routing attacks on Bitcoin

Péter Garamvölgyi

outline

- **background**
- partitioning attack
- delay attack
- evaluation
- countermeasures

routing in the Internet

- routing

  *"routing is the process of selecting a path for traffic in a network, or between or across multiple networks." **

- Autonomous System (AS)

  *"an Autonomous System (AS) is a collection of routers whose prefixes and routing policies are under common administrative control." ***

  ➡ one or more IP prefixes (e.g. 128.6.0.0/16)

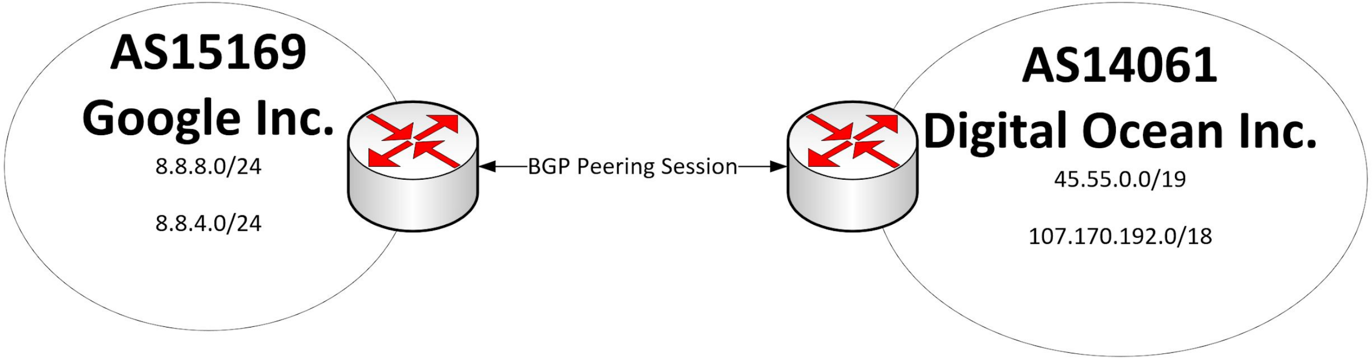
* https://en.wikipedia.org/wiki/Routing
** https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html

routing in the Internet

- intra-AS / IGP (Interior Gateway Protocols)
    - OSPF (Open Shortest Path First)
    - RIP (Routing Information Protocol)
- inter-AS / EGP (Exterior Gateway Protocols):
    - **BGP (Border Gateway Protocol)**

what is BGP?

- network operators establish peers over TCP connections
- routers advertise a list of network routes they have access to
- choose from alternatives based on shortest path
- preference for more specific routes



https://blog.cdemi.io/beginners-guide-to-understanding-bgp

BGP hijacking

- ASes may announce IP ranges they do not own

  e.g. AS wants to attract traffic sent to 100.0.0.0/16

  (a) announce 100.0.0.0/16

  (b) announce a more specific range, e.g. 100.0.0.0/17, 100.0.128.0/17

  announcements more specific than /24 are usually dropped

- BGP is based on trust
- censorship, Man-in-the-Middle interception, black holes
- Pakistan's attempt to block YouTube access takes down YouTube entirely (2008)

the Bitcoin p2p protocol

- p2p broadcast/gossip network
- TCP with default port 8333
- no encryption or integrity checks
- 8 outgoing, up to 125 incoming connections by default

the Bitcoin p2p protocol

- block / transaction propagation
  - ➡ INV — "I have these blocks/transactions: …"
  - ➡ GETDATA — request a single block or transaction by hash
  - ➡ BLOCK — send a block in response to GETDATA
- by default, nodes request block from sender of first INV containing its hash
- nodes wait for 20 minutes after GETDATA before retrying

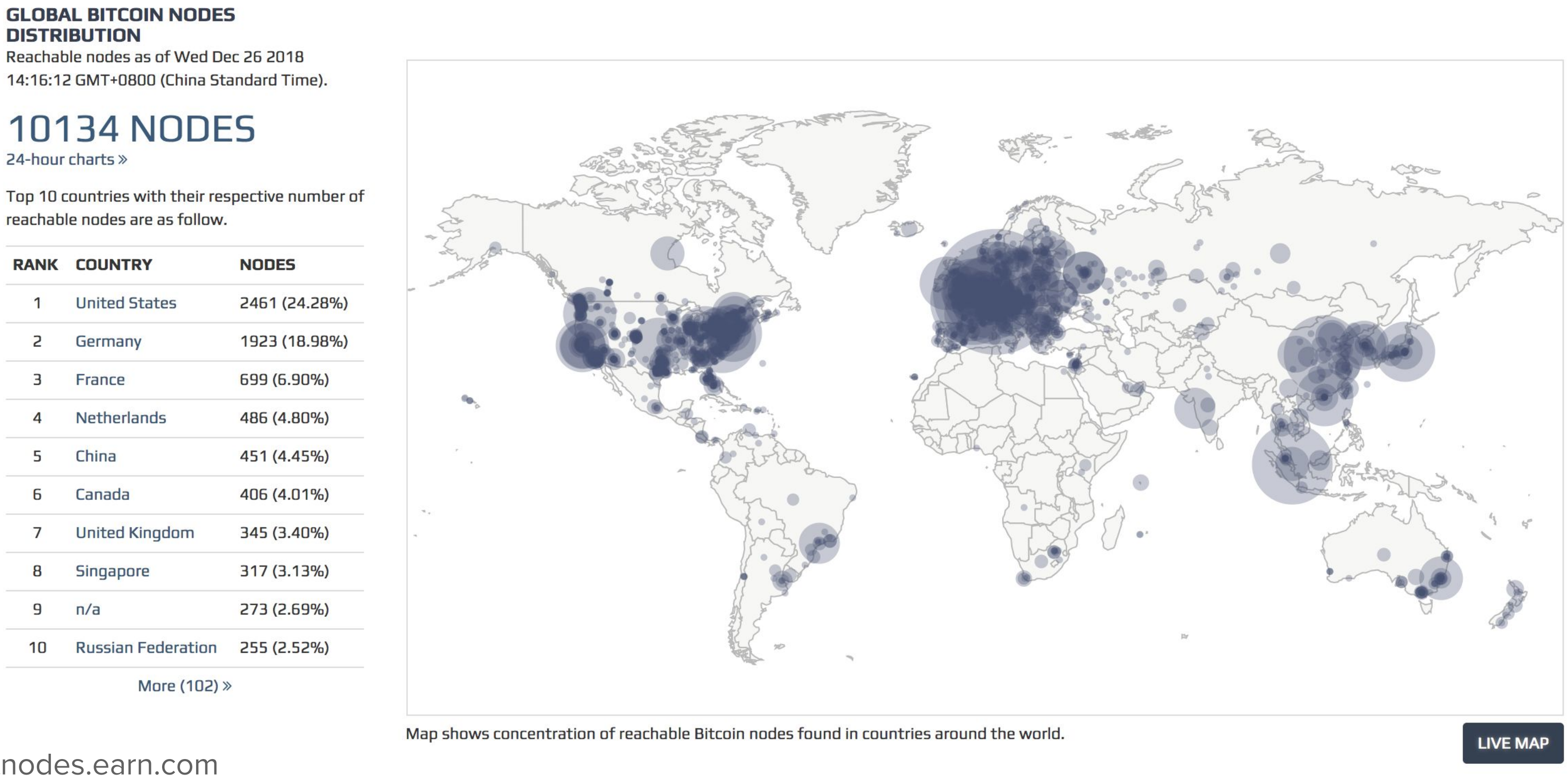
https://en.bitcoin.it/wiki/Protocol_documentation

the Bitcoin p2p protocol

- bootstrapping
  - ➡ manually provide address (command line, database, etc.)
  - ➡ ADDR message
  - ➡ DNS (seed.bitcoin.sipa.be, dnsseed.bluematt.me, seed.bitcoinstats.com, ...)
  - ➡ hardcoded default addresses / hostnames

https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery

Bitcoin network statistics



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Dec 26 2018 14:16:12 GMT+0800 (China Standard Time).

10134 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2461 (24.28%)
2	Germany	1923 (18.98%)
3	France	699 (6.90%)
4	Netherlands	486 (4.80%)
5	China	451 (4.45%)
6	Canada	406 (4.01%)
7	United Kingdom	345 (3.40%)
8	Singapore	317 (3.13%)
9	n/a	273 (2.69%)
10	Russian Federation	255 (2.52%)

More (102) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

https://bitnodes.earn.com

mining pools

- lower risk by increasing reward frequency
- Stratum protocol: JSON-RPC over TCP *
- multi-homing: multiple gateways to the network at multiple ISPs
- manager creates block template, miners find PoW for header
- inter-pool peering agreements

* https://slushpool.com/help/manual/stratum-protocol

outline

- background
- **partitioning attack**
- delay attack
- evaluation
- countermeasures

partitioning attack - overview

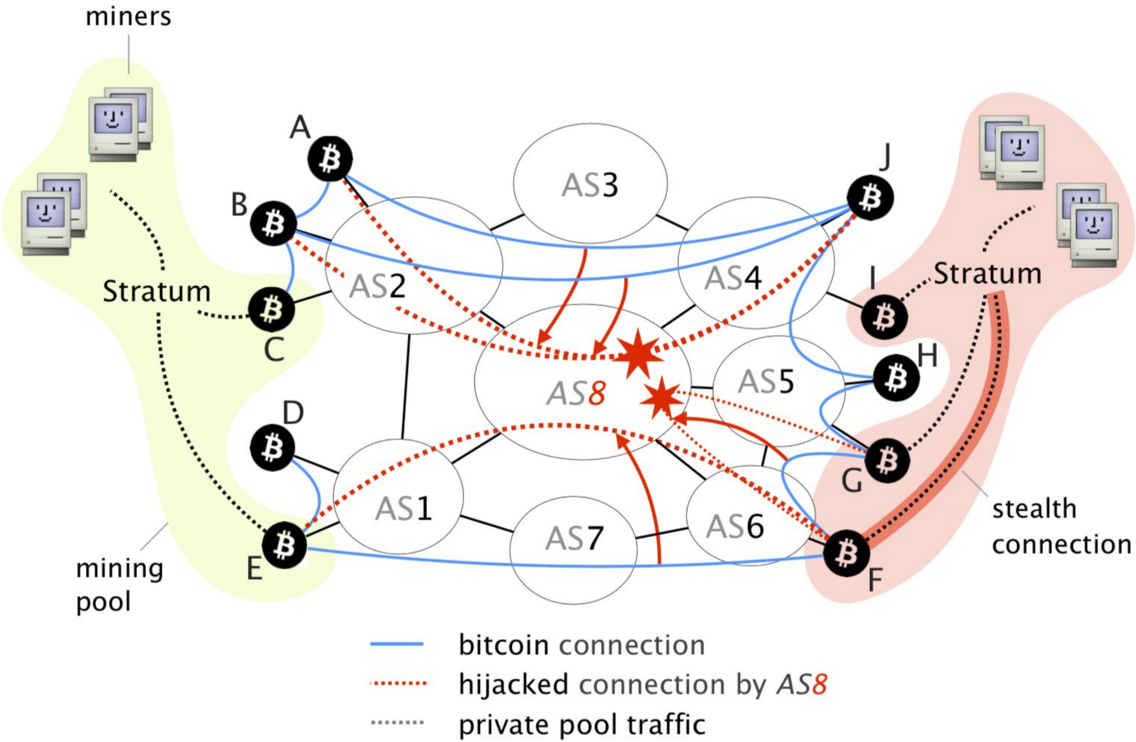
- AS-level adversary wants to isolate a set of nodes P from the rest of the network
  1. divert traffic destined to P
  2. identify relevant traffic
  3. drop packets crossing partition boundary
  4. isolate leaking nodes

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

partitioning attack - overview

P = {A, B, C, D, E, **F**}

1. divert traffic
2. drop packets
3. isolate leaks



Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

attack steps

1. divert traffic destined to P
    - ➜ BGP hijack, announce more specific prefixes
2. identify relevant traffic
    - ➜ TCP:8333, specific IP addresses, Bitcoin header (unencrypted!)
3. drop packets crossing partition boundary
4. isolate leaking nodes
    - ➜ this is the main challenge

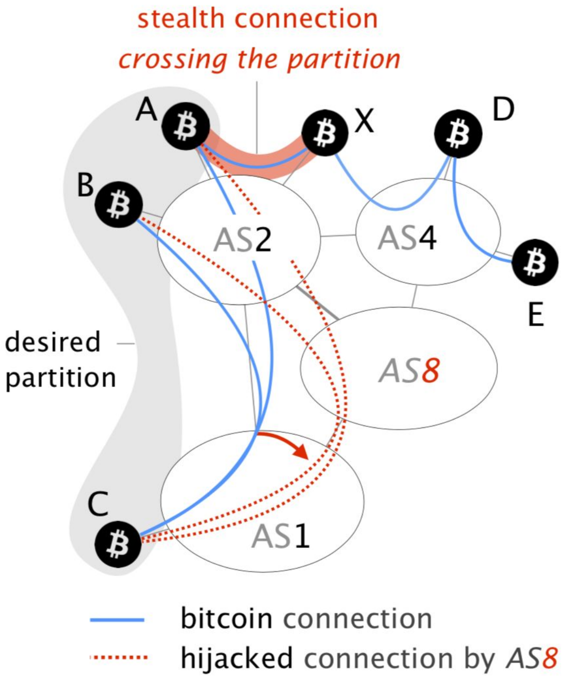
Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

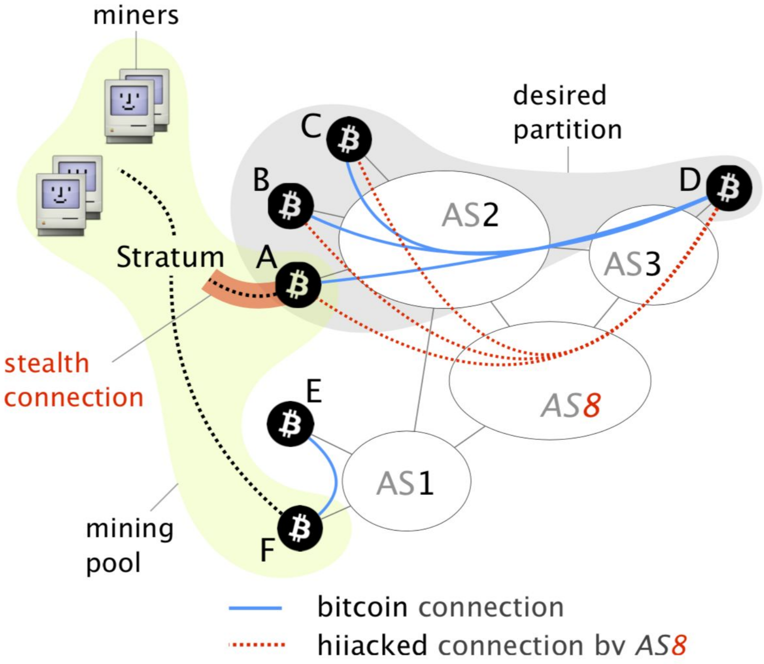
isolating leaks - connection types

- vulnerable connection
  - ➜ can divert via BGP hijack
  - ➜ uses Bitcoin protocol
- stealth connection
  - ➜ intra-AS: cannot do BGP hijack
  - ➜ intra-pool: unique/encrypted protocol
  - ➜ pool-to-pool

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

isolating leaks - connection types





Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

isolating leaks

1. include all or none of the nodes within the same AS

2. include all or none of the nodes within the same pool

3. **find and exclude leaking nodes**

    - inspect INV messages from nodes within P

    - if they advertise blocks mined outside P, they must have a stealth connection

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

partitioning attack - impact

a. targeted attack
   - ➜ Denial-of-Service
   - ➜ double spending

b. network-wide attack
   - ➜ fork => reduced mining power on both sides
   - ➜ all blocks mined on weaker side will be discarded after the attack
   - ➜ revenue loss for miners, risk of double spend

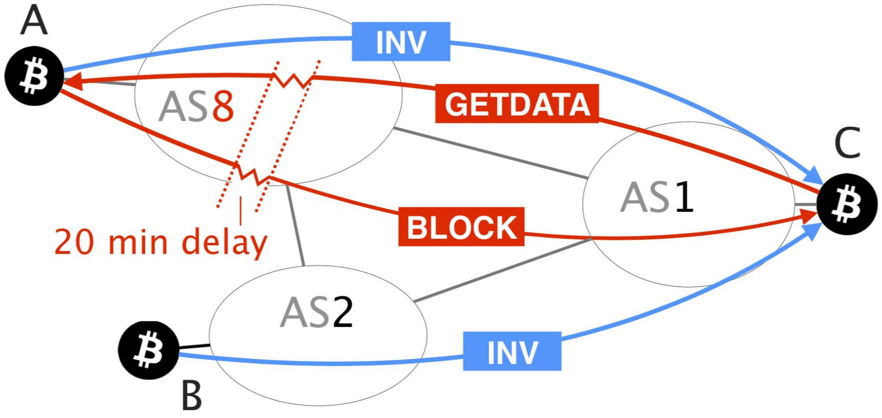
Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

outline

- background
- partitioning attack
- **delay attack**
- evaluation
- countermeasures

delay attack - overview

- slow down block propagation
- tamper with traffic in a way that
  1. prevents node from receiving correct information
  2. but keeps connection alive



Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

delay attack - overview

a. intercept outgoing connection (block #42)

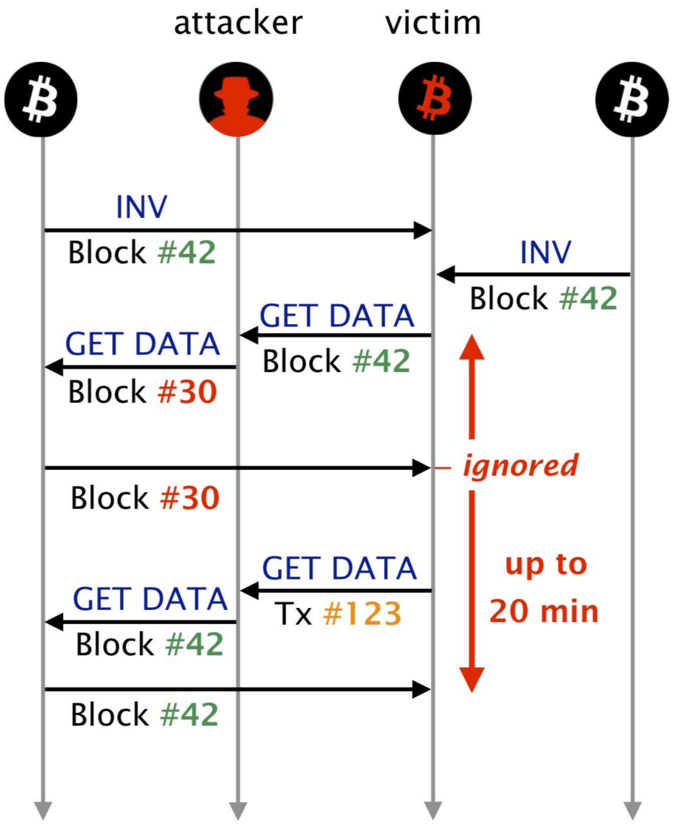
→ change block hash in GETDATA to #30

→ victim gets wrong block (#30); keeps waiting

→ change another GETDATA to #42 this time

→ victim gets #42 with a large delay

- why not just drop?
- why change the second time?

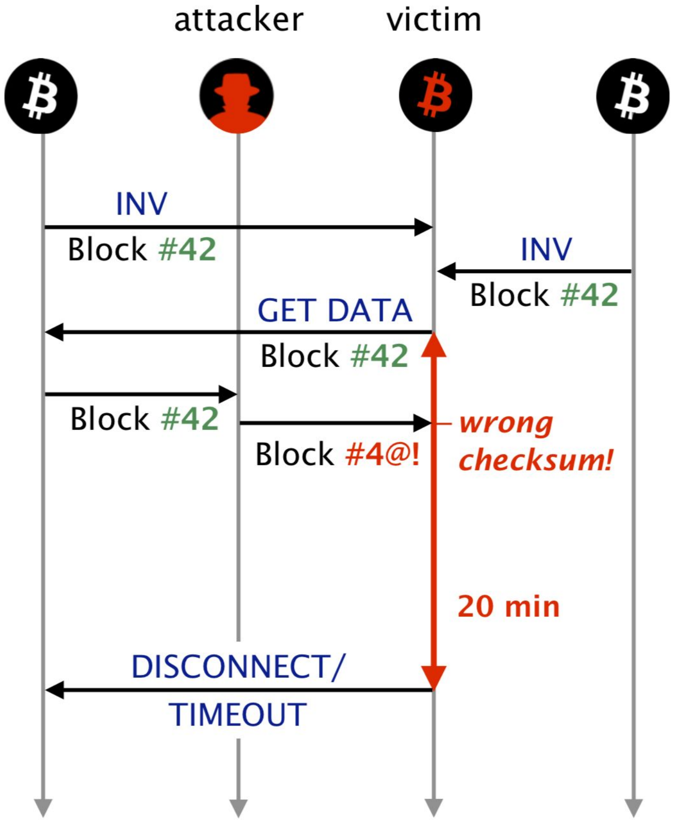


Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

delay attack - overview

a. intercept incoming connection

- ➡ change data in BLOCK
- ➡ victim drops it; keeps waiting
- ➡ timeout after 20 minutes

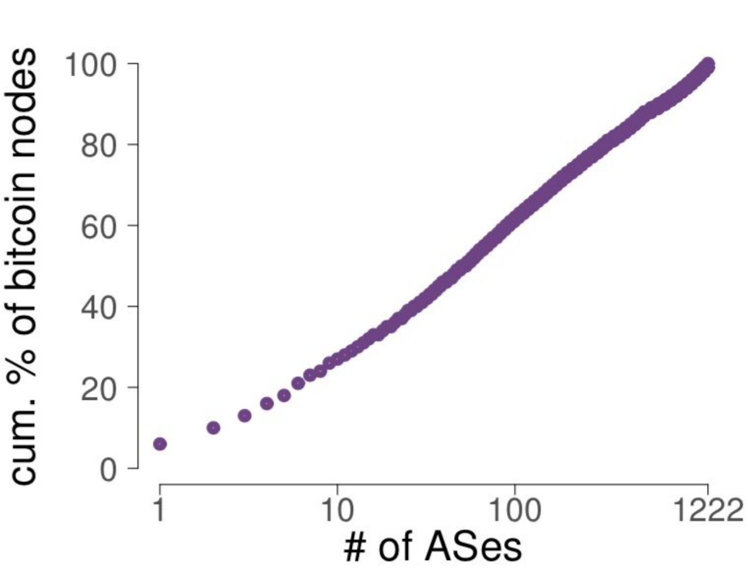


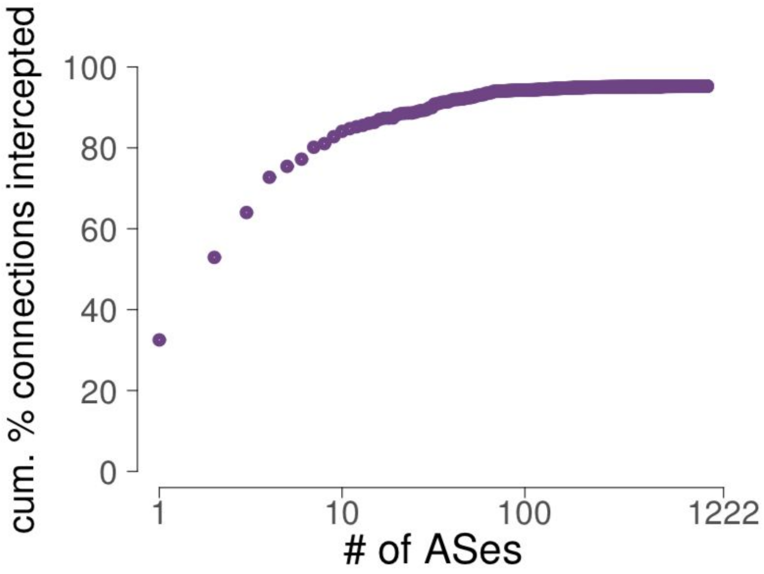
Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

outline

- background
- partitioning attack
- delay attack
- **evaluation**
- countermeasures

network topology





Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

network topology

- a few ASes host most Bitcoin nodes
- a few ASes intercept the majority of Bitcoin traffic
- most Bitcoin nodes are susceptible to BGP hijacks
- mining pools are distributed and multi-homed (2-5)
- Bitcoin routing properties are stable over time

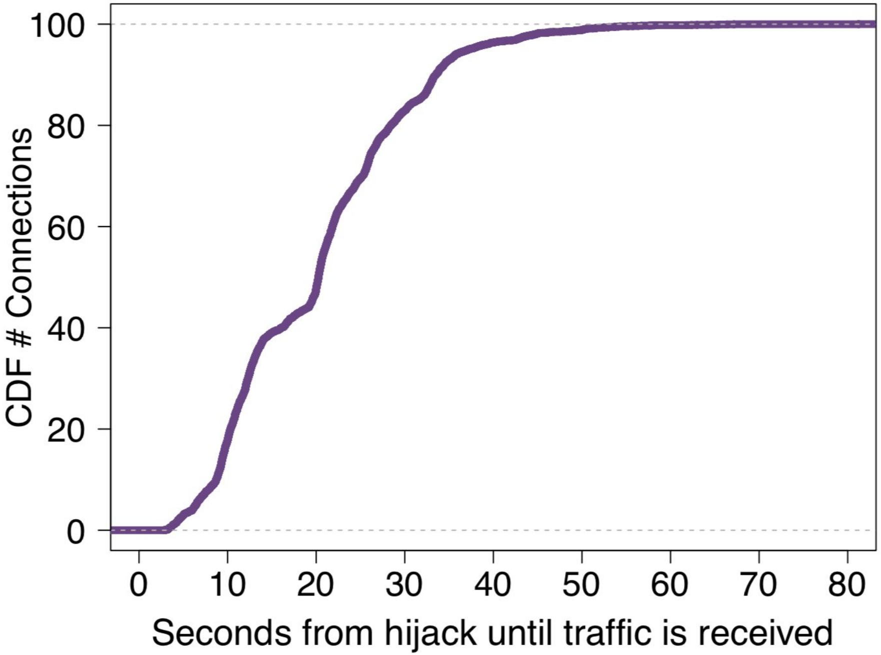
Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

partitioning - speed

- host six Bitcoin nodes under 184.164.232.0/22
- advertise 184.164.232.0/22 using a virtual AS
- advertise 184.164.235.0/24 via another (malicious) virtual AS
- divert all traffic within 90 seconds

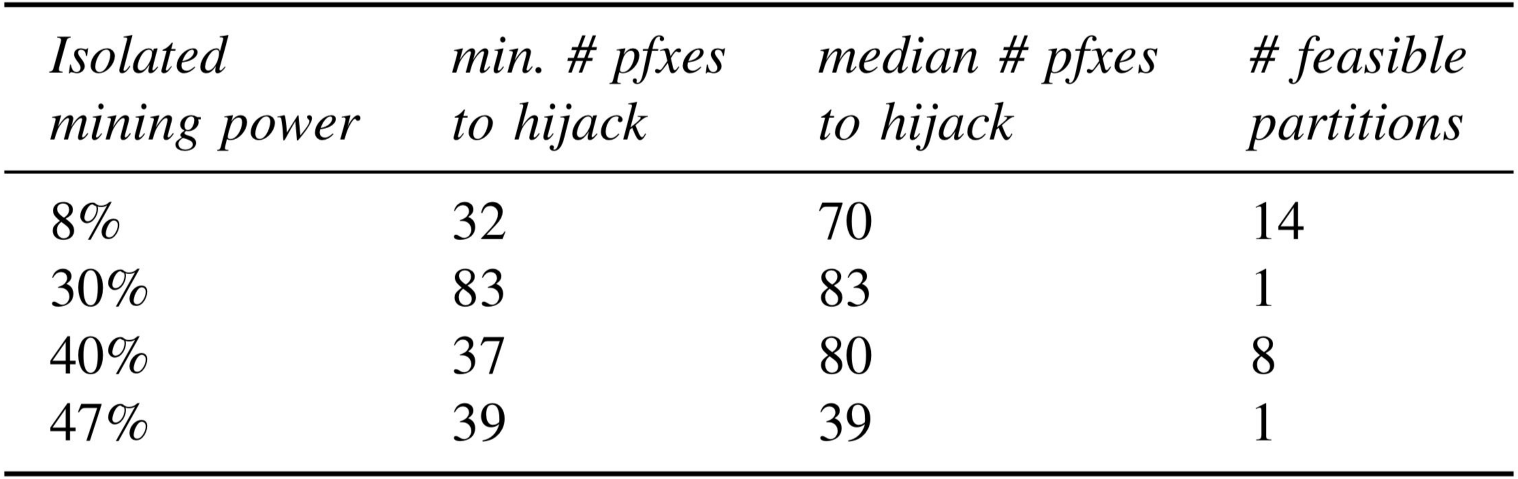
Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

partitioning - speed



Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

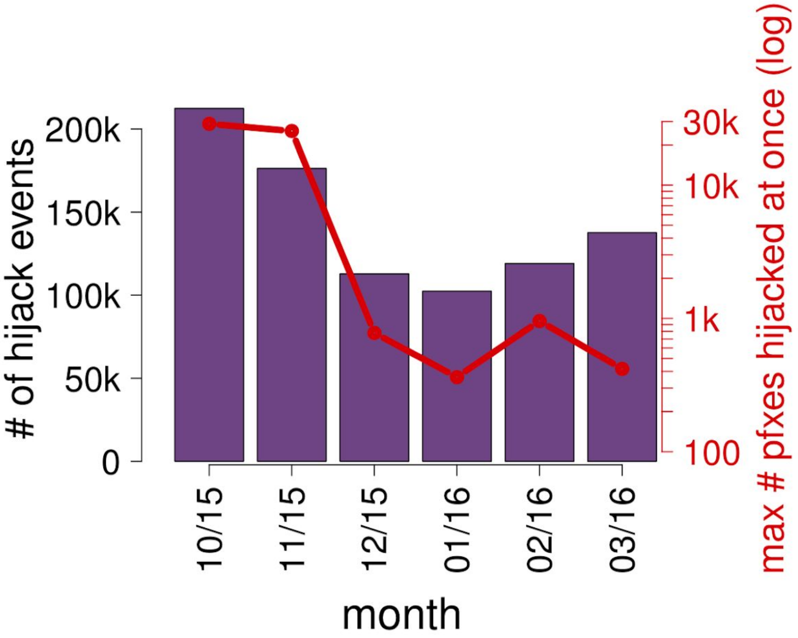
partitioning - impact

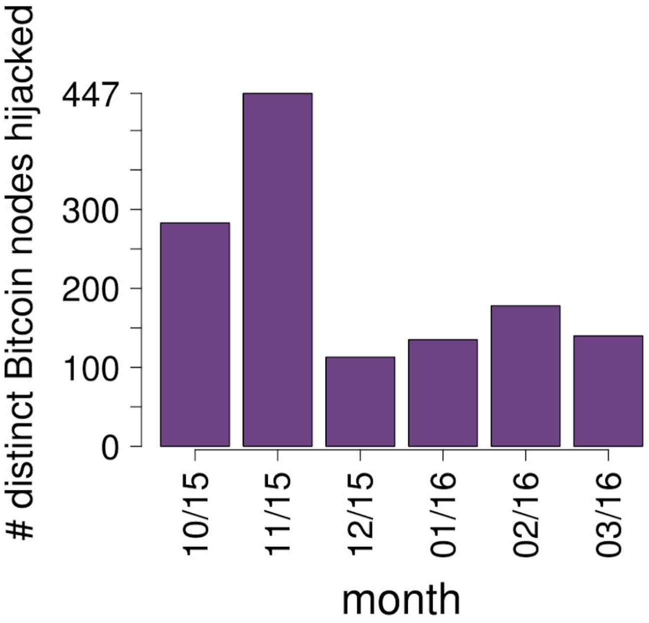


Isolated mining power	*min. # pfxes to hijack*	*median # pfxes to hijack*	*# feasible partitions*
8%	32	70	14
30%	83	83	1
40%	37	80	8
47%	39	39	1

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

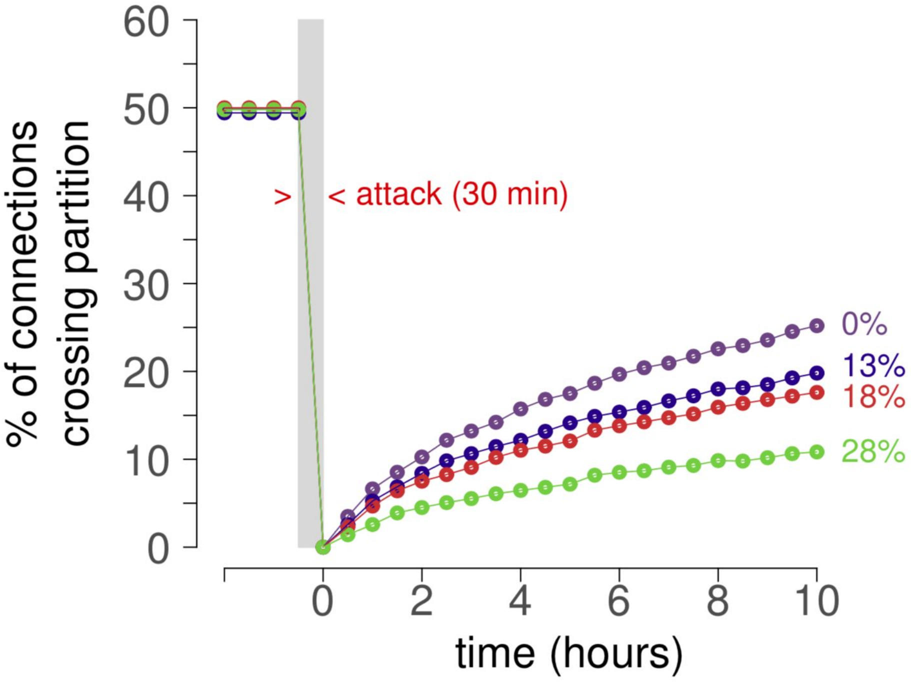
partitioning - frequency





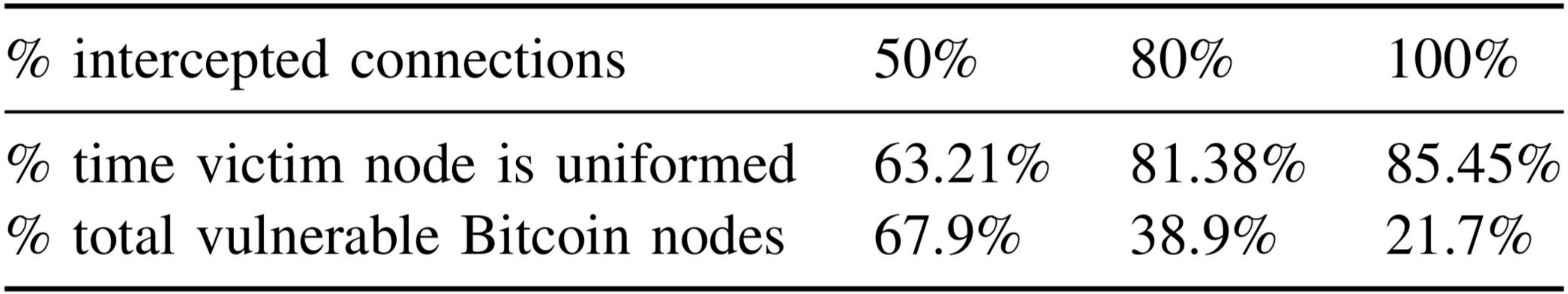
Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

partitioning - recovery



Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

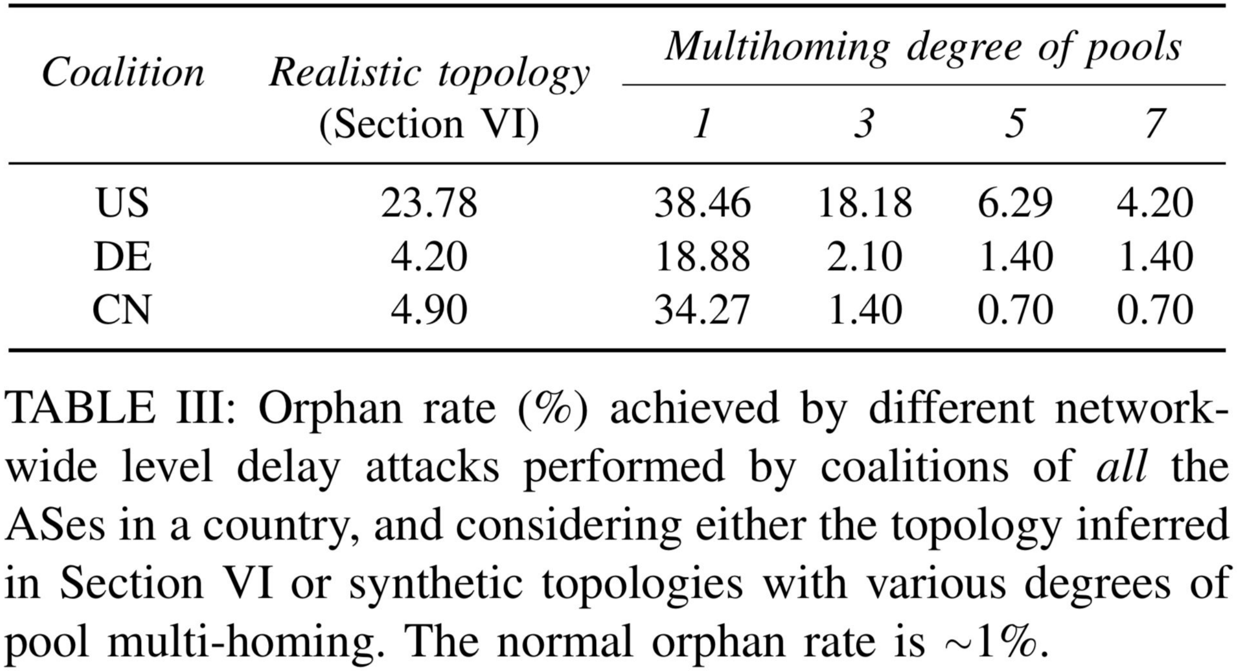
delay - impact (single node)



% intercepted connections	50%	80%	100%
% time victim node is uniformed	63.21%	81.38%	85.45%
% total vulnerable Bitcoin nodes	67.9%	38.9%	21.7%

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

delay - impact (whole network)



Coalition	*Realistic topology* (Section VI)	*Multihoming degree of pools*			
		1	*3*	*5*	*7*
US	23.78	38.46	18.18	6.29	4.20
DE	4.20	18.88	2.10	1.40	1.40
CN	4.90	34.27	1.40	0.70	0.70

TABLE III: Orphan rate (%) achieved by different network-wide level delay attacks performed by coalitions of *all* the ASes in a country, and considering either the topology inferred in Section VI or synthetic topologies with various degrees of pool multi-homing. The normal orphan rate is ~1%.

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

outline

- background
- partitioning attack
- delay attack
- evaluation
- **countermeasures**

countermeasures (short-term)

- increase diversity of node connections
  - ➜ use multiple ASes (directly or through VPN)
- take routing into consideration when establishing connections
  - ➜ use traceroute, check BGP traffic
  - ➜ prevent a single AS from appearing in all paths
- monitor sudden change in round-trip time (RTT) and other anomalies
- prefer peers in same AS and in /24 prefixes

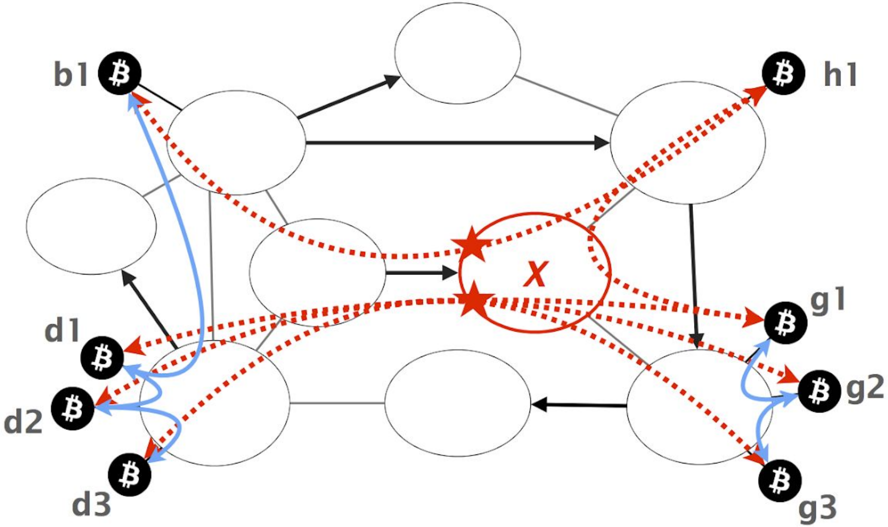
Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

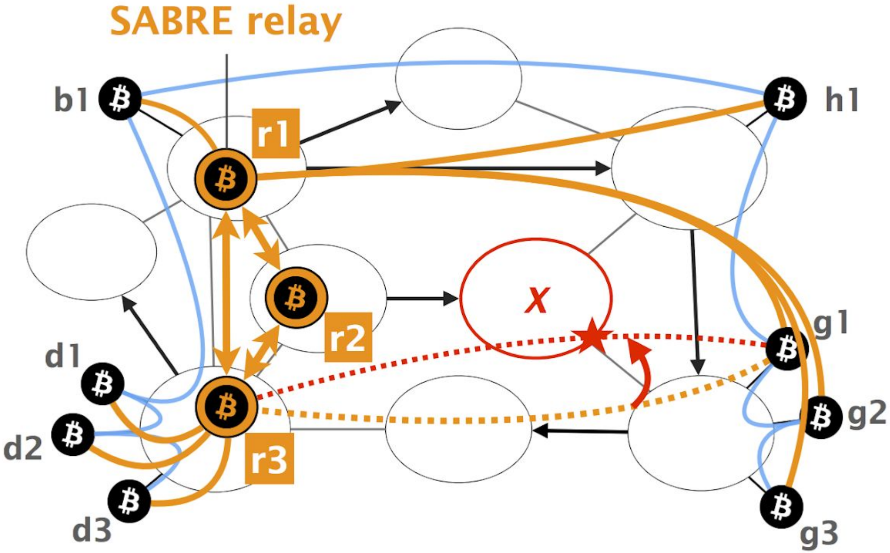
countermeasures (long-term)

- use encryption and/or integrity checks (BIP-151)
- use port negotiation or randomized port
- use UDP heartbeats
- request blocks on multiple connections

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. 2017

SABRE





Apostolaki, M., Marti, G., Müller, J., & Vanbever, L. (2018). SABRE: Protecting Bitcoin against Routing Attacks

references

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies
https://btc-hijack.ethz.ch/files/btc_hijack.pdf

Apostolaki, M., Marti, G., Müller, J., & Vanbever, L. (2018). SABRE: Protecting Bitcoin against Routing Attacks
https://arxiv.org/pdf/1808.06254