Sicherheit und Anonymität von Kryptowährungen

Jonathan Schumann

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

Gliederung

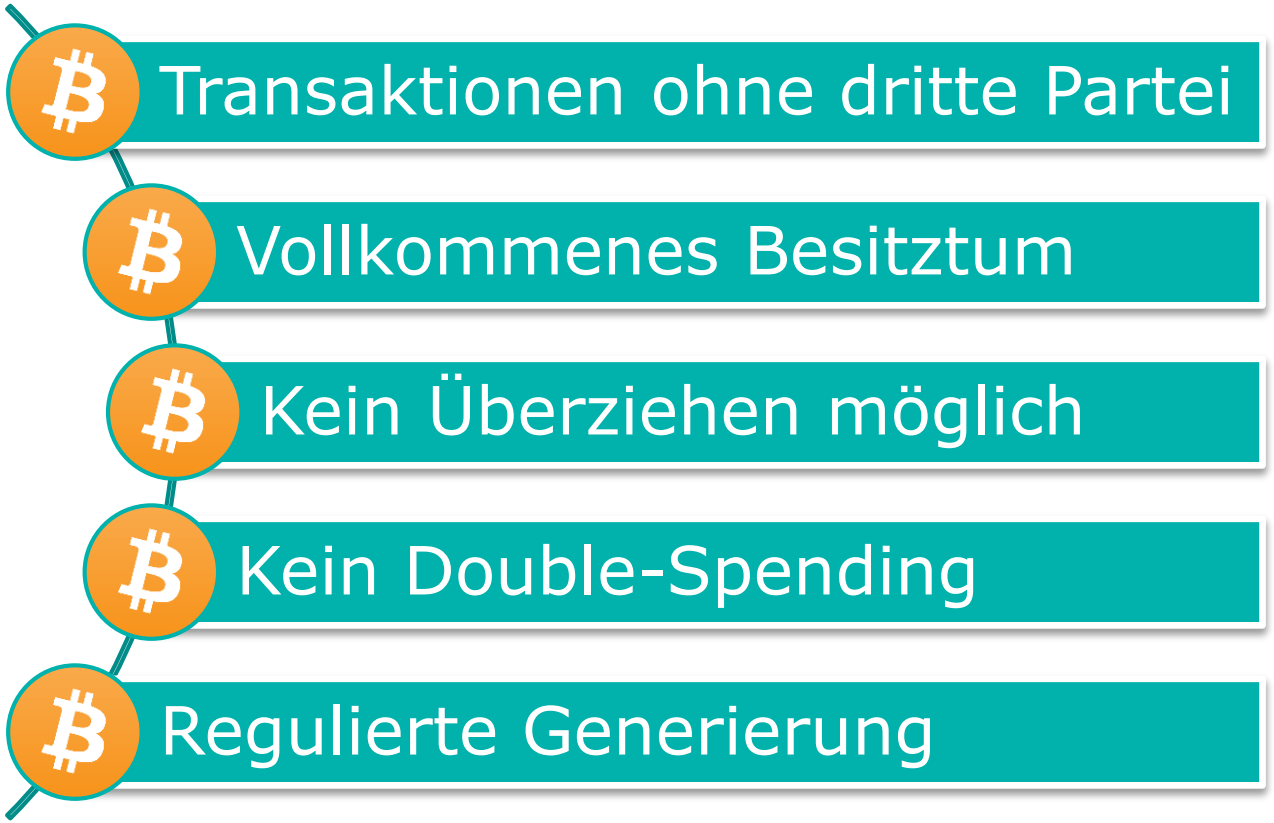
- Kryptowährungen allgemein
- Bitcoin
  - Anforderungen
  - Funktionsweise
- Sicherheit und Anonymität (Bitcoin)
  - Confirmations
  - Anonymität
- Kryptowährungen und Kriminalität
  - Schwarzmarkt
  - Diebstahl
- Fazit

Kryptowährungen Allgemeines

- 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)

Bitcoin - Anforderungen

Anforderungen an Bitcoin

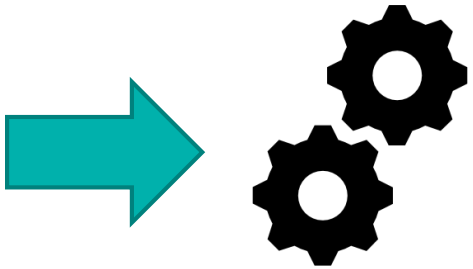


Bitcoin - Adressen

- 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

Bitcoin - Adressen

Keypair



Kryptographisches Verfahren

1GPaJQLww88wLsrcNNzHjFjLaJBsT58awX

Beliebig viele Adressen

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

Bitcoin - Funktionsweise

- 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

Bitcoin - Funktionsweise

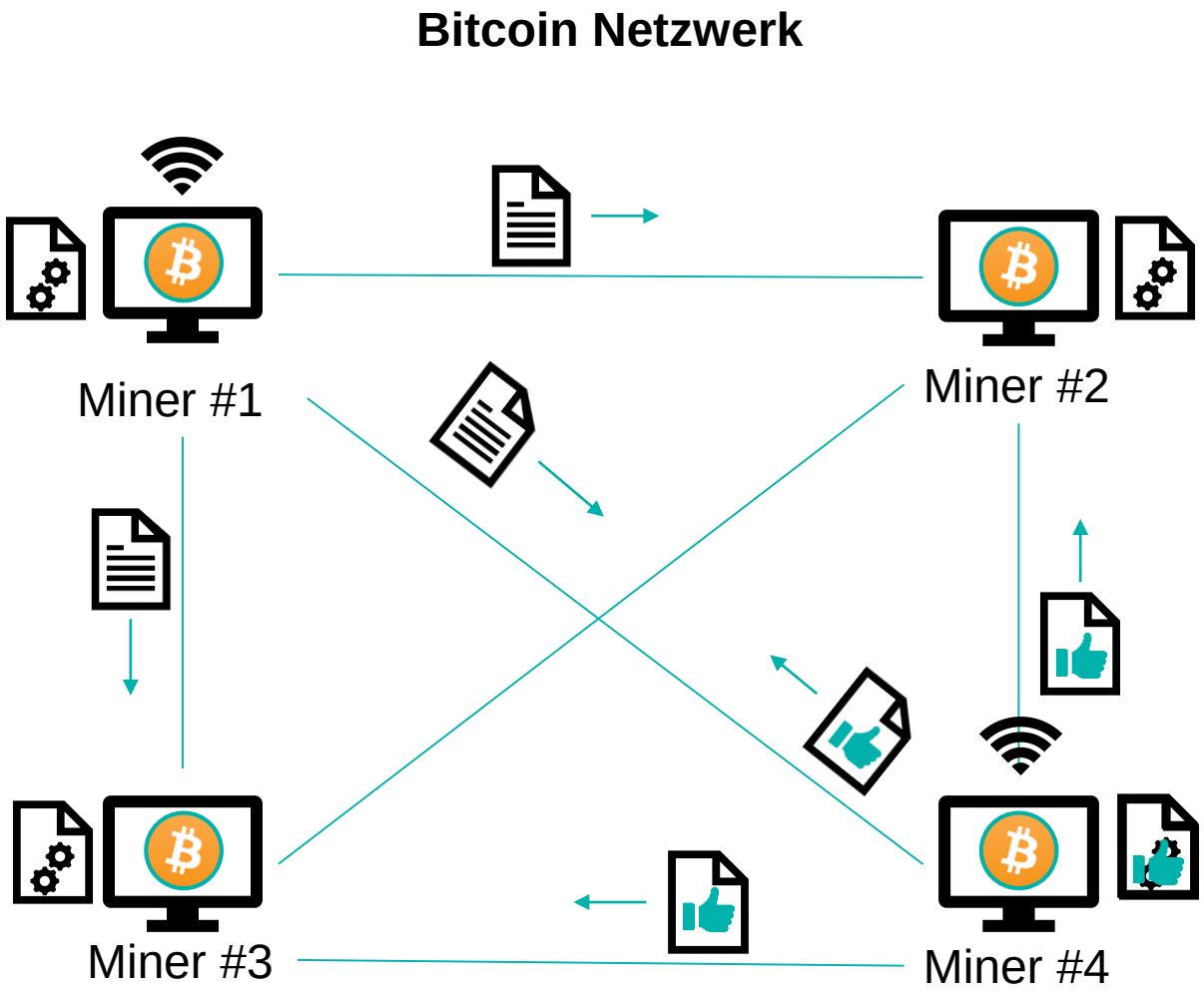
- „Mining“: Einen zulässigen Hash für Blöcke finden
  - Zulässiger Hash: Sha256(Blockheader+Nonce) < Difficulty
  - Leicht verifizierbar
  - Schwer zu erstellen
- „Difficulty“: reguliert die durchschnittliche Mining-Dauer
  - Wird alle 2016 Blöcke angepasst
  - Im Optimalfall 1 Block / 10 Min
- „Coinbase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

Bitcoin - Funktionsweise

- Die Belohnung für Miner halbiert sich alle 210.000 Blöcke.
  - Entspricht ca. 4 Jahren (210.000 * 10Min)
  - Startwert: 50BTC
  - Heute: 12,5BTC
  - Formel:
  - $$\frac{\sum_{i=0}^{32} 210.000*(\frac{50*10^8}{2^i})}{10^8} \approx 21 Millionen$$

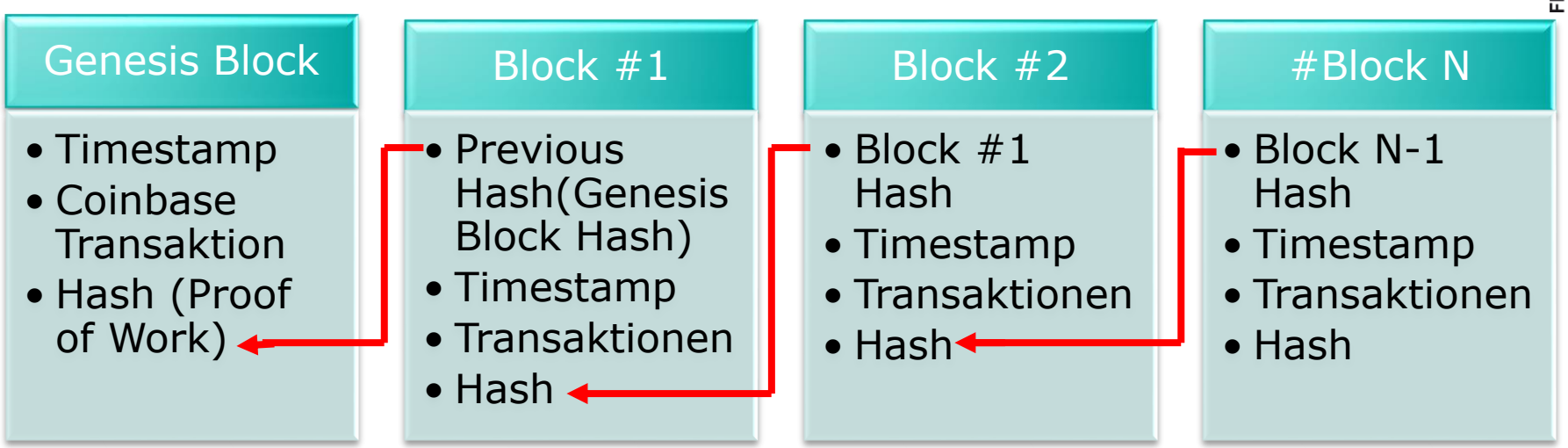
- Transaktionskosten als alleinige Einnahmequelle in der Zukunft

Bitcoin - Funktionsweise



Bitcoin - Funktionsweise

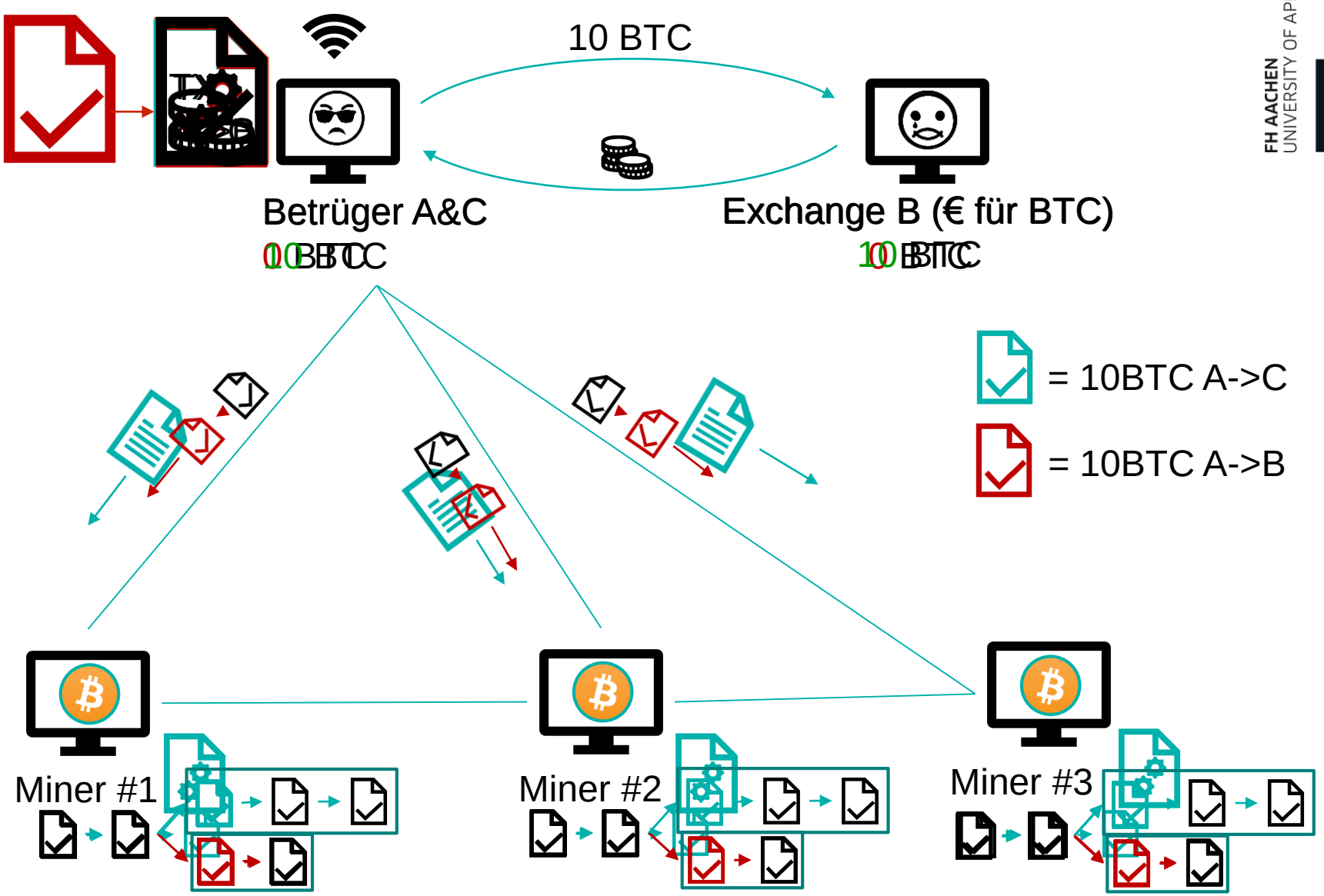
Aufbau der Blockchain



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

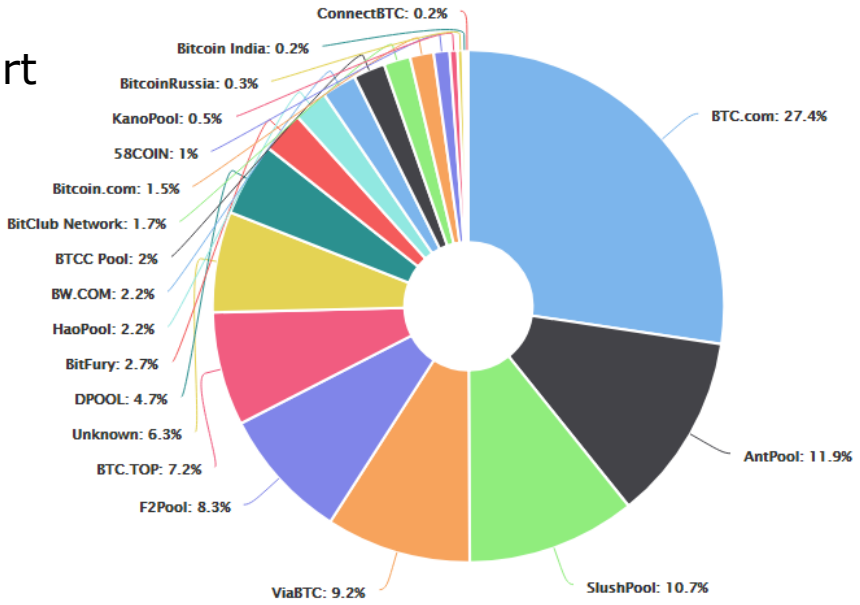
Sicherheit von Bitcoin

Sicherheit von Bitcoin



Sicherheit von Bitcoin

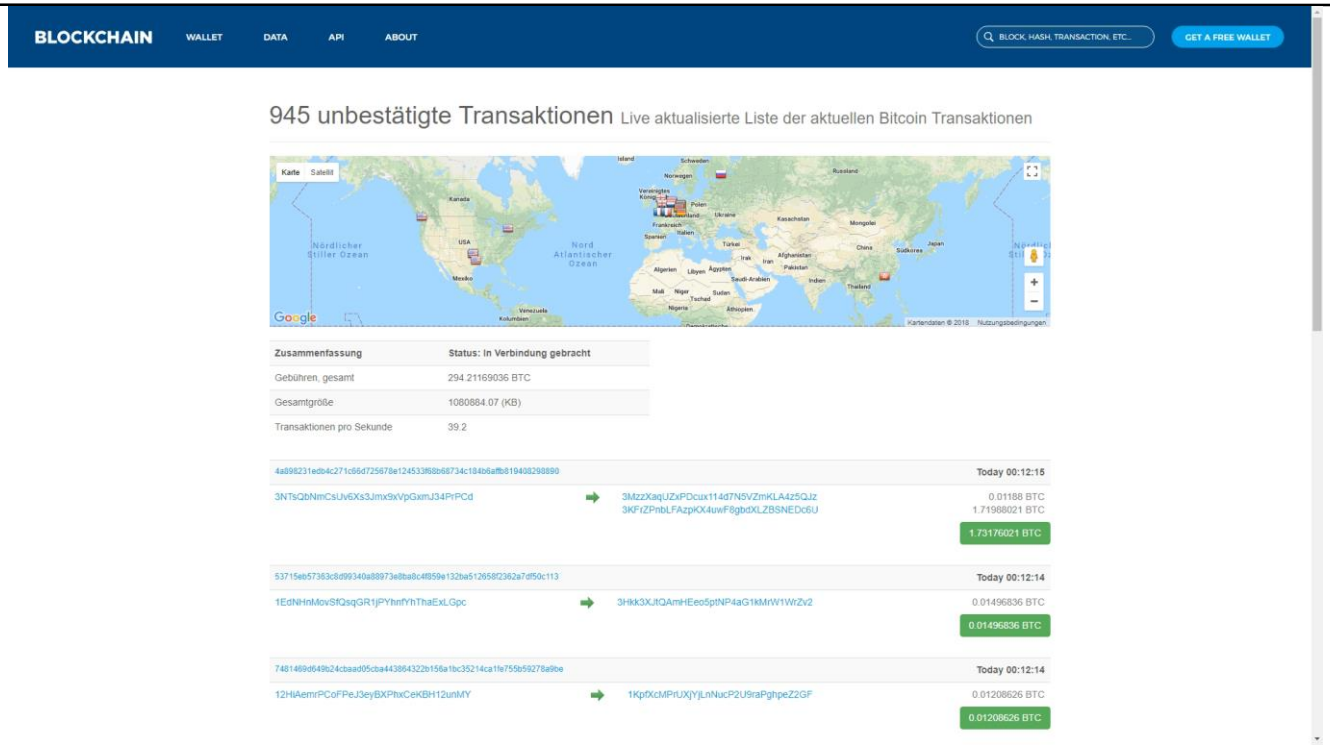
- „Confirmations“: Die Anzahl nachfolgender Blöcke
  - 6 empfohlen
  - Angreifer mit 40% Hashing Power < 1% Chance
  - Angreifer mit 51% Hashing Power = 100% Chance
    - 51% Attacke
    - Angreifer wartet so lange bis er eine 6 Blöcke längere Blockchain als das Netzwerk hat
    - Noch nie erfolgreich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



Ist Bitcoin anonym?

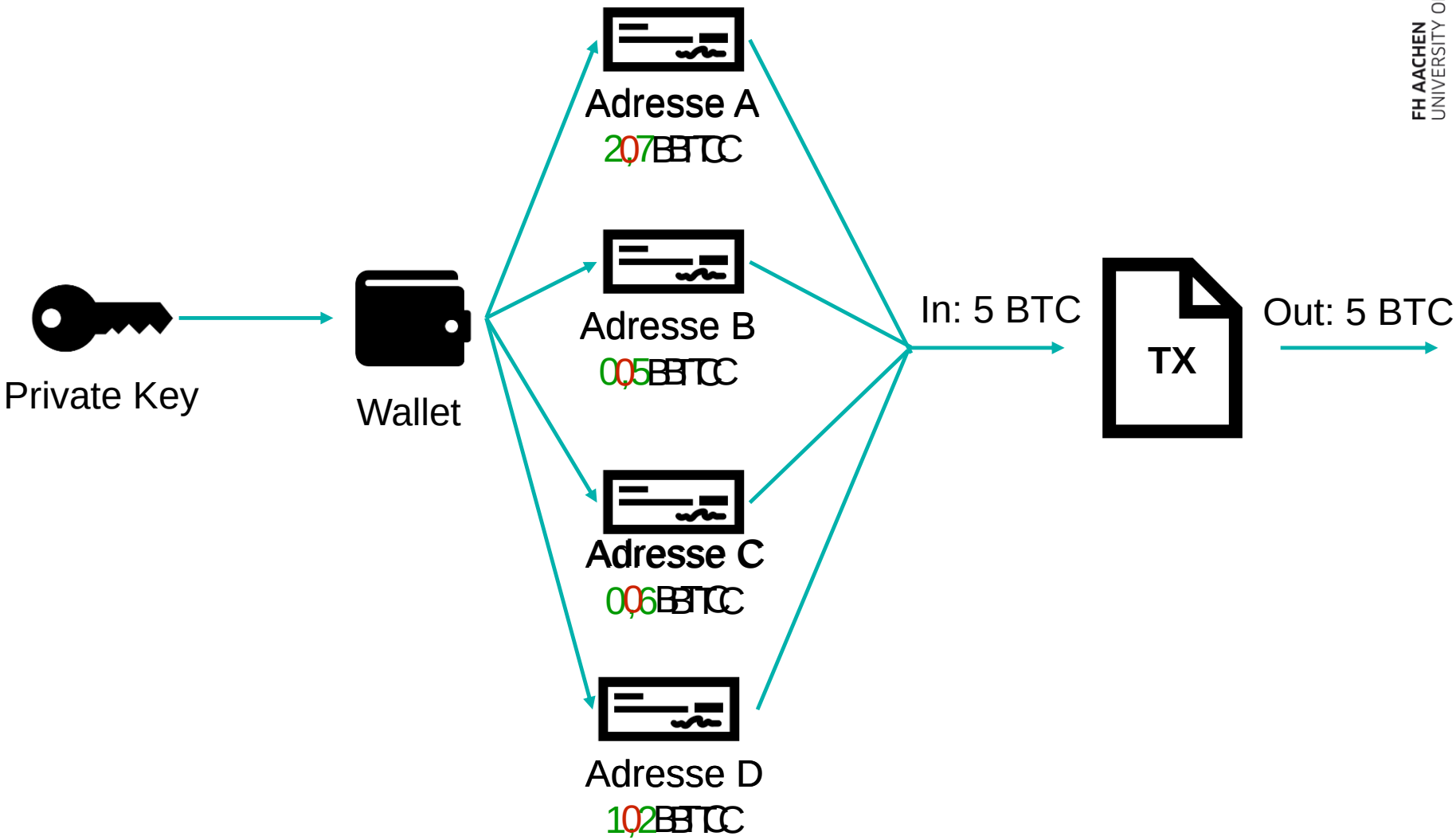
Nicht zwangsweise

Anonymität von Bitcoin

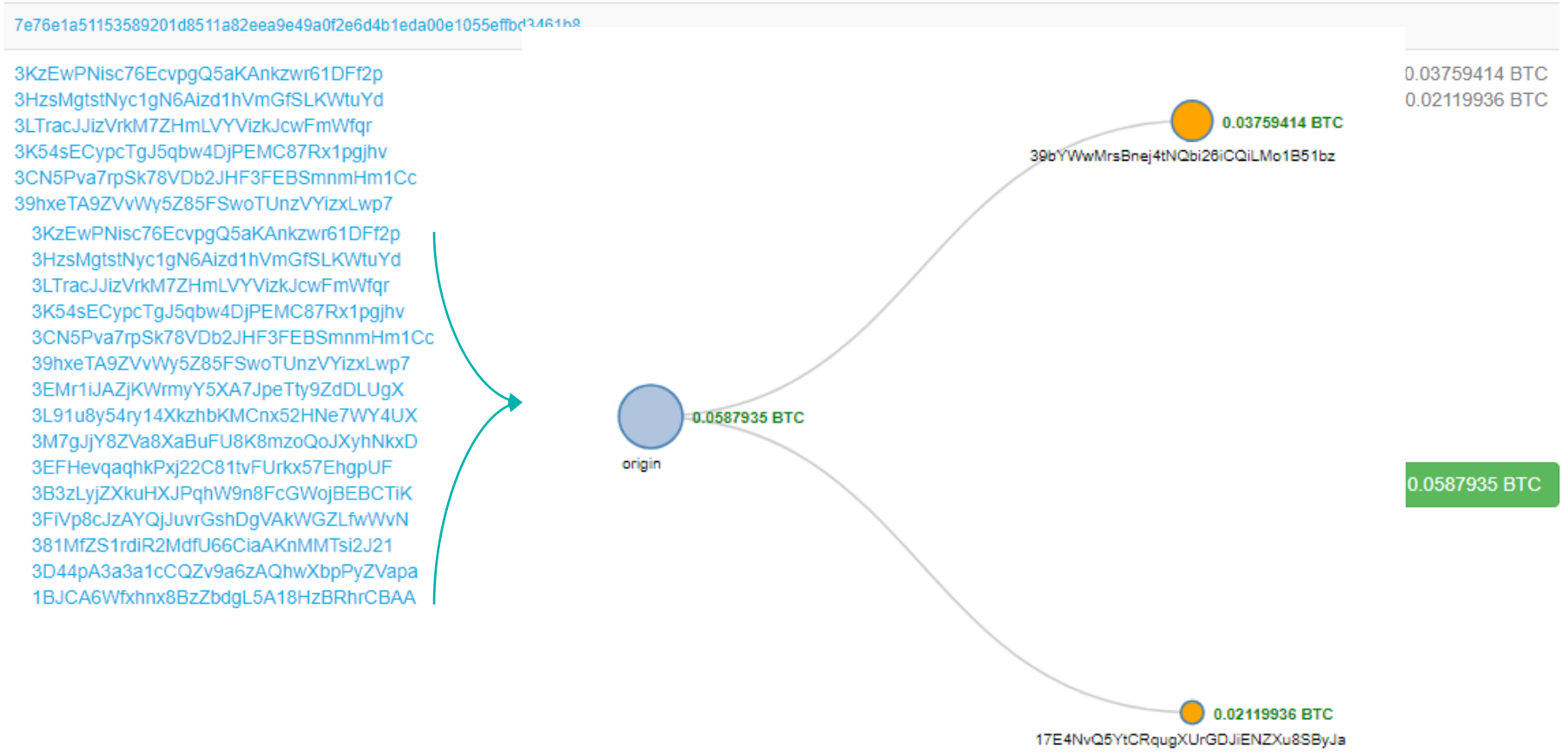


- Pseudonymität:
  - Bitcoin Adressen sind nicht an Personen geknüpft
  - Jede bestätigte/unbestätigte Transaktion ist öffentlich verfügbar
  - Guthaben von Adressen können in der Blockchain nachvollzogen werden

Anonymität von Bitcoin



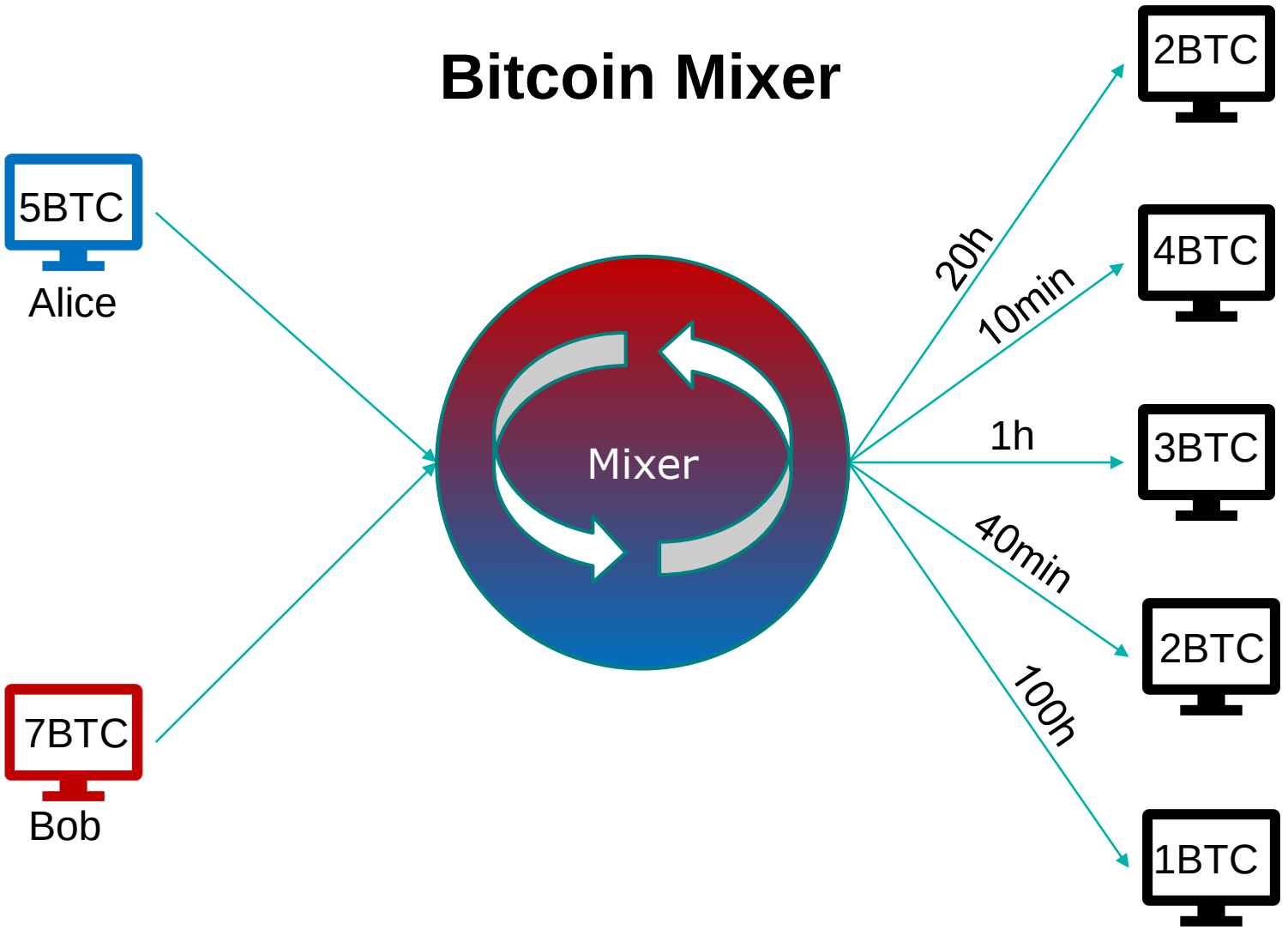
Anonymität von Bitcoin



Anonymität von Bitcoin

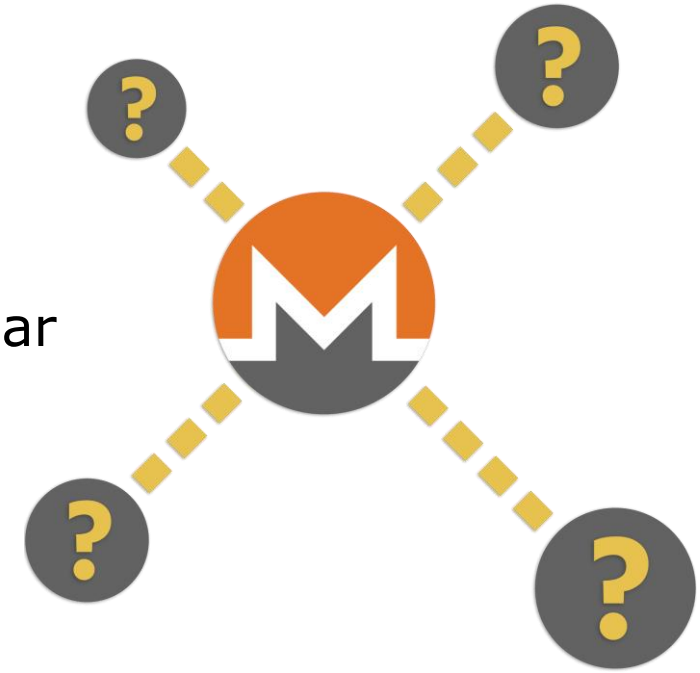
- Bitcoin-Adressen können ggf. IP-Adressen/Personen zugeordnet werden:
  - Posten der Bitcoin-Adresse online
  - Umwandeln von Bitcoin zu Fiat
  - Onlinekäufe mit Bitcoin tätigen
  - Nutzung ohne VPN:

Anonymität von Bitcoin



Kryptowährungen und Kriminalität

- 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 und Kriminalität

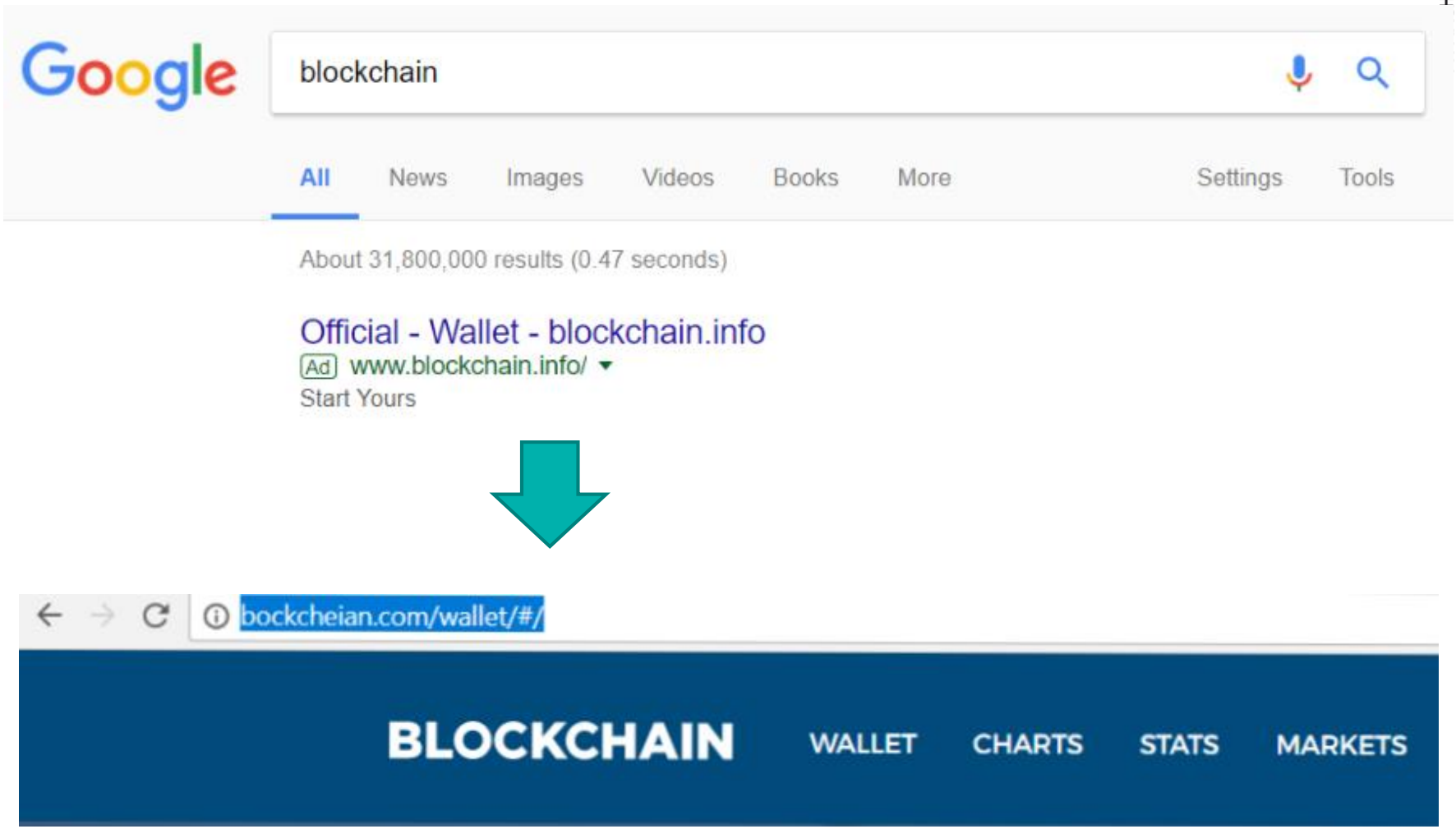
- Kryptowährungen als Währung für Dienstleistungen und illegale Güter:
  - Schnelle anonyme Transaktionen
  - Problemlose Handhabung und Aufbewahrung
  - Von überall auf der Welt zugreifbar
- Kryptowährung als Betrugsplattform
  - Rapider Marktanstieg verursacht FOMO
  - Falsche Kryptowährungen überschwemmen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

Kryptowährungen und Kriminalität

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

Kryptowährungen und Kriminalität

Phishing



Fazit

- 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

Quellen

- 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