

Sicherheit und Anonymität von Kryptowährungen

Jonathan Schumann

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

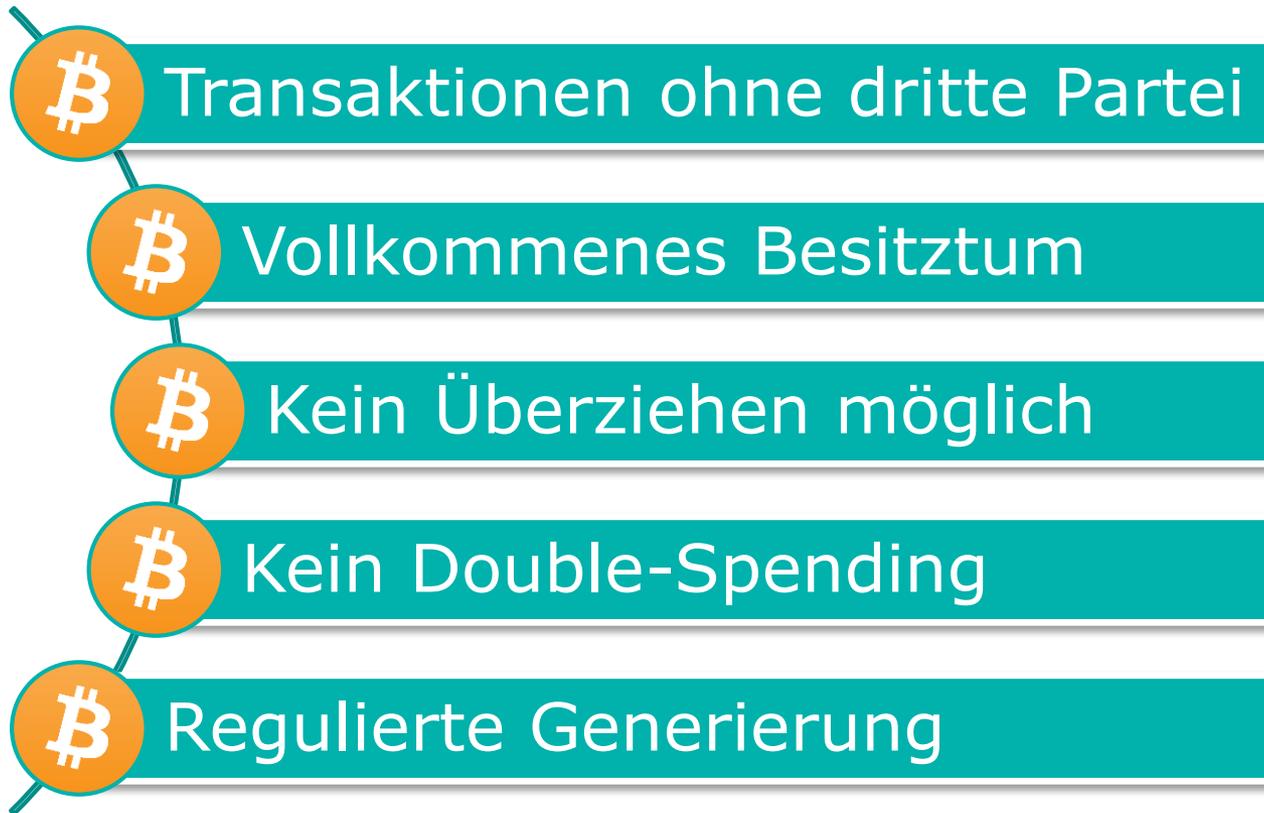


- Kryptowährungen allgemein
- Bitcoin
 - Anforderungen
 - Funktionsweise
- Sicherheit und Anonymität (Bitcoin)
 - Confirmations
 - Anonymität
- Kryptowährungen und Kriminalität
 - Schwarzmarkt
 - Diebstahl
- Fazit

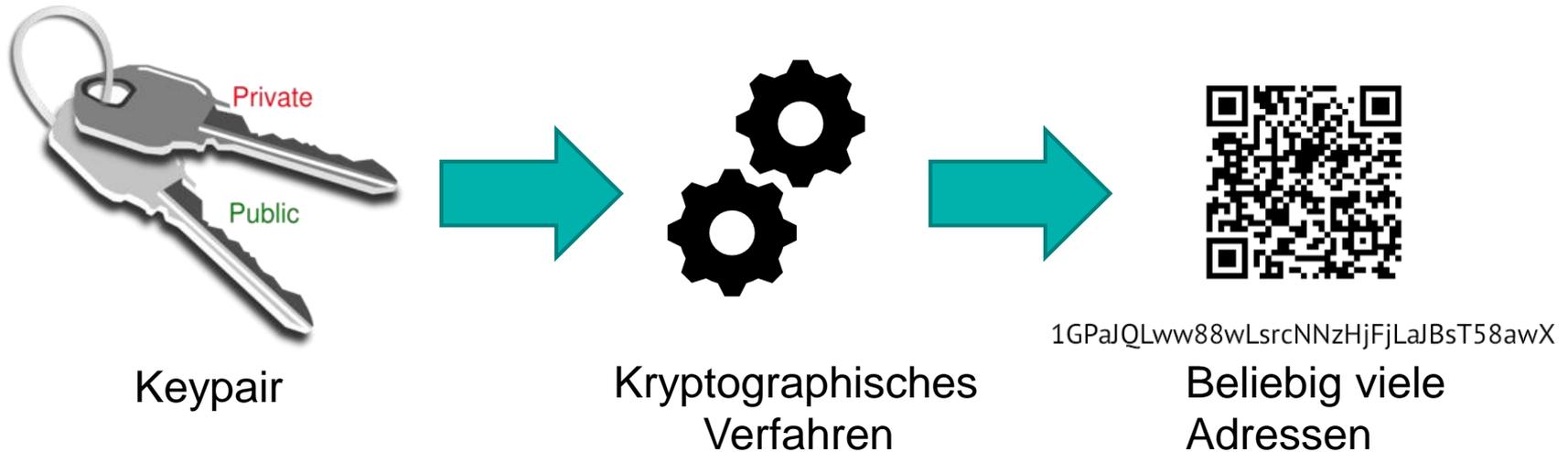
- Digitales Geld
 - Dezentralisiert
 - Kryptographie verifiziert Transaktionen und kontrolliert die Generierung neuer Einheiten
- Mehr als 1600 Digitale Währungen im Umlauf
 - Über 400 Milliarden Dollar (ca. 30.000% in 5 Jahren)



Anforderungen an Bitcoin

- 
- Bitcoin Transaktionen ohne dritte Partei
 - Bitcoin Vollkommenes Besitztum
 - Bitcoin Kein Überziehen möglich
 - Bitcoin Kein Double-Spending
 - Bitcoin Regulierte Generierung

- Adressen werden aus einem Public-Private Keypair generiert
 - Beliebig viele Adressen pro Keypair möglich
 - Adressen werden von „Wallets“ verwaltet
 - Besitzer des Private-Keys hat volle Kontrolle über das Vermögen
 - Bei Verlust des Private-Keys gibt es keine Möglichkeit diesen wiederherzustellen
- Der Private-Key wird genutzt um Transaktionen zu signieren
 - Jeder kann die Signatur mithilfe des Public-Keys überprüfen



- Kann es zu Kollisionen kommen? Ja
 - Beide Besitzer wären in der Lage Bitcoins auf dieser Adresse auszugeben.
 - Wahrscheinlichkeit : $1:2^{256}$

- Eingehende Transaktionen werden vom Netzwerk in einem Block gesammelt:
 - Öffentlich einsehbar
 - Transaktionskosten bestimmen die Priorität
 - FIFO-Prinzip verhindert Double-Spending

Block Aufbau

- Blockheader
 - Block Number
 - Proof of Work
 - Difficulty
 - Previous Hash
 - Timestamp
 - Coinbase Transaction
- Transaktionen

- „Mining“: Einen zulässigen Hash für Blöcke finden
 - Zulässiger Hash: $\text{Sha256}(\text{Blockheader} + \text{Nonce}) < \text{Difficulty}$
 - Leicht verifizierbar
 - Schwer zu erstellen
- „Difficulty“: reguliert die durchschnittliche Mining-Dauer
 - Wird alle 2016 Blöcke angepasst
 - Im Optimalfall 1 Block / 10 Min
- „Coinbase Transaction“: Belohnung für das Mining
 - Vom Miner festgelegte Adresse
 - Beinhaltet Transaktionskosten und neu generierte Bitcoin

- Die Belohnung für Miner halbiert sich alle 210.000 Blöcke.

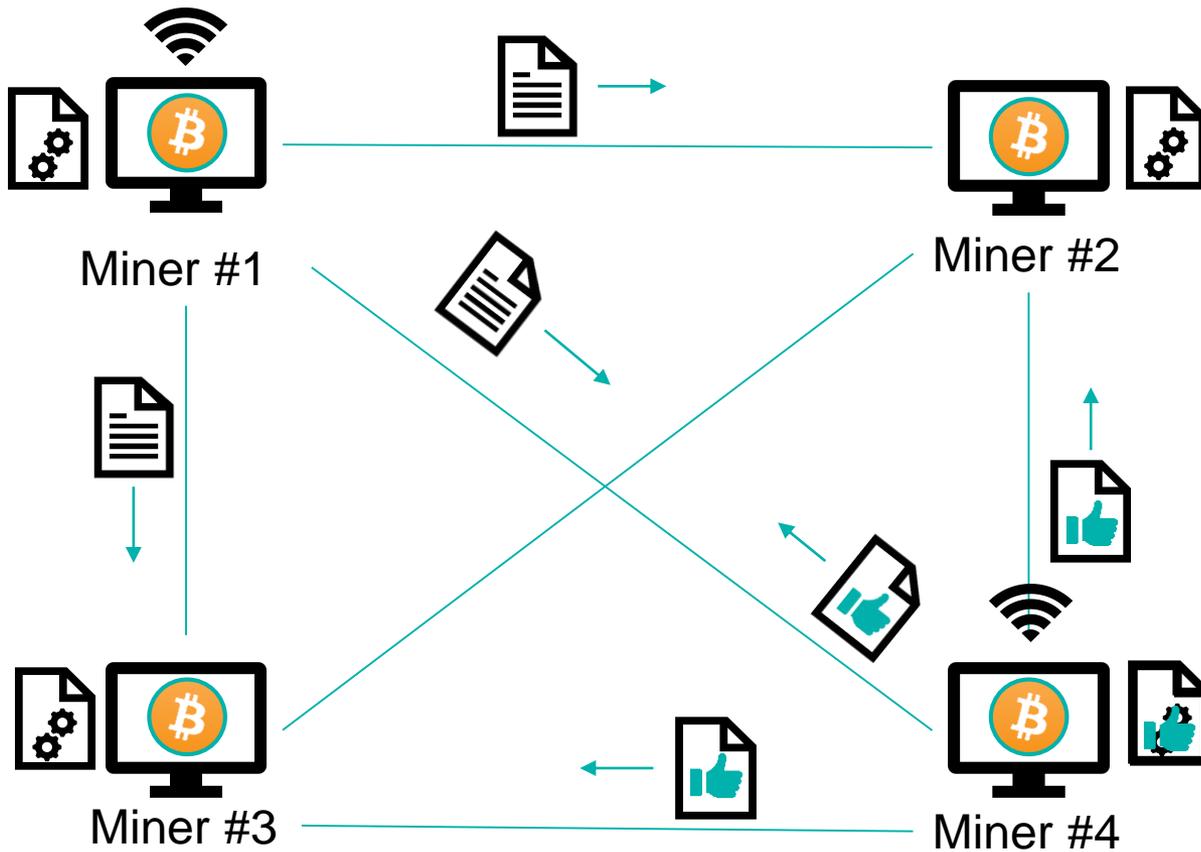
- Entspricht ca. 4 Jahren (210.000 * 10Min)
- Startwert: 50BTC
- Heute: 12,5BTC
- Formel:

- $$\frac{\sum_{i=0}^{32} 210.000 * \left(\frac{50 * 10^8}{2^i}\right)}{10^8} \approx 21 \text{ Millionen}$$

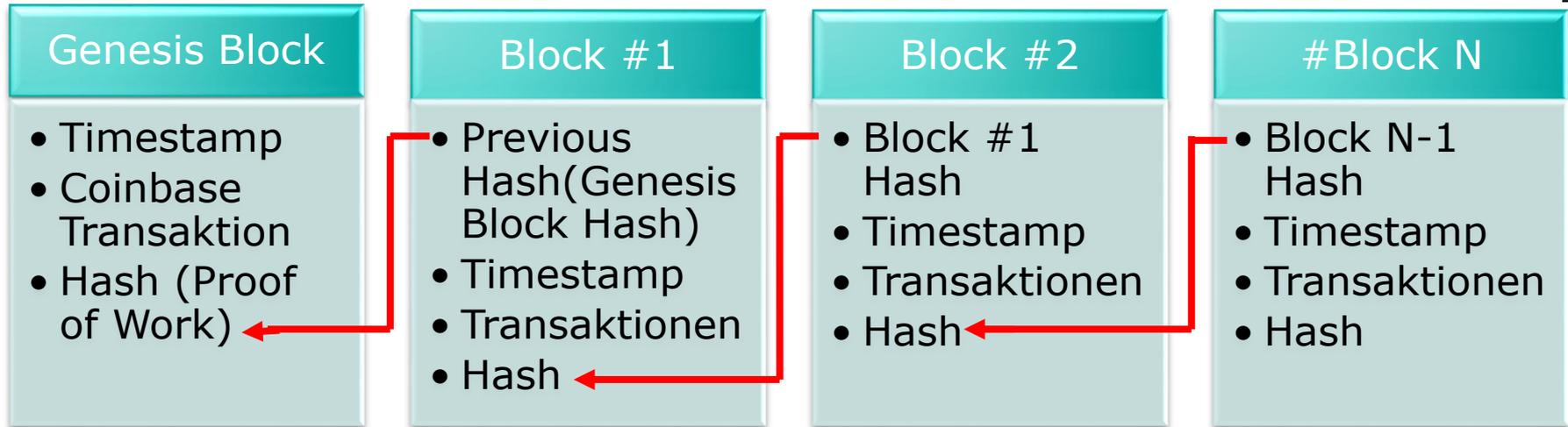


- Transaktionskosten als alleinige Einnahmequelle in der Zukunft

Bitcoin Netzwerk



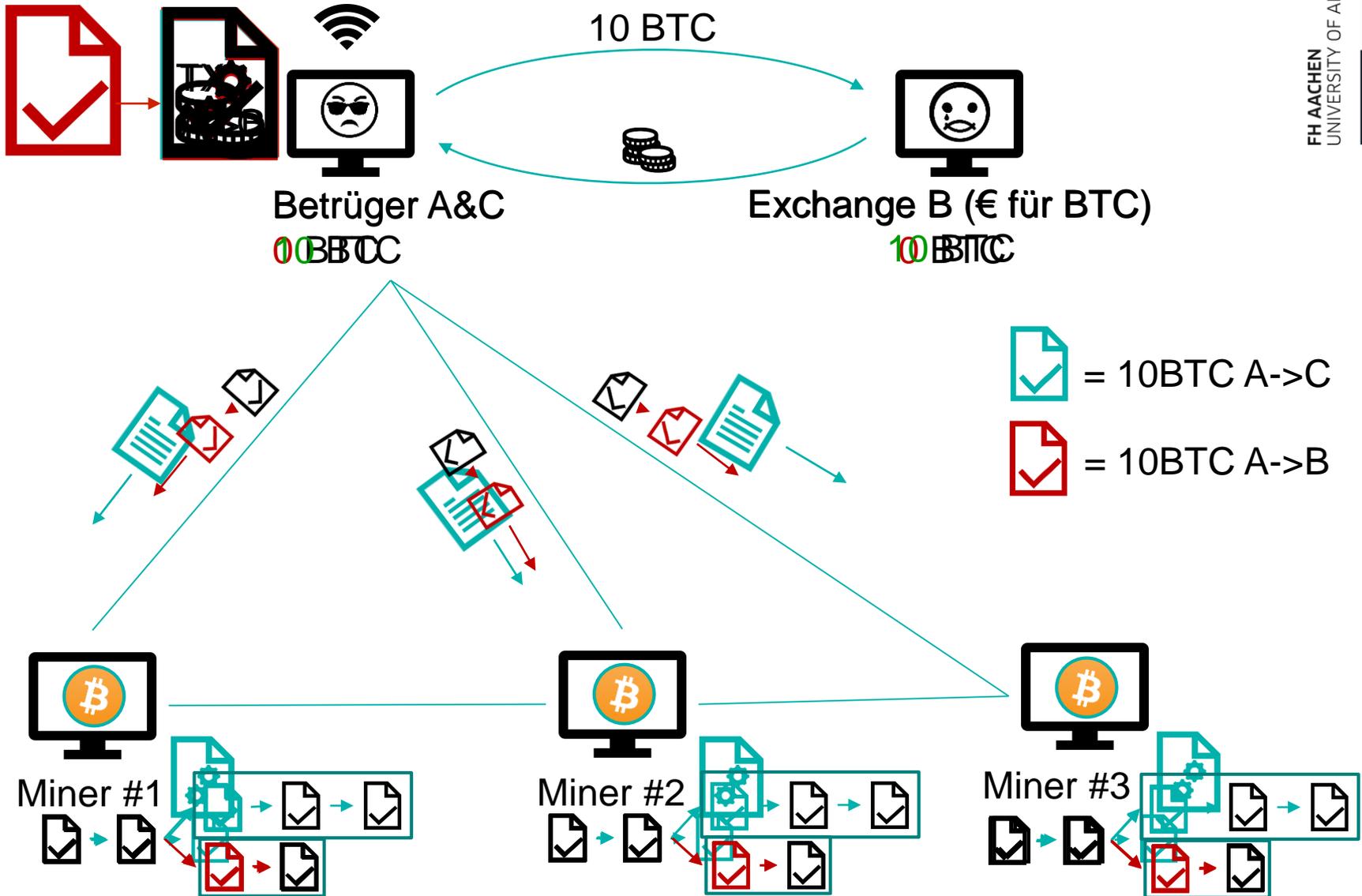
Aufbau der Blockchain



- Blockchain ist zurzeit ca. 167GB groß
- Netzwerk akzeptiert immer die längste Blockchain

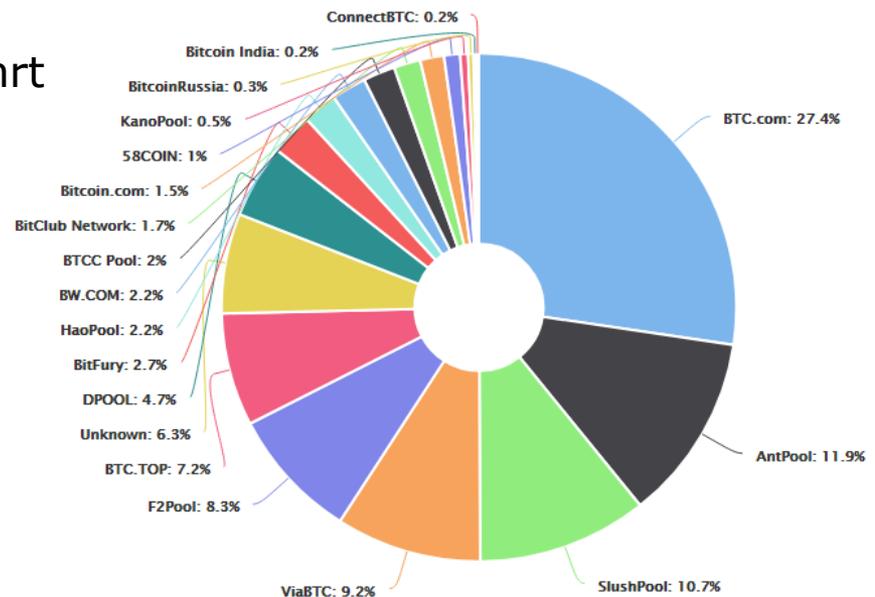
Sicherheit von Bitcoin

Sicherheit von Bitcoin



- „Confirmations“: Die Anzahl nachfolgender Blöcke
 - 6 empfohlen
 - Angreifer mit 40% Hashing Power < 1% Chance
 - Angreifer mit 51% Hashing Power = 100% Chance
 - 51% Attacke
 - Angreifer wartet so lange bis er eine 6 Blöcke längere Blockchain als das Netzwerk hat
 - Noch nie erfolgreich durchgeführt

■ Momentane Verteilung:



Ist Bitcoin anonym?

Nicht zwangsweise

BLOCKCHAIN

[GET A FREE WALLET](#)

945 unbestätigte Transaktionen Live aktualisierte Liste der aktuellen Bitcoin Transaktionen



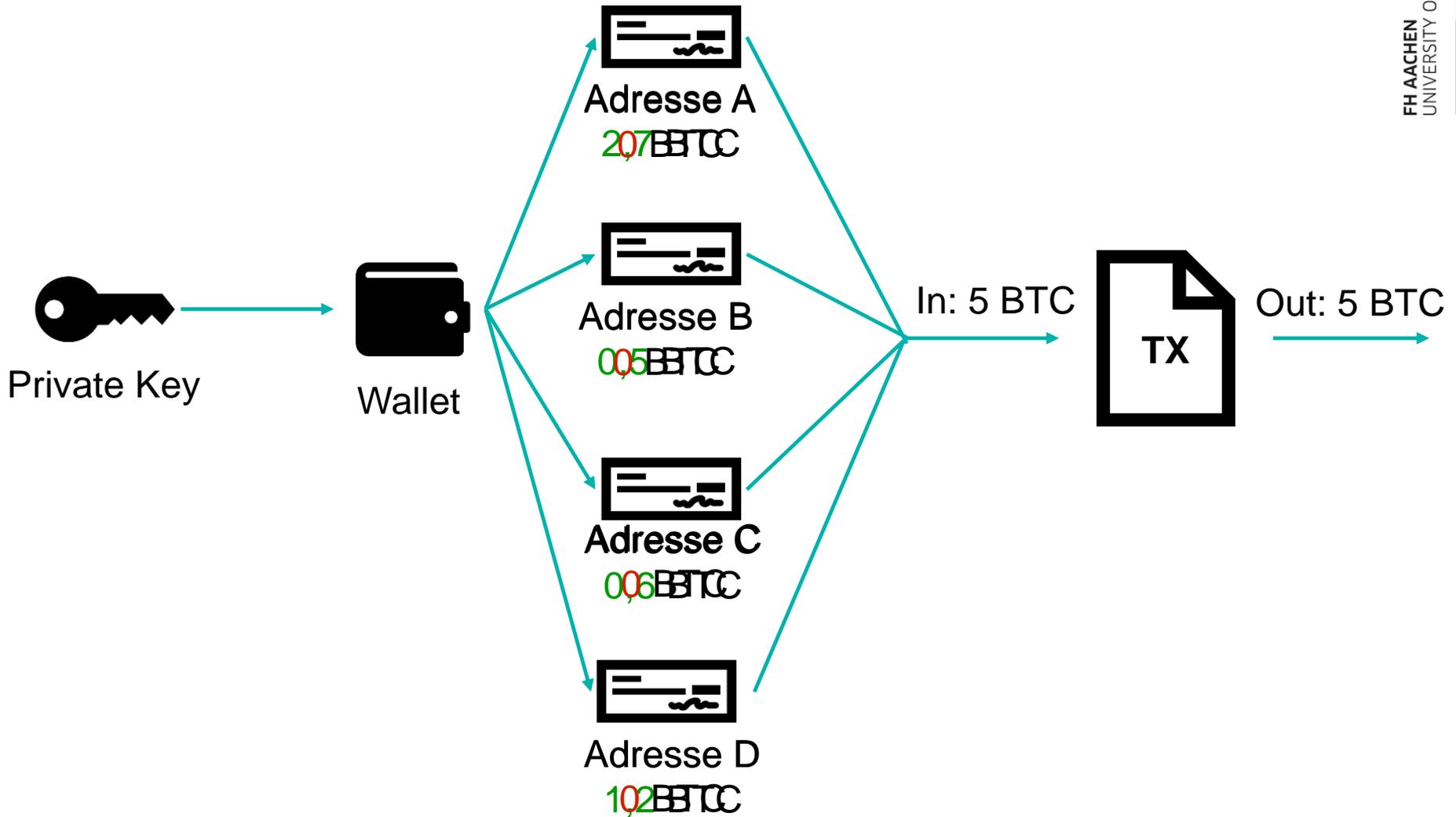
Zusammenfassung	Status: In Verbindung gebracht
Gebühren_gesamt	294.21169036 BTC
Gesamtgröße	1080684.07 (KB)
Transaktionen pro Sekunde	39.2

4a898231ed04c271c650725678e12453386866734c184b6a8f8019482808990	Today 00:12:15
3NTsc2bNmCslJv6Xs3Jmx9VpGxmJ34PrPCd	0.01188 BTC
➔	1.71988021 BTC
3MzzXaqUZxPDCux114d7N5VzmKLA4z5QJz 3KfZPntLFAzPK4uwF9gtXLZBSNE0c6U	- 1.73176021 BTC
53715e857363c8d99340a8973e8ba8c48f59e132ba512658f262a7df50c113	Today 00:12:14
1EdtHnMovSfQsgGRtjPyrhfYnThaExLgpc	0.01496836 BTC
➔	0.01496836 BTC
3H9k3XJtQAmHEeo5pNP4aG1kMw1WzVz2	0.01496836 BTC
7481489d648624cbad05c8a443884322b158a1bc35214ca1fe755859278a8ee	Today 00:12:14
12H4AmrPCoFPeJ3eyBXPhxCeKBH12unMY	0.01208626 BTC
➔	0.01208626 BTC
1Kp0kMPrUXjYLnNucP2UsraPgrpeZ2GF	0.01208626 BTC

■ Pseudonymität:

- ❑ Bitcoin Adressen sind nicht an Personen geknüpft
- ❑ Jede bestätigte/unbestätigte Transaktion ist öffentlich verfügbar
- ❑ Guthaben von Adressen können in der Blockchain nachvollzogen werden

Anonymität von Bitcoin



7e76e1a51153589201d8511a82eea9e49a0f2e6d4b1eda00e1055effbd^{2461h8}

3KzEwPNisc76EcvpgQ5aKAnkzwr61DFf2p
 3HzsMgtstNyc1gN6Aizd1hVmGfSLKWtuYd
 3LTracJJizVrkM7ZHmLVYVizkJcwFmWfqr
 3K54sECypcTgJ5qbw4DjPEMC87Rx1pgjhv
 3CN5Pva7rpSk78VDb2JHF3FEBSmnmHm1Cc
 39hxeTA9ZVvWy5Z85FSwoTUnzVYizxLwp7
 3KzEwPNisc76EcvpgQ5aKAnkzwr61DFf2p
 3HzsMgtstNyc1gN6Aizd1hVmGfSLKWtuYd
 3LTracJJizVrkM7ZHmLVYVizkJcwFmWfqr
 3K54sECypcTgJ5qbw4DjPEMC87Rx1pgjhv
 3CN5Pva7rpSk78VDb2JHF3FEBSmnmHm1Cc
 39hxeTA9ZVvWy5Z85FSwoTUnzVYizxLwp7
 3EMr1iJAZjKWmyY5XA7JpeTty9ZdDLUgX
 3L91u8y54ry14XkzhbKMCnx52HNe7WY4UX
 3M7gJY8ZVa8XaBuFU8K8mzoQoJXyhNkxD
 3EFHevqaghkPxj22C81tvFurkx57EhgpUF
 3B3zLyjZXkuHXJPqhW9n8FcGWojBEBCTiK
 3FiVp8cJzAYQjJuvrGshDgVAKWGLfwWvN
 381MfZS1rdiR2MdfU66CiaAKnMMTsi2J21
 3D44pA3a3a1cCQZv9a6zAQhwXbpPyZVapa
 1BJCA6Wfxhnx8BzZbdgL5A18HzBRhrCBAA

origin
0.0587935 BTC

39bYVwMrsBnej4tNQbi26iCQiLMo1B51bz
0.03759414 BTC

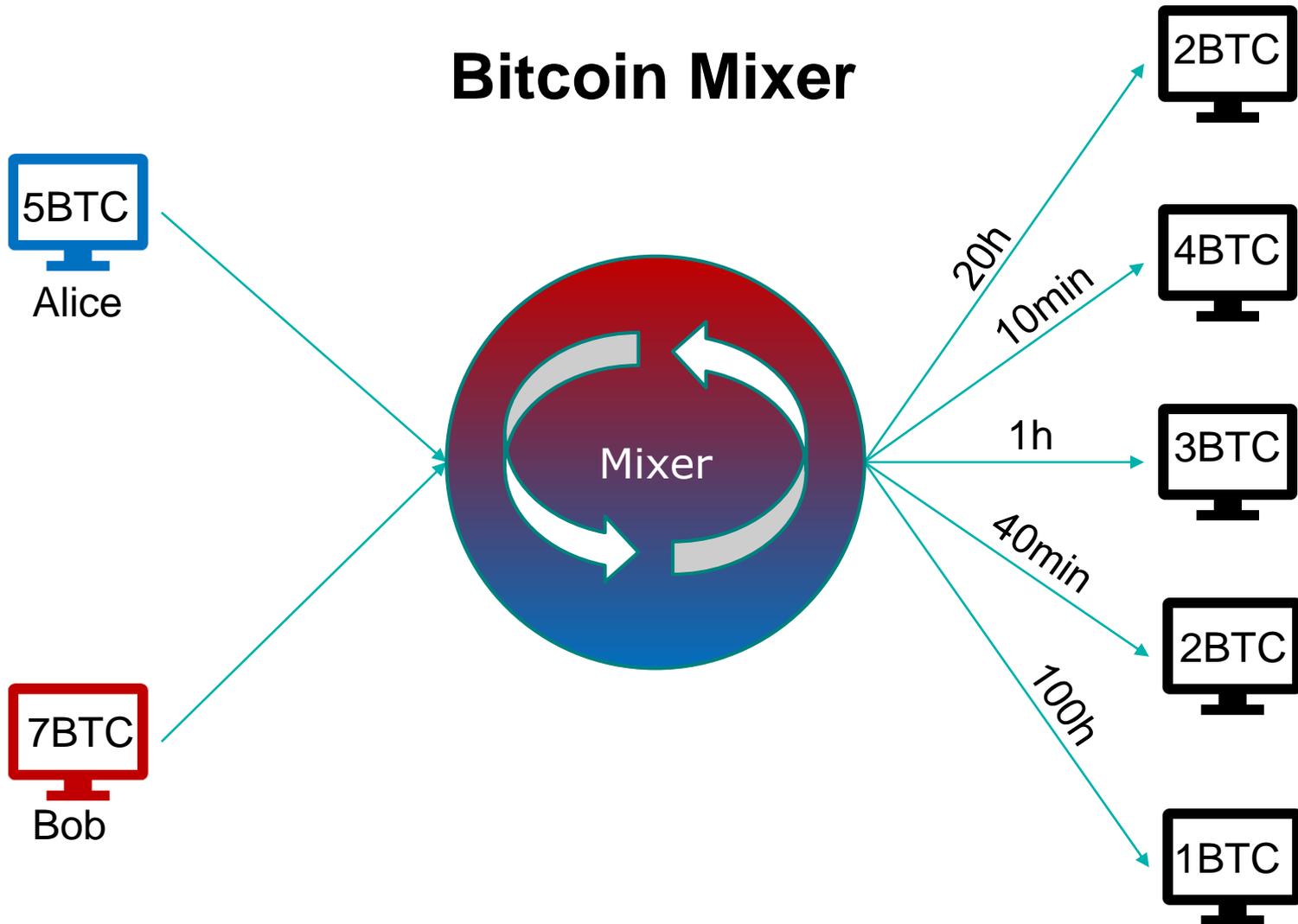
0.03759414 BTC
0.02119936 BTC

0.0587935 BTC

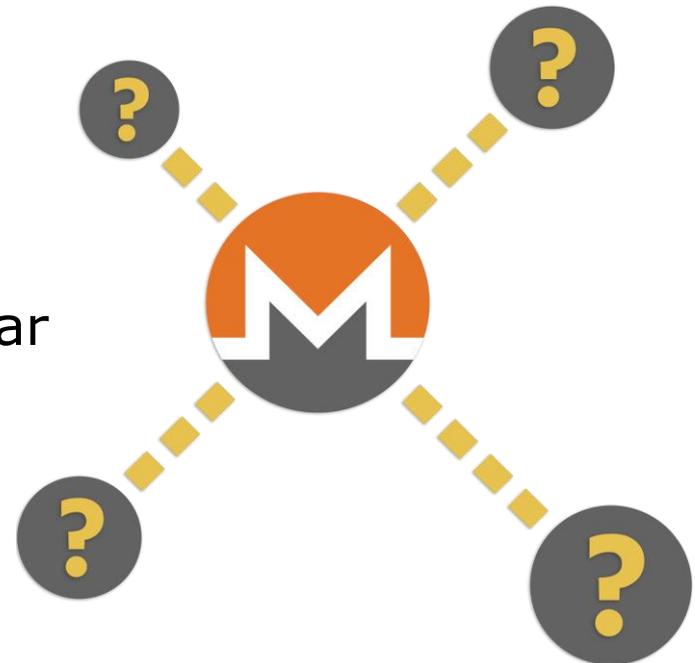
17E4NvQ5YtCRqugXUrGDJiENZXu8SByJa
0.02119936 BTC

- Bitcoin-Adressen können ggf. IP-Adressen/Personen zugeordnet werden:
 - Posten der Bitcoin-Adresse online
 - Umwandeln von Bitcoin zu Fiat
 - Onlinekäufe mit Bitcoin tätigen
 - Nutzung ohne VPN:

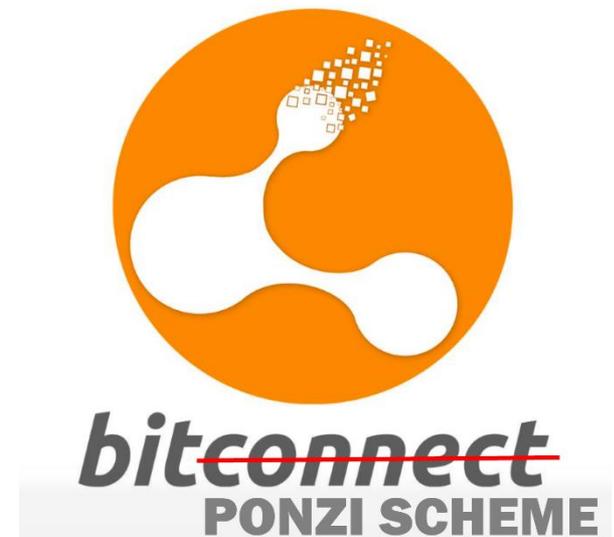




- Umstieg auf alternative Kryptowährungen auf dem Schwarzmarkt
- Bitcoin nur noch verantwortlich für wenige Transaktionen im Darkweb
- Monero (XMR):
 - Blockchain Technologie
 - Stealth-Adressen
 - Transaktionen nicht nachvollziehbar



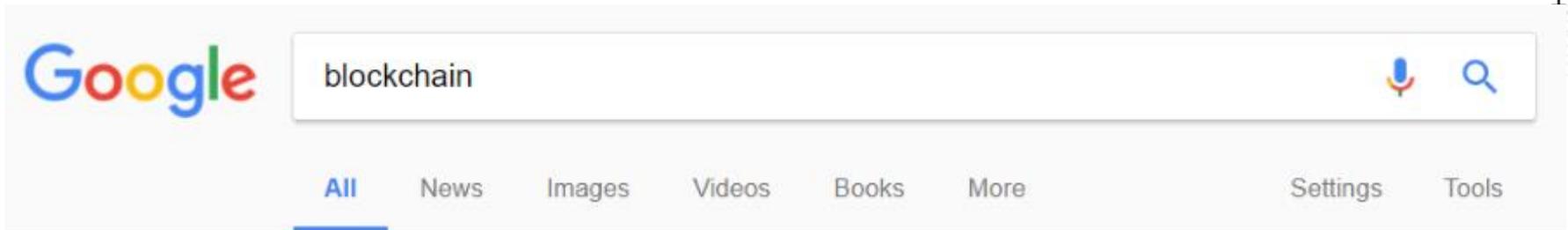
- Kryptowährungen als Währung für Dienstleistungen und illegale Güter:
 - Schnelle anonyme Transaktionen
 - Problemlose Handhabung und Aufbewahrung
 - Von überall auf der Welt zugreifbar
- Kryptowährung als Betrugsplattform
 - Rapider Marktanstieg verursacht FOMO
 - Falsche Kryptowährungen überschwemmen den Markt
 - Bitconnect klaut 2018 erfolgreich 1,5 Milliarden Dollar von seinen Nutzern



- Klauen von Private-Keys:
 - Trojaner
 - Keylogger
 - Phishing
- Unwissenheit ausnutzen:
 - Nutzer austricksen, schon vorgenerierte Private-Keys zu nutzen.



Phishing



- Blockchain Technologie immer noch jung
 - Gibt es noch unentdeckte Sicherheitslücken?
- Bitcoin revolutionär aber:
 - Anonymität nicht gewährleistet
 - Vorreiter für neue Kryptowährungen mit weniger Schwachstellen (Anonymität, Skalierungsproblem, Energieverbrauch,...)
- Kryptowährungen bieten erstmals die Möglichkeit komplett anonym Transaktionen über das Internet zu tätigen
 - Mehr Anonymität bedeutet oft mehr Kriminalität
 - Methoden der Strafverfolgung schwierig
 - Sicherstellung von Geldern teilweise unmöglich

- Bitcoin Whitepaper (<https://bitcoin.org/bitcoin.pdf>)
- Ethereum Whitepaper (<https://github.com/ethereum/wiki/wiki/White-Paper>)
- Bitcoin Wiki (<https://en.bitcoin.it>)
- Block Explorer (<https://blockexplorer.com/>)
- <http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>
- <https://steemit.com/cryptocurrency/@budz82/bitconnect-scam-bitconnect-ponzi-and-bitconnect-pyramid-scheme-trends-exploding-is-the-bitconnect-ponzi-scheme-close-to-its-end>
- <https://www.buybitcoinworldwide.com/anonymity/>
- <https://coinmarketcap.com/>
- <https://coinmixer.se/de/>
- <https://getmonero.org/>
- <https://coinsutra.com/hash-rate-or-hash-power/>
- <https://blockchain.info/>
- <https://www.coindesk.com/eu-law-enforcement-digital-currency-impeding-investigations/>
- https://www.reddit.com/r/btc/comments/7ofrqf/warning_brutal_scam_guy_buys_a_ledger_nano_wallet/
- https://www.reddit.com/r/Bitcoin/comments/74sj7q/warning_when_googling_blockchain_you_get_a_fake/

Danke für ihre
Aufmerksamkeit