



Mittwoch, 7. September 2022, 12.30 bis 13.30 Uhr

BLOCKCHAIN, BITCOIN & CO

EINFACH NUR KRYPTISCH ODER ENDLICH MAL INNOVATIV?



Blockchain, Bitcoin & Co.

Einfach nur kryptisch oder endlich mal innovativ?

Marco Leder



Inhaltsverzeichnis

- Anwendungen und Fakten
- Struktur und Design
- Vor- und Nachteile
- Ausblick



**Universität
Zürich** ^{UZH}

Institut für Informatik

Anwendungen und Fakten

Heutige Anwendungen

- Internationale Zahlungen
- Abstimmungen
- Steuern (Kanton Zug)
- Legislatorische Kontrollen (Irland)
- Versicherung (lemonade insurance)

Fakten

*Satoshi
Nakamoto*
2008



2015

1991

Stuart Haber &
Scott Stornetta

2009

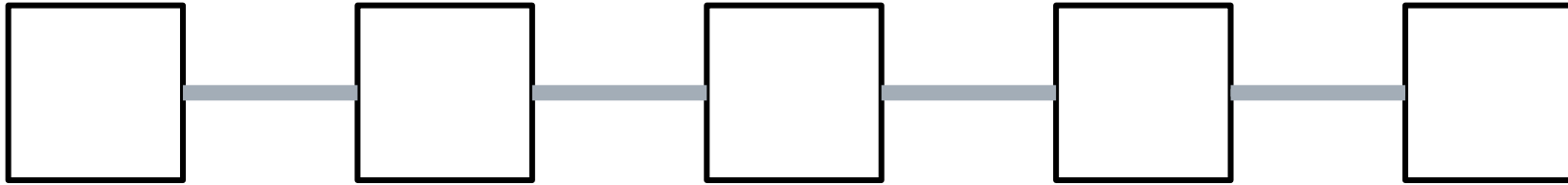


Heute



Einleitung und Fakten

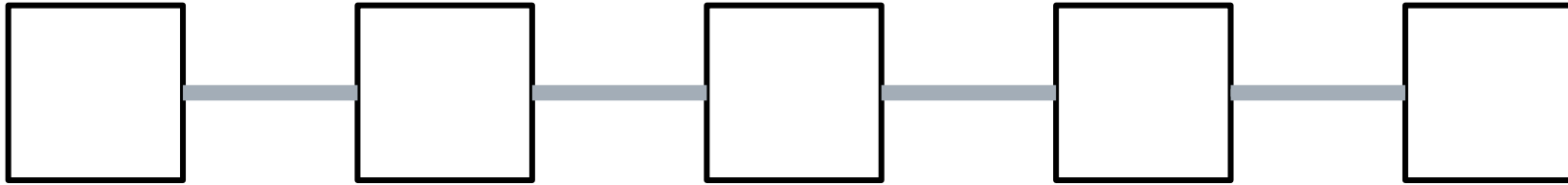
Blockchain



- Inhalt des Blocks?
- Wo existiert diese Kette von Blocks?

Einleitung und Fakten

Blockchain



- Anfügen von Blöcken?
- Nutzen des Systems?

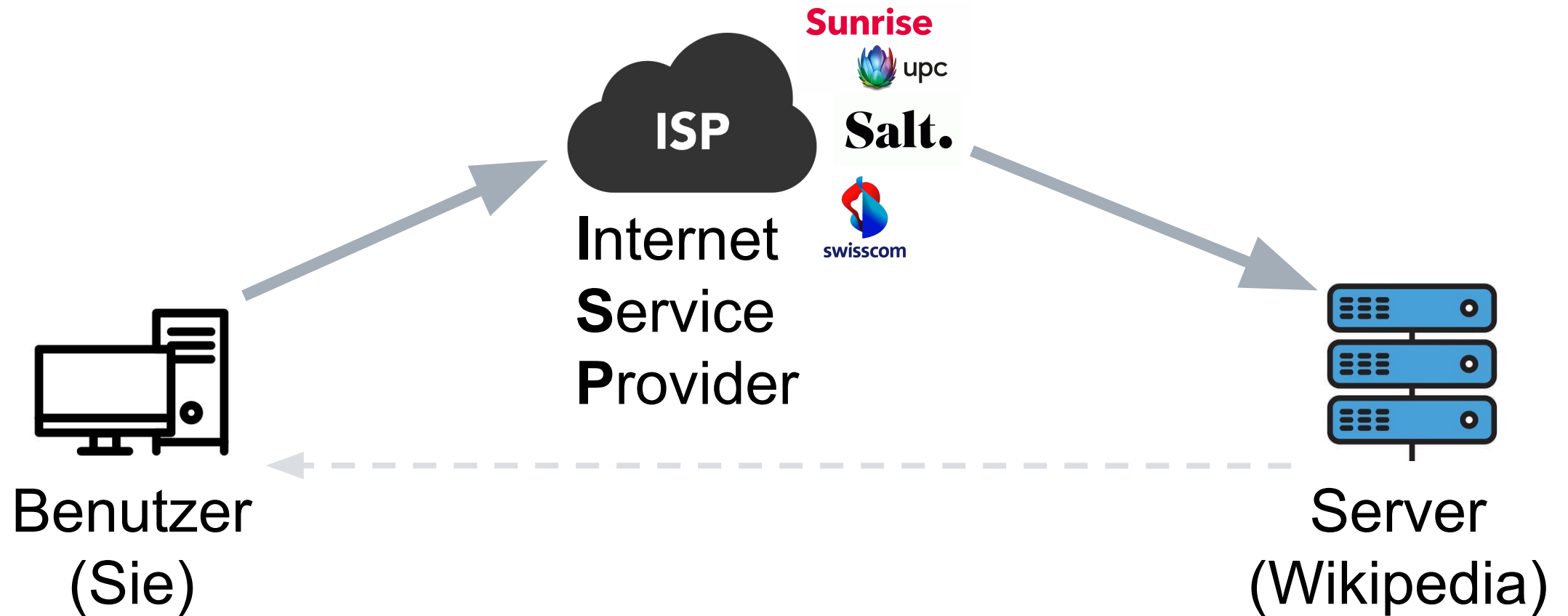


**Universität
Zürich** ^{UZH}

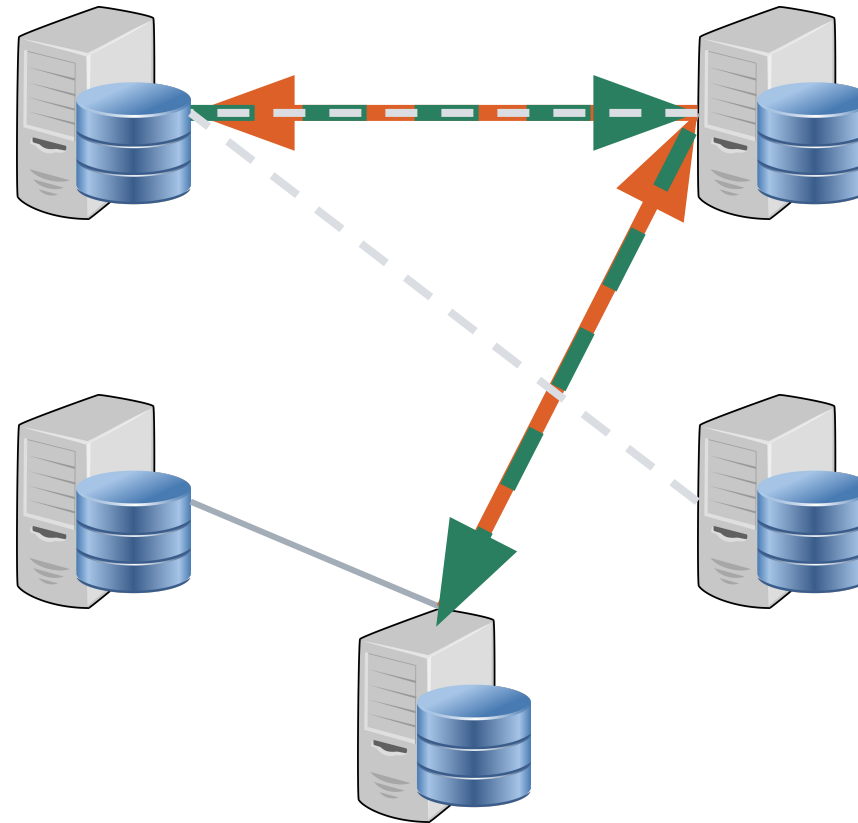
Institut für Informatik

Struktur und Design

Netzwerk - traditionell



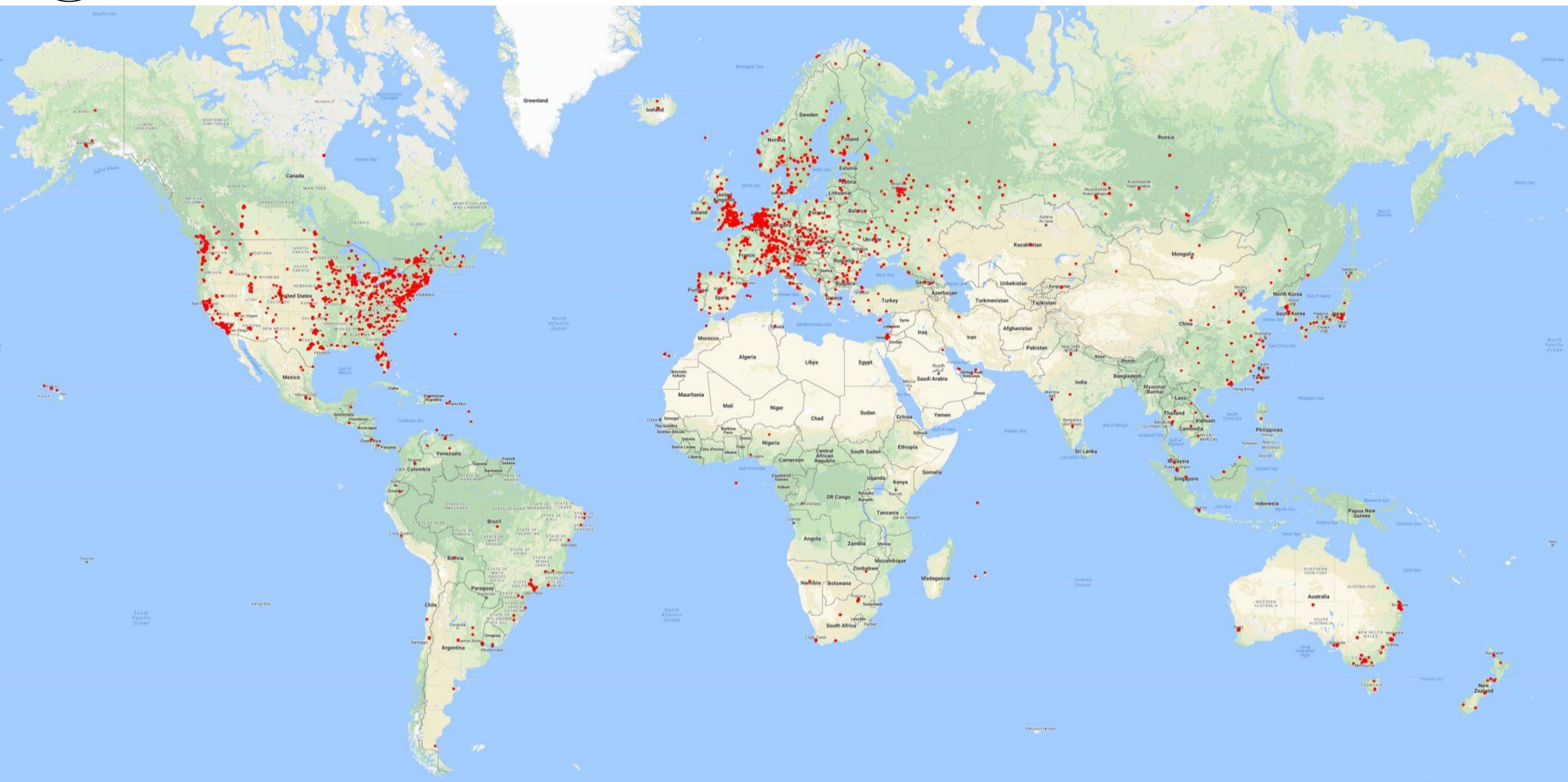
Netzwerk - peer to peer (P2P)



Node



Universität
Zürich ^{UZH}



Infrastruktur

- Blockchain ist eine “distributed ledger technology” (DLT)
- Distributed: Daten sind dezentral an verschiedenen Orten
- Ledger: Kontenbuch / Kassenbuch



BANK #1

TEMPLE	+ £11.00
WYATT	+ £8184.00
SIMONE	+ £4239.00

BANK #2

COLEEN	+ £3407.00
TANNER	+ £2501.00
KELLIE	+ £8871.00

BANK #3

LELAH	+ £4139.00
CLARK	+ £8760.00
MIGUEL	+ £1544.00

BANK #4

KRYSTAL	+ £3641.00
JONIE	£6316.00
TATIANA	+ £8638.00



BANK #1

TEMPLE	+ £11.00
WYATT	+ £8184.00
SIMONE	+ £4239.00

BANK #2

COLEEN	+ £3407.00
TANNER	+ £2501.00
KELLIE	+ £8871.00

BANK #3

LELAH	+ £4139.00
CLARK	+ £8760.00
MIGUEL	+ £1544.00

BANK #4

KRYSTAL	+ £3641.00
JONIE	£6316.00
TATIANA	+ £8638.00



TEMPLE	+ £11.00	COLEEN	+ £3407.00
WYATT	+ £8184.00	TANNER	+ £2501.00
SIMONE	+ £4239.00	KELLIE	+ £8871.00
LELAH	+ £4139.00	KRYSTAL	+ £3641.00
CLARK	+ £8760.00	JONIE	£6316.00
MIGUEL	+ £1544.00	TATIANA	+ £8638.00

Infrastruktur - Ledger

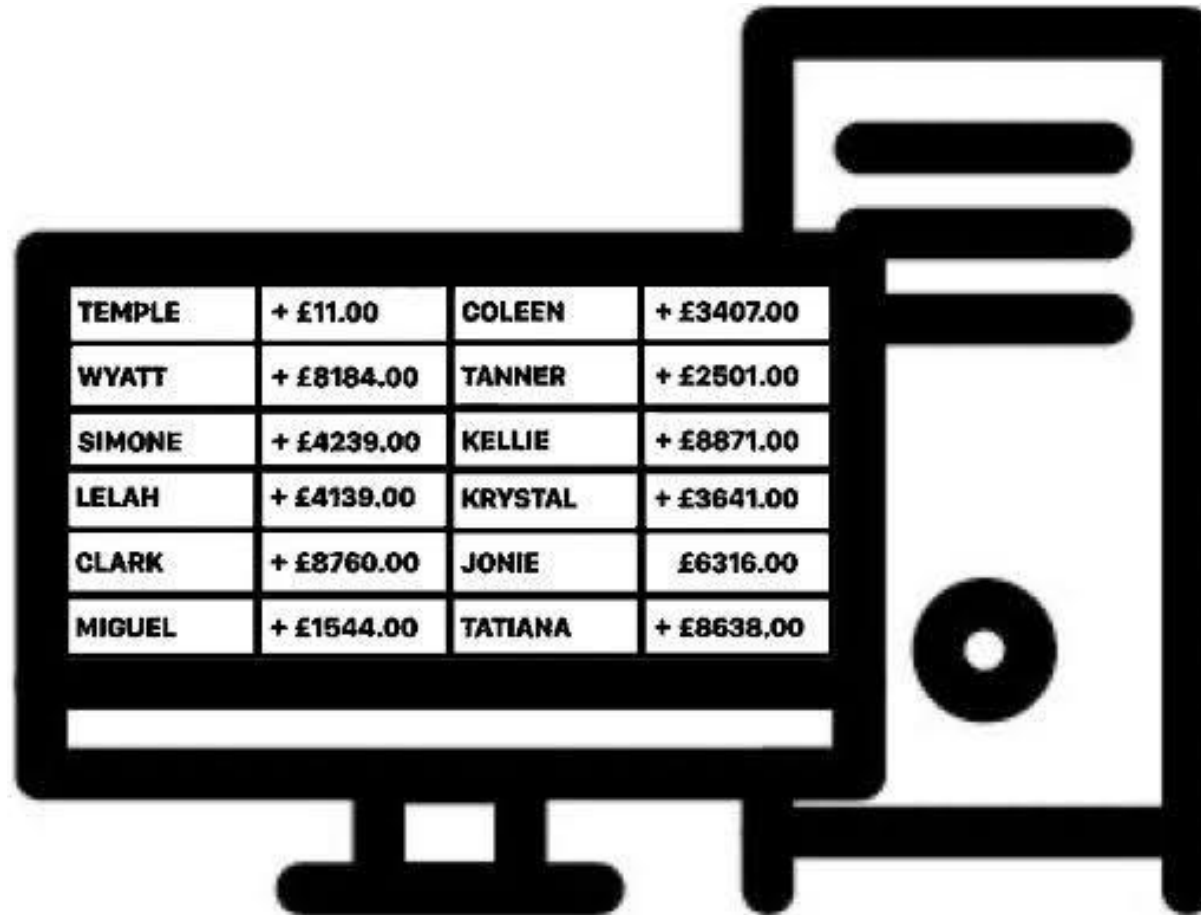
TEMPLE	+ £11.00
WYATT	+ £8184.00
SIMONE	+ £4239.00
LELAH	+ £4139.00
CLARK	+ £8760.00
MIGUEL	+ £1544.00

COLEEN	+ £3407.00
TANNER	+ £2501.00
KELLIE	+ £8871.00
KRYSTAL	+ £3641.00
JONIE	£6316.00
TATIANA	+ £8638.00

TEMPLE	+ £11.00
WYATT	+ £8184.00
SIMONE	+ £4239.00
LELAH	+ £4139.00
CLARK	+ £8760.00
MIGUEL	+ £1544.00

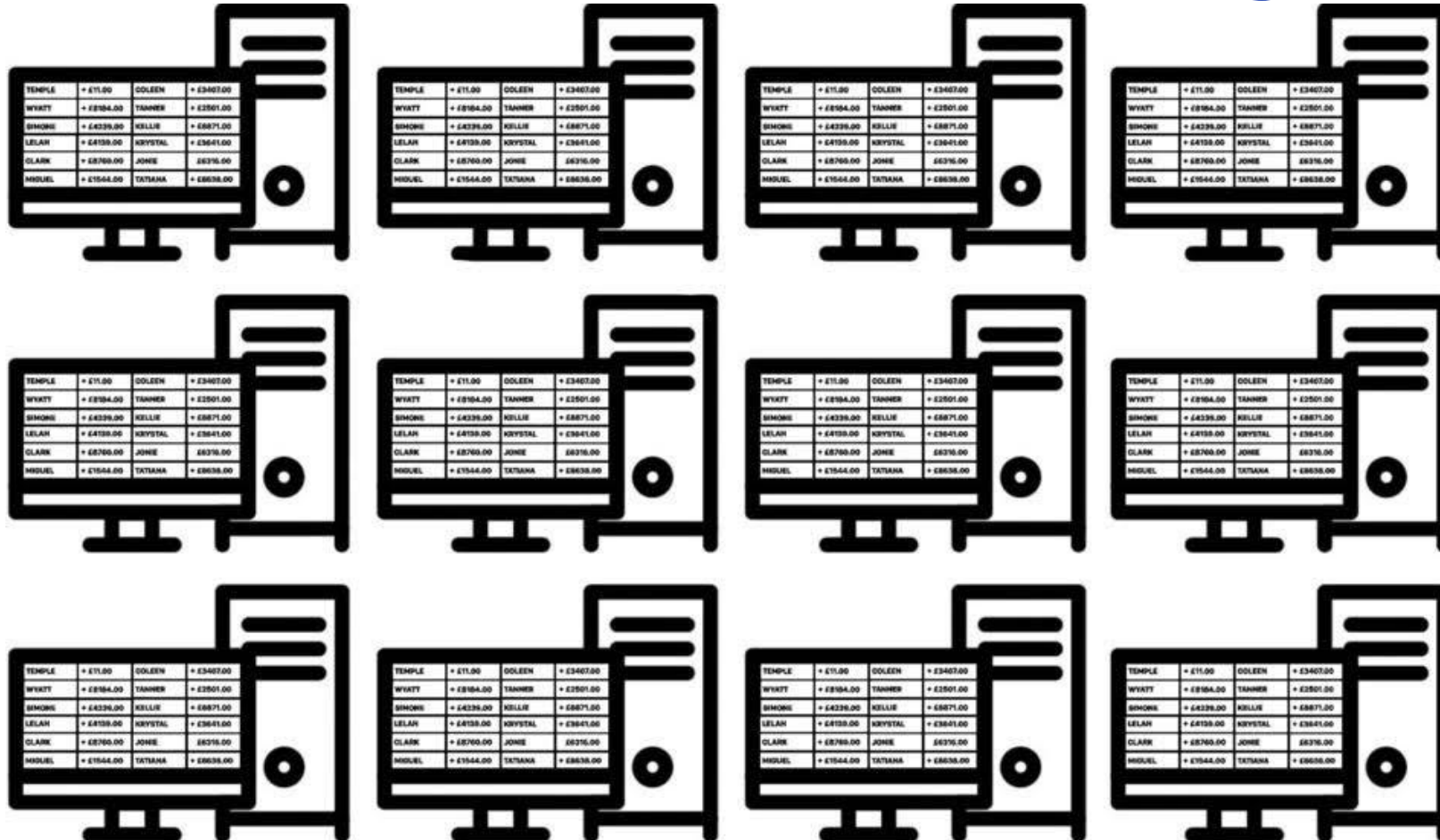
COLEEN	+ £3407.00
TANNER	+ £2501.00
KELLIE	+ £8871.00
KRYSTAL	+ £3641.00
JONIE	£6316.00
TATIANA	+ £8638.00

Infrastruktur - Ledger

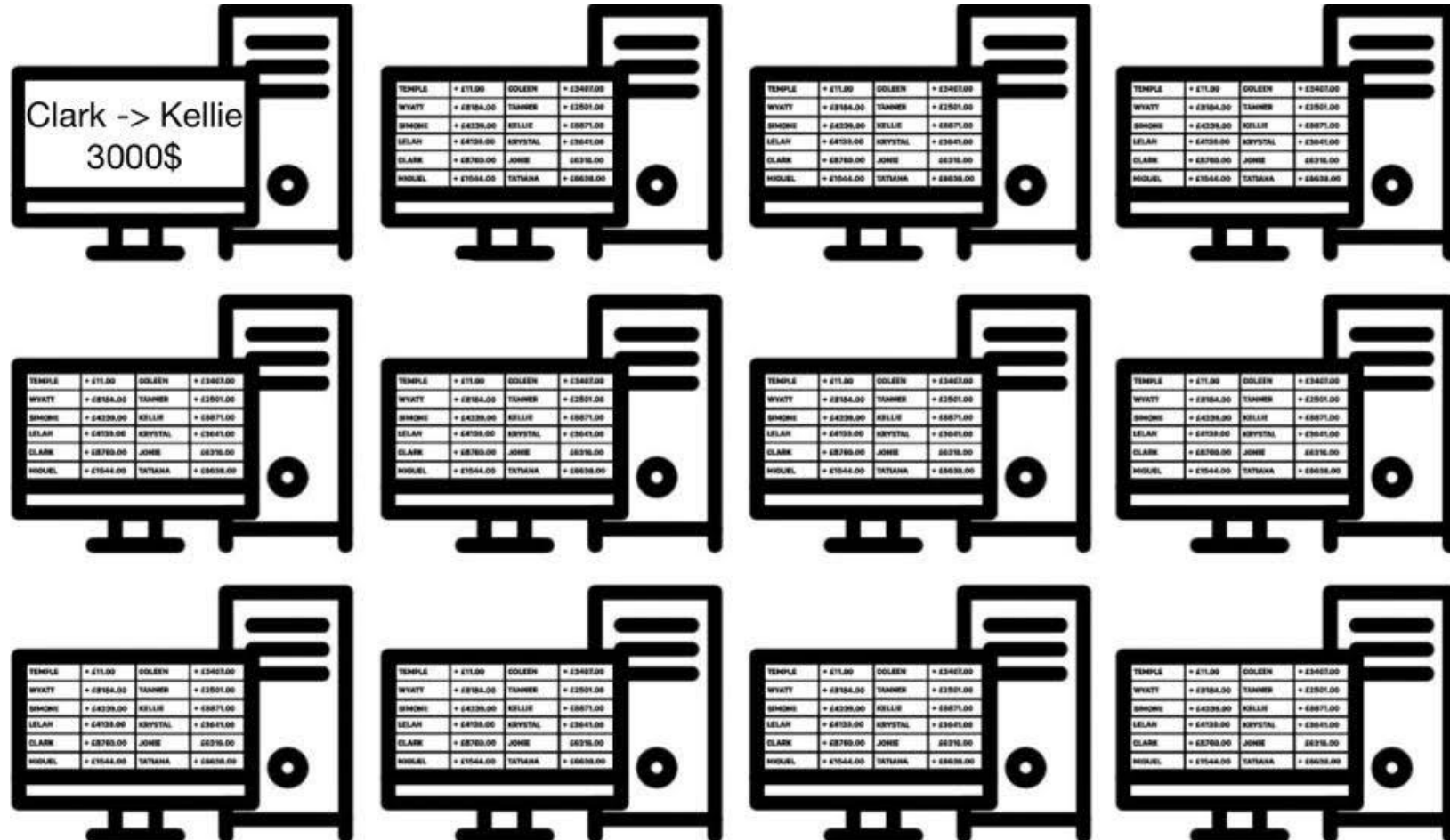


TEMPLE	+ £11.00	COLEEN	+ £3407.00
WYATT	+ £8184.00	TANNER	+ £2501.00
SIMONE	+ £4239.00	KELLIE	+ £8871.00
LELAH	+ £4139.00	KRYSTAL	+ £3641.00
CLARK	+ £8760.00	JONIE	£6316.00
MIGUEL	+ £1544.00	TATIANA	+ £8638.00

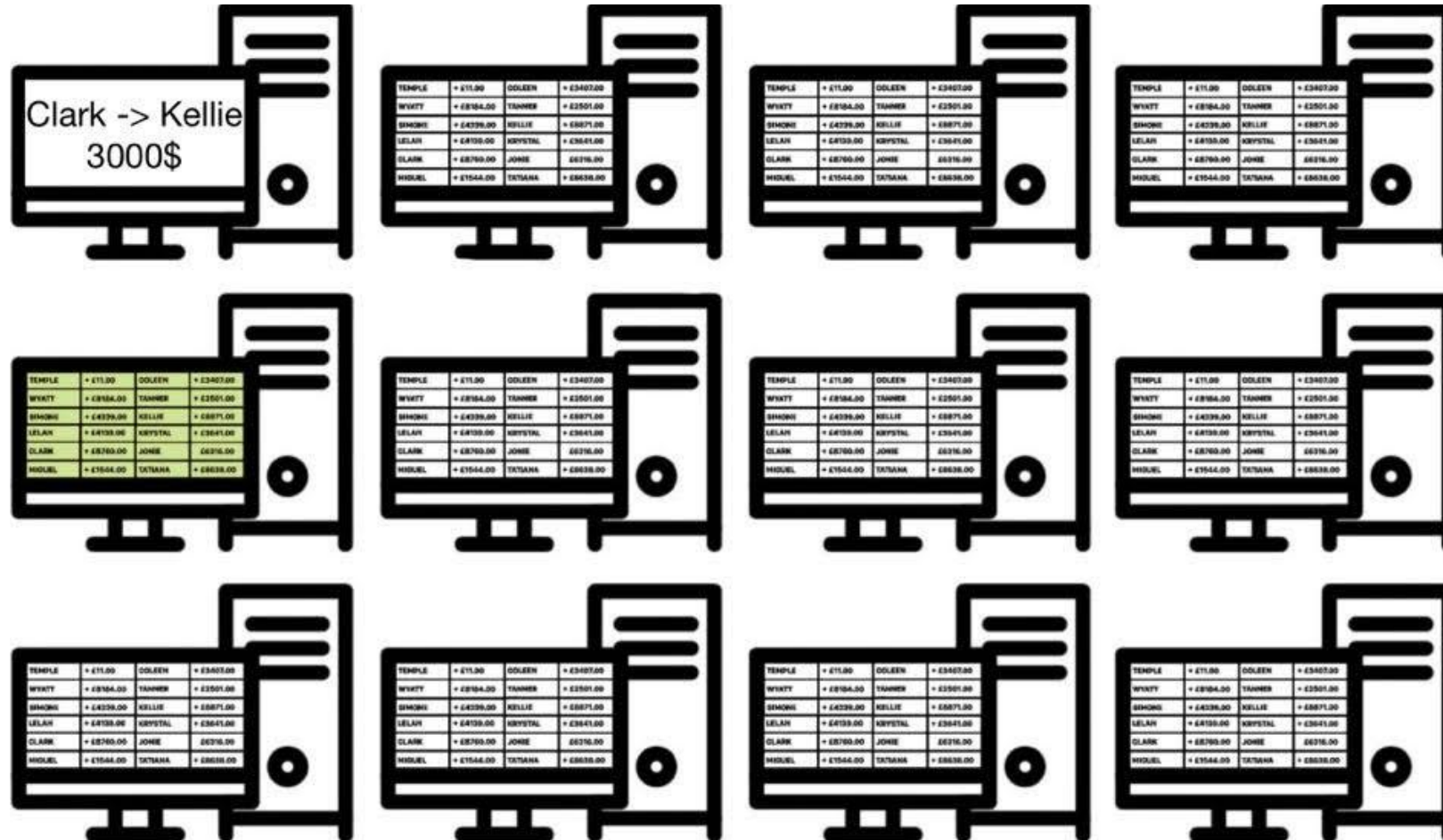
Infrastruktur - distributed Ledger



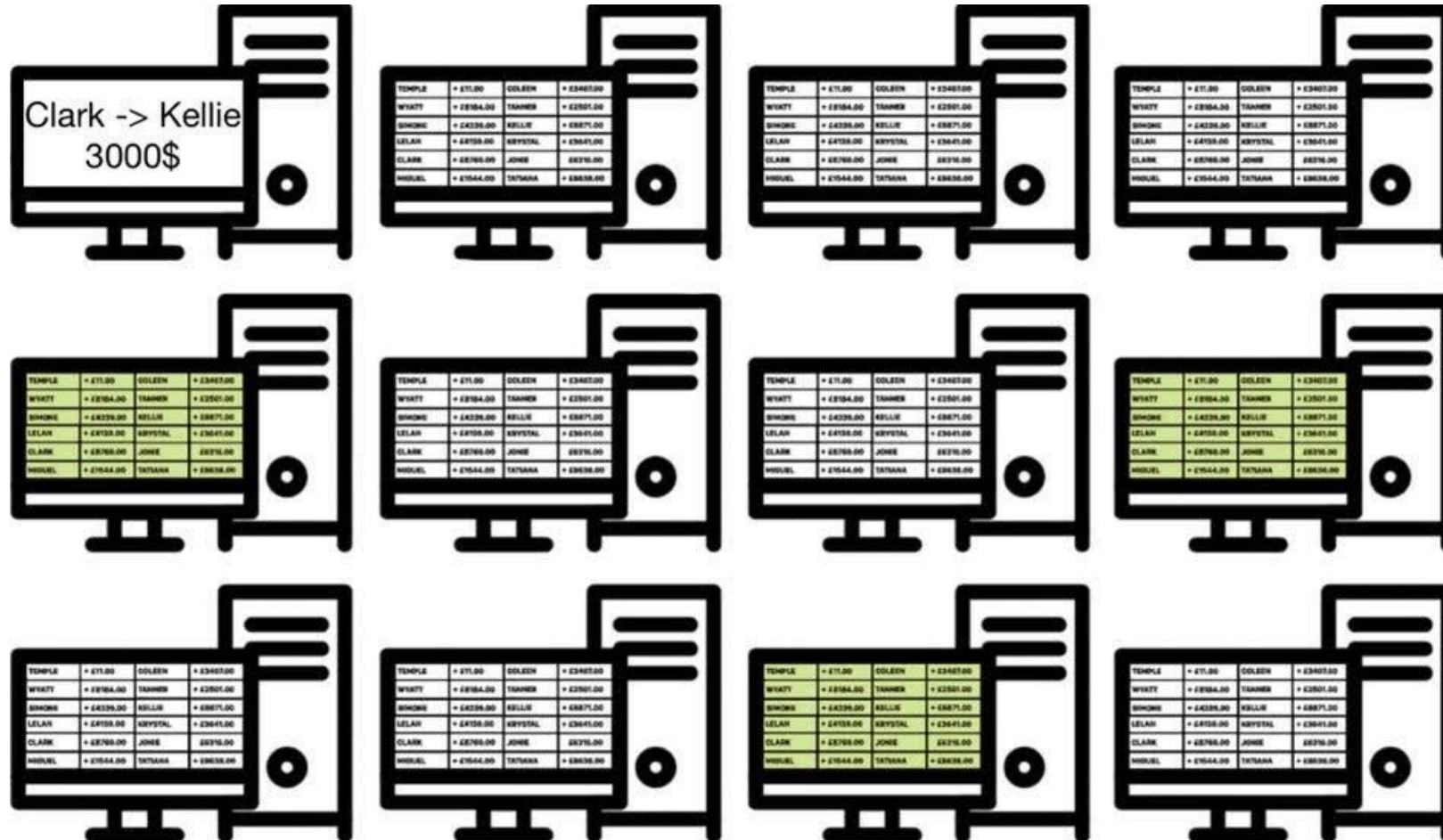
Infrastruktur - Transaktion



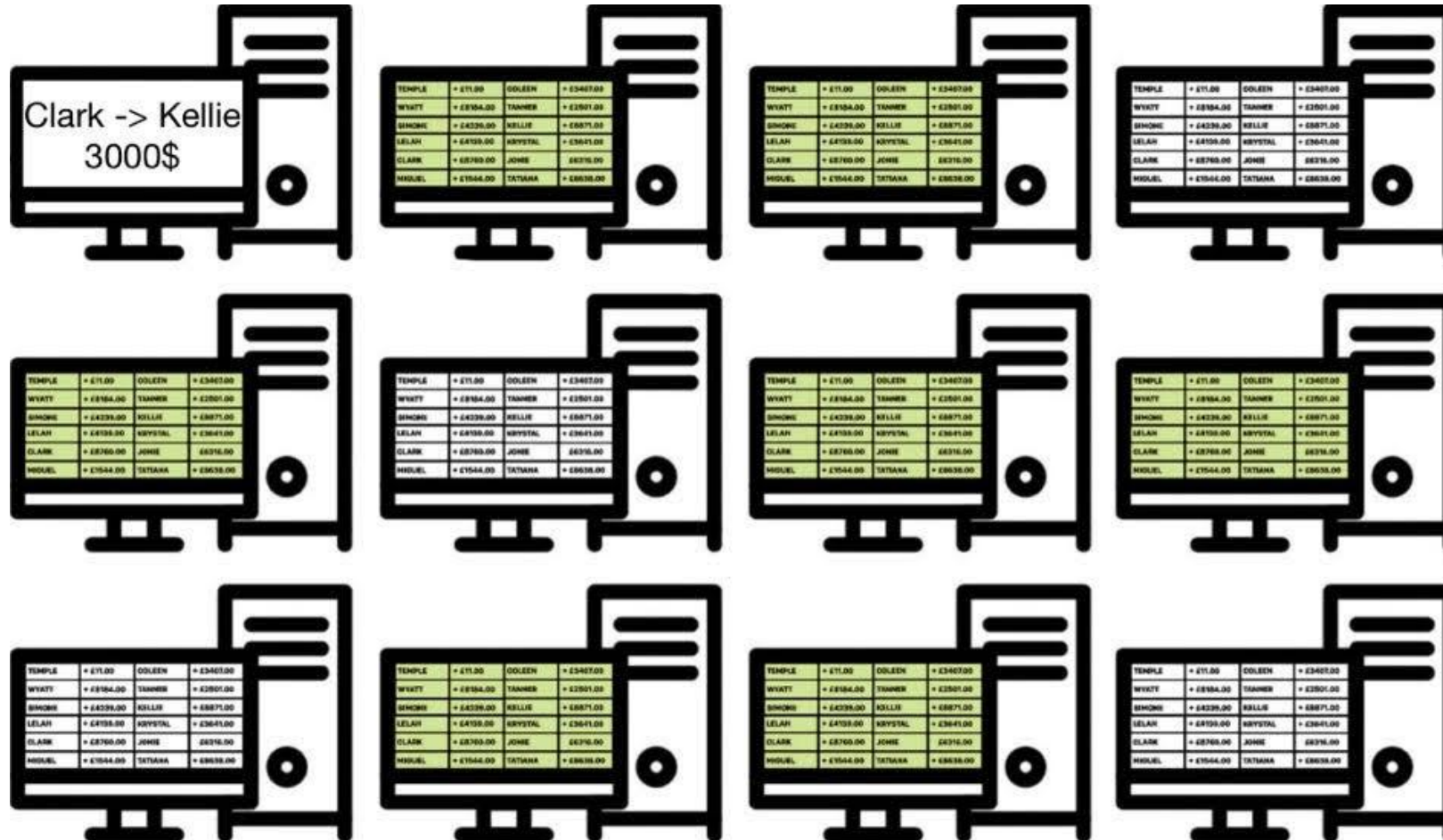
Infrastruktur - Transaktion



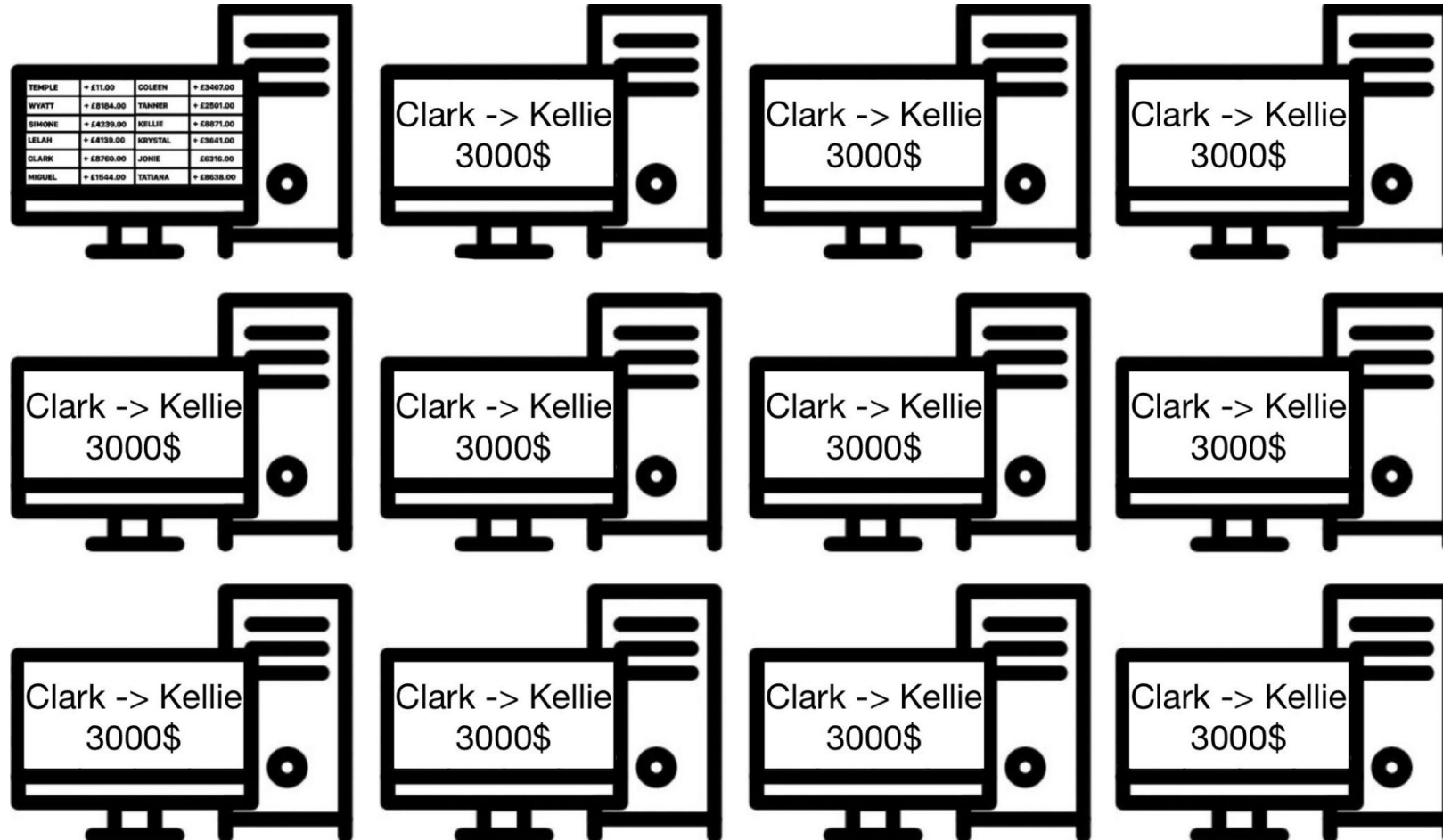
Infrastruktur - Transaktion



Infrastruktur - Transaktion



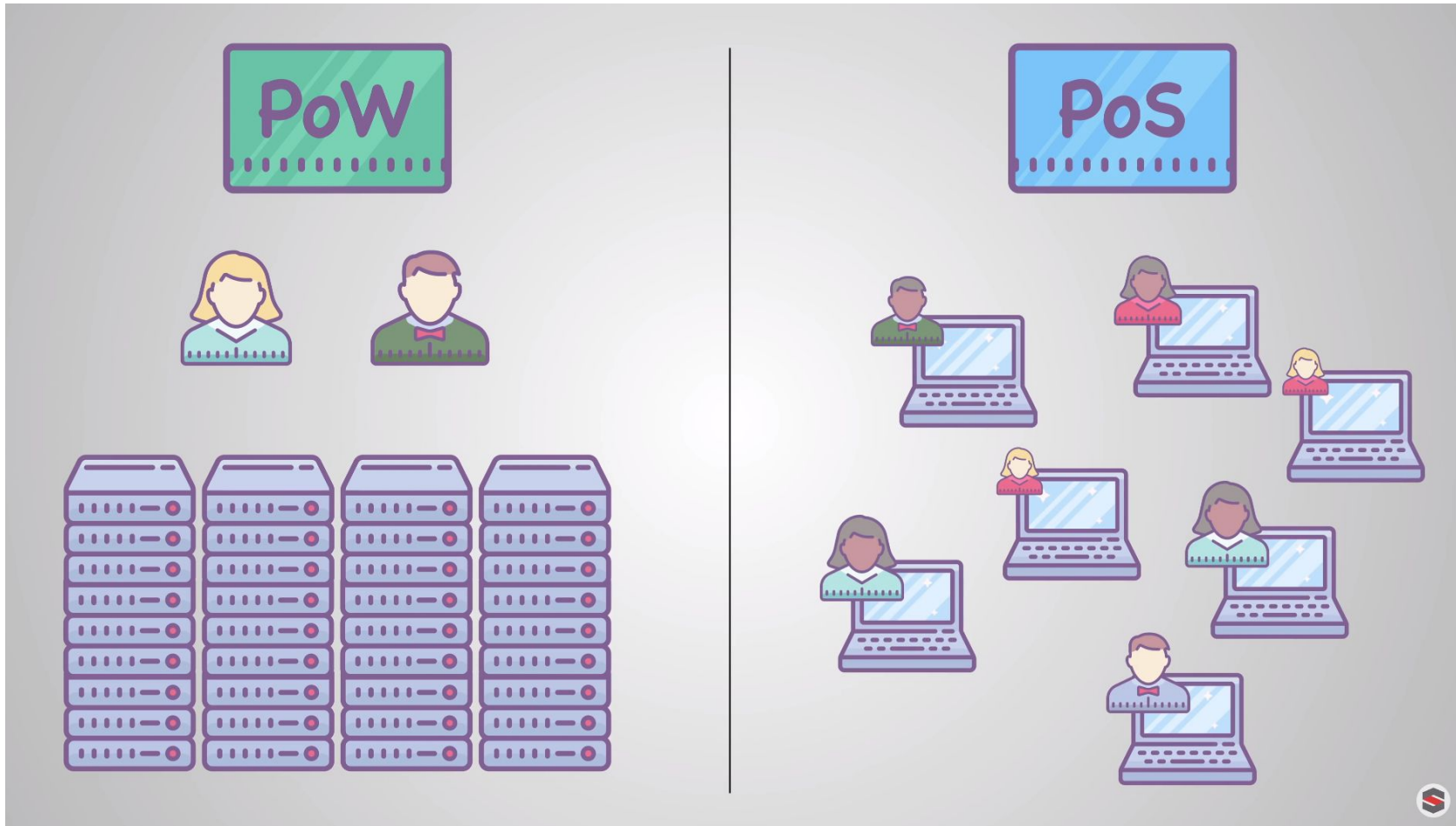
Infrastruktur - Transaktion



Konsensmechanismen

- Einigung über den Status eines Netzwerkes
- Zur Überprüfung der Korrektheit von angehängten Blocks

Konsensmechanismen

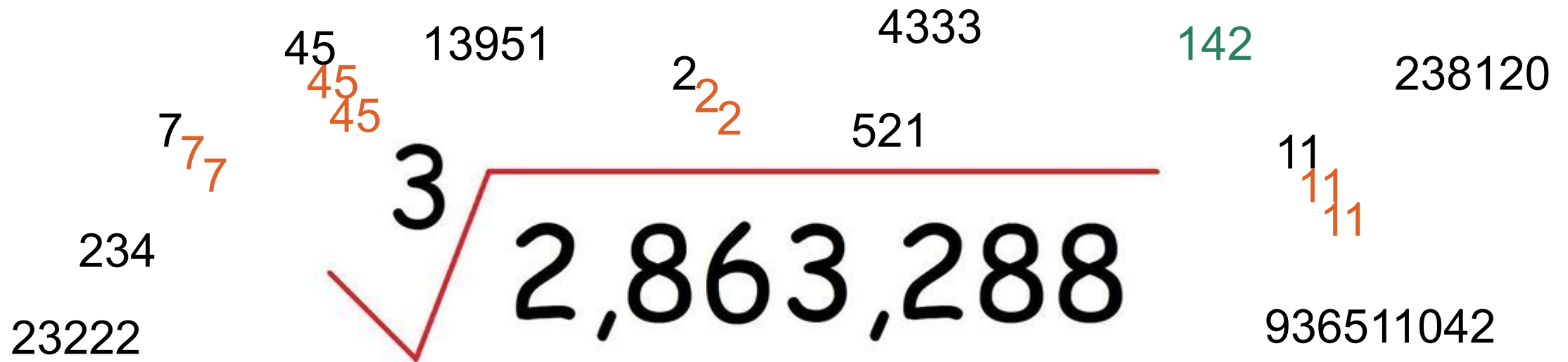


Konsensmechanismus Proof of work (POW)

- Gesucht ist die Lösung eines mathematischen Problems
- Nodes (=Miner) im Netzwerk wenden ihre Rechenleistung auf
- Lösung existiert, jedoch kein Verfahren diese zu berechnen



Konsensmechanismus Proof of work (POW)





Konsensmechanismus Proof of work (POW)

- Ineffizient (doppelte Lösungen)
- Energieintensiv
- Bitcoin braucht **263 TWh** (laut admin.ch)
pro Jahr



Konsensmechanismus Proof of work (POW)

- 263000000000 KWh
- EU (gesamter Transportsektor) **53 TWh** im Jahr 2020

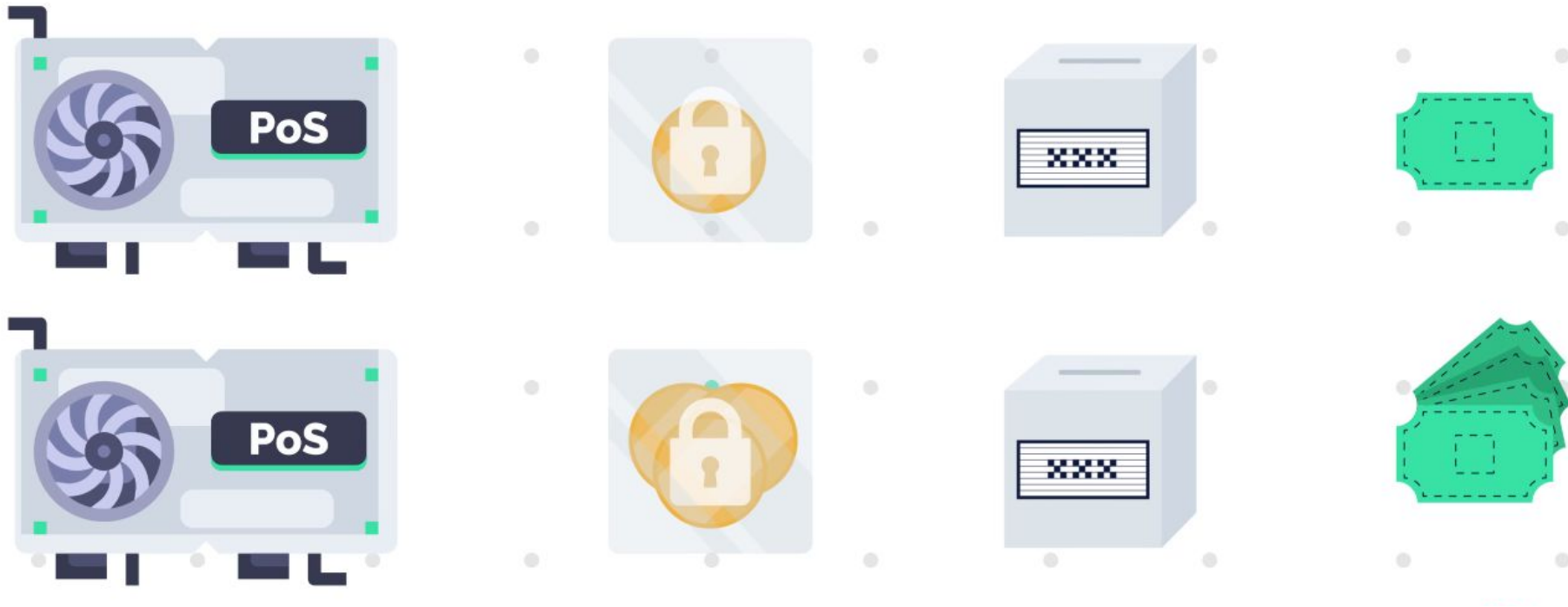
Konsensmechanismus Proof of work (POW)

- Belohnung pro Block: 6.25 Bitcoin bzw. 120'000 CHF
- Ca. alle 10 Minuten ein neuer Block

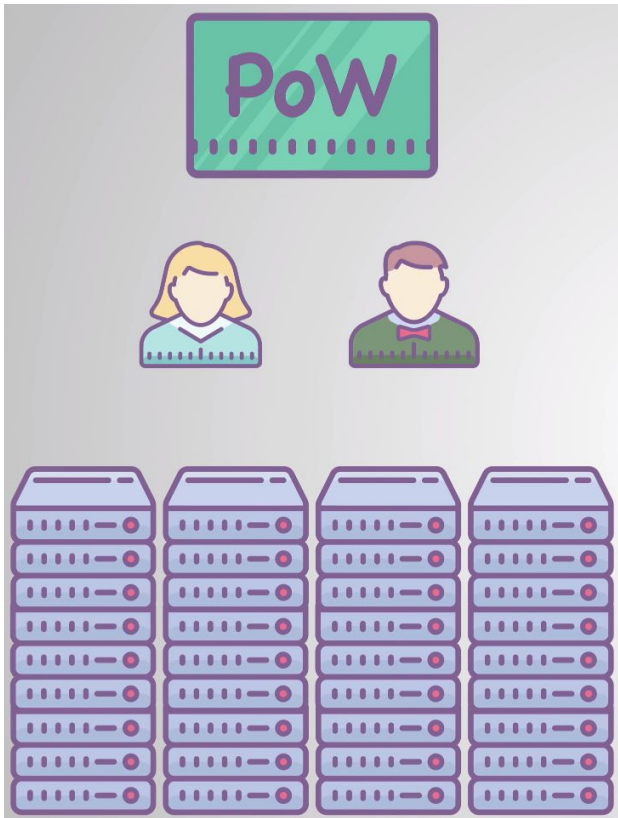
Konsensmechanismus Proof of stake (POS)

- Nodes (=Validators) ihr Vermögen «zur Verfügung»
- Beruht auf dem Prinzip von Depot / Kaution

Konsensmechanismus Proof of stake (POS)

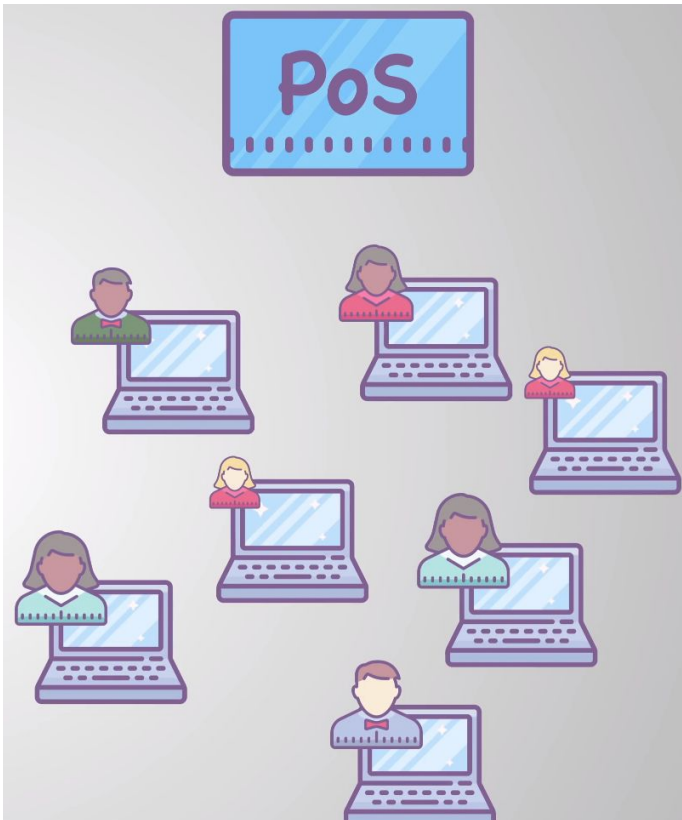


Konsensmechanismen



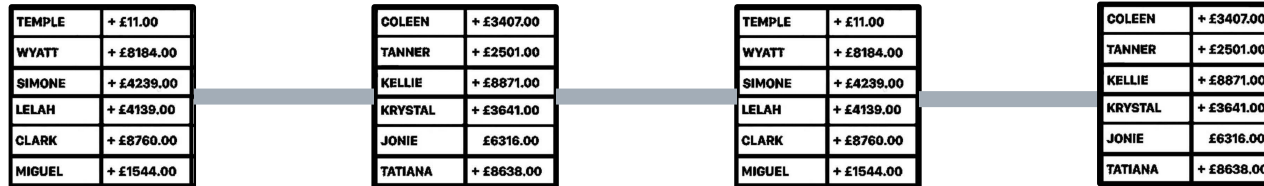
- + Mathematisch fundiert
- + Praxistauglich
- Energieintensiv
- Ineffizient

Konsensmechanismen



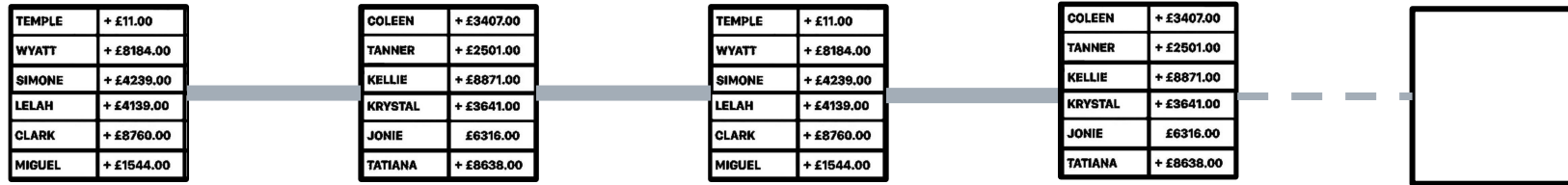
- + Energiesparsam
- + Weniger Hardwarekosten
- Reiche werden reicher
- Schwer umsetzbar

Kurzer Rückblick



- Inhalt des Blocks? Transaktionen
- Existenz der Kette? Verteilt auf Nodes

Kurzer Rückblick



– Anfügen von Blöcken?
Konsensmechanismen

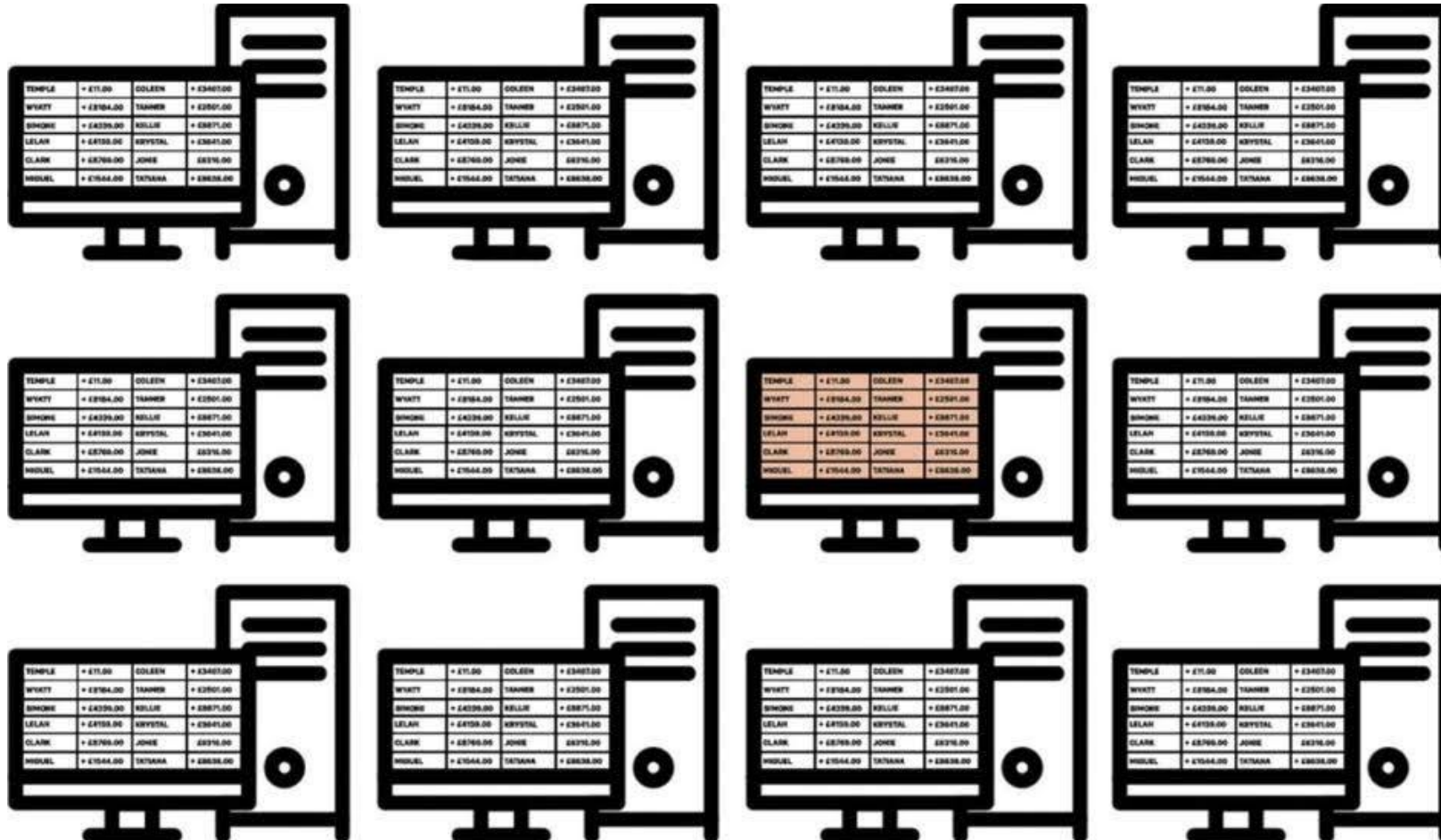


**Universität
Zürich** ^{UZH}

Institut für Informatik

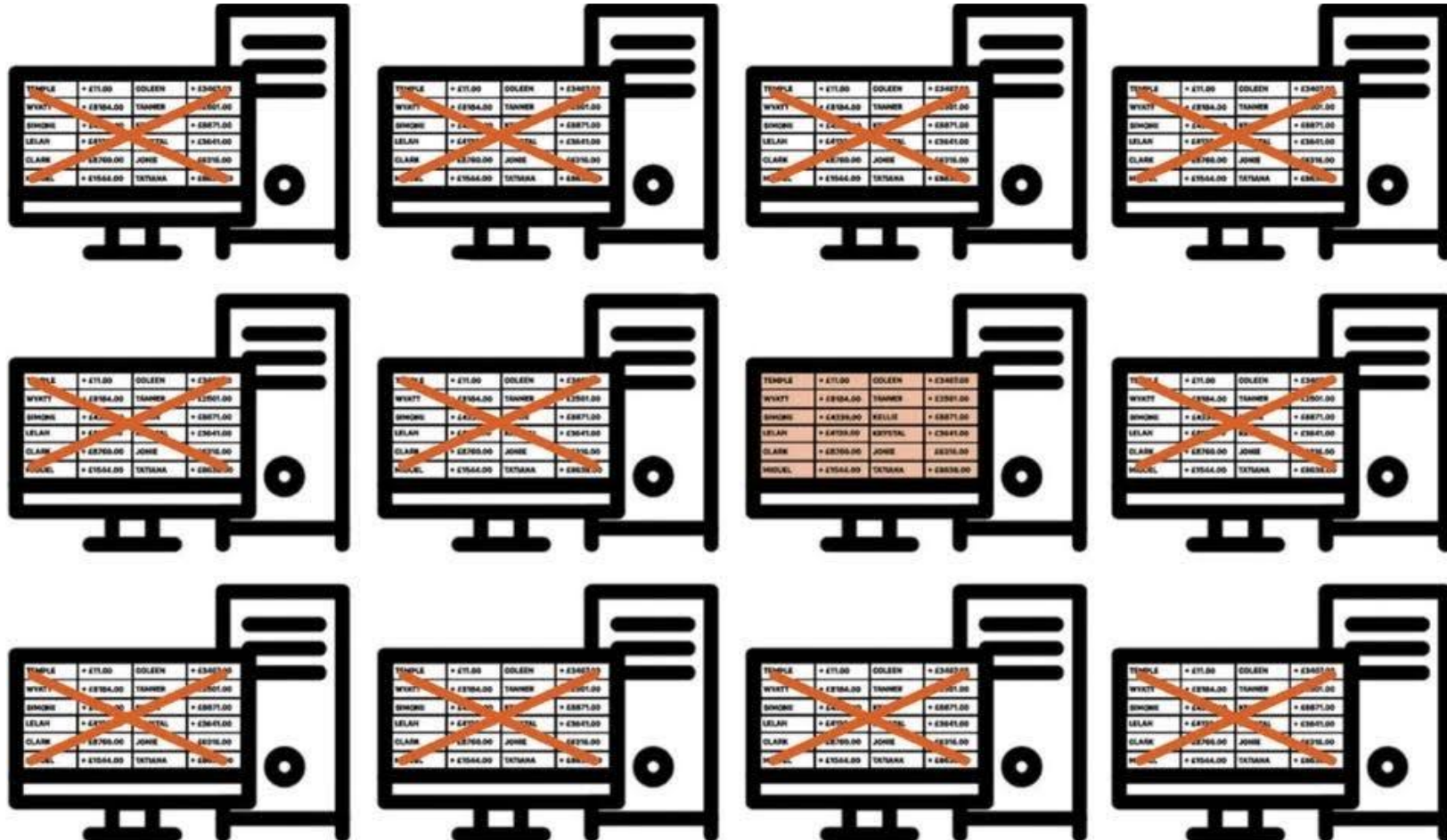
Vor- und Nachteile

Nutzen - Sicherheit

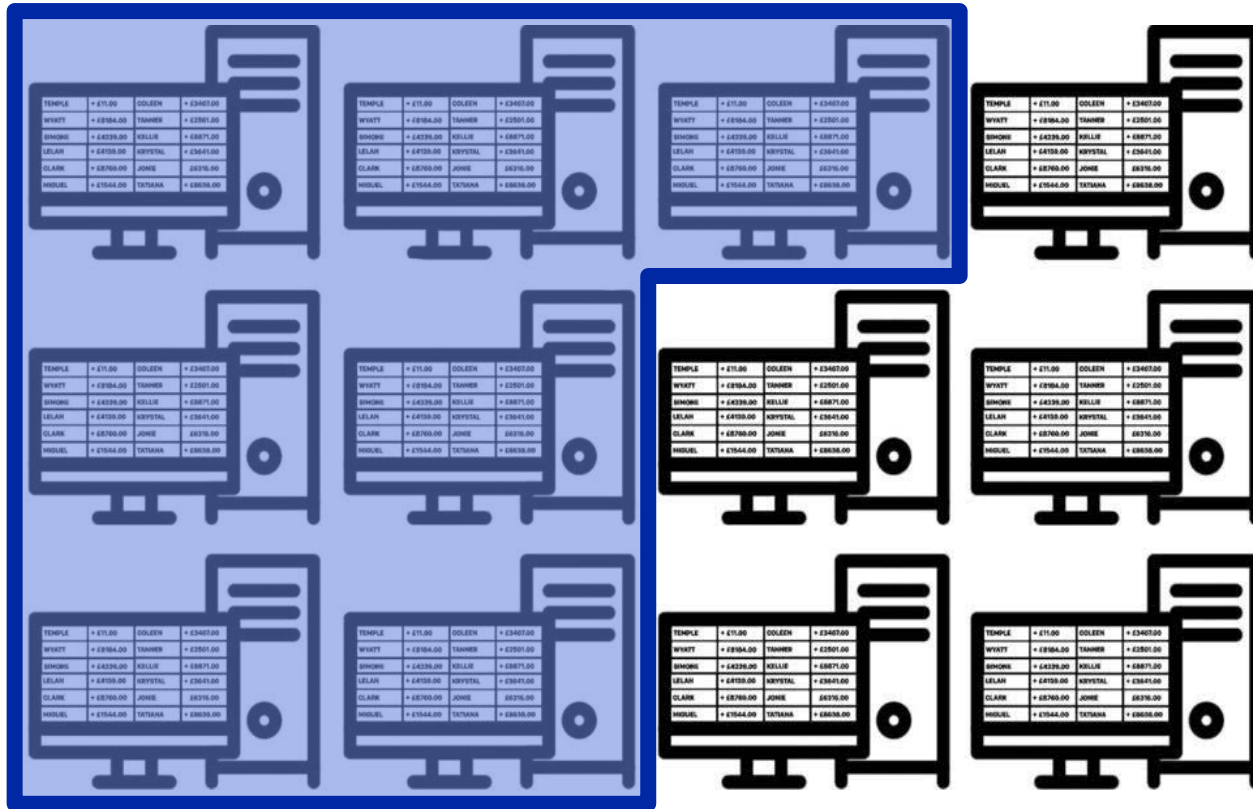


TEMPLE	+ 471.00	GOLEEN	+ 43407.00
WYATT	+ 43764.00	TANNER	+ 43501.00
BINGHE	+ 44339.00	KILLIE	+ 43671.00
LELAN	+ 44709.00	KRYSTAL	+ 43641.00
CLARK	+ 44769.00	JONE	44316.00
MOUEL	+ 47044.00	TATIANA	+ 43638.00

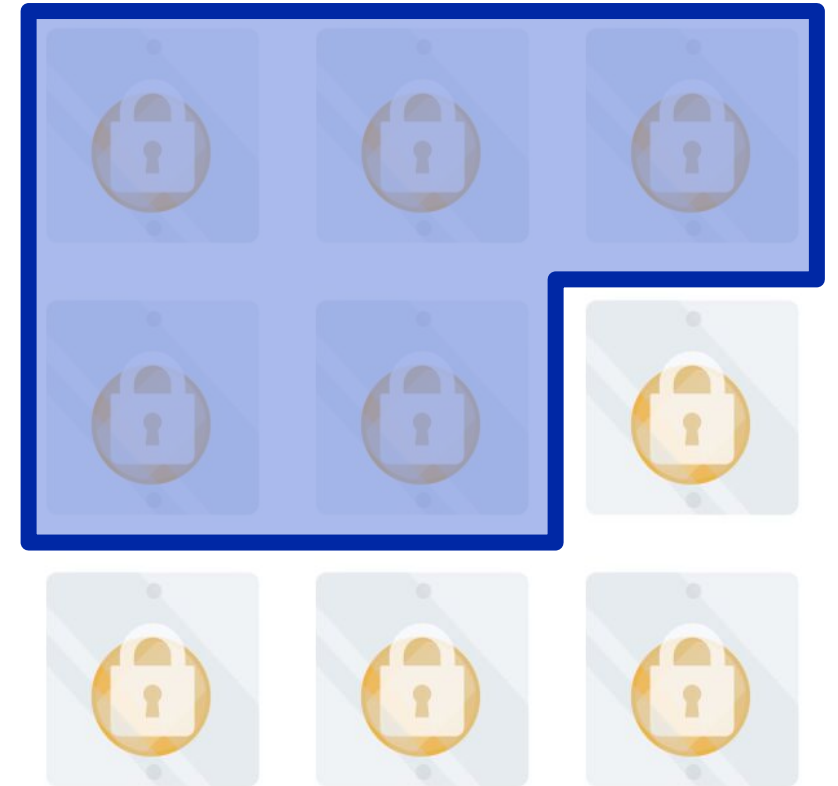
Nutzen - Sicherheit



Problem - Sicherheit



~5800 Nodes bei POW



~96 Milliarden USD bei POS

Nutzen - Anonymität

0x8501b249b3ac9fd252fca8b131410832a3190ec4

0x3eccc30f21b89ebad7703bb4c95991270d904b1b

0x0e59d8fe30f3c3469a87b6d0d01a1cb40b47ddc7

0x432ff5f89540ae719040e06290fbc41478735d17

0x62fd14F88d3ACF90f0d47D5B2c613116bEa74ccf

0x39186ee7CFc8673fFcA941C7932b0fc9fF26F95c

TEMPLE	+ £11.00	COLEEN	+ £3407.00
WYATT	+ £8184.00	TANNER	+ £2501.00
SIMONE	+ £4239.00	KELLIE	+ £8871.00
LELAH	+ £4139.00	KRYSTAL	+ £3641.00
CLARK	+ £8760.00	JONIE	£6316.00
MIGUEL	+ £1544.00	TATIANA	+ £8638.00

Wallet-Adressen auf der Blockchain

Vor- und Nachteile

Vorteile

- Vertrauen und Sicherheit
- Unabhängigkeit
- Anonymität
- Privatsphäre
- Effizienz (Zeit- und Kostenersparnis)

Vor- und Nachteile

Nachteile

- Irreversibel
- Keine regulierende Drittpartei
- Anonymität
- 51% attack
- Komplexität



**Universität
Zürich** ^{UZH}

Institut für Informatik

Ausblick für andere Anwendungen

Ausblick (Siemens, Unilever, Pfizer)

- Nachweis von Besitzern
- Lieferketten
- Edelmetalle
- Rechtsverträge
- Gesundheitswesen
- Smart contracts



**Universität
Zürich** ^{UZH}

Institut für Informatik

Schlusswort

Referenzen

- <https://www.javatpoint.com/history-of-blockchain>
- <https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-in-articles/what-is-blockchain/history>
- <https://101blockchains.com/history-of-blockchain-timeline/>
- <https://kriptomat.io/blockchain/history-of-blockchain/>
- <https://www.youtube.com/watch?v=rYQgy8QDEBI>
- <https://academy.moralis.io/blog/exploring-proof-of-works-electricity-consumption>
- <https://www.aramis.admin.ch/Default?DocumentID=68053&Load=true>
- <https://bitcointalk.org/index.php?topic=27787.0>
- https://www.youtube.com/watch?v=M3EFi_POhps
- <https://www.lemonade.com/>
- <https://www.youtube.com/watch?v=ie-qRQIQT4I>
- <https://www.youtube.com/watch?v=YudpU58uYuM>
- <https://morethandigital.info/blockchain-moeglichkeiten-und-anwendungen-der-technologie/>

**Ihre Meinung
zählt!**

Zugangscode
07092022

