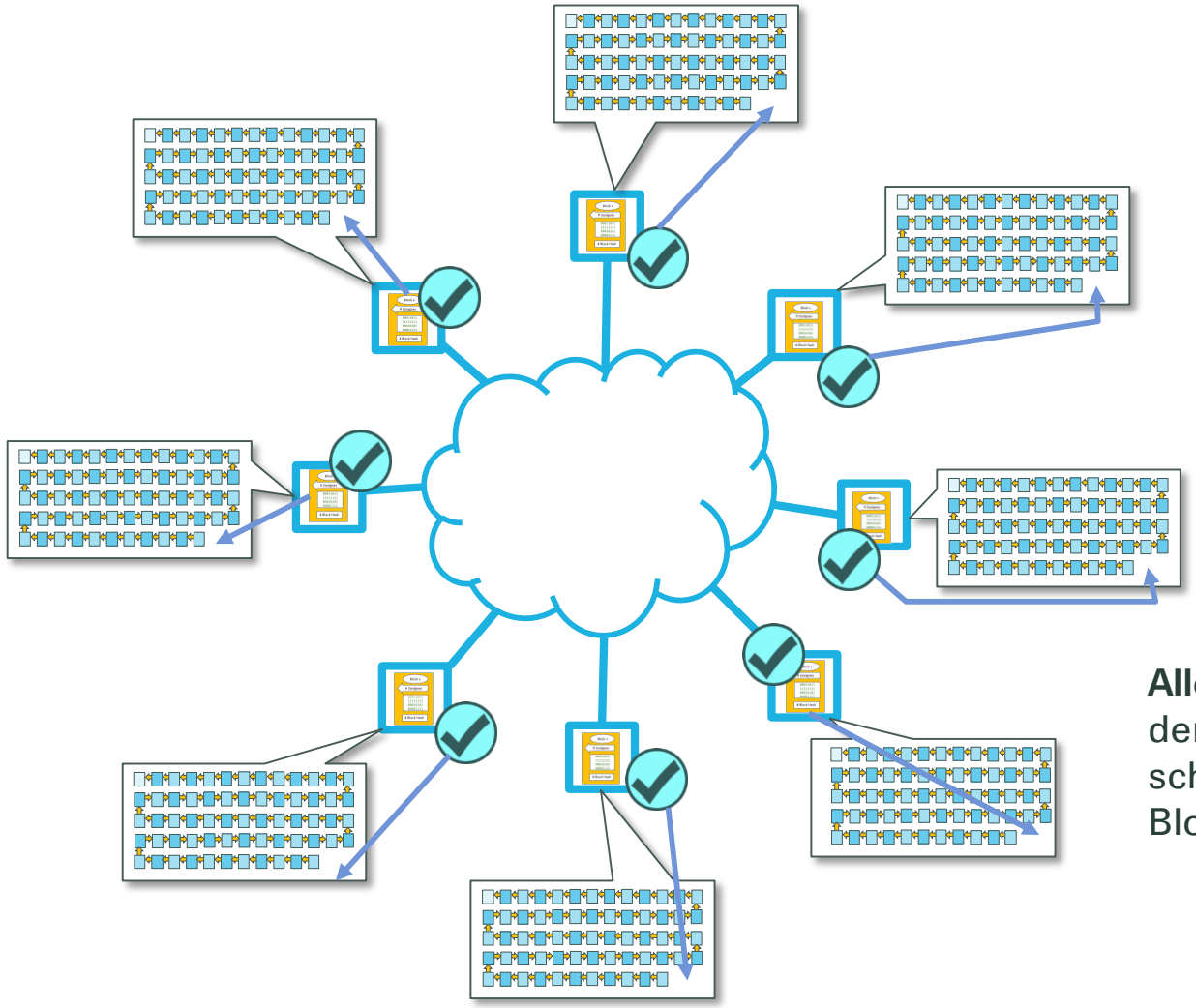
Jeder Rechner validiert nun den Block (verschiedene Methoden je Anwendung)



Hash gefunden! Der Node welcher den Hash zuerst findet, bekommt den sogenannten Block-Reward
12.5 BTC
~ 100'000 CHF

Wie funktioniert eine Transaktion?

Jeder Rechner validiert nun den Block (verschiedene Methoden je Anwendung)



Alle nodes prüfen den Hash und schliessen den Block ab.

Ein Node der Kryptowährung Ethereum

Ethereum Mining Rig @ Olten

> 6 Grafikkarten vom Typ Radeon 580

> 6 * 25 MHash/s

> Stromverbrauch ~ 750 Watt

> Kommunikation rund 10 Mbps

> Rund 16'000 Nodes weltweit

⇨ Seit Sommer 2018 ausser Betrieb wegen negativer Rentabilität...

Die Welt der Kryptowährungen ist volatil!

- Es gibt über 2000 verschiedene Kryptowährungen
- Neue tauchen beinahe täglich auf, andere verschwinden
- Bitcoin is momentan «Platzhirsch», Ethereum auf Platz 2
- aktuell rund 250 mia USD market cap – Januar 2018 fast bei 1'000 Mia USD!

Cryptocurrencies: 2194 • Markets: 18573 • Market Cap: $246,485,851,227 • 24h Vol: $78,476,394,629 • BTC Dominance: 56.6%

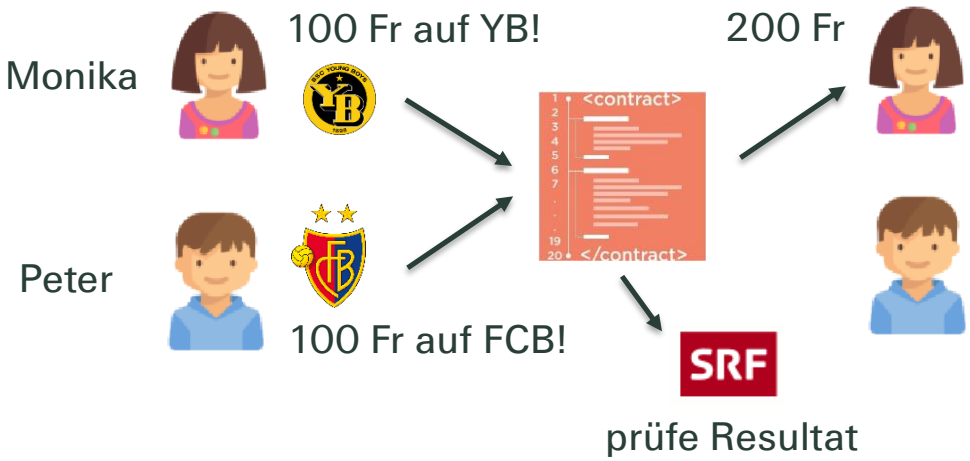
Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$139,397,778,673	$7,868.67	$23,961,533,932	17,715,537 BTC
2	Ethereum	$26,807,492,841	$252.49	$12,413,084,847	106,173,987 ETH
3	XRP	$16,478,588,647	$0.391260	$1,781,562,039	42,116,677,673 XRP *
4	Bitcoin Cash	$7,234,544,225	$406.52	$2,315,846,205	17,796,063 BCH
5	EOS	$5,671,959,819	$6.21	$1,947,513,054	912,660,760 EOS *
6	Litecoin	$5,590,250,963	$90.33	$3,369,406,003	61,884,376 LTC

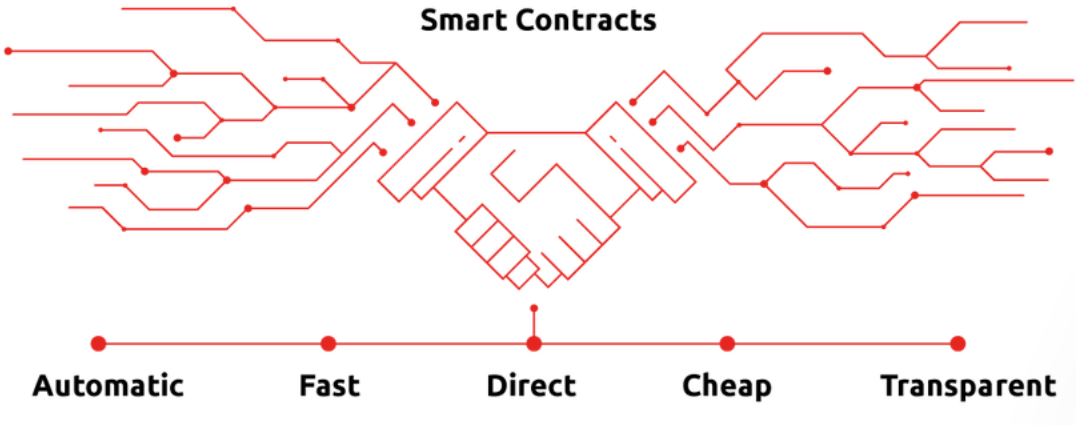
Smart Contracts – die nächste grosse Anwendung der Blockchain

- Smart Contracts sind **öffentlich einsehbare Programme**, welche auf Blockchains gespeichert werden können.
- In Smart Contracts werden **Bedingungen** festgelegt, bei deren Eintreten der Vertrag **ohne weitere Einwirkung der beiden Vertragsparteien ausgeführt werden.**
- Smart Contracts haben das Potenzial, Vertragssicherheit in diversen Anwendungen zu gewährleisten wo heute Intermediäre benötigt werden.



Mögliche Anwendungsfelder von Blockchain-basierten Smart Contracts

- Online Wetten / Glücksspiel
- (Parametrische) Versicherung
- Wertschriftenhandel / Börse
- Fremdwährungshandel
- Verschreibung von Immobilien / Grundbucheinträge



Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.