HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Bitcoin Sicherheit

Marc Herschel, 7.6.2019

Gliederung

Sektion 1 Allgemeines und Best Practices aus Anwendersicht

- Wallets und Verwahrung
- Anonymität mit Bitcoin? / Mixer vs. CoinJoin
- Sicherheit durch Proof of Work

Sektion 2 Angriffe auf das Bitcoin Netzwerk

- 51% Angriff
- Blacklisting
- Sybil Angriff
- Routing Angriff
- DoS Angriff

Gliederung

Sektion 1 Allgemeines und Best Practices aus Anwendersicht

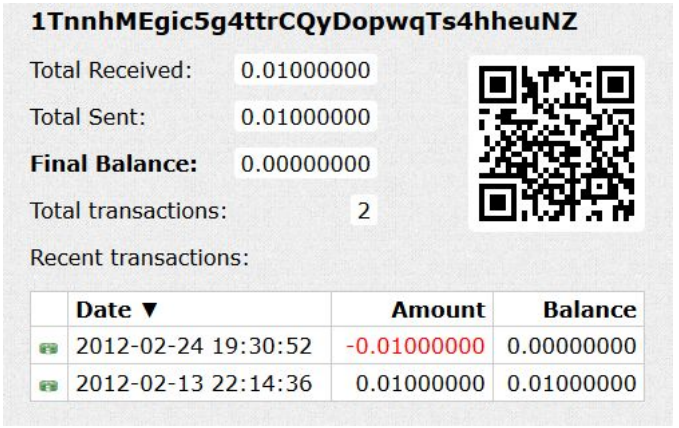
- Wallets und Verwahrung
- Anonymität mit Bitcoin? / Mixer vs. CoinJoin
- Sicherheit durch Proof of Work

Fundamentales Sicherheitsprinzip

- Dezentralisierung
  - Basiert nicht auf Zugangsberechtigungen/Accounts und „vetting“
  - => Identitätendiebstahl nicht im traditionellen Sinne möglich
  - Alle Teilnehmer kontrollieren das Netz und nicht eine Entität
  - Keine Ende-zu-Ende Verschlüsselung beim Zahlungsverkehr
  - Transaktionen öffentlich einsehbar => Transparenz
  - Konsens um schädliche Aktoren zu verhindern

Nachteil: Nutzer müssen ihre Keys sicher verwahren

Schwächster Punkt: Nutzer



1TnnhMEgic5g4ttrCQyDopwqTs4hheuNZ

Total Received:	0.01000000
Total Sent:	0.01000000
Final Balance:	0.00000000
Total transactions:	2

Recent transactions:

	Date ▼	Amount	Balance
	2012-02-24 19:30:52	-0.01000000	0.00000000
	2012-02-13 22:14:36	0.01000000	0.01000000

- Kryptographisch schlechte Schlüssel

`sha256("sausage") = 30caae2f……a683 =` `1TnnhMEgic5g4ttrCQyDopwqTs4hheuNZ`

- Verlust des Wallets
  - Diebstahl, mangelhafte Backups, Verlust des Passphrase
  - Beispiel: Stefan Thomas – 7.000BTC ~ 140.000$
- Fehlender Gesunder Menschenverstand
  - Nutzungen unsicherer Drittparteidienste
  - Transaktionen außerhalb der Blockchain

Lost coins only make everyone else's coins worth slightly more.
Think of it as a donation to everyone. – Satoshi Nakamoto

Das Problem mit den Dritten

- Bitcoin in Verbindung mit „Trusted Third Parties“ hebt nahezu alle Vorteile der Dezentralisierung auf
- Leider nicht vermeidbar mit Exchange Seiten

Negativ Beispiel: **MT.Gox**

- Ursprünglich Tauschbörse von Sammelkarten
- 2011: Erster Hack, Preis 1 BTC = 1 ct gesetzt und schnell zugeschlagen
- August 2013: 60% des weltweiten Handelsvolumen
- 2015: CEO festgenommen, 7.000 BTC durch Hack entschwunden, 643.000 BTC durch Insider entwendet

Ebenfalls Problematisch: Online Hot Wallets, Online Backups (unverschlüsselt)

Cold Storage: HW Wallets / Paper Wallets

Großteil der Coins **immer** „kalt“ lagern und diversifizieren!

HW Wallets:

- Gelten als relativ sicher, Trezor listet 9 wichtige Updates über 4 Jahre
- Recovery Seed wird am Anfang erstellt, garantiert Wiederherstellung
- Kritischer Abschnitt: Erwerb – Angreifer verkaufen möglicherweise modifizierte HW Wallets.

Paper Wallets:

- HW Wallets sind am Ende „glorifizierte USB Sticks“ => als reines Backup ohne Sicherung des Seeds nicht brauchbar
- Nur Off-Site Lagerung des Seeds garantiert Zugang im Falle von Verlust

Anonymität und Tracking

- Pseudonym, **nicht** anonym!
- Blockchain und Transaktionshistorie jederzeit einsehbar
- Mittlerweile Tracking und Monitoring Firmen unterwegs
- Linking von Pseudonymen über z.B. Exchange Seiten oder Bestellungen bei Händlern möglich
- Deswegen Mehrfachadressnutzung unbedingt vermeiden
- Spezielle Wallets und Verfahren können Tracking zwar nicht verhindern, aber erschweren

CHAINALYSIS REACTOR - INVESTIGATION SOFTWARE SUITE

Chainalysis cryptocurrency investigation software helps law enforcement and financial institutions identify and stop bad actors who are using cryptocurrencies for illicit activity such as fraud, extortion, and money laundering. With an intuitive graphical interface, Chainalysis Reactor enables users to easily conduct in-depth investigations into the source and provenance of cryptocurrency transactions.

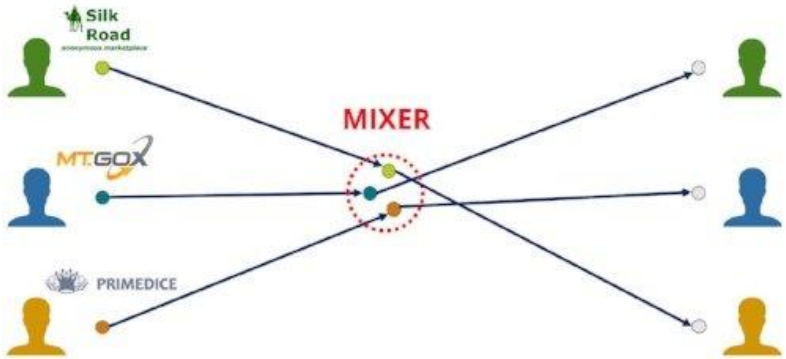
Start from anywhere — Have a ransom note with a cryptocurrency address? Have some plain text that contains cryptocurrency references? Paste it into Reactor and it will automatically find connected paths to identify potential suspects in investigations.

Clear evidence — Document your investigation process in Reactor to provide a clear record of your findings. Evidence from Chainalysis has been used successfully in court cases worldwide.

Multi-currency support — Conduct investigations across Bitcoin, Bitcoin Cash, Ether, Litecoin, and other top cryptocurrencies.

https://www.chainalysis.com/

Mixer



- Mittlerweile „antike“ Technik aus der Adaptionszeit
- Meistens über Hidden Services implementiert
- Verstößt gegen das Prinzip der Dezentralisierung
- Mixer **muss** vertraut werden
- Idee: Verschiedene Teilnehmer stellen Mixer Coins zur Verfügung, Mixer zahlt diese wieder an die Teilnehmer aus
- Mixer nimmt meist selbst noch eine Gebühr
- Unsicheres Verfahren, oftmals ein Buffet für Betrüger (Exit Scams, …)

CoinJoin

- Mehrere Teilnehmer führen eine Transaktion gemeinsam aus
- Prinzip: Zusammenführen von Transaktionen
- Teilnehmer signieren nur wenn ihre Transaktion korrekt ist

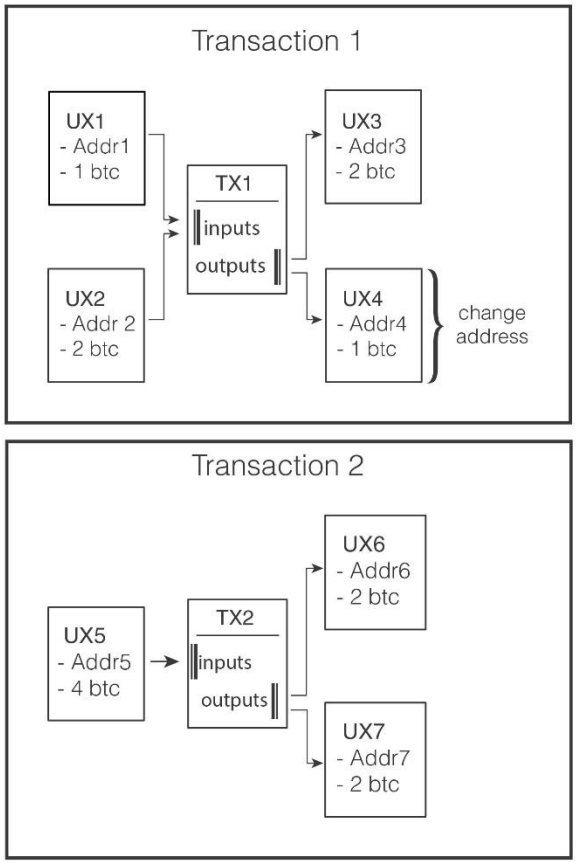
Ziel: Verschleierung der Zuordnung *Input* : *Output*

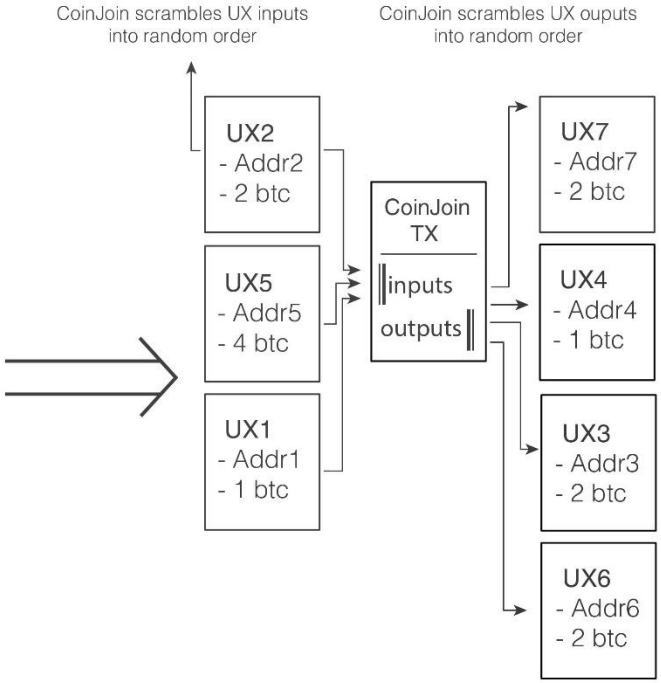
Vorteil:

- Kein Trust zwischen Teilnehmern notwendig

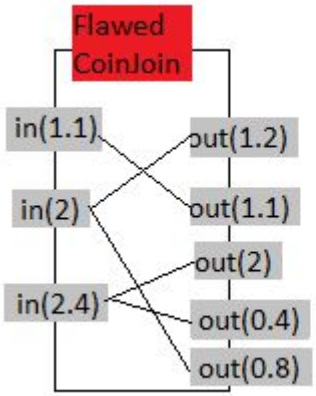
Mögliche Probleme:

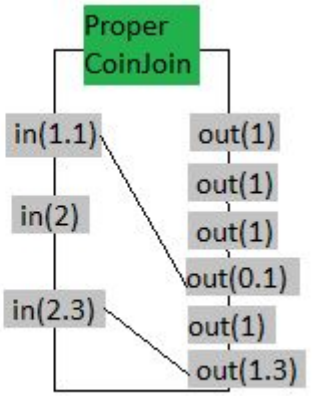
- Flagging von Coins aus CJ Transaktionen
- DoS Attacken durch blockierende Teilnehmer, Sybil
- Server zur Koordination verwendet, ohne blinding kann dieser IO zuordnen

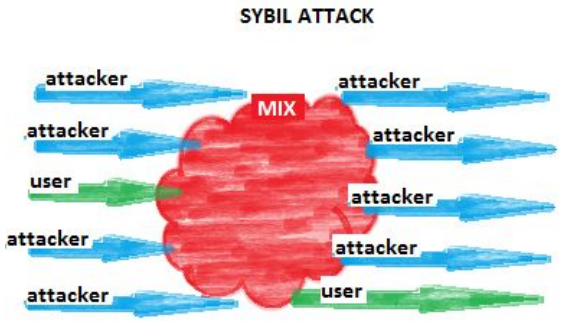




Hash (txid)	39f791a562f61a9ad19851429f92ffc45e a2ca18a799dea2738215427c5a30c0	
Block Id	573091	5861 confirmation
Time (UTC)	2019-04-24 22:28 (a month ago)	
Coindays destroyed	29.22	
Input count	96	
Output count	230	
Input total	41.54319767 BTC	230,432.00 USD
Output total	41.54289736 BTC	230,430.00 USD
Fee	0.00030031 BTC	1.67 USD







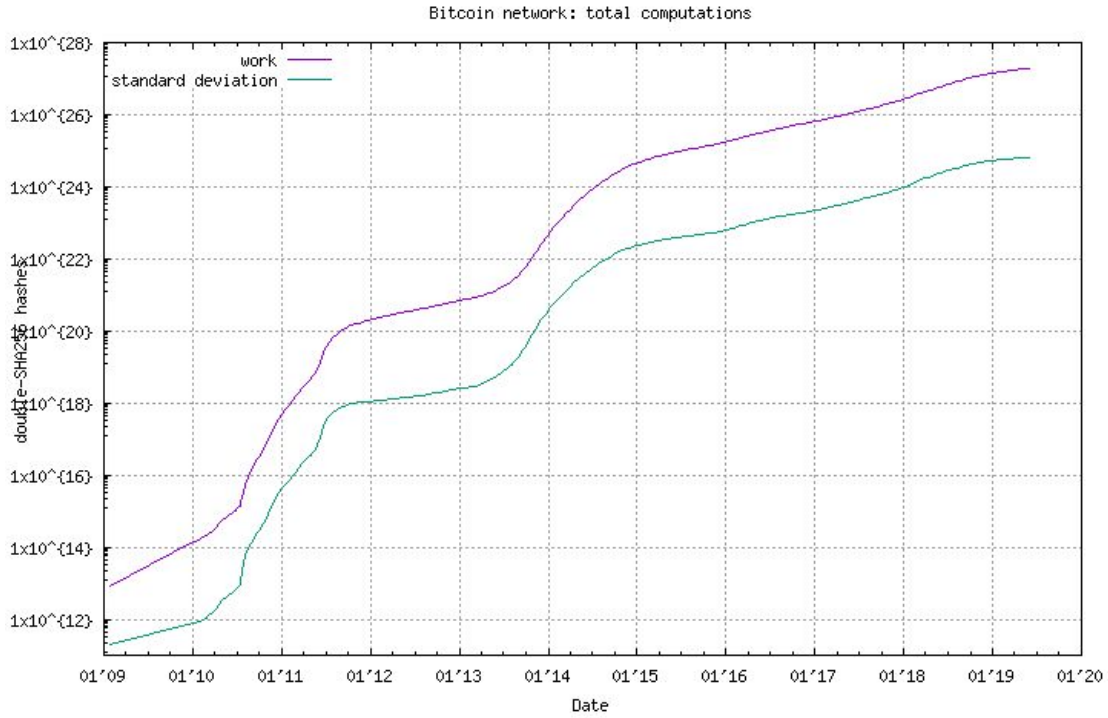
Implementation: z.B. Wasabi Wallet

Proof of Stake

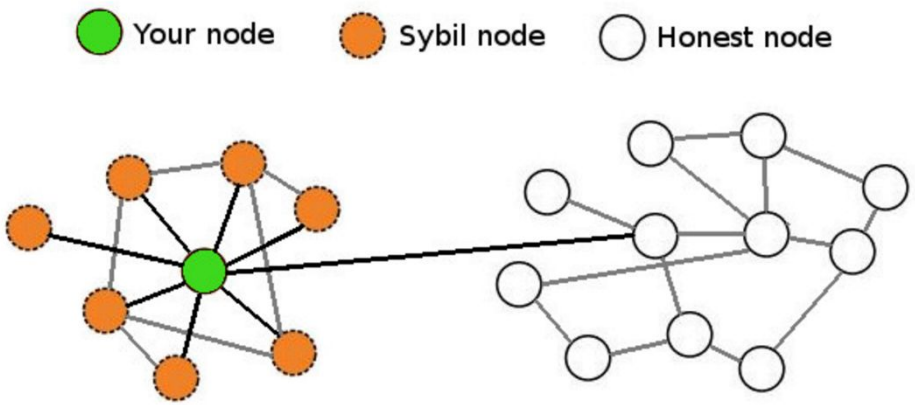
- Statt der Lösung eines mathematischen Problems darf derjenige mit dem höchsten Anteil (Stake) einen Block validieren
- PoS hat keinen mining reward sondern nur die Gebühren
- Wahrscheinlichkeit den Block zu validieren steigt mit dem Stake

Problem: „*The rich get richer*“

- Durch z.B. große Hacks von 3rd Party Seiten könnte ein Individuum in den Besitz einer großen Summe Coins kommen
- PoW hat mit den Minern und den verbrauchten Ressourcen also einen echten Gegenwert und finalisiert so Blöcke endgültig



http://bitcoin.sipa.be/



- „Echte“ Blockchain immer die mit dem meisten PoW

Damit ist Bitcoin thermodynamisch sicher!

- Sybil Angriffe schwierig, da ein einziges „Honest Node“ zum entlarven ausreicht!
- Neue Blockchain bräuchte momentan 10^28 Hashes!

Gliederung

Sektion 2 Angriffe auf das Bitcoin Netzwerk

- 51% Angriff
- Blacklisting
- Sybil Angriff
- Routing Angriff
- DoS Angriff

51% Angriff

Was ist ein 51% Angriff?

- Angriff auf den Konsens Mechanismus
- Basiert auf Mehrheit der Network Hashrate (>50%)

Was kann man damit erreichen?

- Erlaubt teilweise Kontrolle des Netzwerkes
  - 100% aller Block Rewards
  - Kontrolle über Transaktionen
  - Blacklisting

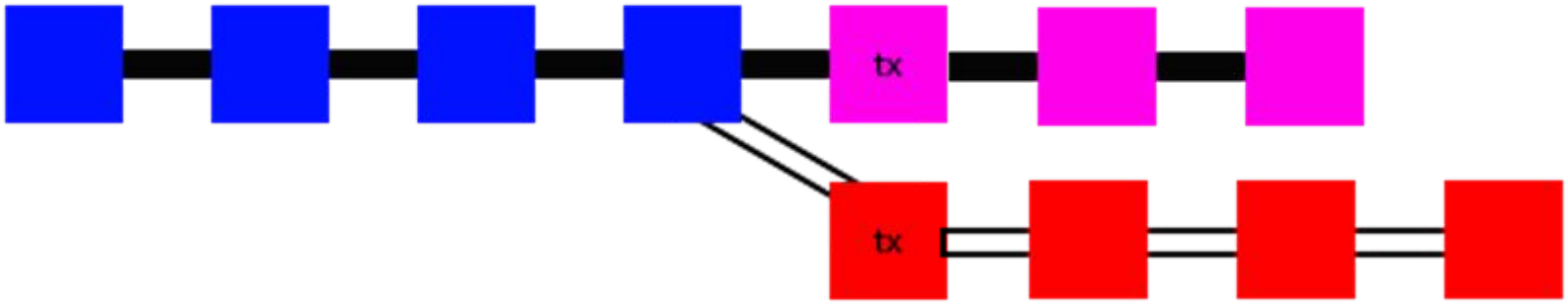
Double Spending

- Prinzipiell: Einen Bitcoin Betrag zweimal ausgeben
- Zahlungstransaktionen sind mit „0/unconfirmed“ anfangs geflaggt

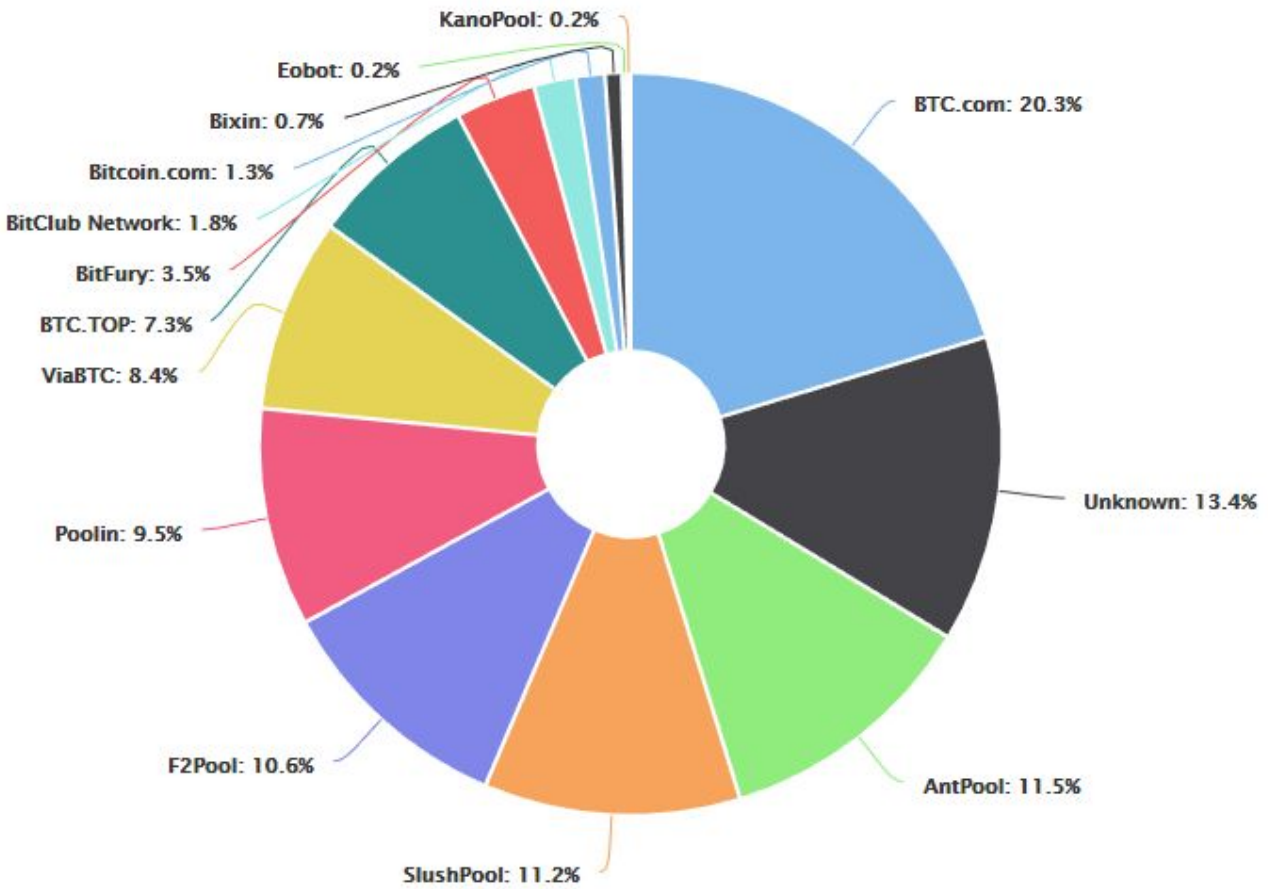
  Händler warten auf *n* Bestätigungen
- Mit >50% Network Hashrate erzeugt man immer die längste Kette

Double Spending

n = 2



Mining Pool Network Hashrate Anteil



- Größter Pool bei ungefähr 20%
- Geringe Chance auf erfolgreiche 51% Attacke alleine
- Gefahr auf Kollusion zwischen Pools besteht

Mietkosten eines 51% Angriffes

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$138.27 B	SHA-256	60,795 PH/s	*$697,275*	0%
Ethereum	ETH	$26.18 B	Ethash	149 TH/s	*$130,984*	5%
BitcoinCashABC	BCH	$7.25 B	SHA-256	2,740 PH/s	*$31,429*	2%
Litecoin	LTC	$6.47 B	Scrypt	390 TH/s	*$64,913*	3%
BitcoinSV	BSV	$4.09 B	SHA-256	1,487 PH/s	*$17,057*	4%
Monero	XMR	$1.47 B	CryptoNightR	308 MH/s	*$6,578*	6%
Dash	DASH	$1.29 B	X11	3 PH/s	*$8,628*	10%
EthereumClassic	ETC	$898.92 M	Ethash	9 TH/s	*$7,951*	90%
Zcash	ZEC	$526.12 M	Equihash	5 GH/s	*$25,102*	5%
BitcoinGold	BTG	$450.16 M	Zhash	4 MH/s	*$1,808*	51%
Ravencoin	RVN	$233.72 M	X16R	12 TH/s	*$18,800*	10%
Monacoin	MONA	$204.98 M	Lyra2REv2	23 TH/s	*$2,374*	60%
Bytecoin	BCN	$170.10 M	CryptoNight	491 MH/s	$82	136%
Verge-Blake (2s)	XVG	$141.55 M	Blake (2s)	370 TH/s	*$48*	14%
Aeternity	AE	$132.51 M	CuckooCycle	586 KH/s	*$1,903*	0%
Sia	SC	$127.37 M	Sia	3 PH/s	*$1*	0%

Blacklisting

Punitive Forking

- Erfordert >50% Network Hashrate
- Marc soll keine Transaktionen mehr machen können
  - Umgehe alle Nodes mit Transaktionen von Marc
  - Akzeptiere selber keine Transaktionen von Marc
- Man kündigt seine Strategie an
- Restlichen Miner (<49%) werden folgen

Blacklisting

Feather Forking

- Spieltheoretischer Ansatz
- Man gebe seine Strategie vorher bekannt
- q sei der Anteil an der Netzwerk Hashrate, $0 < q < 1$
- $k = 1$ sei die Anzahl der Bestätigungen nach der man aufgibt den Block zu umgehen

  ➢ Chance den Block zu umgehen beträgt q^2

Blacklisting

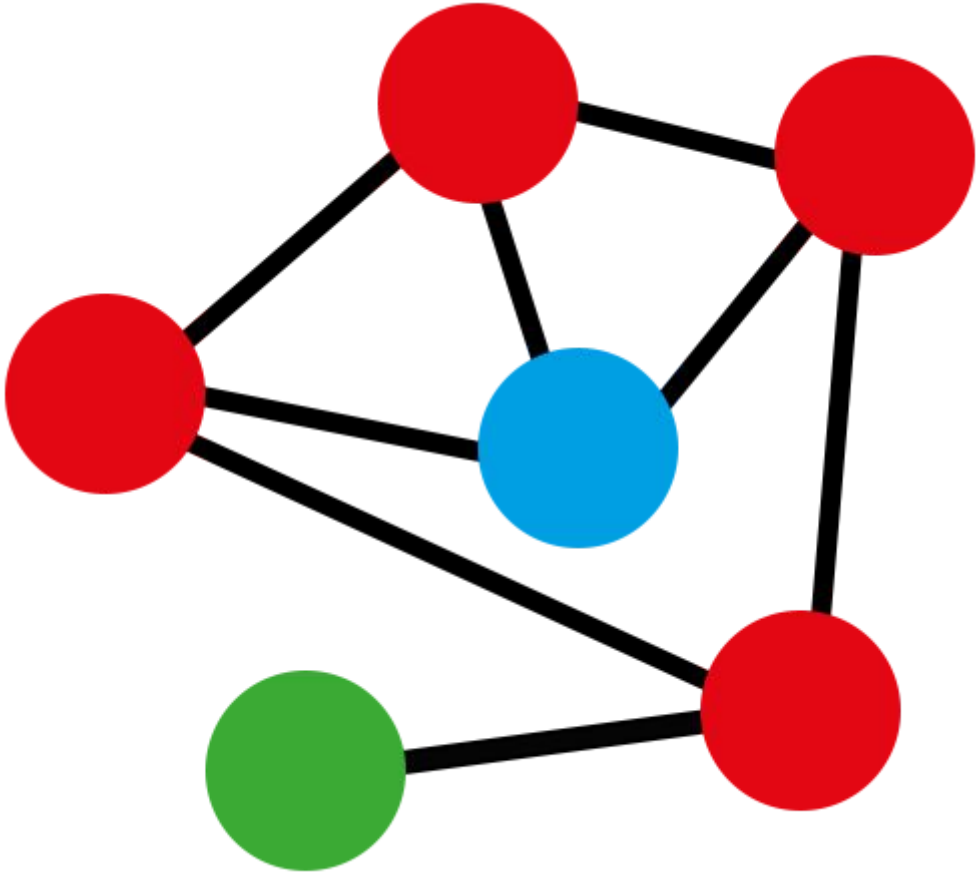
- Mining Pool mit 20% Anteil, $q = 0.2$

$$E(include) = (1 - q^2) * BlockReward * Marc's\ tx\ Gebuehr$$

$$E(don't\ include) = BlockReward$$

- Marc müsste $BlockReward * q^2$ an Transaktionsgebühren zahlen
  - $0{,}04 * 12{,}5\ BTC = 0{,}5\ BTC \simeq 3410\$$

Sybil Angriff



- Angriff auf ein Peer-to-Peer Netzwerk
  - Falsche Identitäten (Nodes)

Möglichkeiten

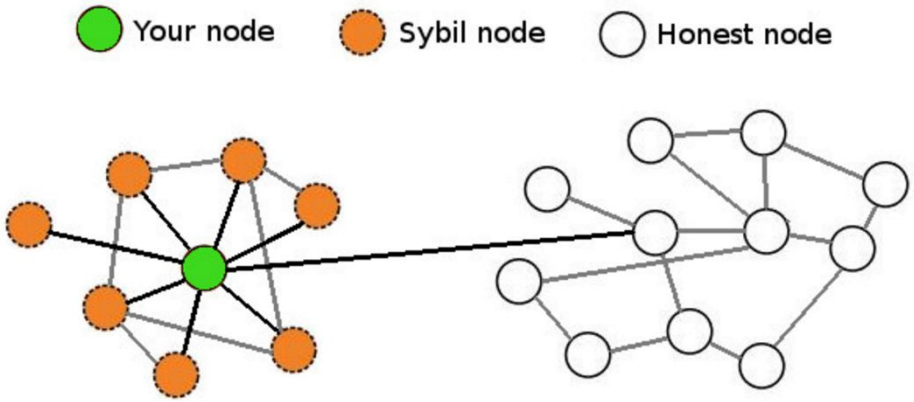
- Informationen nicht weiterleiten
  - Netzwerk getrennt
- Falsche Informationen weiterleiten

Sybil Angriff

- Kosten um eine Identität zu erstellen erschweren den Prozess

 Proof of Work => Rechenleistung

- Eine Verbindung zu einer “Honest Node” reicht um Angriff zu entlarven



Routing Angriff

- „Zentralisierte Host Netzwerke“

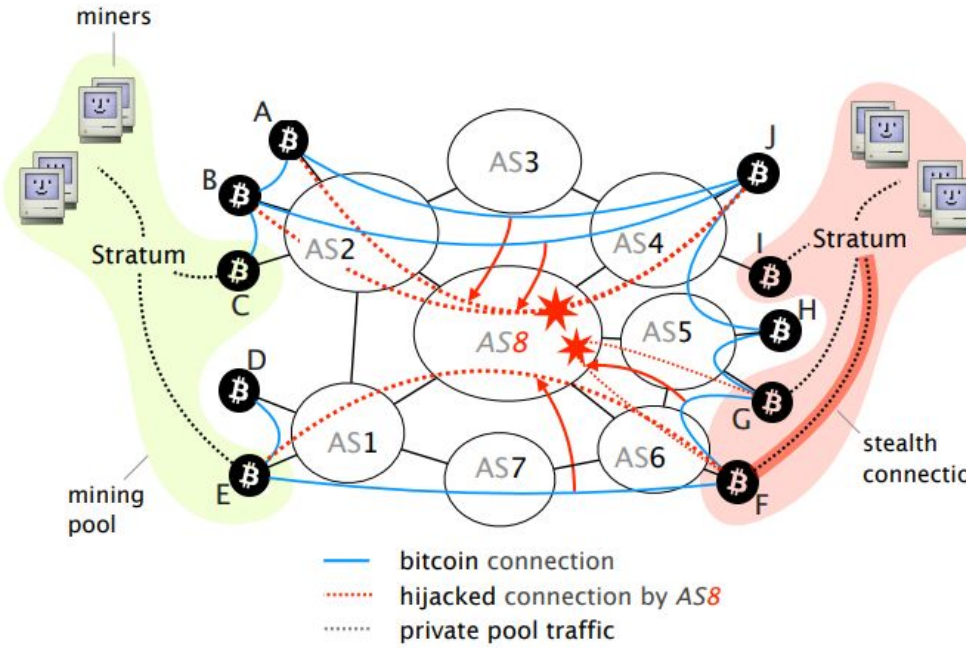
 13 ISPs hosten 30% des gesamten Bitcoin Netzwerkes

 60% der Bitcoin Verbindungen gehen über nur 3 ISPs

- Möglichkeit für infizierte bzw. bösartige ISPs den Bitcoin Verkehr zu beeinflussen, die über den jeweiligen Knoten gehen

Routing Angriff Szenario

- Angreifer teilt das Netzwerk
  - Zwei oder mehr Teile
- Zieht Verkehr zwischen den Teilen an
  - z.B. BGP Hijacking
- Leitet diesen jedoch nicht weiter
- Zwei parallele Blockchains entstehen
  - Am Ende des Angriffs wird die kürzere verworfen



DoS Angriff

- Denial of Service Angriff
- „Angriff auf die Verfügbarkeit eines Dienstes“
  - Verlangsamung
  - Vollständige Verhinderung des Zugriffs
- Sehr viele verschiedene Varianten
- Satoshi Client beinhaltet eine Vielzahl an Abwehrmechanismen gegen DoS Angriffe

DoS Angriff

Transaction DoS

- Spezial angefertigte Transaction
- scriptPub verwendet 200x OP_CHECKSIG & OP_TRUE
- Transaktion hat eine Größe von 955 Kbytes
- 200x 955 Kbytes hashen => >3 Minuten Rechenzeit
- Seit Satoshi Client Version 0.8.0 nicht mehr möglich

DoS Angriff

- Flooding schwierig aufgrund von Transaktionsgebühren
- Möglichkeit für anspruchsvolle Angriffe besteht

- Generell eher gegen Online Wallets und Exchange Services in Form eines DDoS

  Wirtschaftlicher Schaden

Vielen Dank für Ihre Aufmerksamkeit!

Sie können jetzt gerne Fragen zum Vortrag stellen