Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

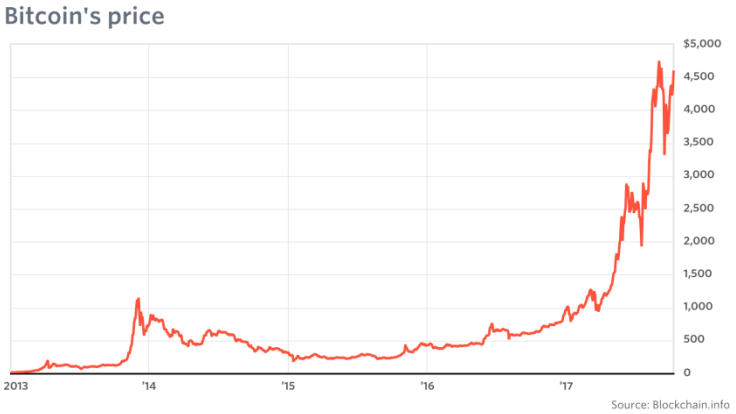
Maria Apostolaki[1], Aviv Zohar [2], Laurent Vanbever[1]

Presented by Pascal Blöchlinger

[1]ETH Zürich, [2] The Hebrew University

Motivation

- Money
- Security
- Rising interest
- Lacking knowledge of participants



Overview

- Bitcoin
- Hijacking Connections
- Partitioning attack
- Delay attack
- Experiment on real network
- Possible Protections
- Conclusion and Problems

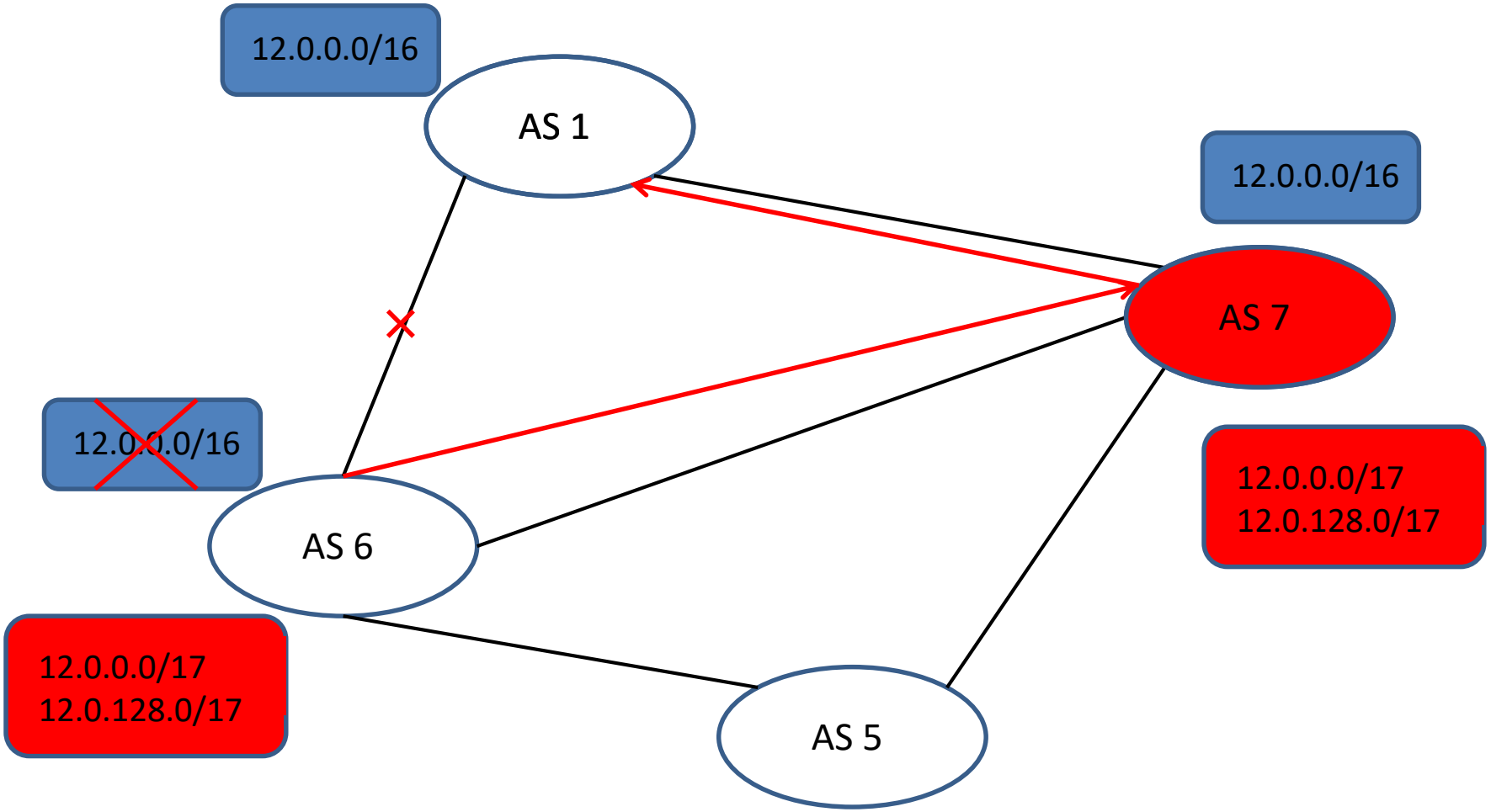
BGP

- Autonomous system (AS):
  - Collection of connected IP routing prefixes under control of network operator with routing policy (RFC 1771)
  - Normally ISP‘s (Internet Service Provider)
- Border Gateway Protocol (BGP):
  - Standardized routing protocol, based on paths, network policies, or rule-sets
  - Defines forwarding rules

Hijacking Routes

- BGP works over announcing IP-prefixes between ASes
- Adversary can announce more precise path to node he wants to get the traffic from
  - Ex. Announce 12.0.0.0/16 and 12.0.128.0/17 instead of 12.0.0.0/17
  - Most ASes filter more precise than /24
  - If original announces /24 part of the traffic can be rerouted to adversary with another /24 announcement

Hijacking Routes



Bitcoin

- Biggest Crypto currency
- ca 150 Billion (03/18)
- Transactions are grouped to blocks
- Blocks are attached to global ledger
- Proof of work for creation of new block
- New block every ca every 10 minutes
- Chain with most work wins (longest normally)

Bitcoin Infrastructure

- Nodes work to complete blocks
  - Transaction fee for proof of work
- Nodes have TCP connections to 8 other nodes
  - Inserting messages not possible
  - Not encrypted nor authenticated
  - Port 8333
- Three messages:
  - INV: New block exists
  - GET DATA: Request block from peers
  - BLOCK: Get a block

Mining pools

- Rare for each node to complete block
  - Payout sporadic
- Mining pools split work and rewards
  - Have non observable communication
- Mining pools are often multihomed
  - Mining pool often use gateways to different AS for more independence

Partitioning network

- Idea: Isolate set of Nodes totally from the network
  - Attack few nodes
    - 0-confirmation double spending vulnerability
  - Attack bigger sets
    - Loss of revenue for smaller Partition
    - Likely to reverse Transactions
    - Selfish mining attacks
    - High risk of double spending

Partitioning network

1. Gather information about bitcoin nodes
   - Identify mining pool gateways
   - Associate Nodes to AS
2. Find set of nodes to attack
   i. Either include all or no node of one AS
   ii. Either include all or no gateway of same miningpool

Partitioning network

Set P: nodes to be disconnected from rest of network

Set L: nodes that leak information from rest of network

Set U: Nodes that haven't be observed yet

Rule 1: If bitcoin message is sent to P\L -> drop

Rule 2: If P sends information about block from outside -> add to L

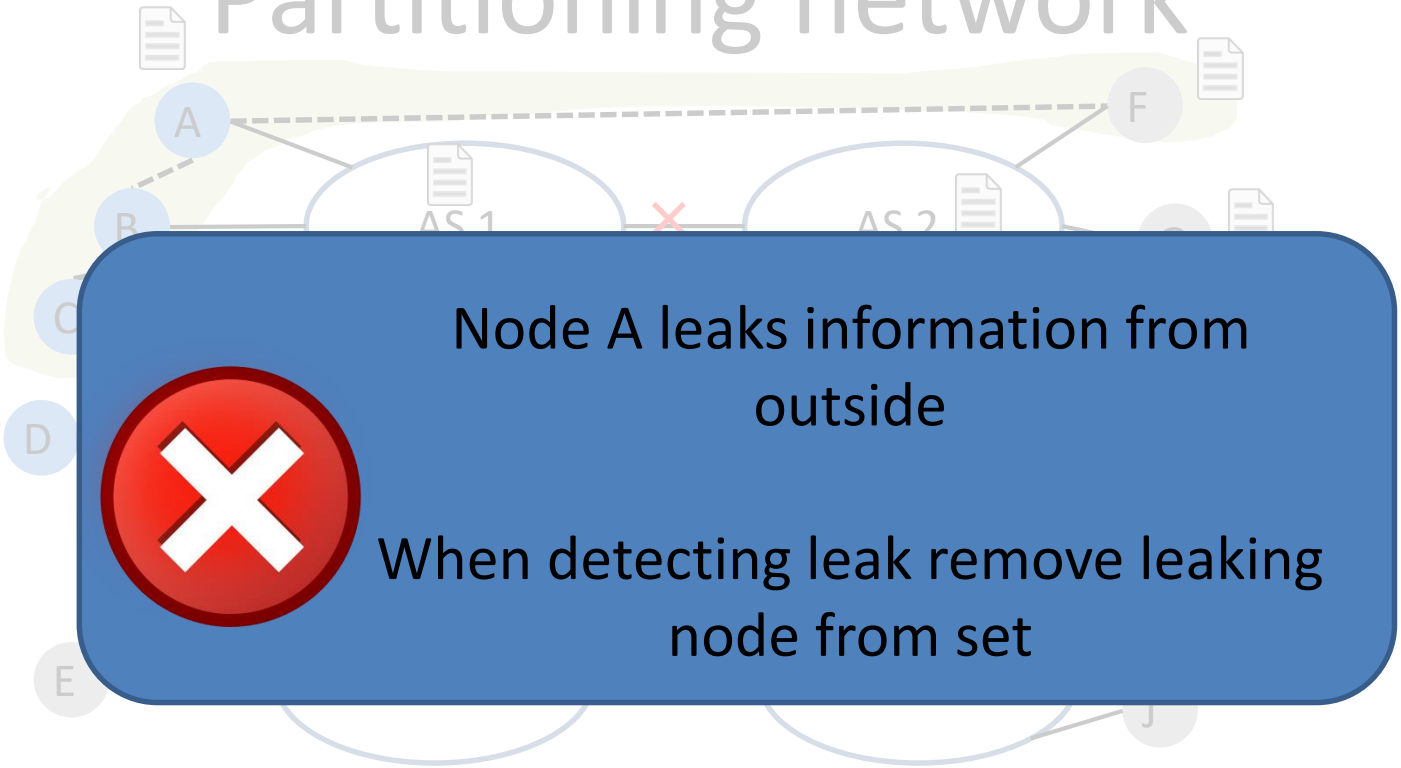
Rule 3: Be careful with unobserved nodes, can potentially leak

Partitioning network

Mining pools have secret communications and multiple gateways

No mining pools
No secret communiction
Most partitions possible
{A,E} not possible as B and A are from AS 1

Partitioning network

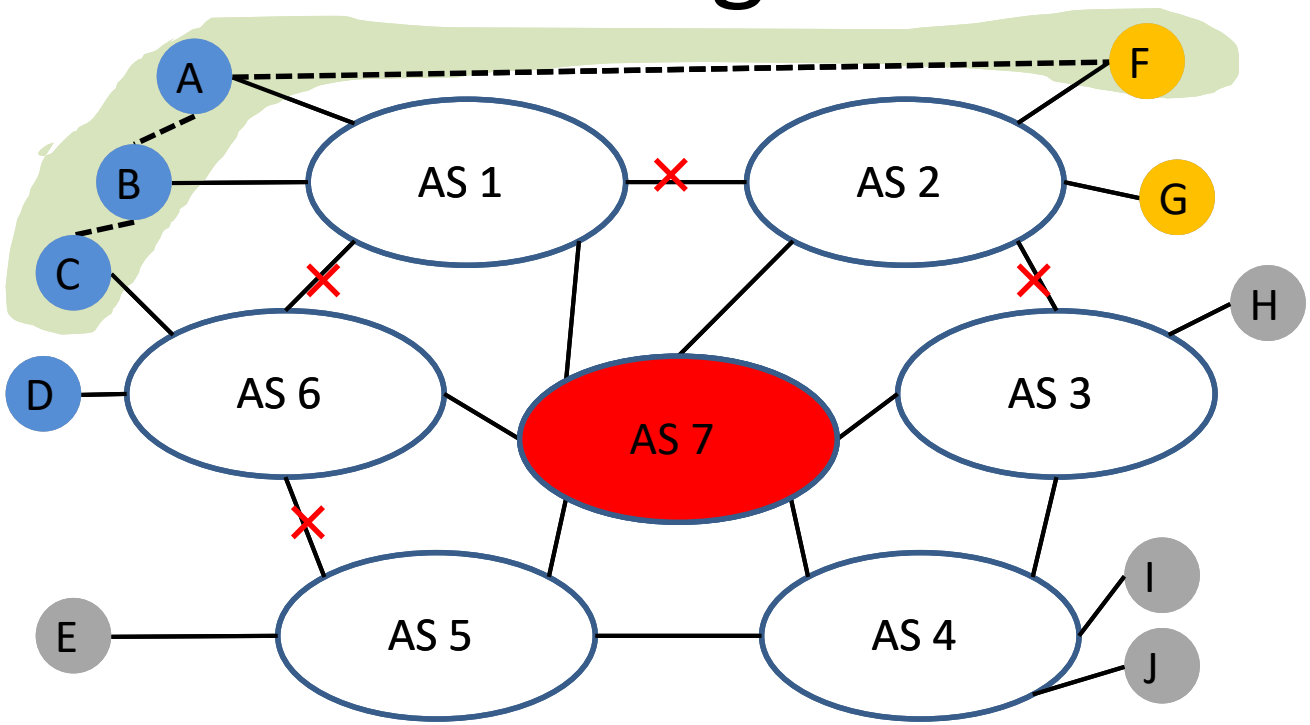


Node A leaks information from outside

When detecting leak remove leaking node from set

{A,B,C,D} should be disconnected

Partitioning network



{A,B,C,D} not possible -> use {A, B, C, D, F, G}

Delay attacks

- Idea: Delay block propagation to set of nodes:
  - 0-confirmation vulnerability
  - Denial of service
  - Block races/ wasting mining power
  - Selfish mining attacks

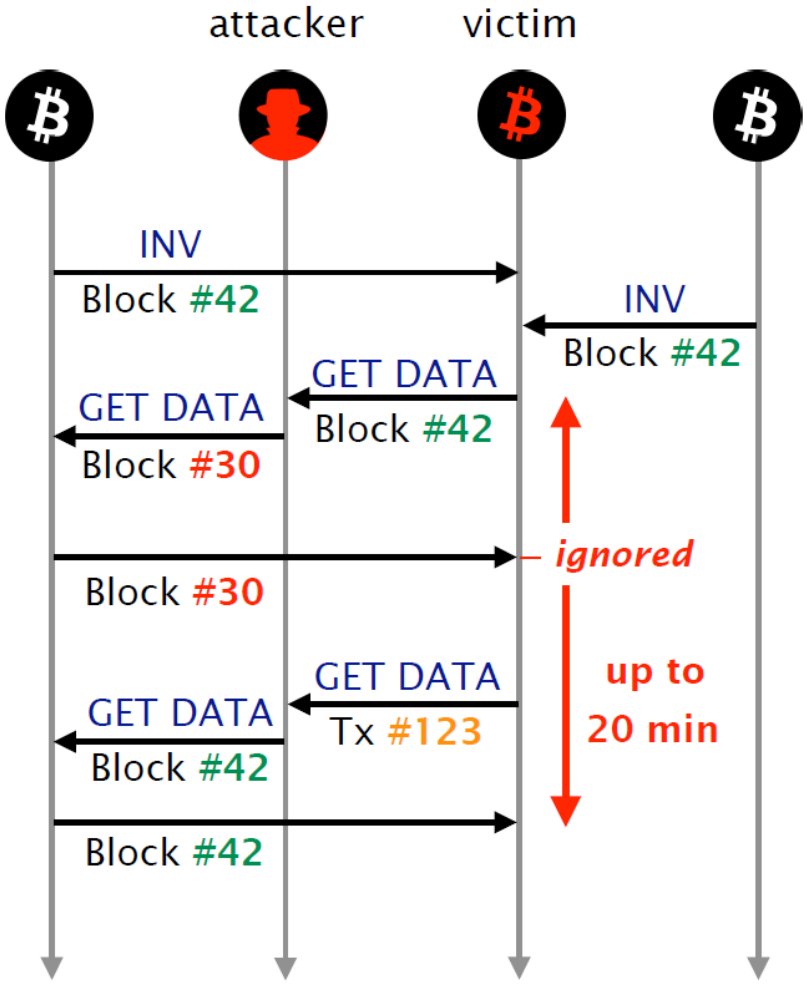
Delay attacks

No MAC to ensure integrity of message

Just dropping would result in detection with non matching TCP numbers

Requested block arrives within 20 minutes connection isn't lost and can be used

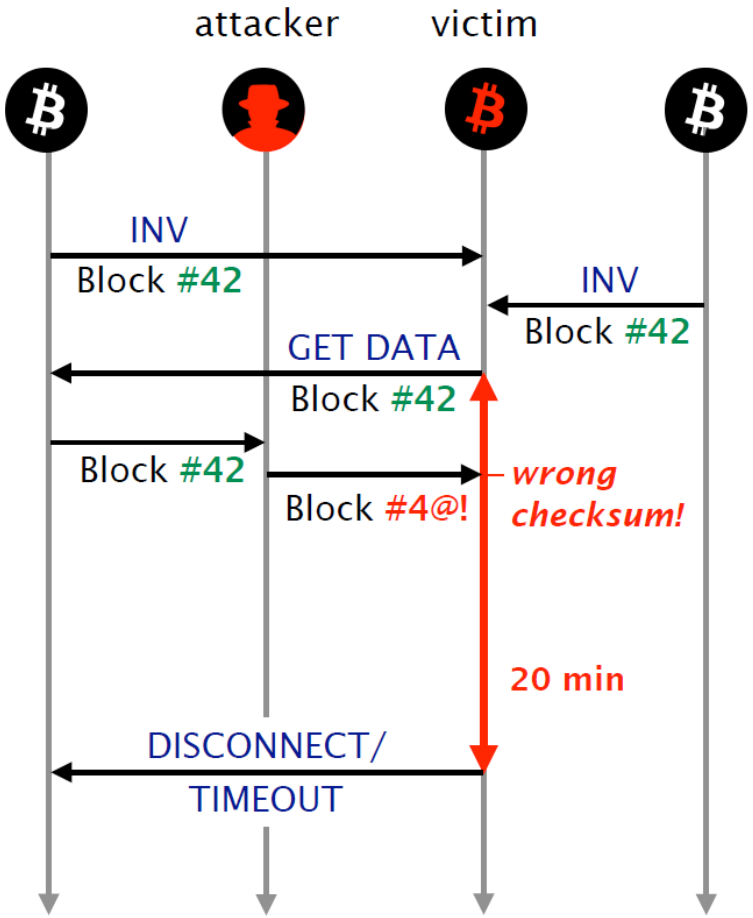
Can be used on only when only part of the communication can be hijacked



Delay attacks

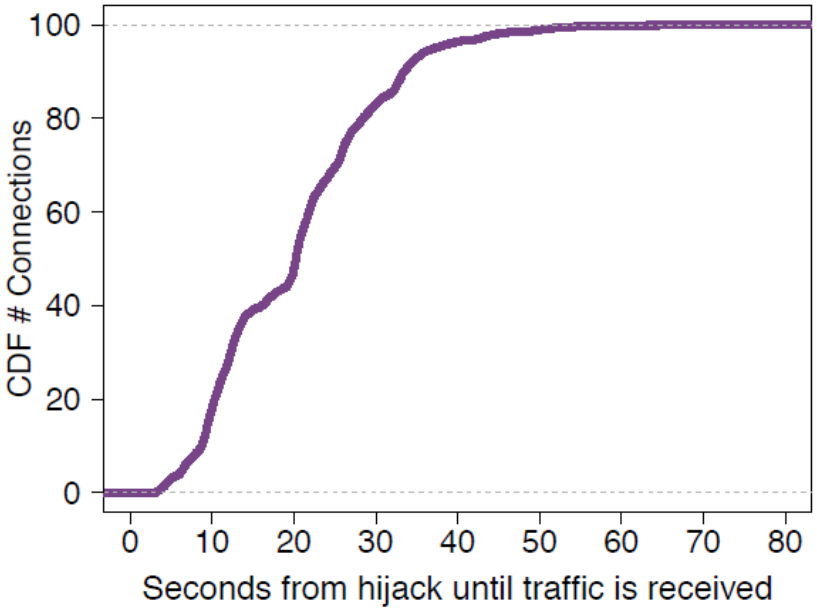
Connection is lost after attack

Can be used on only when only part of the communication can be hijacked



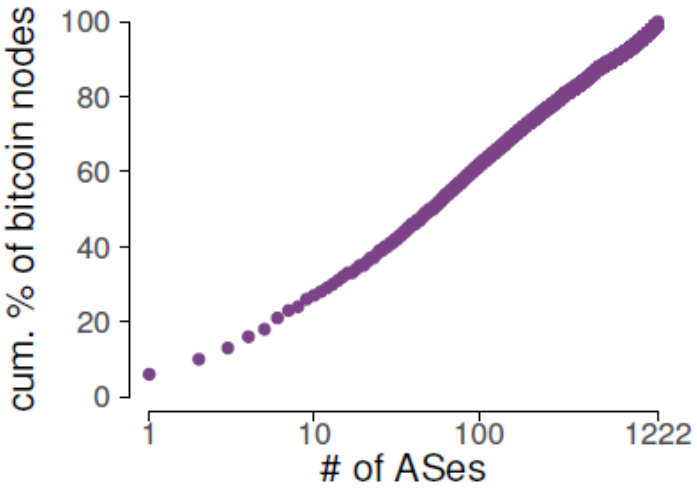
Experiments Partition

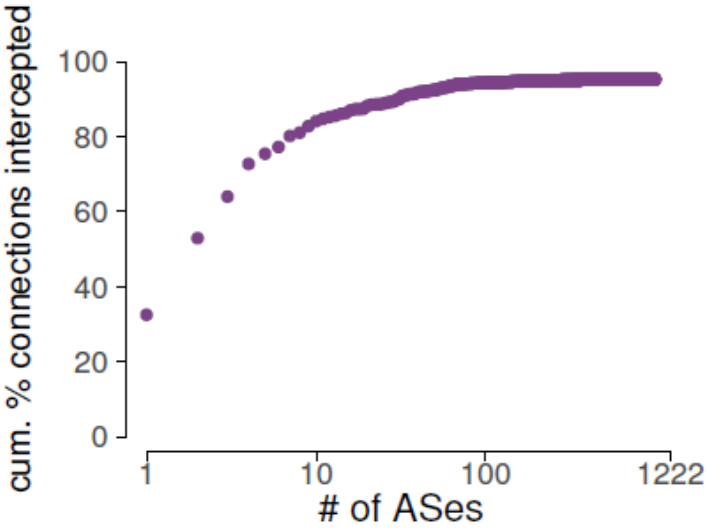
- Attack own nodes
  - 90 s to highjack all traffic



Experiments Partition

- How much need to attack large number
  - 13 ASes host 30% of bitcoin nodes
  - 50 Ases host 50% of bitcoin nodes





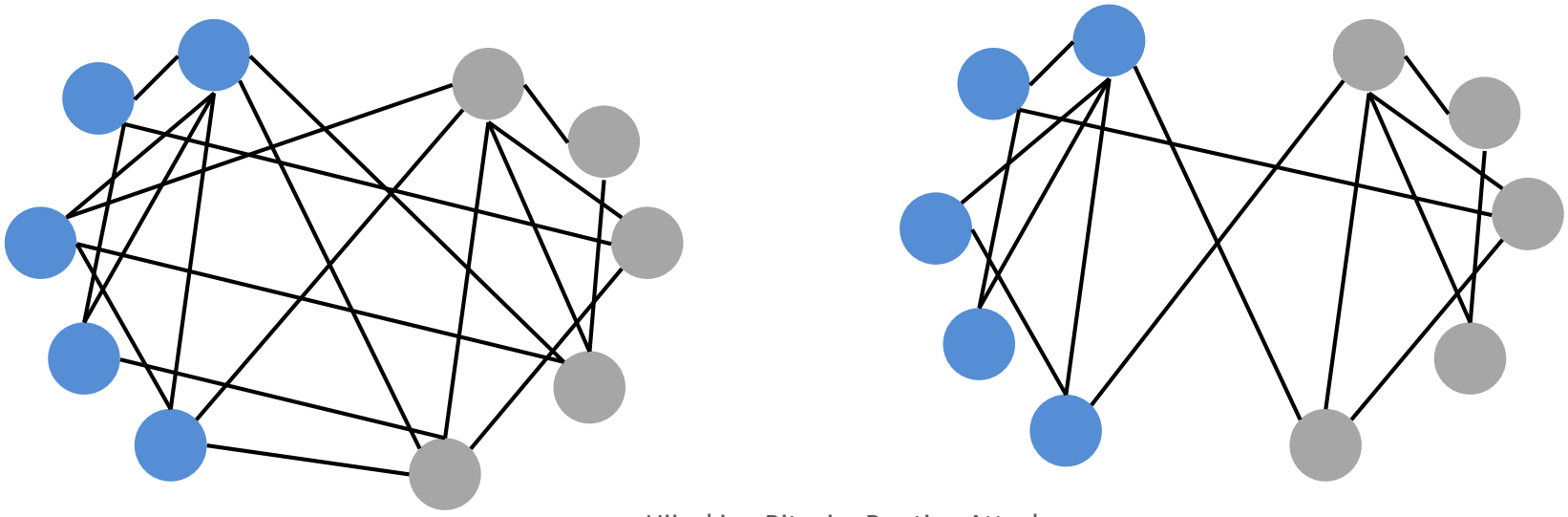
Experiments Partition

- How much need to attack large number
  - 63 Prefixes to hijack 20% of network
  - Larger mining power must not be more prefixes

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

Recovery from partition

- Reconnection to other partition is fast
- Stay sparsely connected for long time
  - After 10 hours only half as many connections as before attack between both sides



Experiments Delay

- Delay attacks are only doable by large coalitions of powerful players

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

- Multihoming of mining pools is good protection against delay attacks

Possible Protections

- Encrypt bitcoin messages
- Use port 8333 to start connection, agree on different ports to send and receive data
  - Harder to dected Bitcoin traffic, can't filter on ports
- Check with regular traceroutes and add connections if one AS appear in all peer paths
- Monitor round trip time
- Increase number of connections

Conclusion

- First paper to consider routing attacks with crypto currencies
- Easy solutions to fix big problem

Problems in paper

- Delay attacks not a problem at all
- Never tested against larger number of nodes in practice
- AS-level adversary is not to most common

My Opinion

- Interesting idea of how to attack a blockchain
- Can it be used on other blockchain currencies as well
- Best used with other attacks like double spending
- General Model

Further Work

- Apply same attacks on other Cryptocurrencies
- Test against larger amounts of Nodes (Ethics problem)