Angriffe auf Bitcoin

Routing, Bribery und Selfish-Mining

Robin Meis
robin.meis@rwth-aachen.de

21.07.2018

„Bitcoin seems to be a very promising idea. I like the idea of basing security on the assumption that the CPU power of honest participants outweighs that of the attacker. [...] “

Hal Finney

Ziel

$$CPUPower > 50\%$$

Double-Spending Angriff

Doppeltes Versenden der selben Bitcoins an zwei unterschiedliche Empfänger

Warum?

Finanzielle Interessen Einzelner

Staatliche Regulierung

- Kontrolle
- Spekulation
- Geldwäsche
- Umweltschutz
- $\rightarrow$ Schwächung von Vertrauen

Angriffe

Routing

Bribery

Selfish-Mining

DNS

Angriffe auf Netzwerkebene

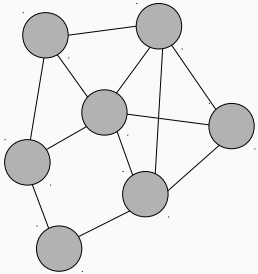
Initialer Verbindungsaufbau

Seed Domains

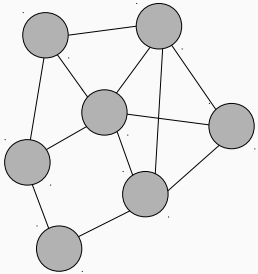
Einkompilierte IP Adressen

Danach Anfragen an Nodes

DNS

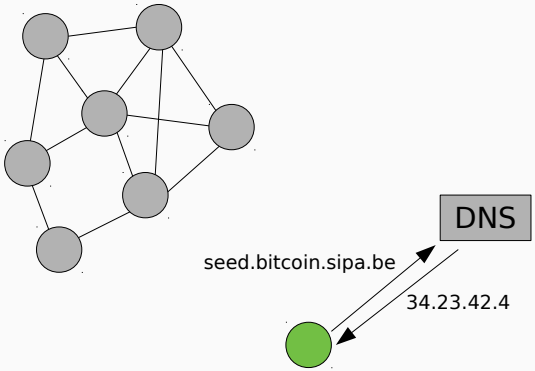


DNS

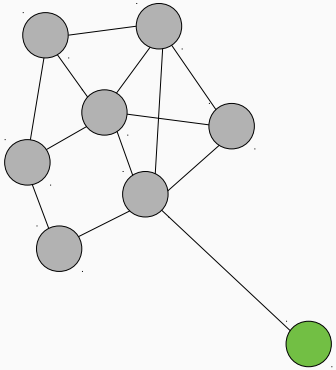


DNS

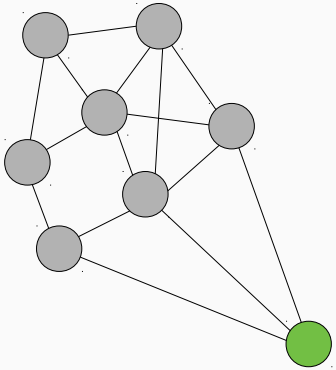
DNS



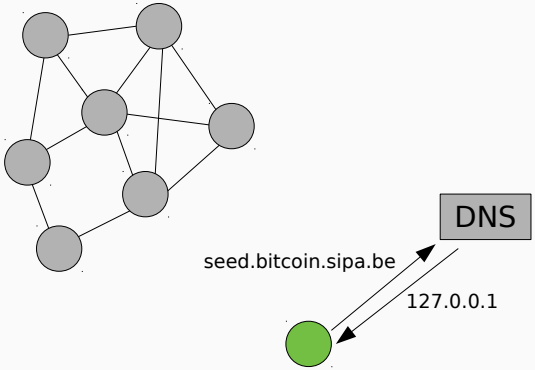
DNS



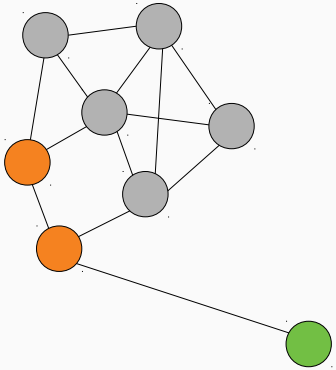
DNS



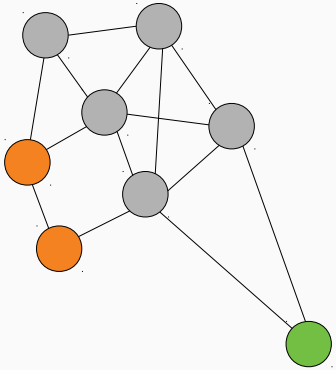
DNS



Statische Nodes



Statische Nodes



Routing

Angriffe auf Netzwerkebene

CIDR

Beschreibt IP Adressbereiche

CIDR 137.226.155.0/27

CIDR

Beschreibt IP Adressbereiche

CIDR 137.226.155.0/27

Präfix 137.226.155.0

CIDR

Beschreibt IP Adressbereiche

CIDR 137.226.155.0/27

Präfix 137.226.155.0

Netzmaske 27 $\equiv$ 32 (30) Adressen

Autonome Systeme

Einzelne Netzwerke des Internets

Kommunikation innerhalb eines autonomen Systems

Austausch von Daten über Router

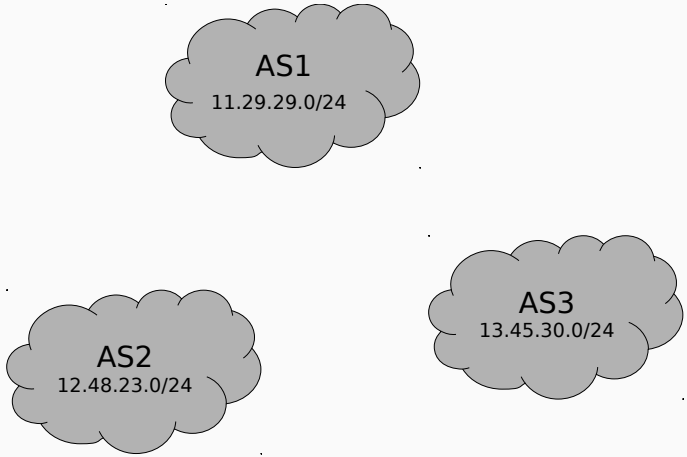
BGP

Border **G**ateway **P**rotocol

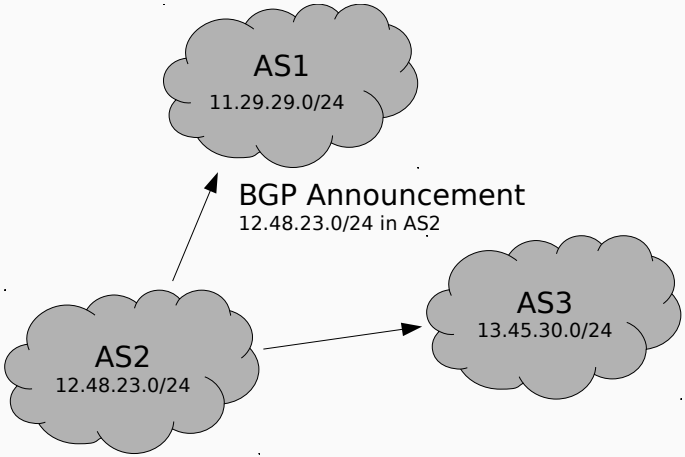
Legt Routen zwischen autonomen Systemen an (Announcements)

BGP Hijacking ermöglicht anlegen unberechtigter Pfade

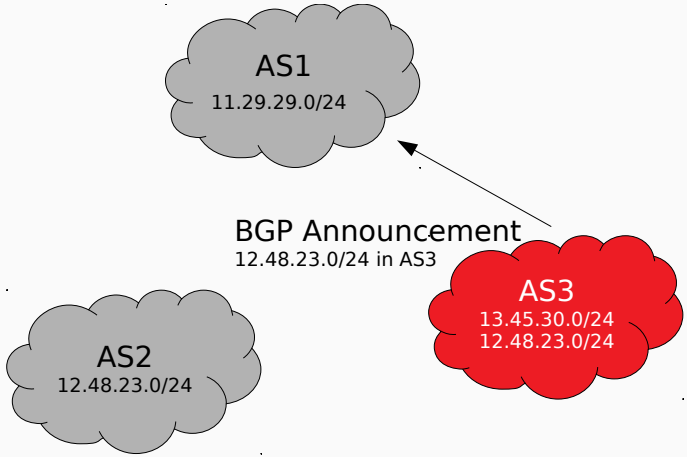
BGP



BGP


AS1
11.29.29.0/24
BGP Announcement
12.48.23.0/24 in AS2
AS3
13.45.30.0/24
AS2
12.48.23.0/24

BGP Hijacking



Angriffe mittels BGP

- Aktive Angriffe
  - Veränderung von Routen
  - Umleitung von Verkehr für ein Subnetz
  - Betreiber des AS kann Daten verändern oder verwerfen

Angriffe mittels BGP

- Aktive Angriffe
  - Veränderung von Routen
  - Umleitung von Verkehr für ein Subnetz
  - Betreiber des AS kann Daten verändern oder verwerfen
- Passive Angriffe
  - Routen bleiben unverändert
  - Angriff auf über ein AS weitergeleitete Daten

Angriffe mittels BGP

- Aktive Angriffe
  - Veränderung von Routen
  - Umleitung von Verkehr für ein Subnetz
  - Betreiber des AS kann Daten verändern oder verwerfen
- Passive Angriffe
  - Routen bleiben unverändert
  - Angriff auf über ein AS weitergeleitete Daten
- Hybride Angriffe
  - Kombination beider Angriffe
  - Datenmenge wird gesteigert

Verbindung zwischen Bitcoin Nodes

Unverschlüsselte TCP Verbindungen

Verbindung zu mindestens 8 Nodes in unterschiedlichen /16 Netzen

Maximal 125 Verbindungen

Angriff: Teilung des Bitcoin Netzwerks

Blockade von Datenströmen ermöglicht Teilung

$\rightarrow$ Zwei verschiedene Partitionen

Transaktionen werden blockiert

Ermöglicht Double Spending Angriffe

Angriff: Verzögerung der Datenströme

Austausch zwischen Nodes wird verzögert

Maximal 20 Minuten

Miner arbeiten weiterhin an bereits gefundenen Blöcken

Zentralisierung

P2P Netzwerk gilt als dezentralisiert

30% der Clients in 13 autonomen Systemen

50% der Clients in 50 autonomen Systemen

900 Präfixe sind ausreichend zur Übernahme von 50%

$\rightarrow$ Aus Routing Sicht stark zentralisiert

Bribery

Kaufen von Rechenleistung

Mieten von Miningkapazität

Dienstleister vermieten Miner

Anonymitätsproblem

Vertrauensproblem

Negative Gebühren in Pools

Pool bietet negative Gebühren

Anziehungswirkung auf Miner

Vertrauen wird stückweise aufgebaut

Angriff leicht erkennbar

Langsames Poolwachstum

Selfish Mining

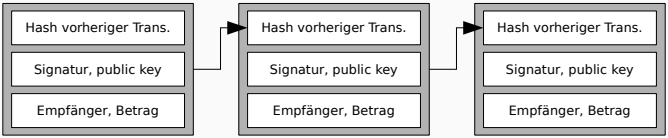
Verschwenden von Rechenleistung

Grundlagen

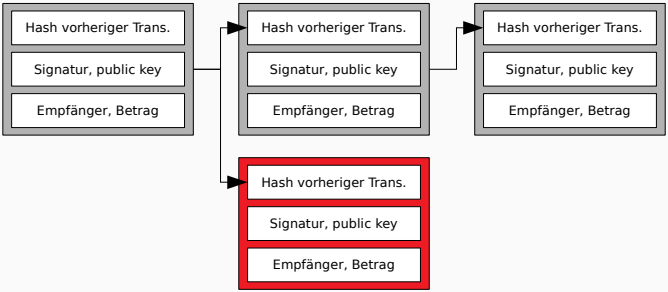
Pool mit ausreichender Größe

Pool kann kleiner als 50% sein

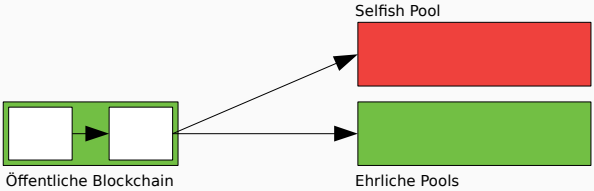
Aufbau der Blockchain



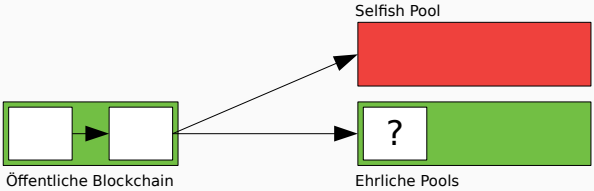
Fork


Hash vorheriger Trans.
Signatur, public key
Empfänger, Betrag
Hash vorheriger Trans.
Signatur, public key
Empfänger, Betrag
Hash vorheriger Trans.
Signatur, public key
Empfänger, Betrag
Hash vorheriger Trans.
Signatur, public key
Empfänger, Betrag

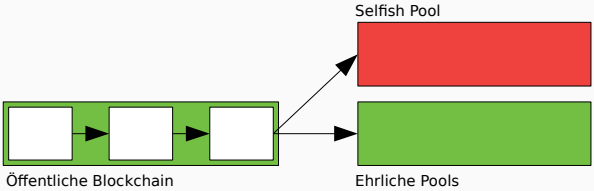
Ehrliche Miner



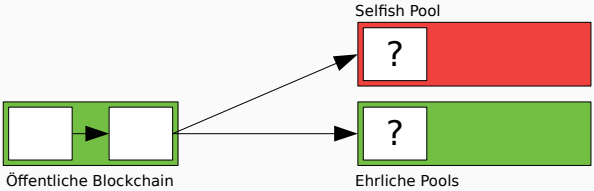
Ehrliche Miner



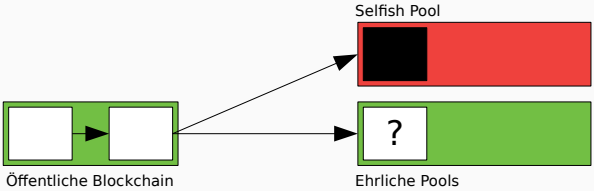
Ehrliche Miner



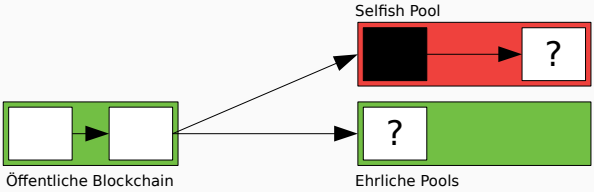
Selfish Mining (1)



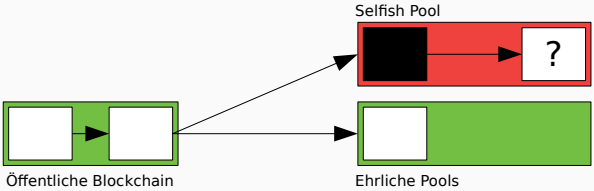
Selfish Mining (1)



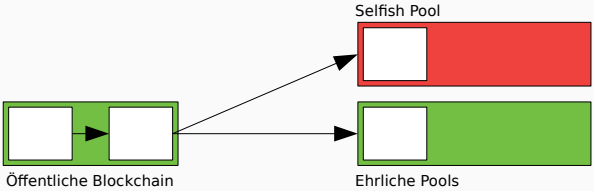
Selfish Mining (1)



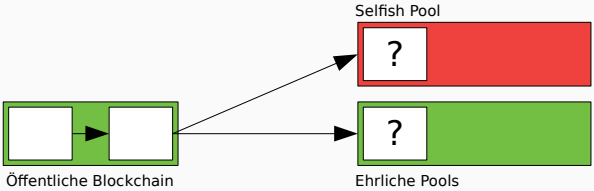
Selfish Mining (1)



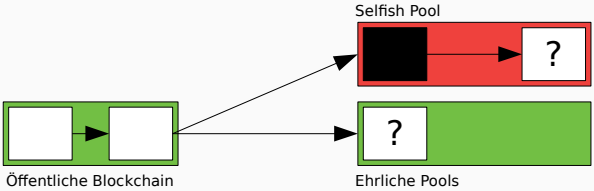
Selfish Mining (1)



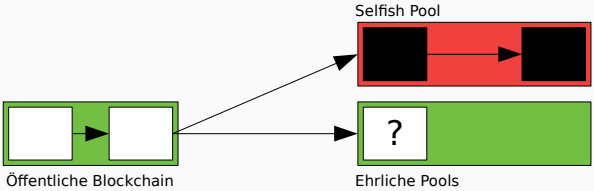
Selfish Mining (2)



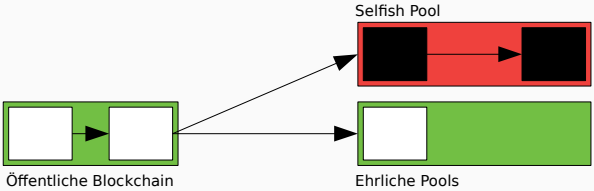
Selfish Mining (2)



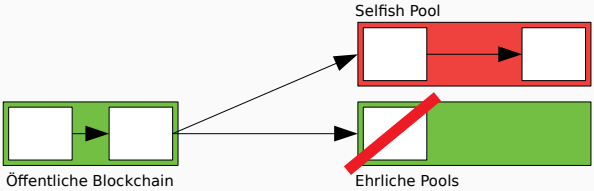
Selfish Mining (2)



Selfish Mining (2)



Selfish Mining (2)



Folgen

Ehrliche Miner verlieren Ertrag

Rechenleistung und Energie werden verschwendet

Kombination aller Angriffe

Einrichtung eines Pools

Negative Gebühren ziehen Miner an

Kombination aller Angriffe

Einrichtung eines Pools

Negative Gebühren ziehen Miner an

Verringerung der Mining Leistung

- Partitionierung durch BGP Hijacking
- Selfish Mining

Updates

Sicherheitslücken schließen

Softfork

Kompatibilität zwischen alten und neuen Versionen

Gültigkeit neuer Blöcke wird durch neue Kriterien festgelegt

Bestehende Nodes erkennen neue Blöcke als gültig

Alte Blöcke behalten Gültigkeit

Hardfork

Ehemals ungültige Blöcke werden gültig

Veraltete Software kann nicht länger am Netzwerk teilnehmen

Demokratie

Updates können verhindert werden

Updates müssen von mindestens 50% der Miner akzeptiert weden

Veraltete Miner gefährden Sicherheit

Folgen erfolgreicher Angriffe

Fallende Kurse

Finanzielle Verluste

Vertrauensverlust

Fazit

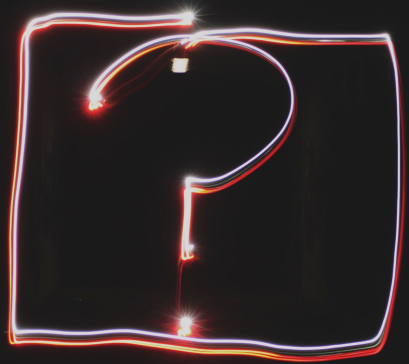
Übernahme von 50% möglich

Finanzielles Risiko als Abschreckung

Staatliche Einflussnahme möglich

Stärkung der Sicherheit ist kontinuierlicher Prozess

https://unsplash.com/photos/8xAA0f9yQnE



Fragen

Quellen I

Bitcoin Wechselkurs.
https://www.finanzen.net/devisen/bitcoin-euro-kurs.
[Online; abgerufen 09.07.2018].

EU-Kommission will Bitcoin-Regulierung vorantreiben.
http://www.spiegel.de/wirtschaft/unternehmen/krytowaehrungen-eu-kommission-will-bitcoin-regulierung-vorantreiben-a-1195484.html.
[Online; abgerufen 05.07.2018].

Hardfork.
https://en.bitcoin.it/wiki/Hardfork.
[Online; abgerufen 07.06.2018].

Quellen II

Re: Bitcoin P2P e-cash paper.
https://www.mail-archive.com/cryptography@metzdowd.com/msg09975.html.
[Online; abgerufen 25.06.2018].

Satoshi Client Node Discovery.
https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery.
[Online; abgerufen 03.06.2018].

Seed domains.
https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp#L132.
[Online; abgerufen 03.06.2018].

Quellen III

Softfork.
`https://en.bitcoin.it/wiki/Softfork`.
[Online; abgerufen 07.06.2018].

Apostolaki, M., Zohar, A., and Vanbever, L. (2016).
Hijacking bitcoin: Large-scale network attacks on cryptocurrencies.
CoRR, abs/1605.07524.

Bonneau, J. (2016).
Why buy when you can rent?
In Clark, J., Meiklejohn, S., Ryan, P. Y., Wallach, D., Brenner, M., and Rohloff, K., editors, *Financial Cryptography and Data Security*, pages 19–26, Berlin, Heidelberg. Springer Berlin Heidelberg.

Quellen IV

Eyal, I. and Sirer, E. G. (2014).
Majority is not enough: Bitcoin mining is vulnerable.
In Christin, N. and Safavi-Naini, R., editors, *Financial Cryptography and Data Security*, pages 436–454, Berlin, Heidelberg. Springer Berlin Heidelberg.

Huitema, C. (2000).
Routing in the Internet.
Prentice-Hall.

Liu, C. and Albitz, P. (2006).
DNS and Bind.
O'Reilly Media, Inc.

Quellen V

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016).

Bitcoin and cryptocurrency technologies: a comprehensive introduction.

Princeton University Press.

Zhang, R. and Preneel, B. (2017).

Publish or perish: A backward-compatible defense against selfish mining in bitcoin.

In *Cryptographers' Track at the RSA Conference*, pages 277–292. Springer.