Blockchain

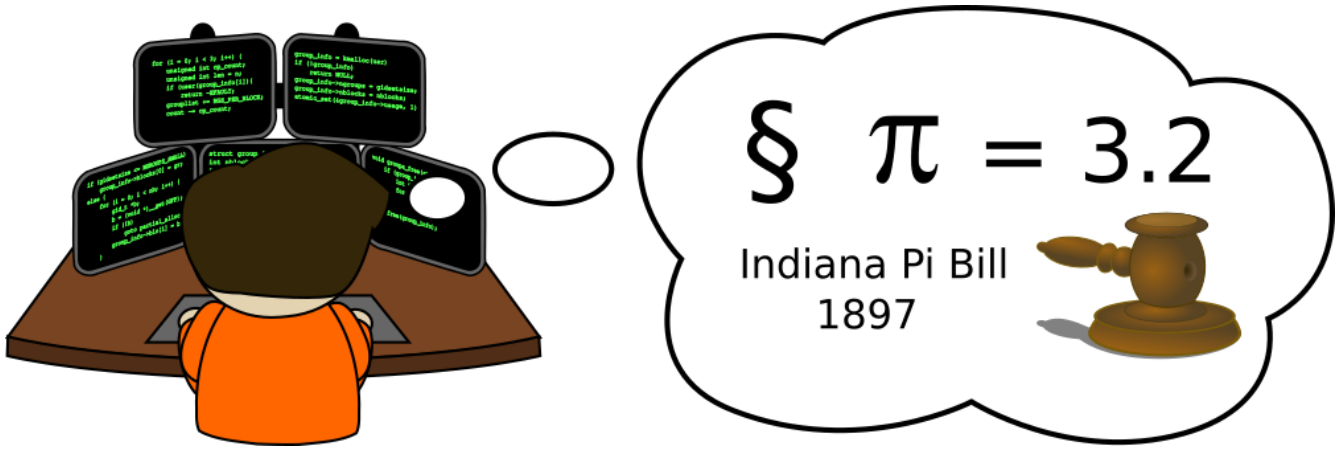
Digitalisierung und dezentrale Konsensfindung

Andreas Pieper

11. Januar 2020

#Kryptoregulierung #Geldwäschegesetz

Gesetzgebung für rechtsfreie Räume?



- Was ist Recht? Was ist richtig?
- Blockchain-API - Was hilft der Staat-Kryptoland-Schnittstelle?
- Aktuell: Aufhebung des Trennungsgebots - Geschäftsbanken dürfen nun Kryptoguthaben verwahren.

Krypto-Überblick

Bitcoin und Co

- 07/08 - globale Finanzkrise -> massive staatliche *Eingriffe*
- 2008 - White Paper von Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
- Korruptionsresistenzes Protokoll bzw. **Verfassung**
- dezentrales und automatisiertes Dokumentationswerkzeug
  - ***Wer schreibt, der bleibt.*** -
- Hauptanwendung: supersouveränes Geldsystem und Spekulationsobjekt
- Open-Source-Philosophie: **Fork me**

Krypto-Überblick

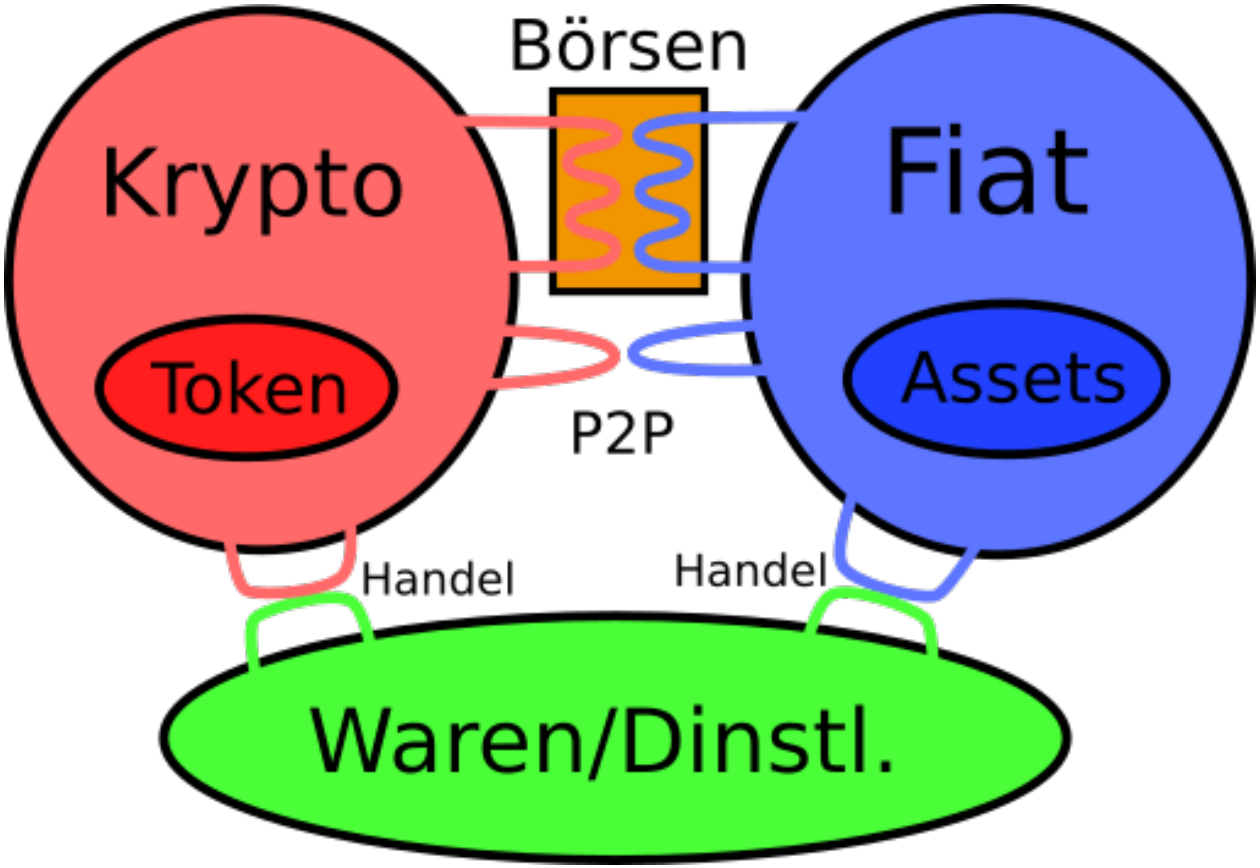
Marktentwicklung

- 2013 - Bitcoin-Hype
- 2017 - ICO-Hype (Ethereum)
- heute - ca. $ 200 Milliarden

#	Name	Price	Change	M. Cap	Supply	Volume
1	BTC Bitcoin	$7.342,90	5,10%	$133,2 B	18,14 M	$27 B
2	ETH Ethereum	$133,63	4,68%	$14,58 B	109,13 M	$9,99 B
3	XRP XRP	$0,193382	2,82%	$8,38 B	43,34 B *	$1,26 B
4	USDT Tether	$1,00	0,40%	$4,12 B	4,11 B *	$31,54 B
5	BCH Bitcoin Cash	$221,68	13,45%	$4,04 B	18,2 M	$2,5 B
6	LTC Litecoin	$42,02	5,21%	$2,68 B	63,78 M	$3,2 B

Parallele Systeme

Rote Pille vs. Blaue Pille



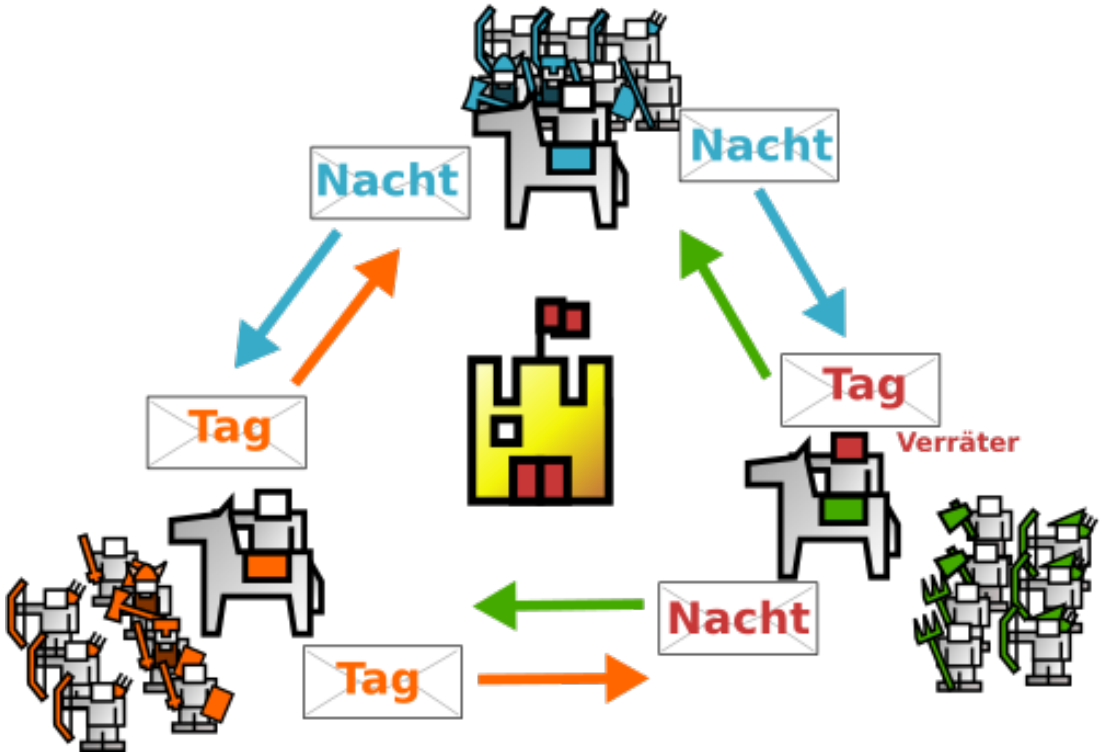
Digitalisierung

Folgen im letzten Jahrzehnt:

- Aufstand der Empörten (David Kiesel auf 36C3 [2019], Peter Kruse im dt. Bundestag [2009])
- Fragmentierung und Polarisierung der Gesellschaft - oder neue Vielfalt?
- Vertrauensverlust in Medien, Politik, Wirtschaft ...
- Strukturierung-, Autokraten-, System- oder Kommunikationsproblem?
- Informationsasymmetrie -> Chancen und Risiken für Händler
- Anwendungsfall der Blockchain: Konsens- und Vertrauensgenerator!

Byzantinischer Fehler

1982 - Das Problem der verteilten Generäle - Lamport, Shostak und Pease

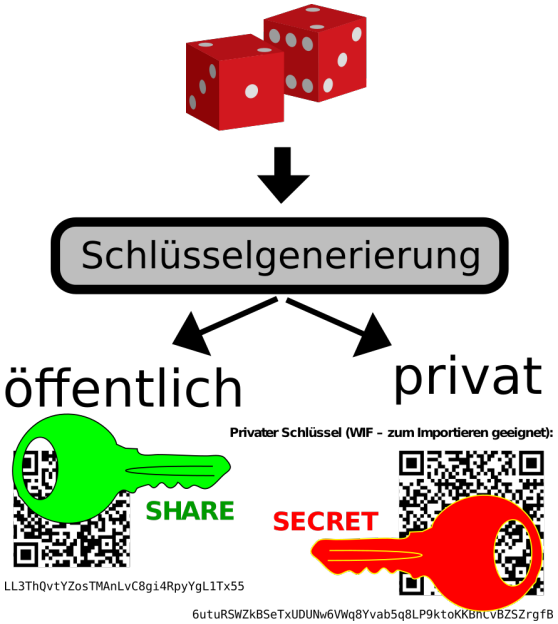


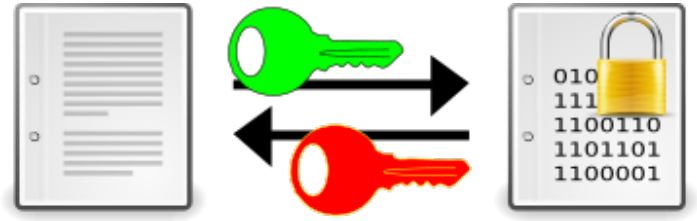
Konsensfindungsproblem bei ausschließlicher P2P-Kommunikation und Falschspielern

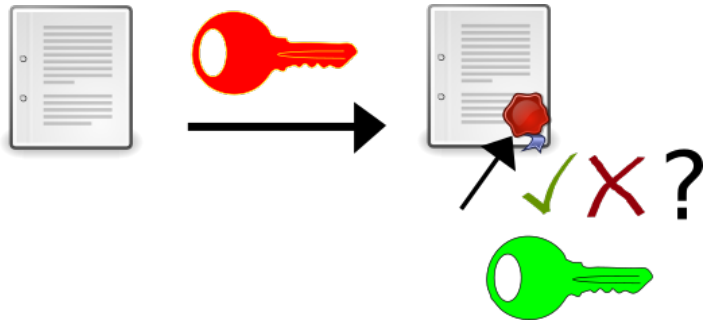
- 1. Problem - Sicherer Nachrichtenaustausch

Asymetrische Verschlüsselung

Was kann ein privater Schlüssel?



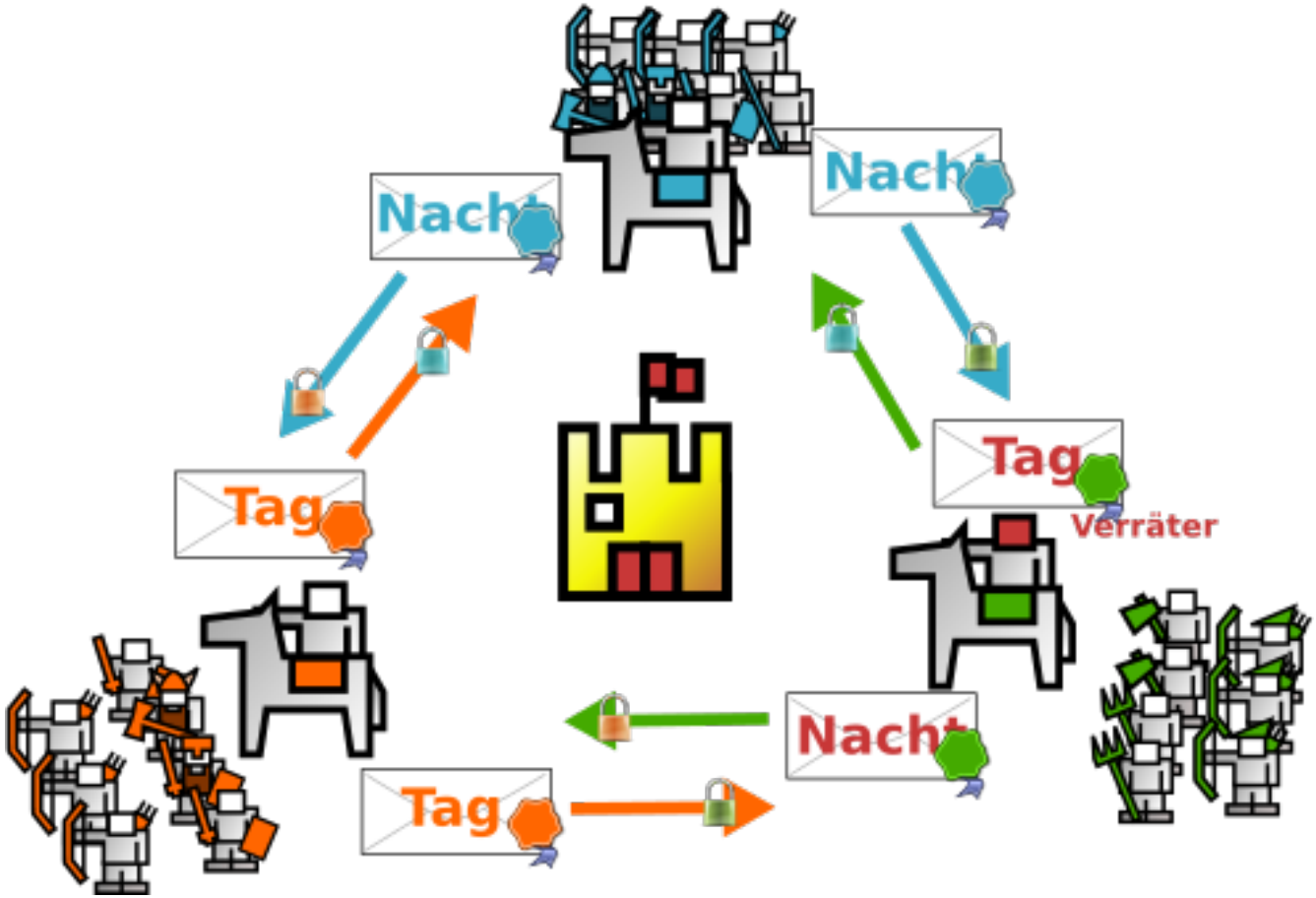




- ab 1978 RSA-Kryptosystem
- Internet-Zertifikate - https
- Mail-Verschlüsselung - Open**PGP**
- Übertragungs-Protokolle - **S**SH
- Kryptokonten - *Bitcoin u. Co* - **Identitätsnachweis**

Byzantinischer Fehler

Das Problem der verteilten Generäle



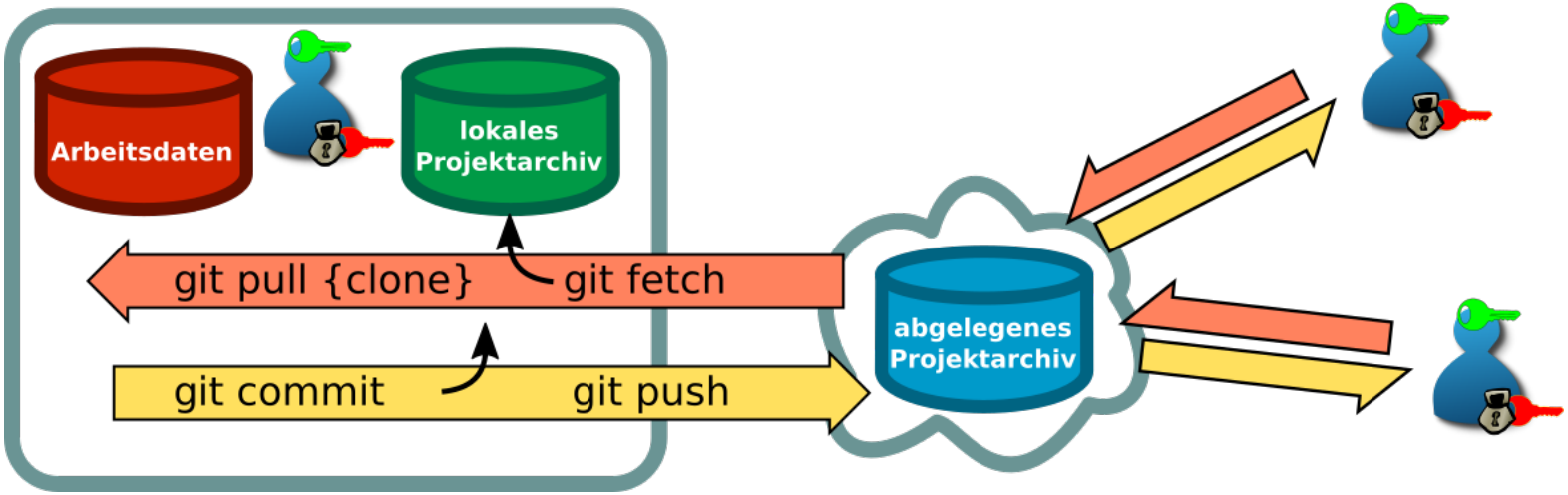
Sichere Boten durch RSA (asymmetrische Verschlüsselung)

- 2. Problem - Konsensfindung

Versionskontrolle - Git

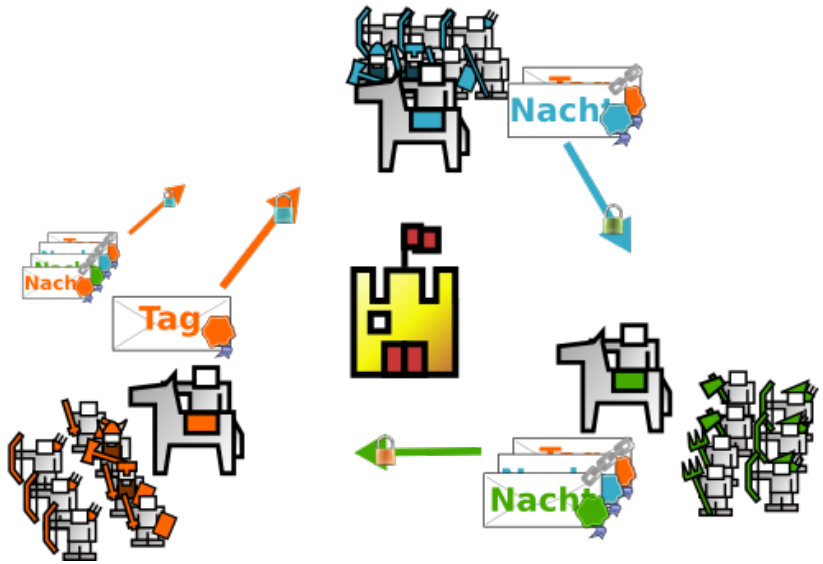
Was ist die Blockchain 0.1?

- Hash-Funktion (dt. Streuwertfunktion)
- nur Änderungen werden in einer Datenbank protokolliert und mit Vorgängerversion *gehasht*
- Manipulationen im *Geschichtsbuch* (Block-Kette) würden auffallen.
- maximale Redundanz -> individuelle Souveränität
- Basiswerkzeug für moderne **IT-Projektarbeit**



Byzantinischer Fehler

Das Problem der verteilten Generäle



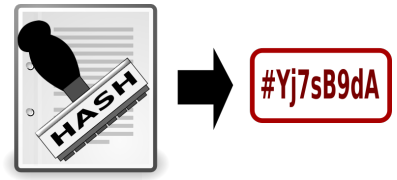
Prinzipiell gelöst, aber ausfallanfälliges Protokoll durch reduzierten Kommunikationsgraphen

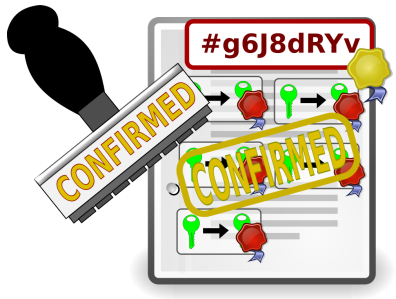
- Mehr Automatisierung, Fehlertoleranz, Dynamik und Dezentralisierung?
- Problem: Forks (dt. Gabelungen)
- Lösung: ***Nachweis des Glücks*** mittels Hash-Funktion-Schwellwert

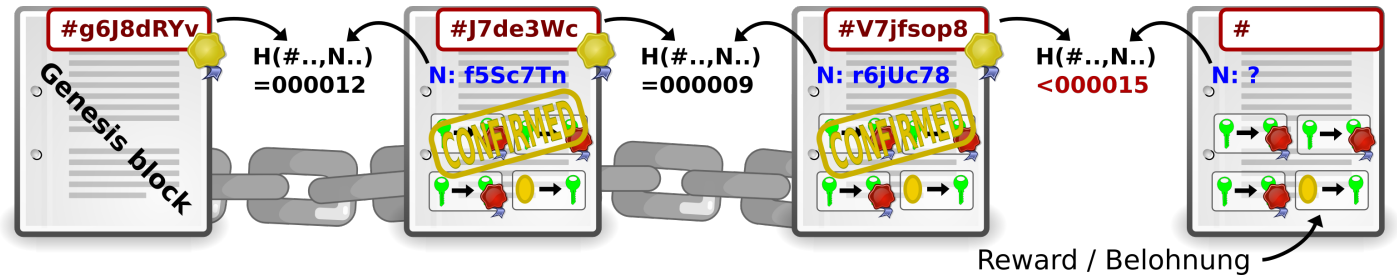
Die automatisierte Konsens-Daten-Kette

Eine Vergewaltigung der Hash-Funktion?

- Ein Hash (dt. Streuwert) ist ein **Fingerabdruck** eines Datenblocks.
- Der letzte Hash ist der Fingerabdruck und das neue **Kopfgeld-Rätsel** zugleich.
- Dezentralisierung durch **zufällige** Blockersteller



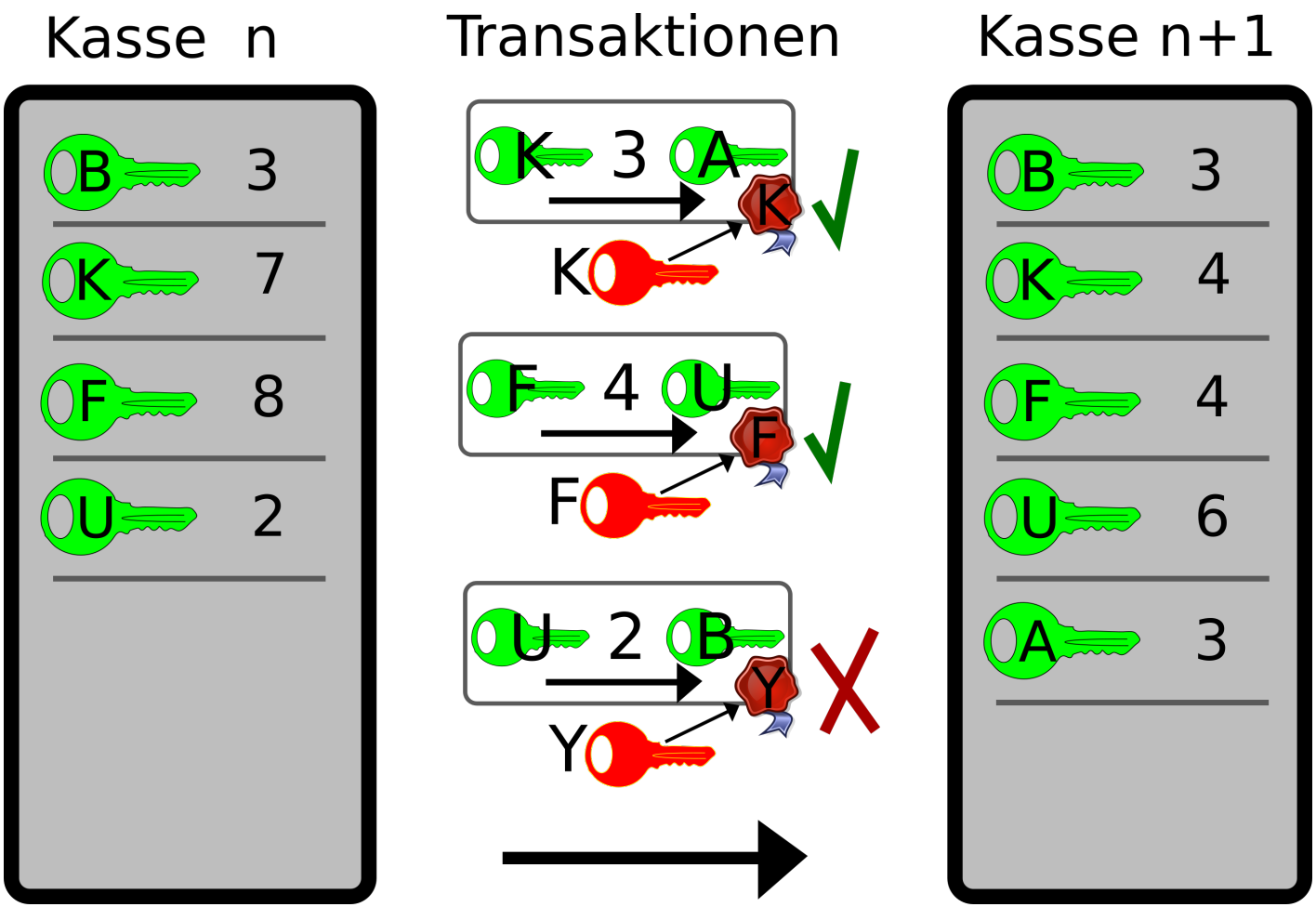




- Coins werden nicht berechnet. Coins werden gedruckt und wegen der Konsensarbeit akzeptiert.

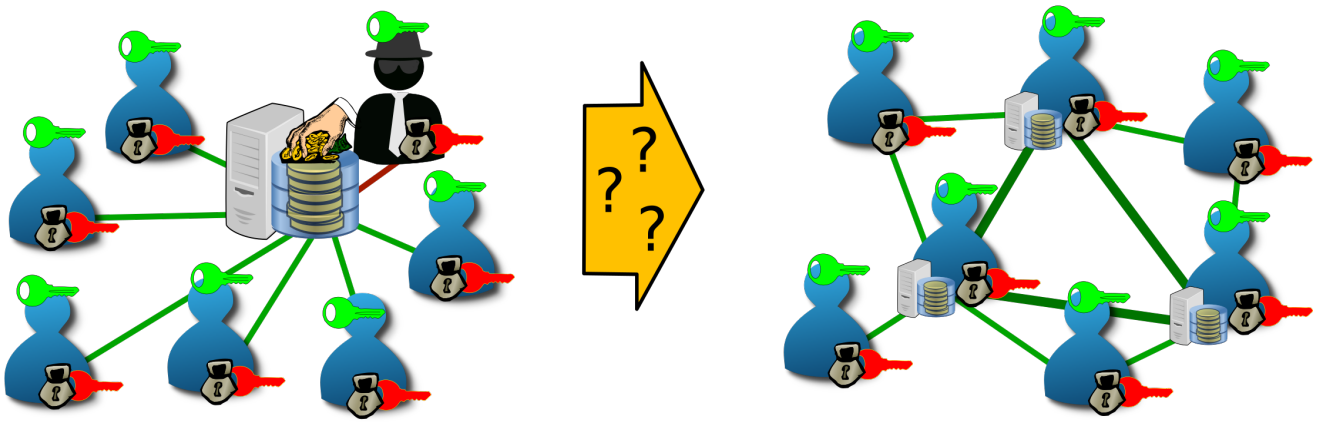
Digital Ledger

Wie funktioniert ein Krypto-Kassenbuch?



Alternativer Zugang

Systemkontrolle - Macht



- Effizienz der Konsensfindung
- dezentrale Systemkontrolle
- Korruptionresistenz

Wie entsteht Geld?

Flüssiges und standardisiertes Vertrauen

- Vertrauen ist *Kapital*.
- Geld ist kondensiertes Vertrauen. quasi $E = mc^2$
- Geld ist ein Skalierungswerkzeug einer freien arbeitsteiligen Gesellschaft.
- Geld ist akzeptiertes Tauschmittel.

Wie entsteht Geld?

Flüssiges und standardisiertes Vertrauen

- Vertrauen ist *Kapital*.
- Geld ist kondensiertes Vertrauen. quasi $E = mc^2$
- Geld ist ein Skalierungswerkzeug einer freien arbeitsteiligen Gesellschaft.
- Geld ist akzeptiertes Tauschmittel.

- Fiat: *Vertrauen* durch Ehrfurcht gegenüber dem Gewaltmonopol.
  - **Proof-of-Force** -
- Blockchain: Vertrauen durch Korruptionsresistenz.
  - **Proof-of-Trust** -

Theorem

Forking is not a bug, it's a feature for creation trust.

Kategorisierung

Coin und Token

Coins / Währungen

- Entlohnung zur Bereitstellung der Infrastruktur und Konsensbildung
- Nutzungsgebühr - dienen dem Spamschutz auf der Blockchain

Token / Wertmarken

- **sekundäre Werteinheiten** auf einer Blockchain
  zB. ERC20-Token auf der Etherium-Blockchain
- sind gebunden an Blockchain-Identitäten
- stellen externe Beteiligungen oder Rechte dar
  zB. ICOs
- Eltern-Blockchain ist das *Clearinghaus*

Kategorisierung

Blockchain und Kassenbuch

dezentrale Blockchain

- Quellcode ist technisch und rechtlich **leicht forkbar**.
- keine Partei kann Konsensbildung diktieren oder manipulieren
- Bitcoin, Ethereum, Litecoin

semi-dezentrale Blockchain

- sehr **hohe Fork-Hürde**
- eine Gruppe hat einen sehr hohen Einfluss auf die Konsensbildung
- EOS, Binance Coin, IOTA, Lisk, Steem

zentrales Kassenbuch (DLT)

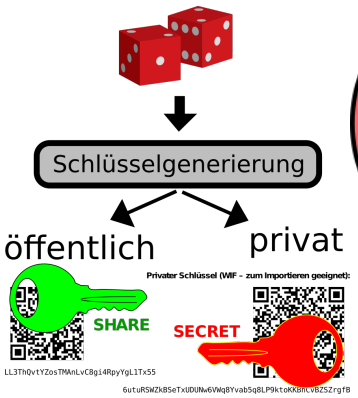
- Quellcode oder Datenbank sind nicht öffentlich bzw. rechtlich geschützt. **Fork unmöglich**.
- Stabel-Coins, Assets oder staatliche Kryptowährungen
- Ripple, Tether, PetroDollar, Libra

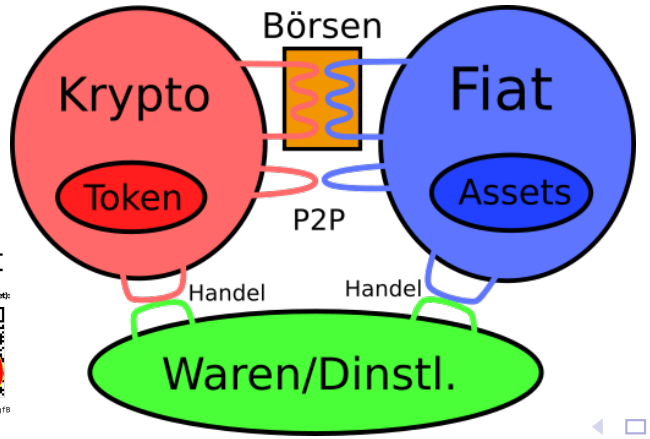
Zusammenfassung

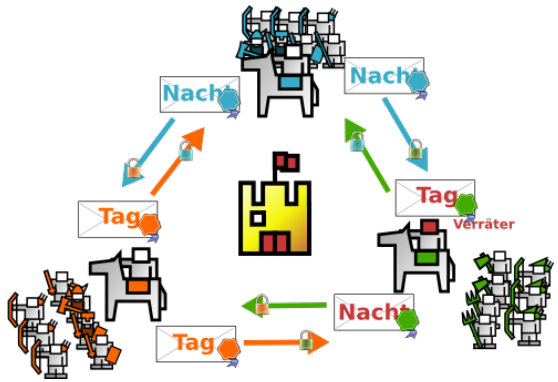
Was haben wir gelernt?

- Blockchain - autom. Konsensfindung
- Asym. Schlüsselpaare - Digitale Souveränität
- Forks - *Krypto-Land* ist durch ein extremes Rechtssystem nicht okkupierbar
- Aufgabe: Schaffung von Rechtssicherheit für *juristische Personen* an der Krypto-Fiat-Grenze

Vielen Dank für die Aufmerksamkeit







Goethe, Faust, zweiter Teil

Das Geheimnis der Geldschöpfung

Franz Xaver Steifensand (Jacques Alfred van Muyden): Laboratorium / Wagner erschafft den Homunculus

Volker Pohlenz: Kaiserliche Pfalz. Acryl auf Leinwand

Zu wissen sey es jedem der's begehrt:
Der Zettel hier ist tausend Kronen werth.
Ihm liegt gesichert, als gewisses Pfand,
Unzahl vergrabnen Guts im Kaiserland.
Nun ist gesorgt, damit der reiche Schatz,
Sogleich gehoben, diene zum Ersatz.
(Faust, V.6057–6062)