Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

Taehwa Lee

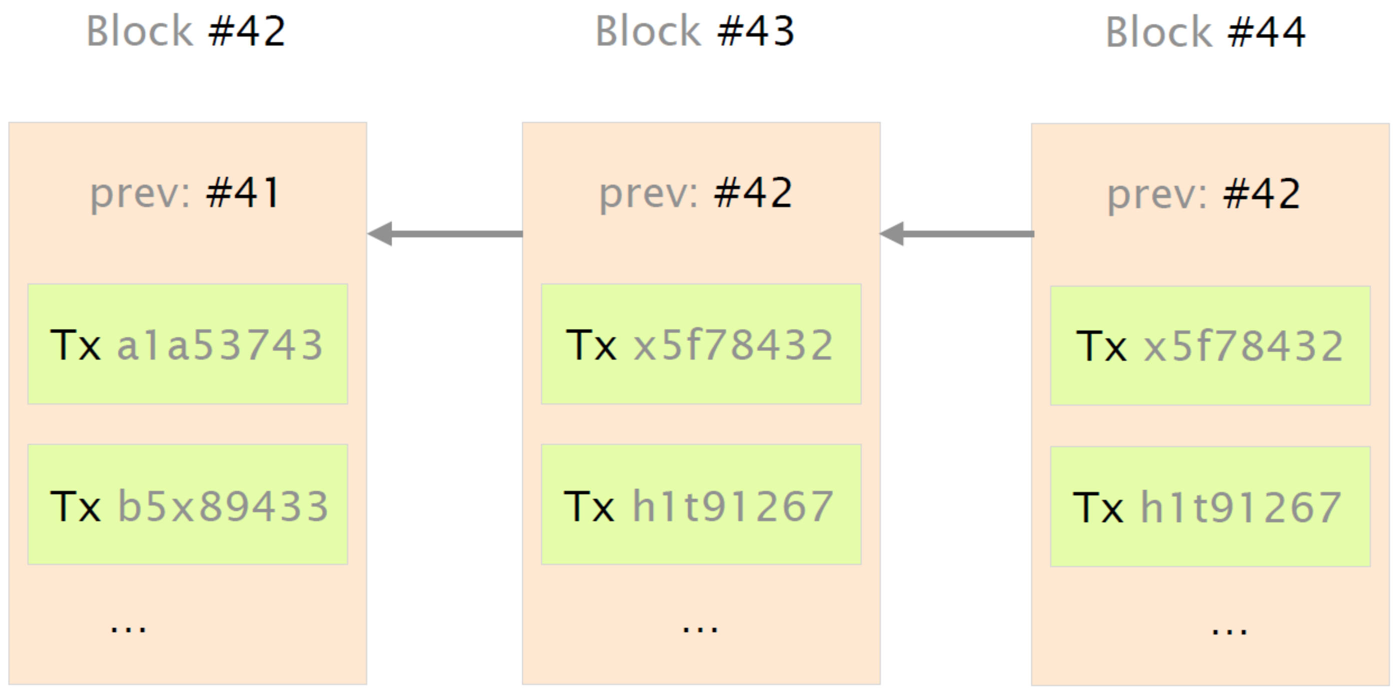
Maria Apostolaki , ETH Zürich apmaria@ethz.ch
Aviv Zohar The Hebrew University avivz@cs.huji.ac.il
Laurent Vanbever ETH Zürich lvanbever@ethz.ch

Introduction

- Bitcoin is highly decentralized, therefore robust
- Is Bitcoin safe?

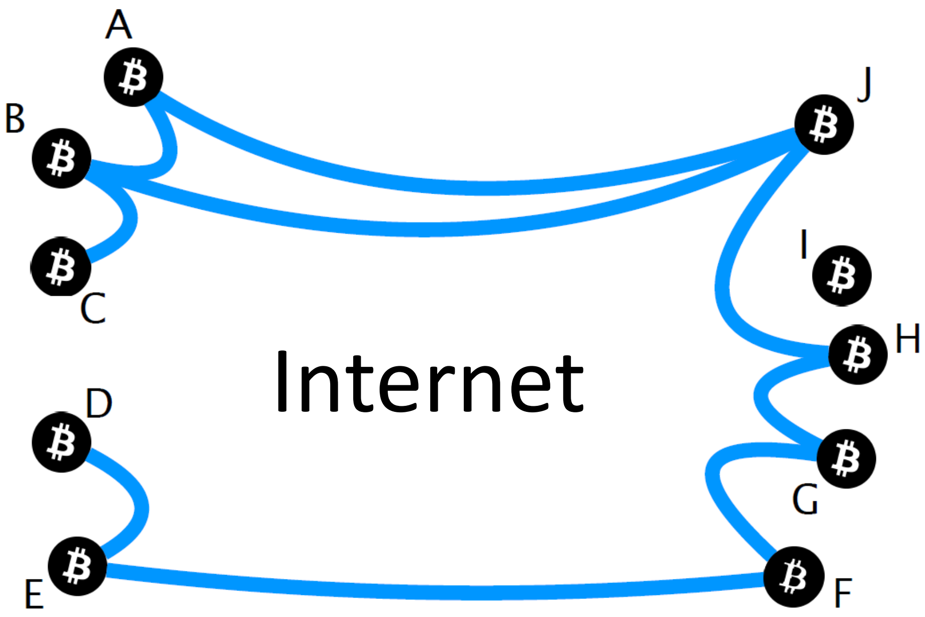
Background – Blockchain

- Transactions are stored in the block
- Blockchain is a chain of Blocks



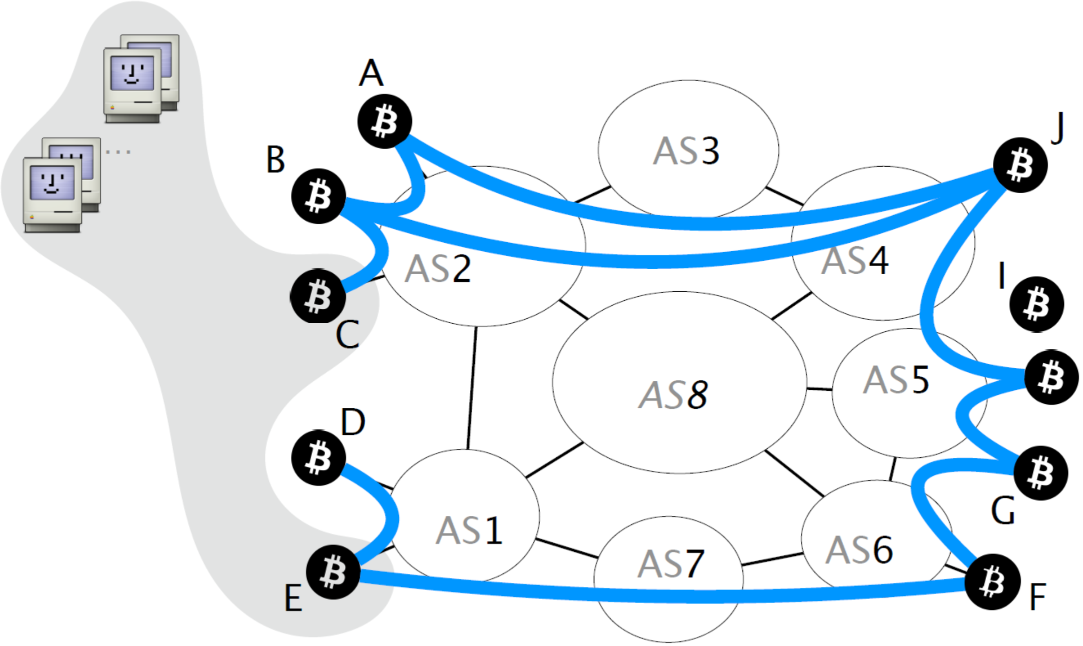
Background – Blockchain

- The blockchain reaches consensus by miners
  - Miners get incentives for each consensus
- Bitcoin is a distributed network of the blockchain node
  - Establish random connections between nodes



Background – BGP

- The Internet is composed of Autonomous Systems (ASes)
- BGP computes the forwarding path across the ASes



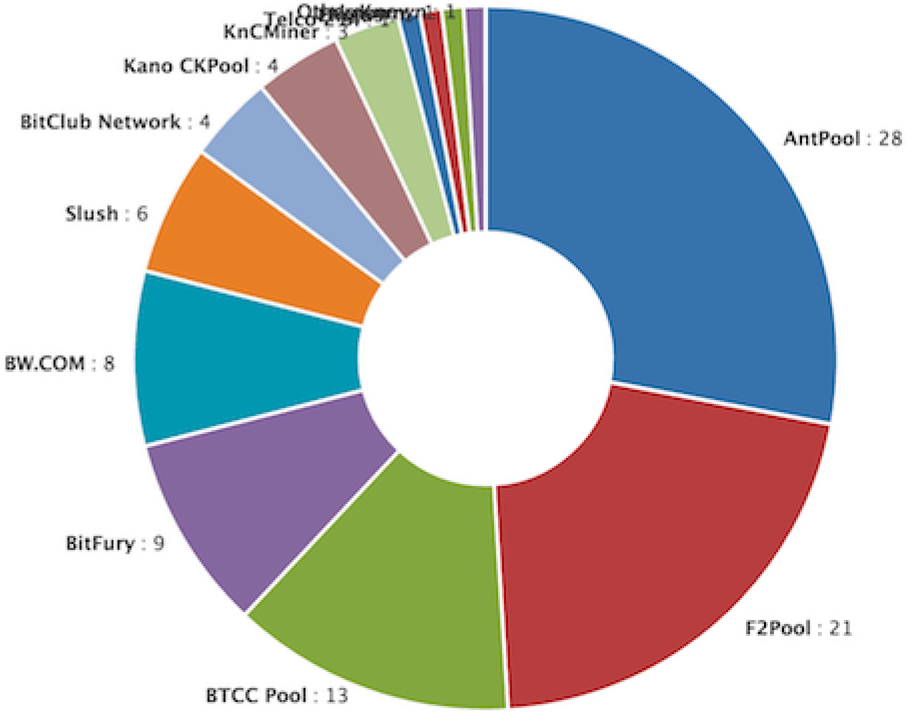
Background – Bitcoin Problems

- Bitcoin is highly decentralized making it robust to routing attacks, in theory

- In practice, Bitcoin is highly centralized, both from a routing and mining viewpoint

Background – Bitcoin Problems

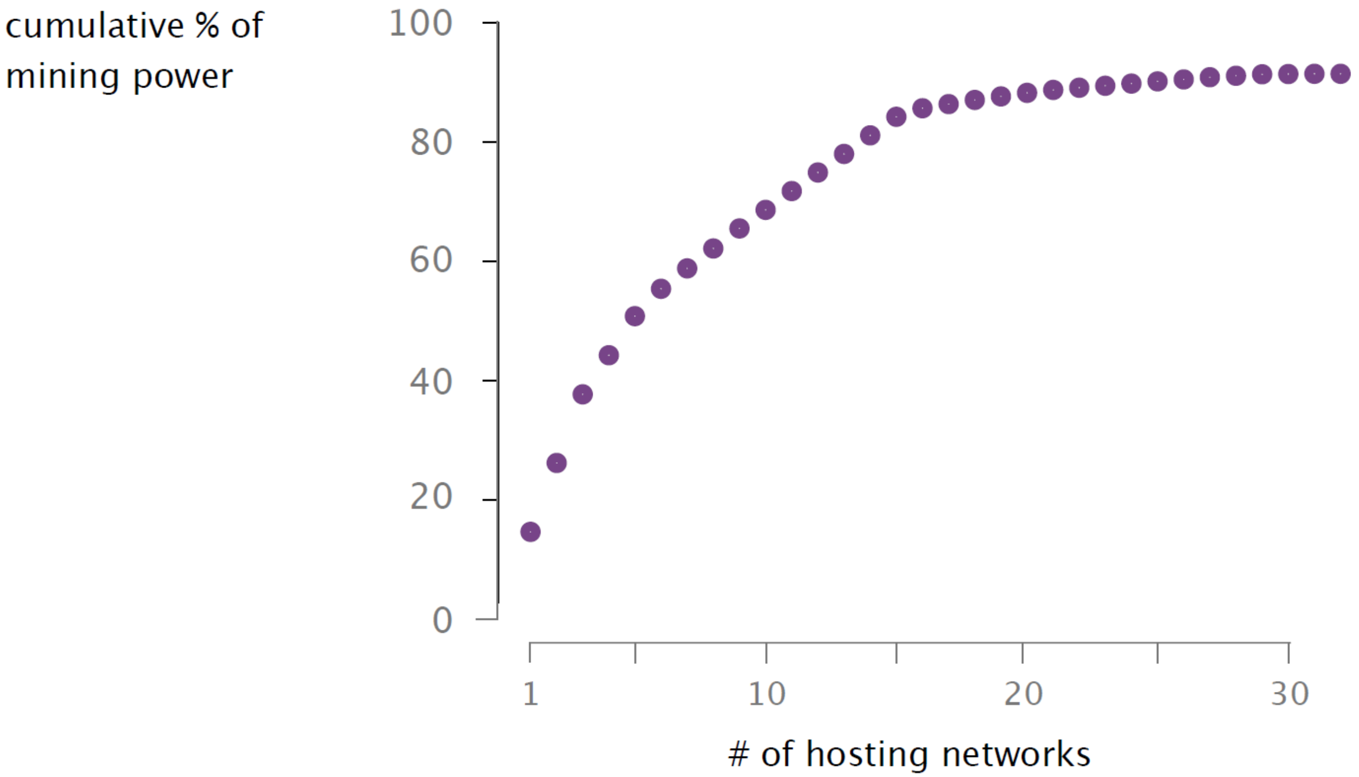
- 51% attack
- 3 mining pools have 62% mining power



* https://www.bitcoinmining.com/bitcoin-mining-pools/

Background – Bitcoin Problems

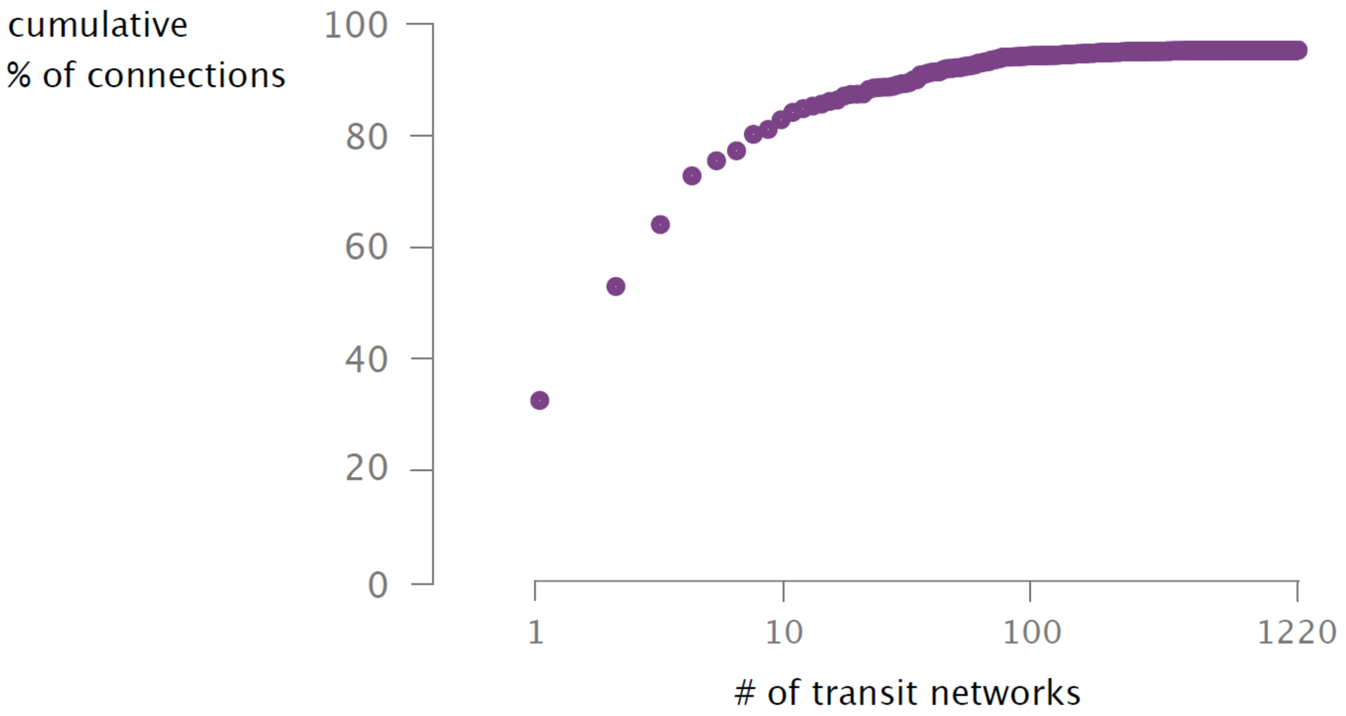
- 68% of the mining power is hosted in 10 ASes only
  - The public Internet is composed of some 63,000 ASes*



* https://blog.apnic.net/2019/01/16/bgp-in-2018-the-bgp-table/

Background – Bitcoin Problems

- 3 transit ASes make more than 60% of all connections
  - The public Internet is composed of some 9,000 transit ASes*



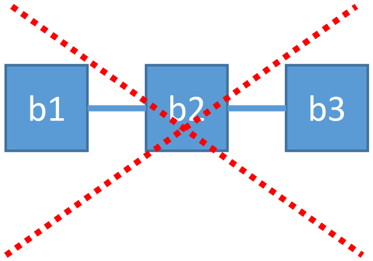
* https://blog.apnic.net/2019/01/16/bgp-in-2018-the-bgp-table/

Attacks

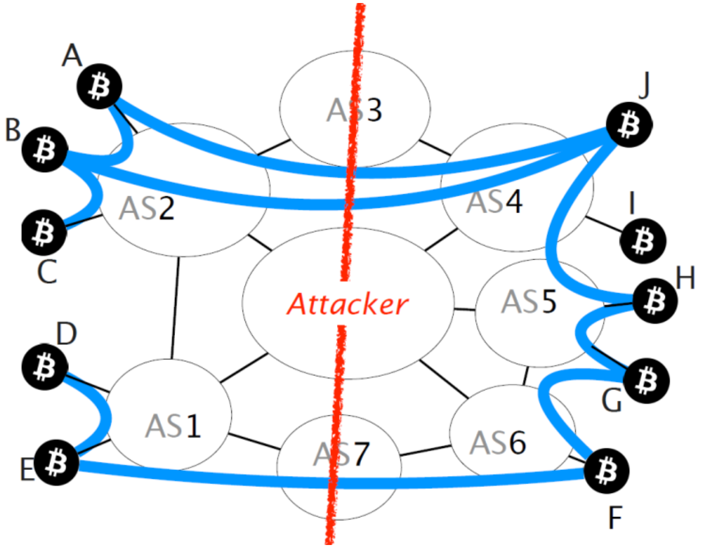
- This paper shows two routing attacks through two methods:
  - Partitioning the network in half to cause double spending
  - Delay block propagation to cause double spending

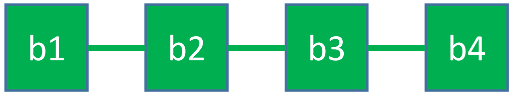
Partition

- The goal of a partitioning attack is to split the Bitcoin network into two disjoint components
    - Causing fork for double spending by the longest chain rule



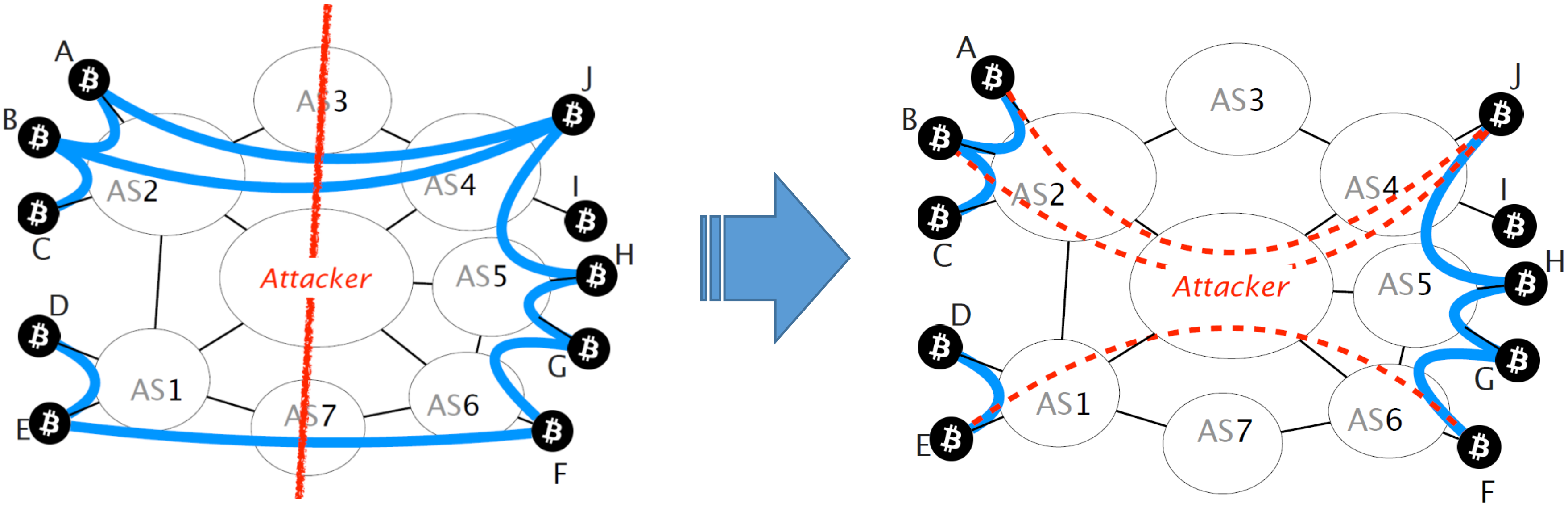
TXs in this chain will be invaild





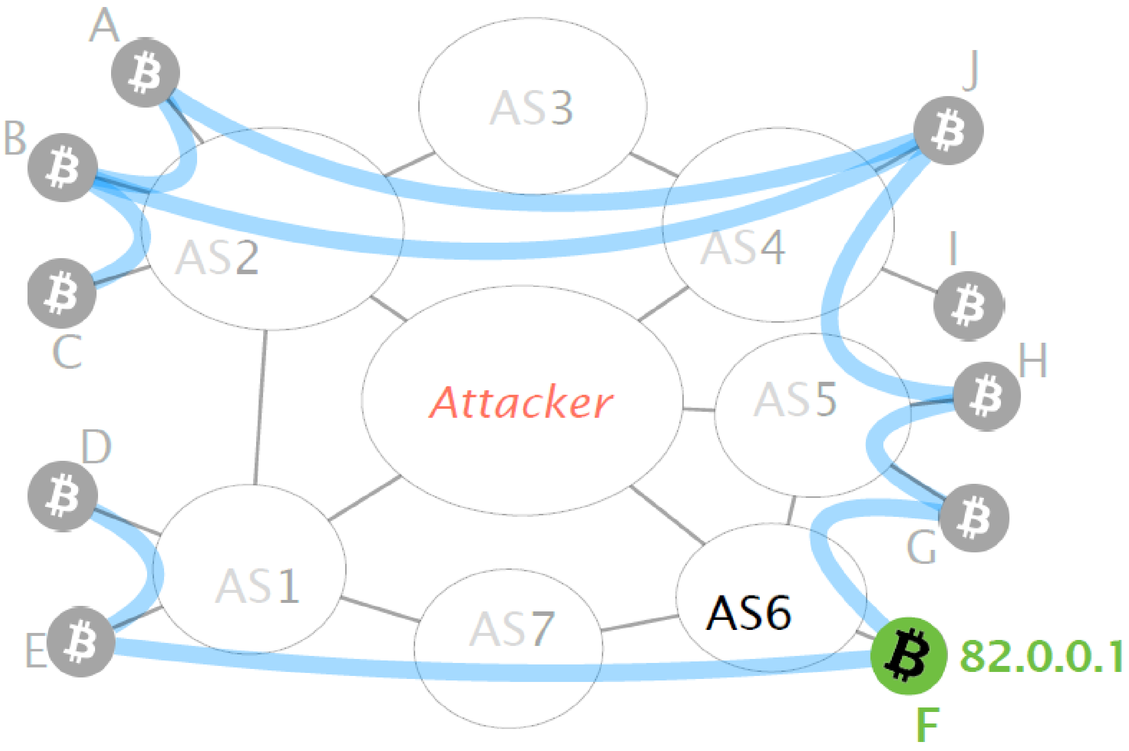
Partition

- Let’s say an attacker wants to partition the network into the left and right side
- To do so, the attacker will manipulate BGP routes to intercept any traffic to the nodes in the right



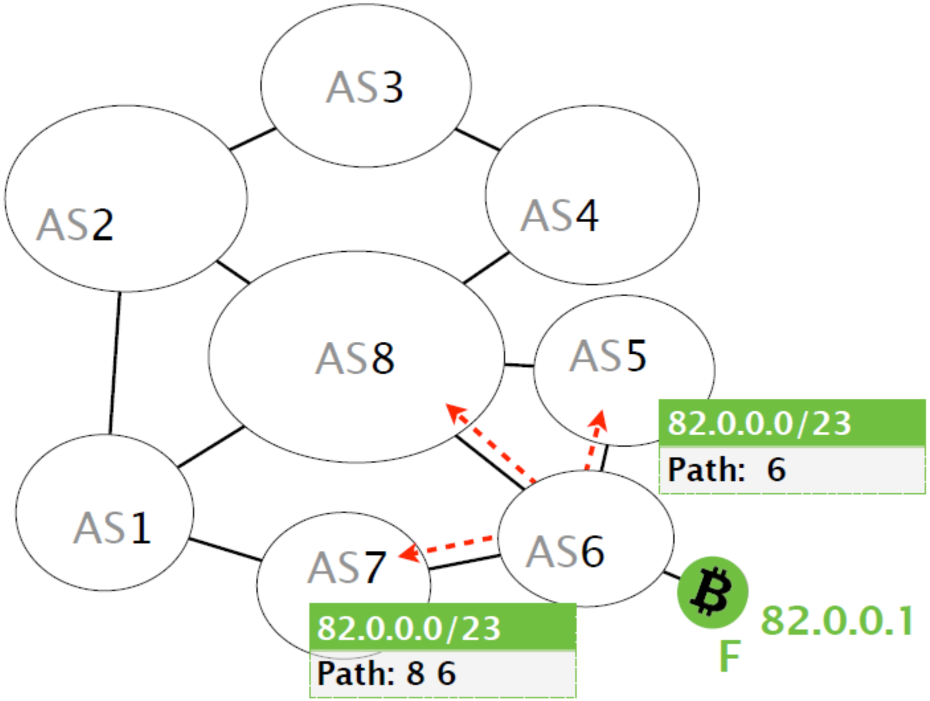
Partition

- Let’s focus on node F and AS6



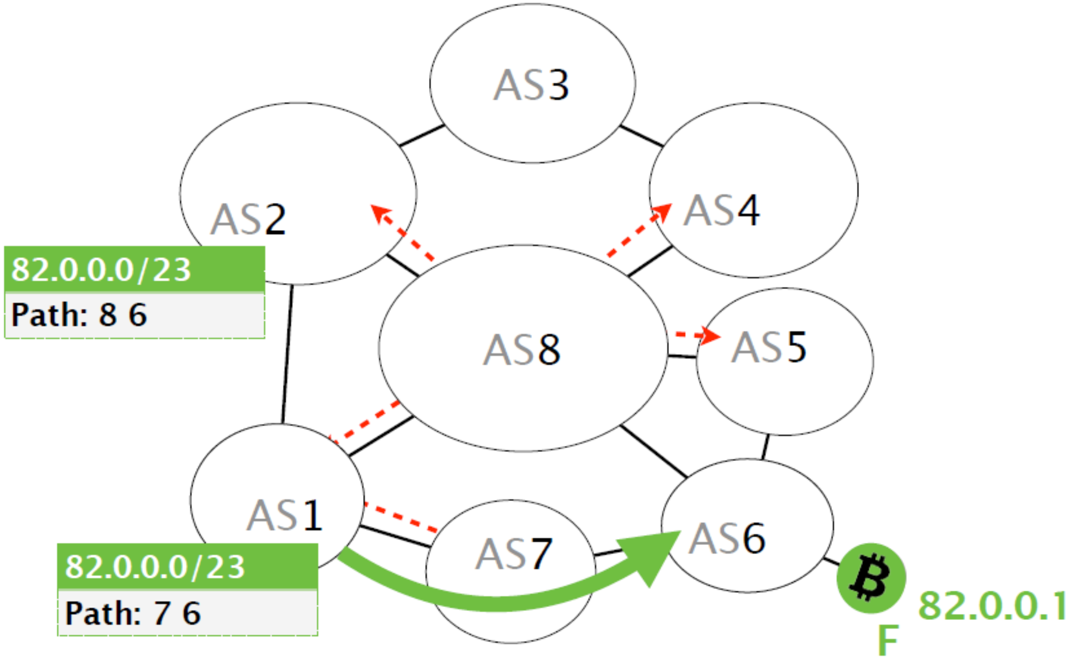
Partition

- AS6 will create a BGP advertisement with /23 prefix



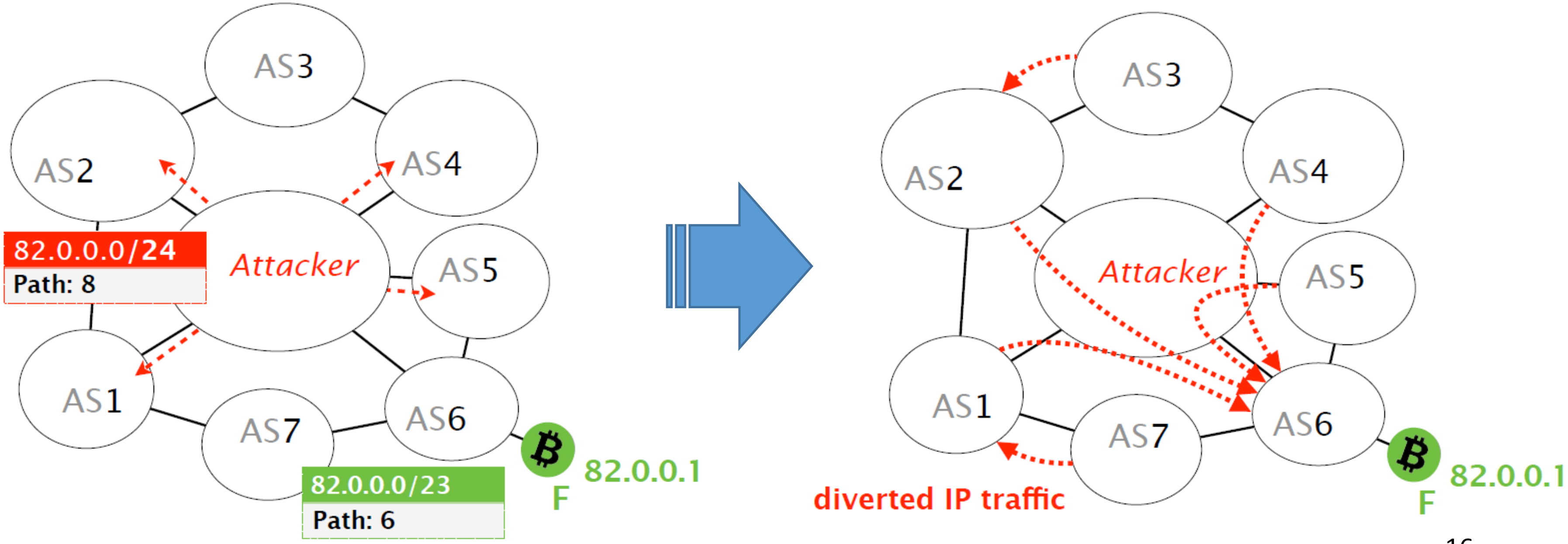
Partition

- AS6’s advertisement is propagated AS-by-AS until all ASes in the Internet learn about it
- BGP does not check the validity of advertisement
  - Any AS can announce any prefix



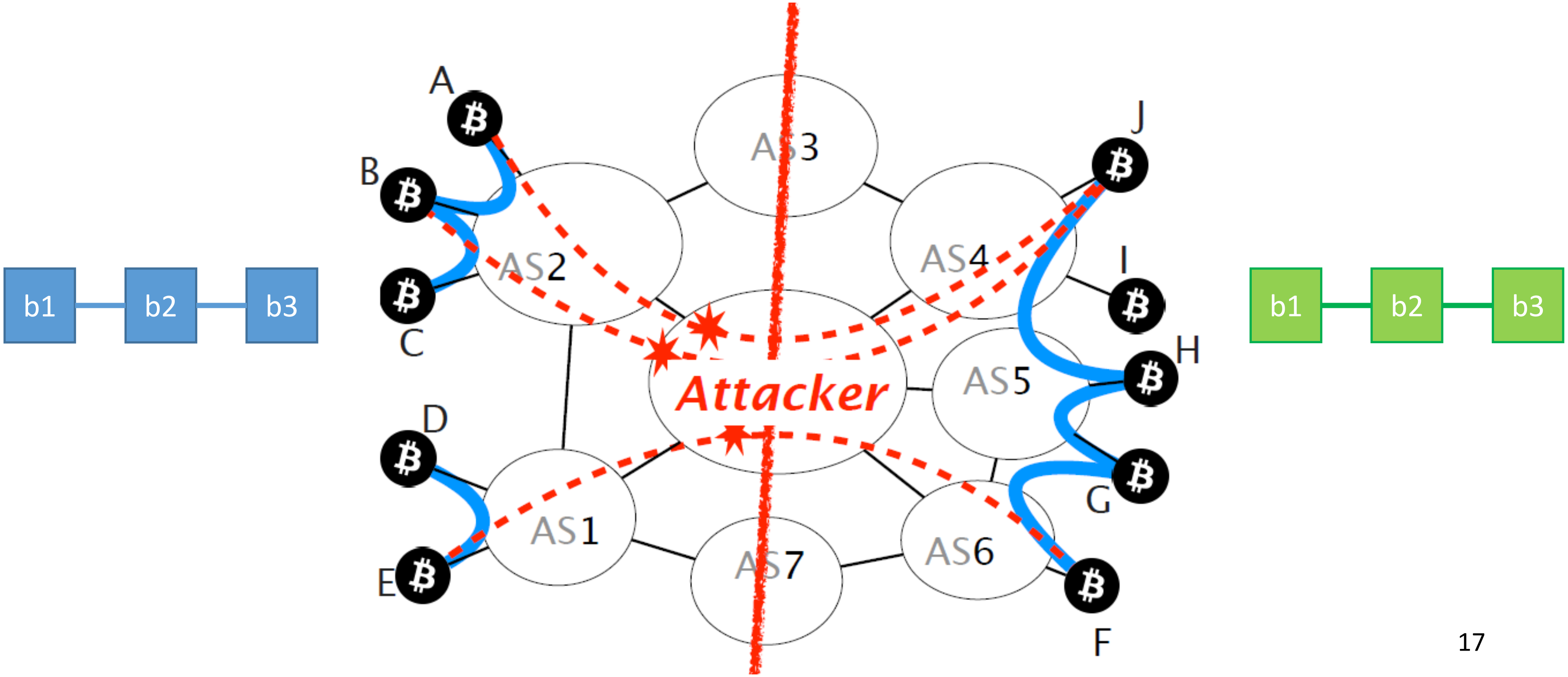
Partition

- Routers prefer more specific prefixes
- Consider that the attacker advertises a more specific prefix covering F's IP address
- Traffic to node F is hijacked



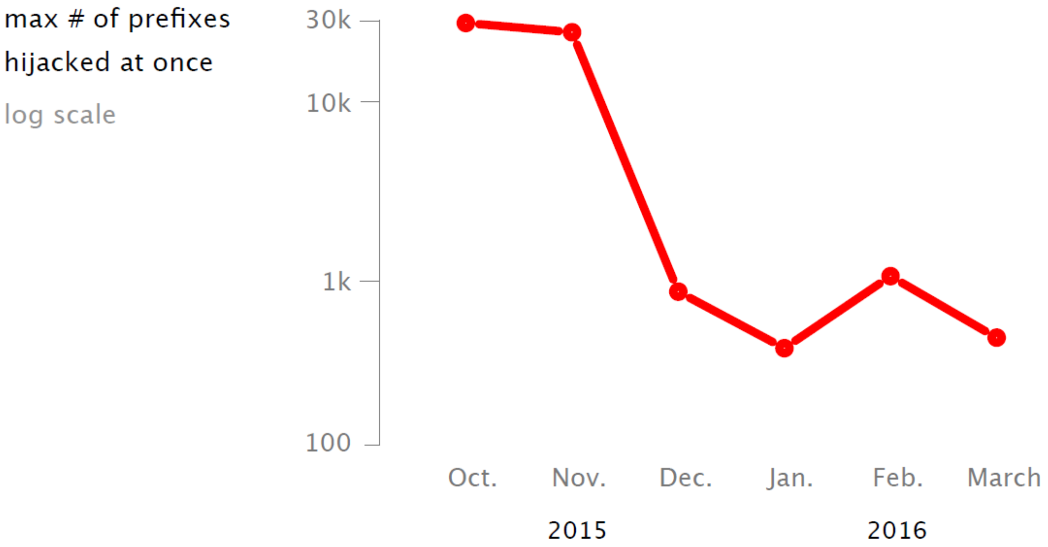
Partition

- By hijacking the IP prefixes pertaining to the right nodes, the attacker can intercept all their connection
- The attacker can drop all connections crossing the partition: partition is created!



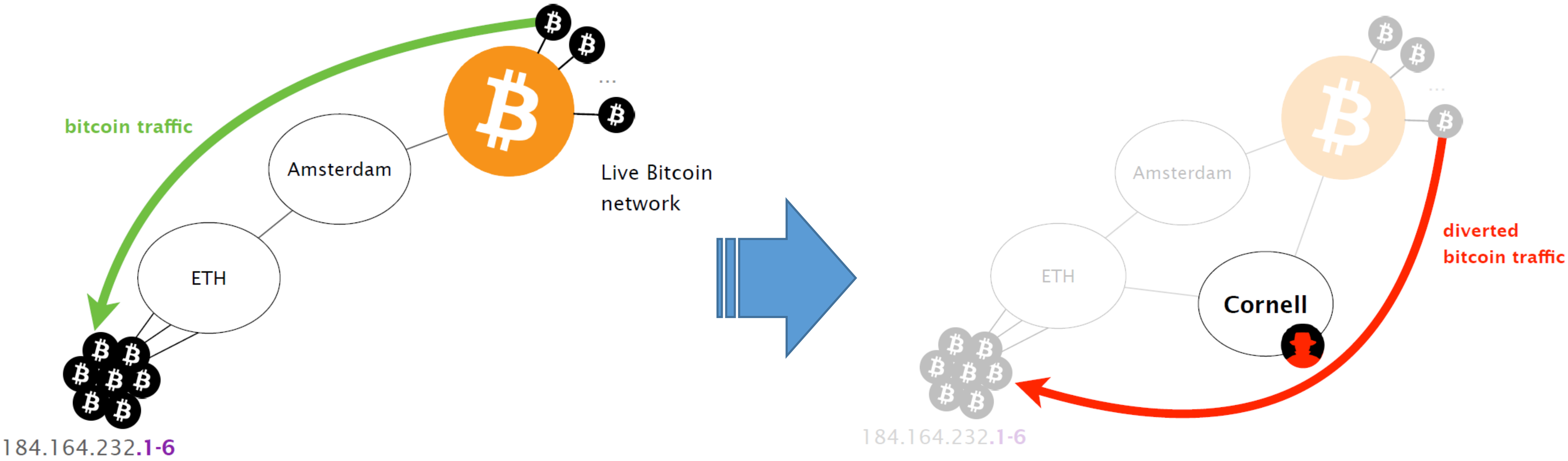
Partition (Evaluation)

- Splitting the mining power by half can be done by hijacking less than 100 prefixes
  - Hijacks involving up to 1k of prefixes are frequently seen on the Internet today



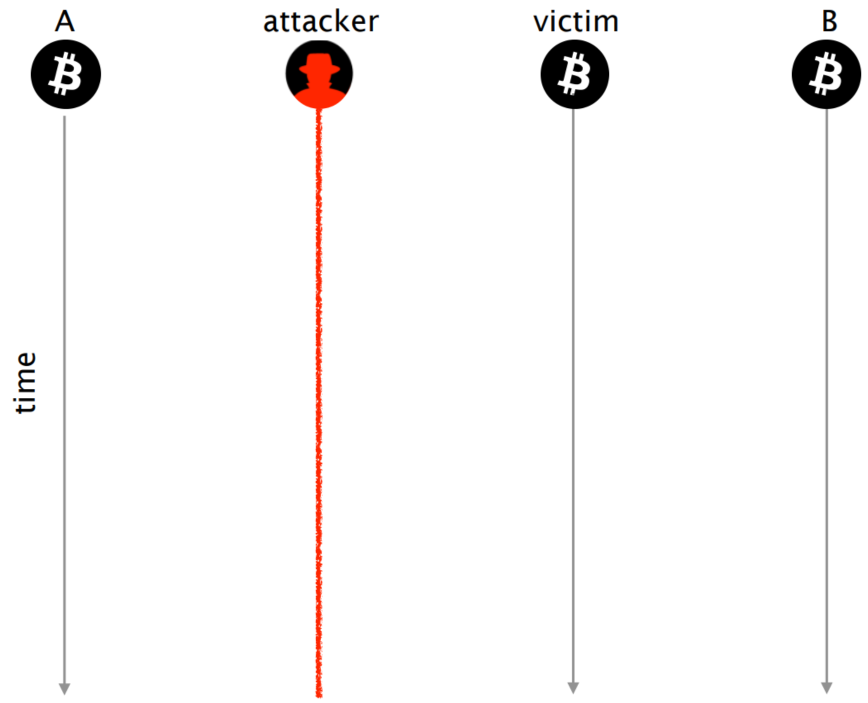
Partition (Evaluation)

- Takes less than 2 minutes for the attacker to intercept all the connections
  - Mitigating hijacks is a human-driven process, and it often takes hours to be resolved



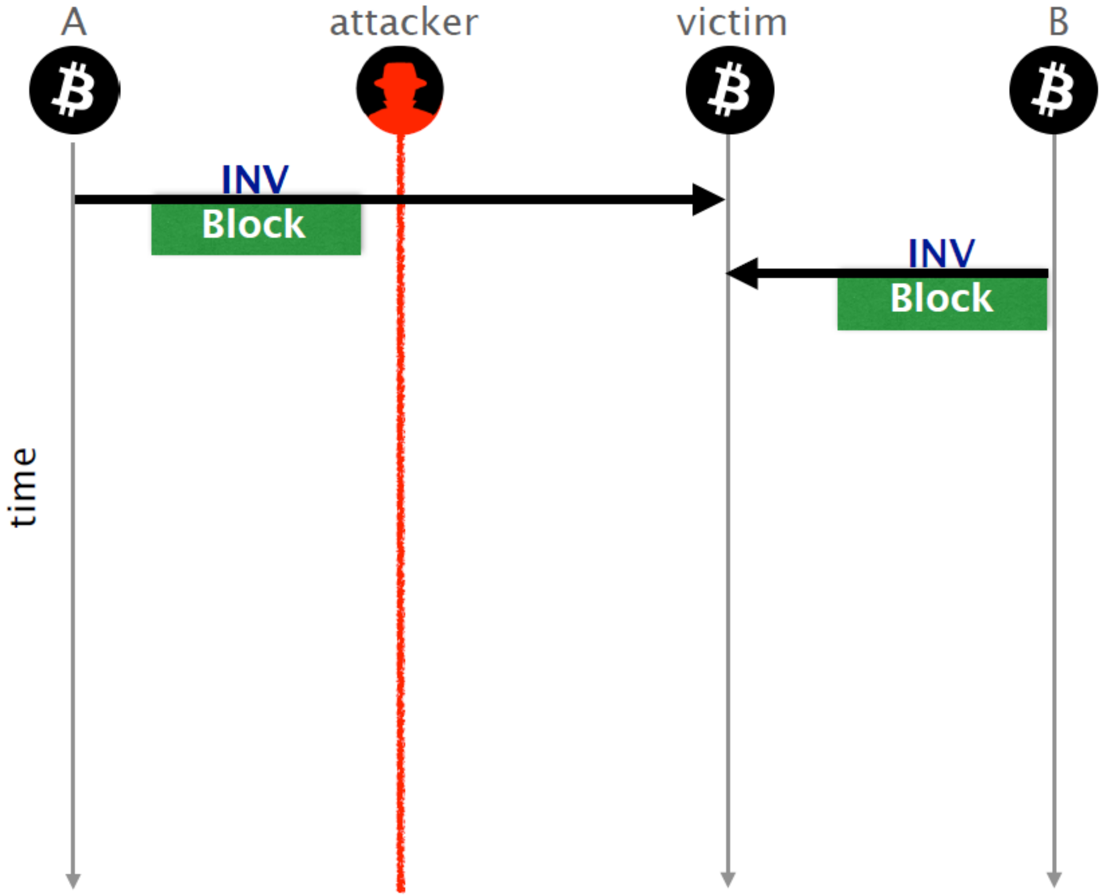
Delay

- The goal of a delay attack is to keep the victim uninformed of the latest block
  - Wide range of exploits such as double spending, revenue losses



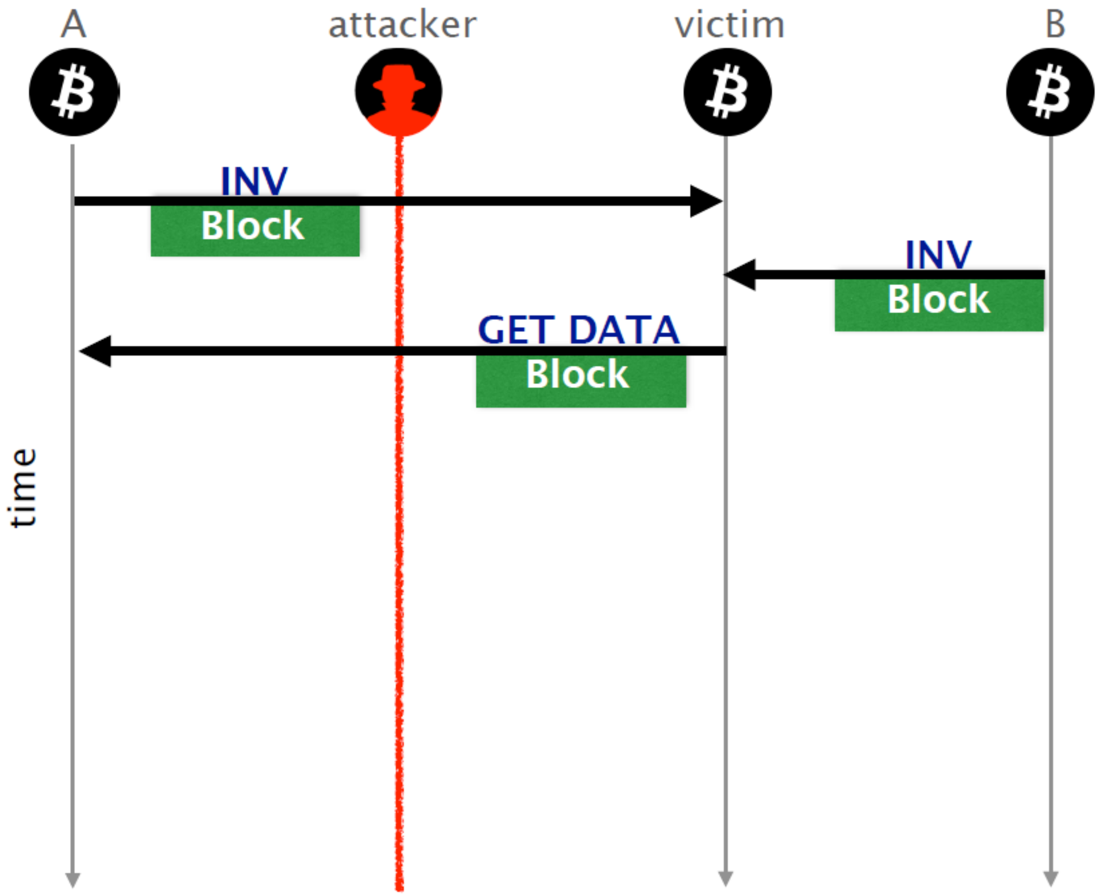
Delay

- The victim receives two advertisements for the block



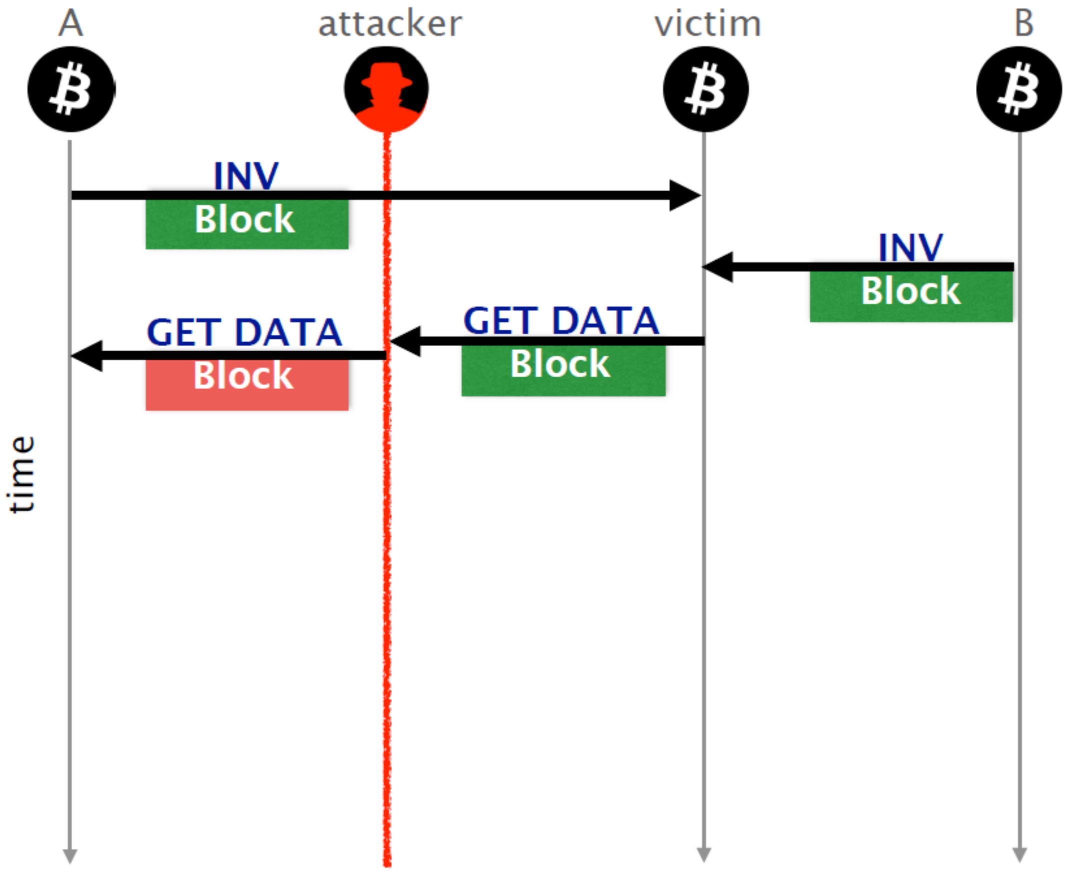
Delay

- The victim requests the block to one of its peer, say A



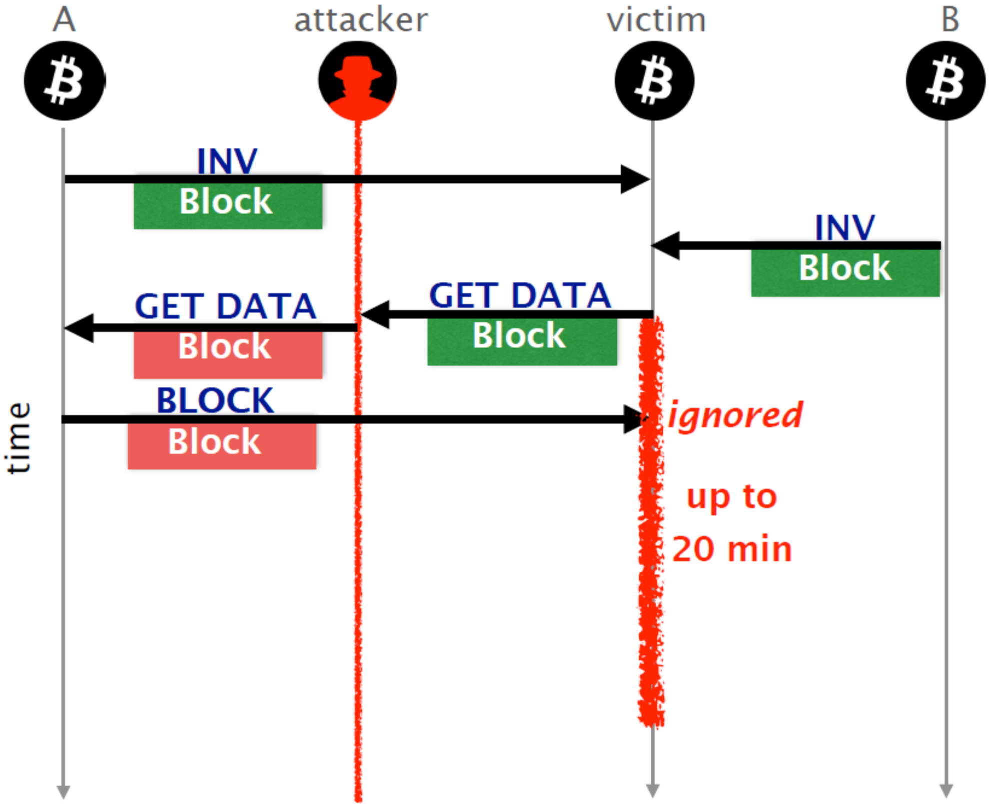
Delay

- Instead, the attacker could intercept the GETDATA and modify its ID of the requested block to trigger the delivery of an older block



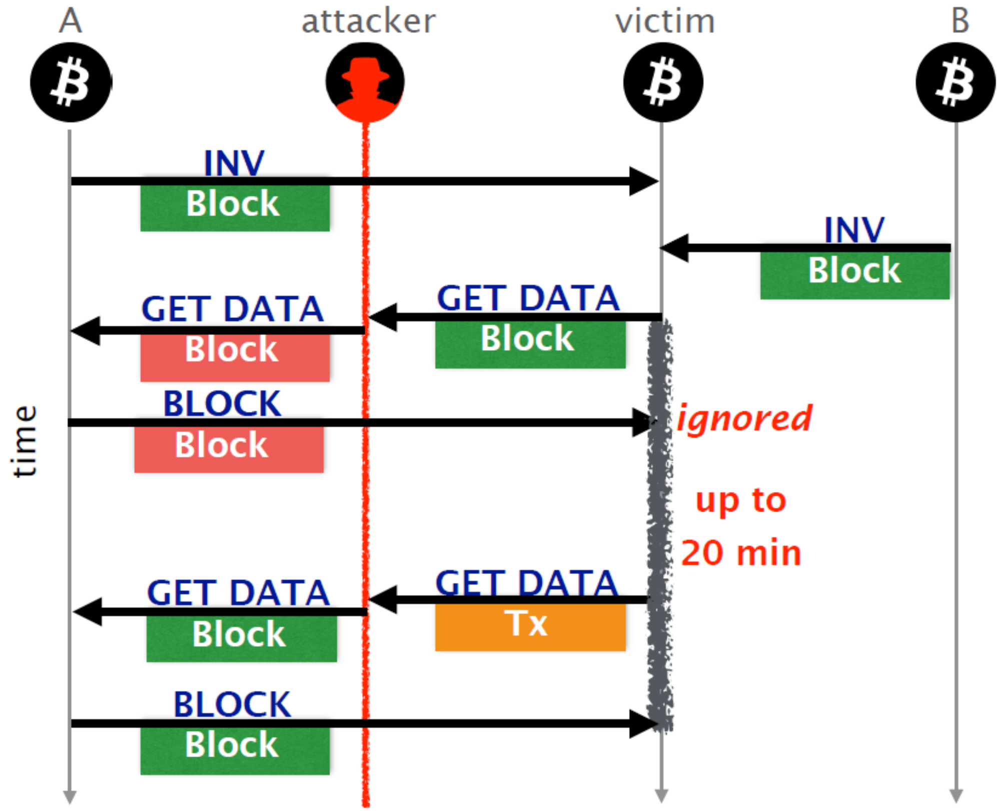
Delay

- The delivery of an older block triggers no error message at the victim
  - The victim will wait for 20 minutes for the actual block to be delivered



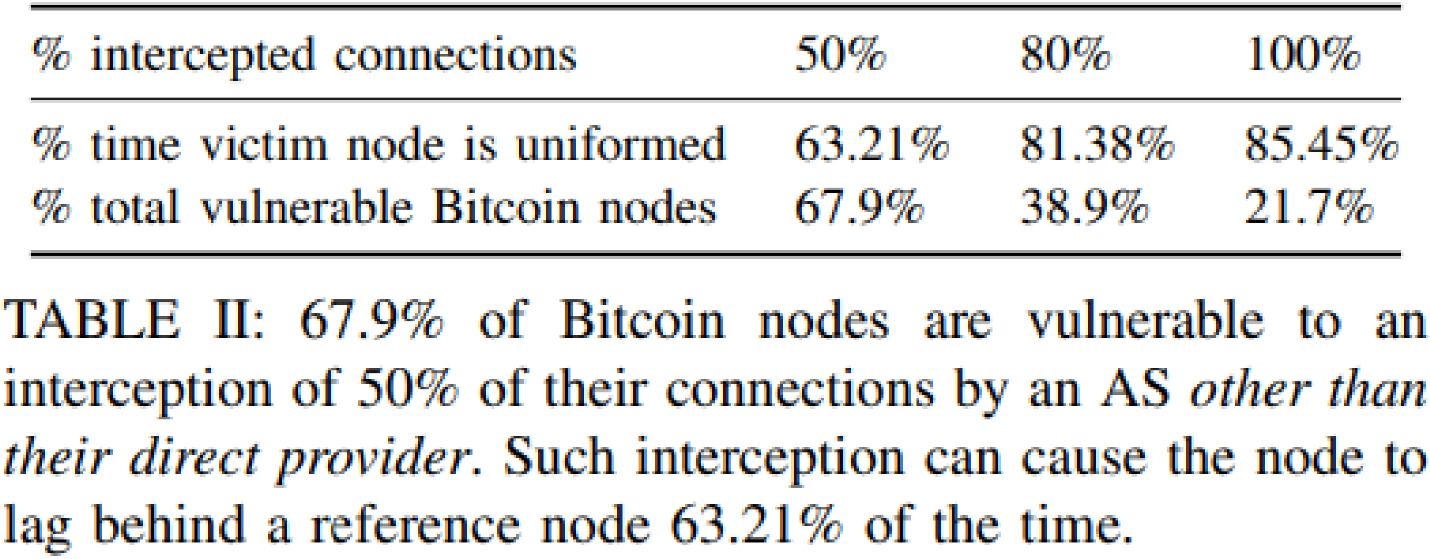
Delay

- The attacker can trigger the block delivery by modifying another GETDATA message
  - The block is delivered before timeout to keep the connection for the next attack



Delay (Evaluation)

- Delay attackers intercepted 50% of connections
    - Effectiveness -> waste 63.21% of a node’s mining power by intercepting 50% of its connections
    - Practicality -> for 67.9% of the nodes, there is at least one AS other than their provider that intercept more than 50% of their connections

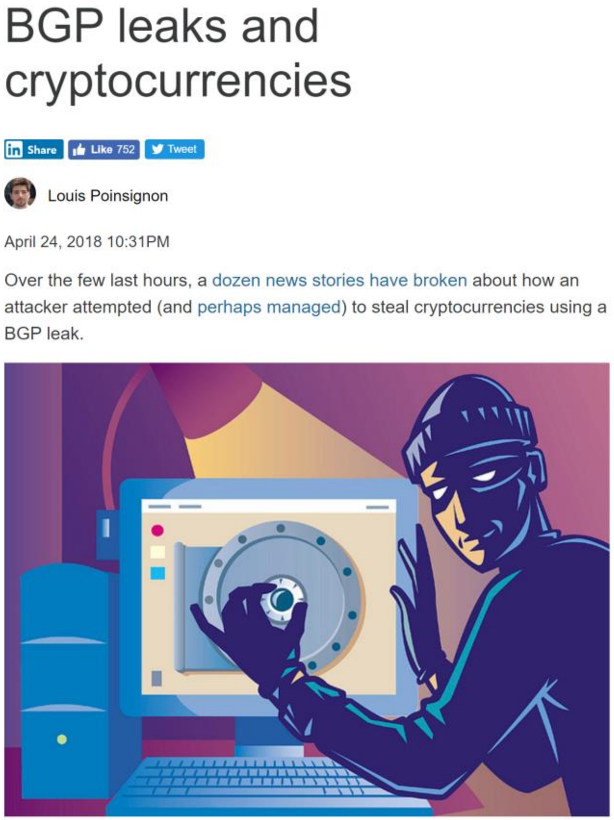


% intercepted connections	50%	80%	100%
% time victim node is uniformed	63.21%	81.38%	85.45%
% total vulnerable Bitcoin nodes	67.9%	38.9%	21.7%

TABLE II: 67.9% of Bitcoin nodes are vulnerable to an interception of 50% of their connections by an AS *other than their direct provider*. Such interception can cause the node to lag behind a reference node 63.21% of the time.

Use case

- Expensive attacks
  - Can earn cash, therefore good ROI

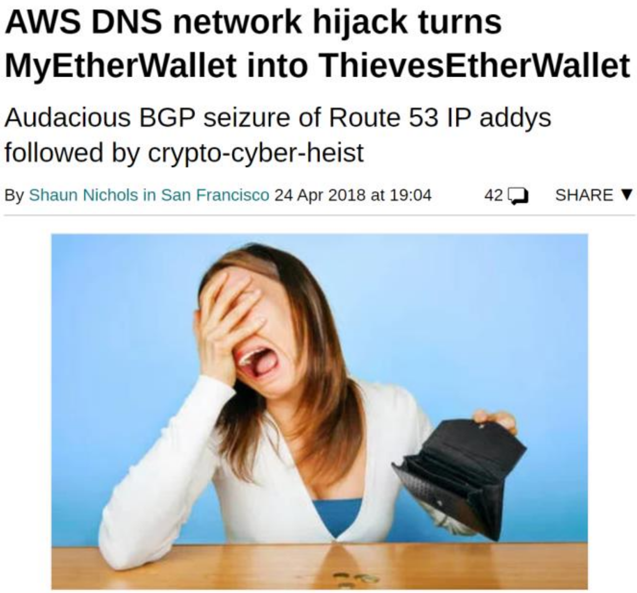


BGP leaks and cryptocurrencies

Louis Poinsignon

April 24, 2018 10:31PM

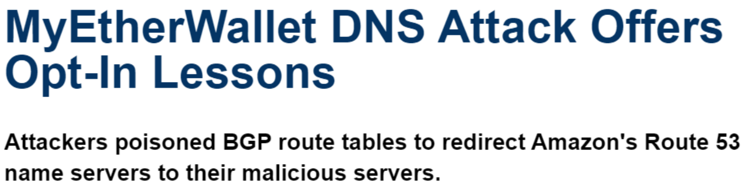
Over the few last hours, a dozen news stories have broken about how an attacker attempted (and perhaps managed) to steal cryptocurrencies using a BGP leak.



AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet

Audacious BGP seizure of Route 53 IP addys followed by crypto-cyber-heist

By Shaun Nichols in San Francisco 24 Apr 2018 at 19:04 42 SHARE ▼



MyEtherWallet DNS Attack Offers Opt-In Lessons

Attackers poisoned BGP route tables to redirect Amazon's Route 53 name servers to their malicious servers.

Defense

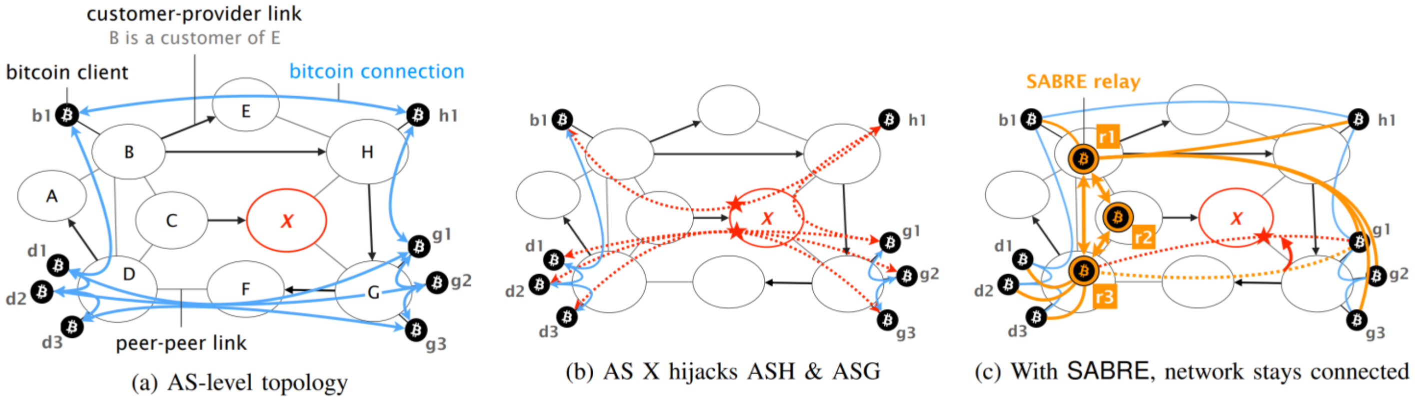
- Short-term
  - Increase the diversity of node connections
  - Select different BGPs not to be isolated
  - Detect changes of RTT due to the hijacking attack
- Long-term
  - Encrypt Bitcoin Communication and/or adopt MAC to Prevent delay attacks
  - Use distinct control and data channels
    - Negotiate a set of random TCP ports to connect each other using the well-known port
    - Use them to establish the actual TCP connection to exchange Bitcoin data

Related Work

- AS-level adversaries
  - Y. Sun, A. Edmundson, L. Vanbever, O. Li, J. Rexford, M. Chiang, and P. Mittal, “RAPTOR: Routing attacks on privacy in TOR.” in USENIX Security, 2015.
  - Routing attacks on a distributed system running atop the Internet
- Bitcoin attacks
  - E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in 24th USENIX Security Symposium (USENIX Security 15), 2015, pp. 129–144.
  - Similar impact than delay attacks when performed against a single node
- BGP security issues
  - X. Shi, Y. Xiang, Z. Wang, X. Yin, and J. Wu, “Detecting prefix hijackings in the Internet with Argus,” ser. IMC ’12. New York, NY, USA: ACM, 2012, pp. 15–28.
  - BGP hijacking

Follow-up paper

- SABRE is an additional overlay network which allows communication, even if the Bitcoin network is partitioned
  - secure relay-to-relay connections
  - remains reachable by Bitcoin clients
  - relay blocks



(a) AS-level topology

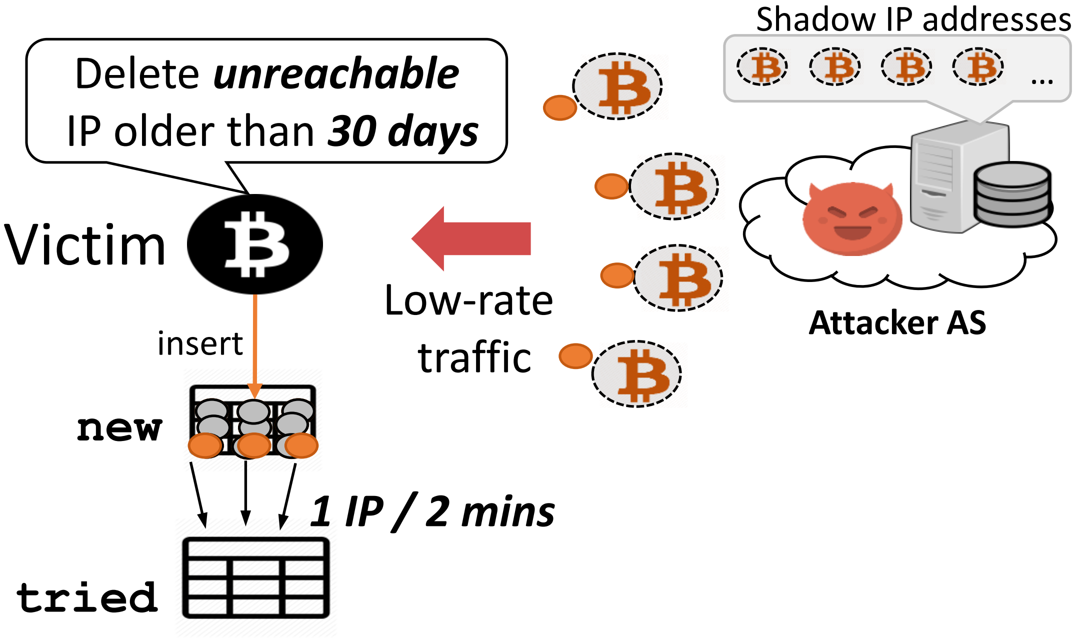
(b) AS X hijacks ASH & ASG

(c) With SABRE, network stays connected

Fig. 2: SABRE protects the Bitcoin network from AS-level adversaries aiming to partition it. Without SABRE, AS X can split the network in half by first diverting traffic destined to AS H and AS G using a BGP hijack and then dropping the corresponding connections (Fig. 2b). With SABRE, the network stays connected (Fig. 2c).

Follow-up paper

- Tran, Muoi, et al. "A stealthier partitioning attack against bitcoin peer-to-peer network." *2020 IEEE Symposium on Security and Privacy (SP)*.
  - attack can isolate Bitcoin nodes in a ***stealthy*** manner
  - Mitigating the Erebus attack is ***hard***
- Tran, Muoi, Akshaye Shenoi, and Min Suk Kang. "On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin."
  - ***Route-Aware Peering :*** peers are selected based on the ***routing paths*** to the peers



QnA

- 오범석 : As I know, there are lots of papers introducing various attacks toward BGP. In this sense, the concept of BGP is easy but has several problems. Was there an attempt to change or develop a better BGP protocol?
  - RPKI, BGPsec
  - But, hard to apply

- 한상구 : SABRE is cited as system that robust against BGP hijacking in other papaers many times, but it seems bitcoin does not implemented this system. Is there any problem to accept this system?
  - No advantage for ISP

- 김경태 : What is the difference between the Eclipse, Erebus attack, and Bitcoin hijacking attack, and countermeasures for each attack?
  - Bitcoin hijacking attack : BGP hijacking
  - Eclipe attack : Permissionless p2p network
  - Erebus attack : Low-traffic and wait

Thanks