Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

Maria Apostolaki [*]
Aviv Zohar [†]
Laurent Vanbever [*]

IEEE S&P ‘17

[*] ETH zürich [†] האוניברסיטה העברית בירושלים THE HEBREW UNIVERSITY OF JERUSALEM

Presenter : Jaehyun Ha

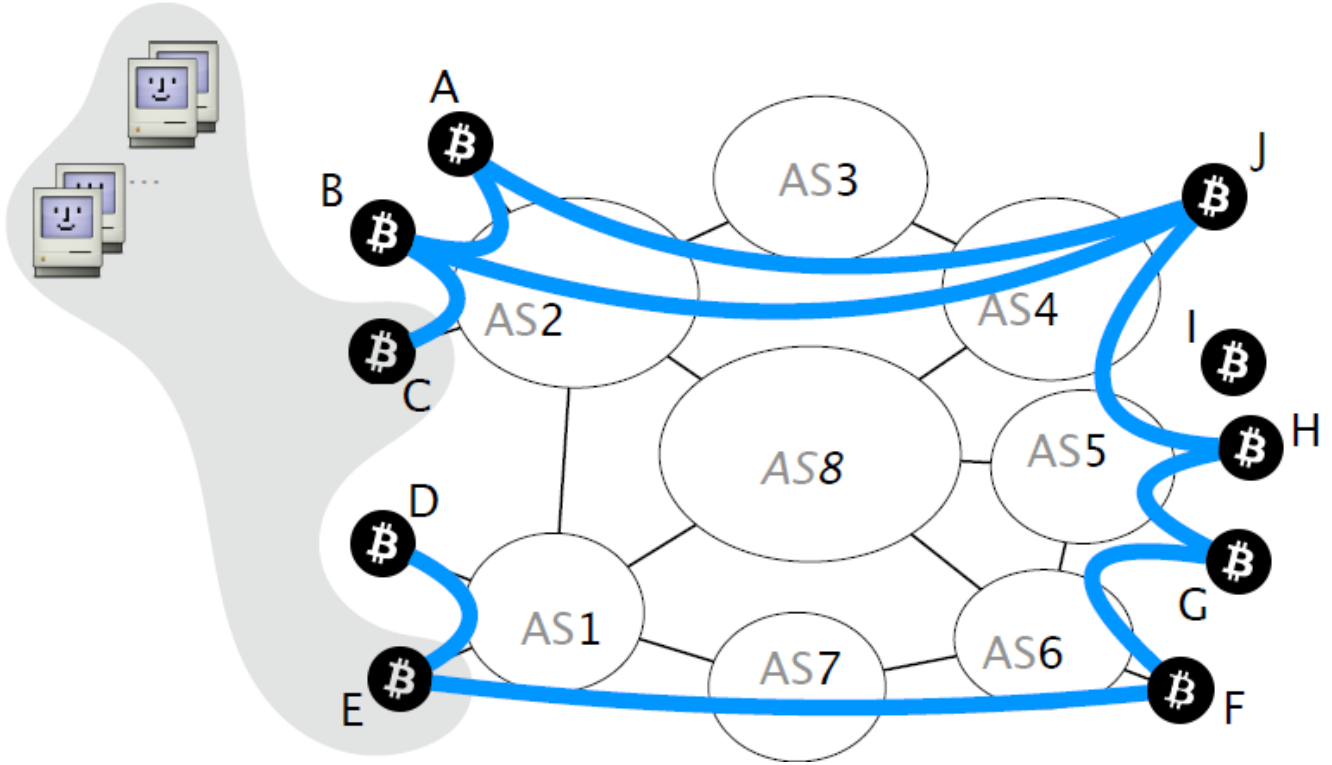
NetS&P Research Lab @ KAIST

Is Bitcoin robust against routing attacks?

Backgrounds

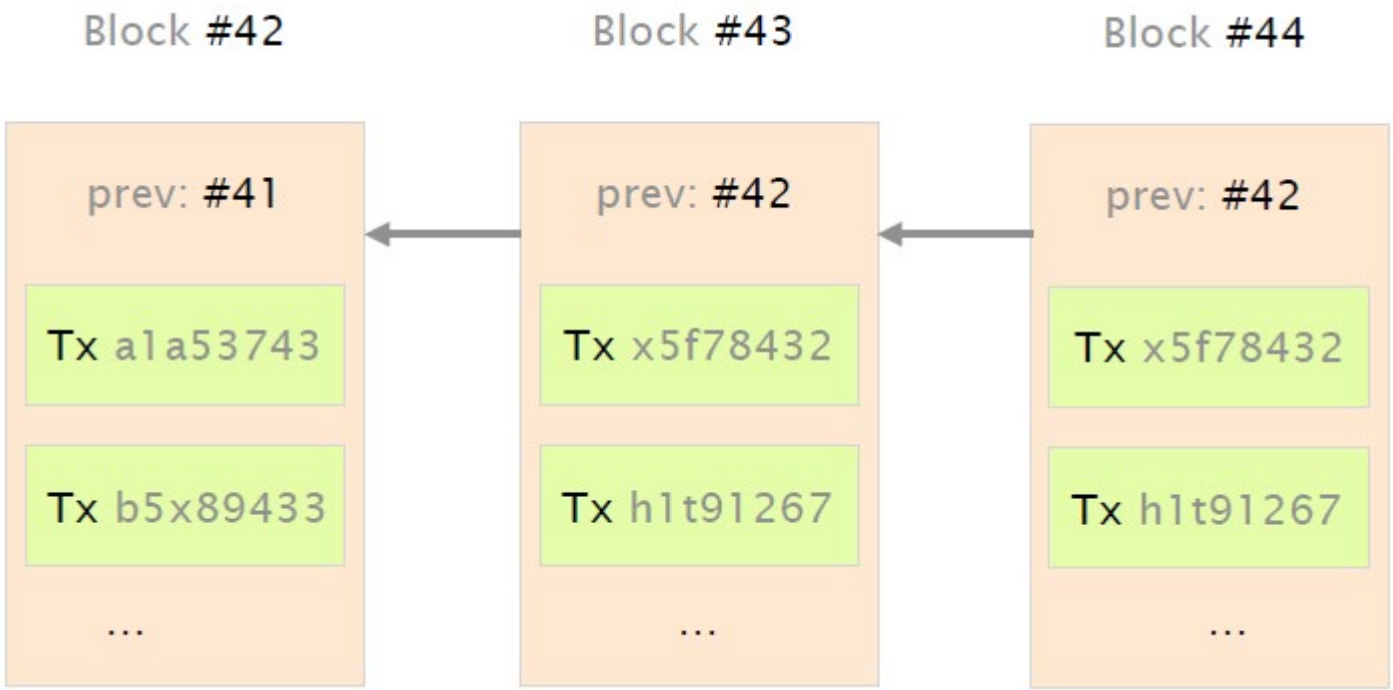
Background: Bitcoin

- **Bitcoin** is a distributed network of nodes, where each nodes establish random connections between each other (highly decentralized in theory)
- Bitcoin connections are routed over the internet, using BGP



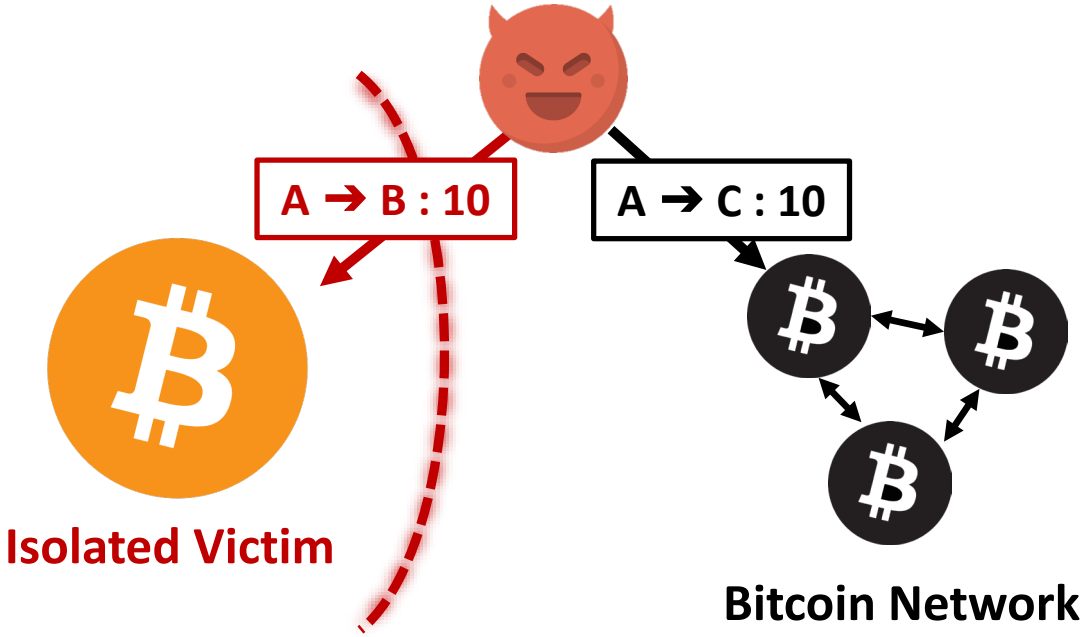
Background: Bitcoin

- Each node keeps a ledger of all transactions ever performed : “the blockchain”
- Transactions are stored in block, and blockchain is a chain of blocks
- Blockchain is extended by miners, which follow consensus rules (PoW)



Background: Bitcoin Partitioning Attacks

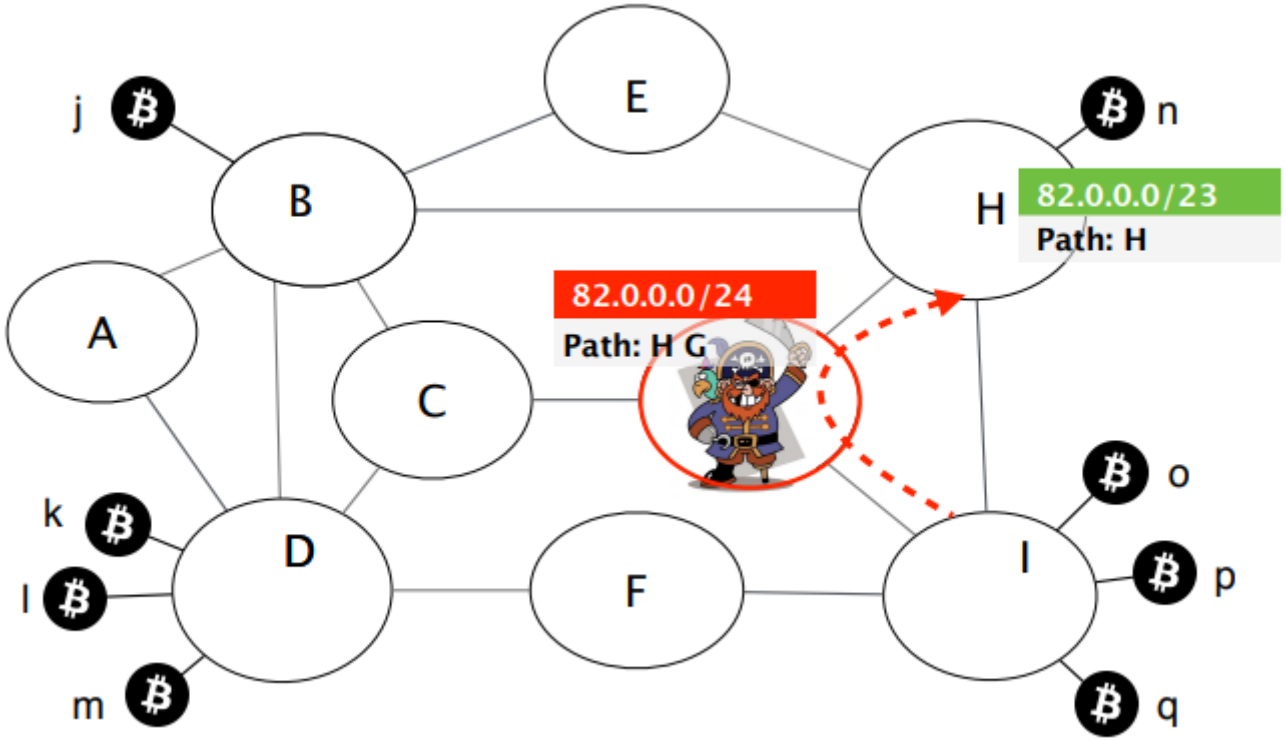
- **Partitioning Attacks** isolates a (set of) victim bitcoin nodes from the rest of the Bitcoin Network
- Partitioning enables/improves extra exploitations (e.g., Double spending, selfish mining)



Double-spending attack

Background: Routing Attacks

- **Routing Attack:** An attack on the Internet Service Provider level to affect uptime or participation in a web-enabled system



BGP-Hijacking

Is Bitcoin robust against routing attacks?

Yes…? Because

- Bitcoin is highly decentralized
- Hard for few malicious ASes to partition targets

Is Bitcoin robust against routing attacks?

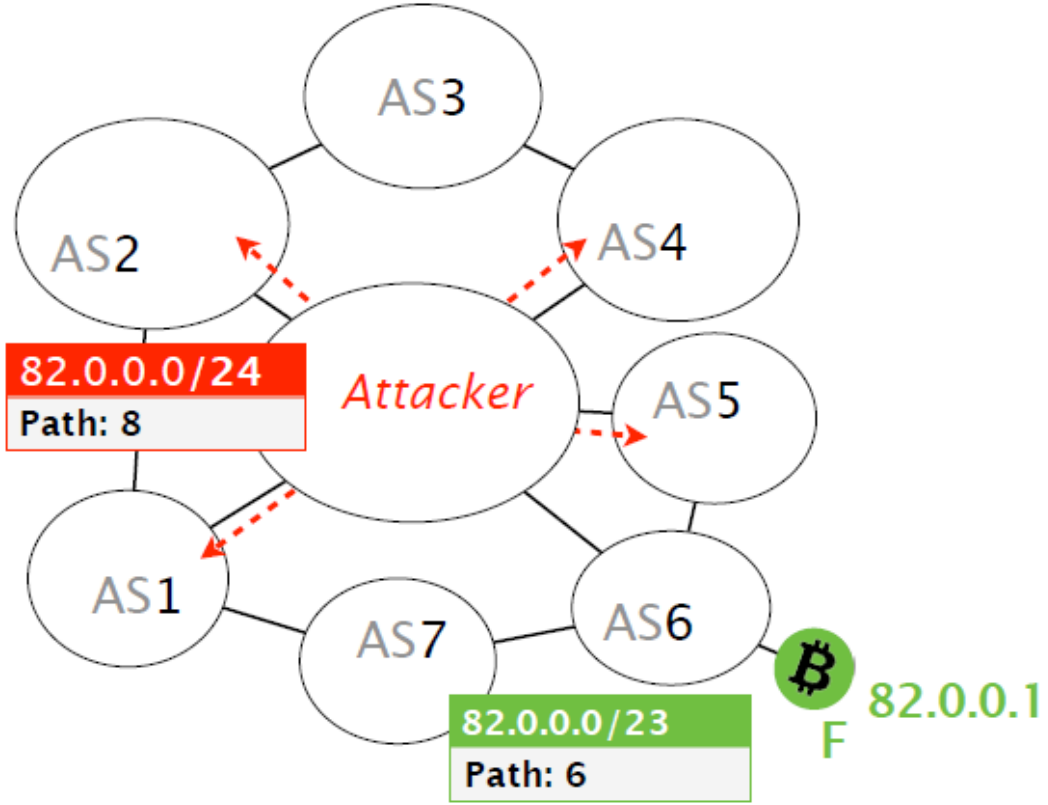
Authors' answer : No.

- In practice, Bitcoin is highly centralized
- Bitcoin messages are propagated unencrypted

Vulnerabilities

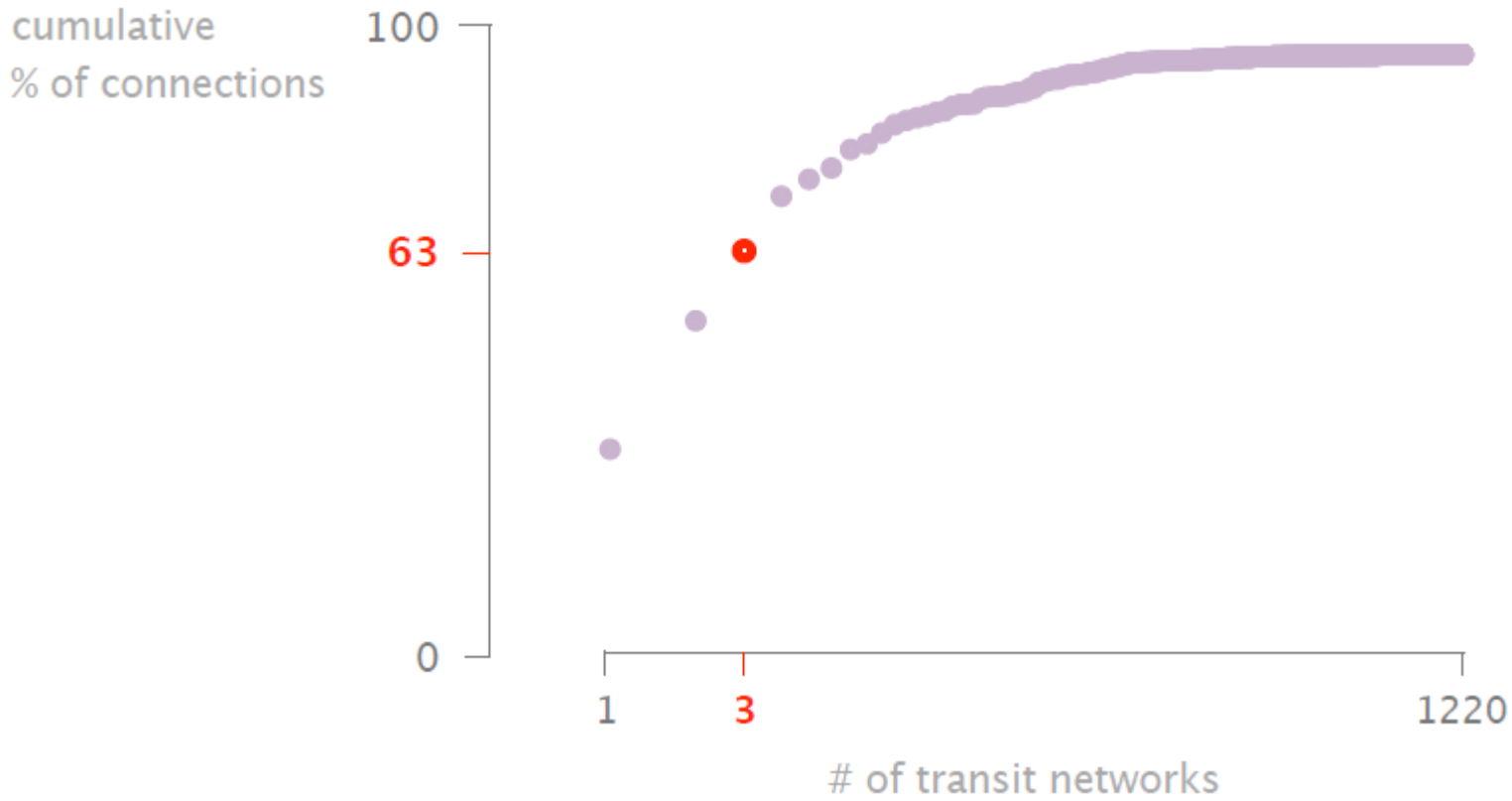
Vulnerabilities (1) : Internet Routing Vulnerability

- BGP does not check the validity of advertisements
- Attacker can hijack the traffic by advertising more specific prefixes



Vulnerabilities (2) : Bitcoin is highly centralized

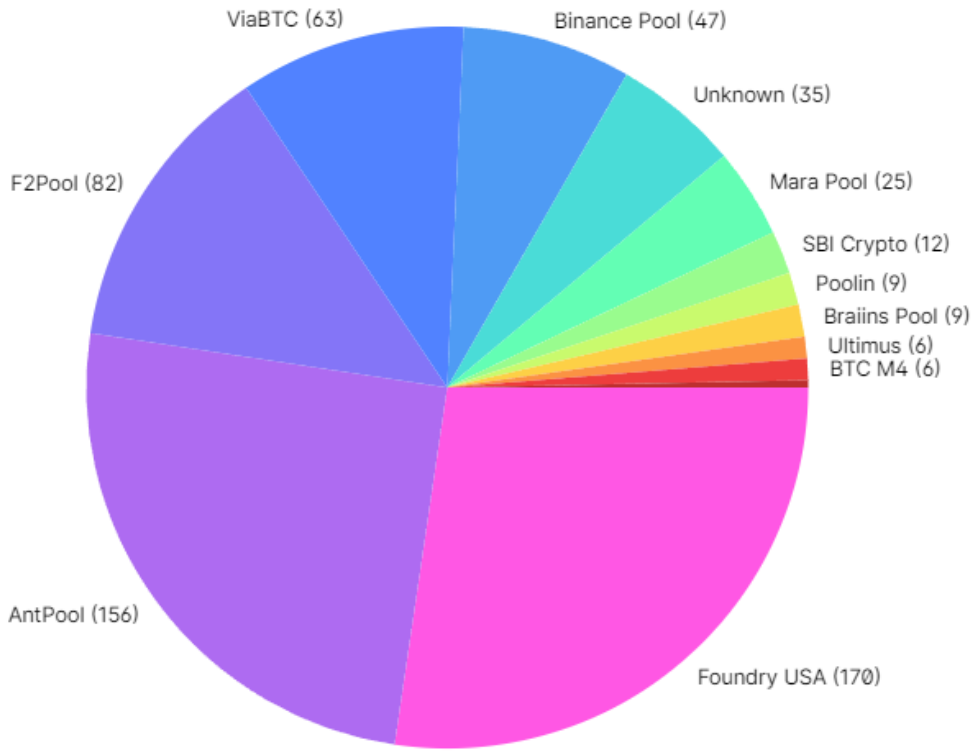
- Bitcoin is highly centralized both from routing and mining viewpoint



3 transit networks see more than 60% of all connections

Vulnerabilities (2) : Bitcoin is highly centralized

- Bitcoin is highly centralized both from routing and mining viewpoint

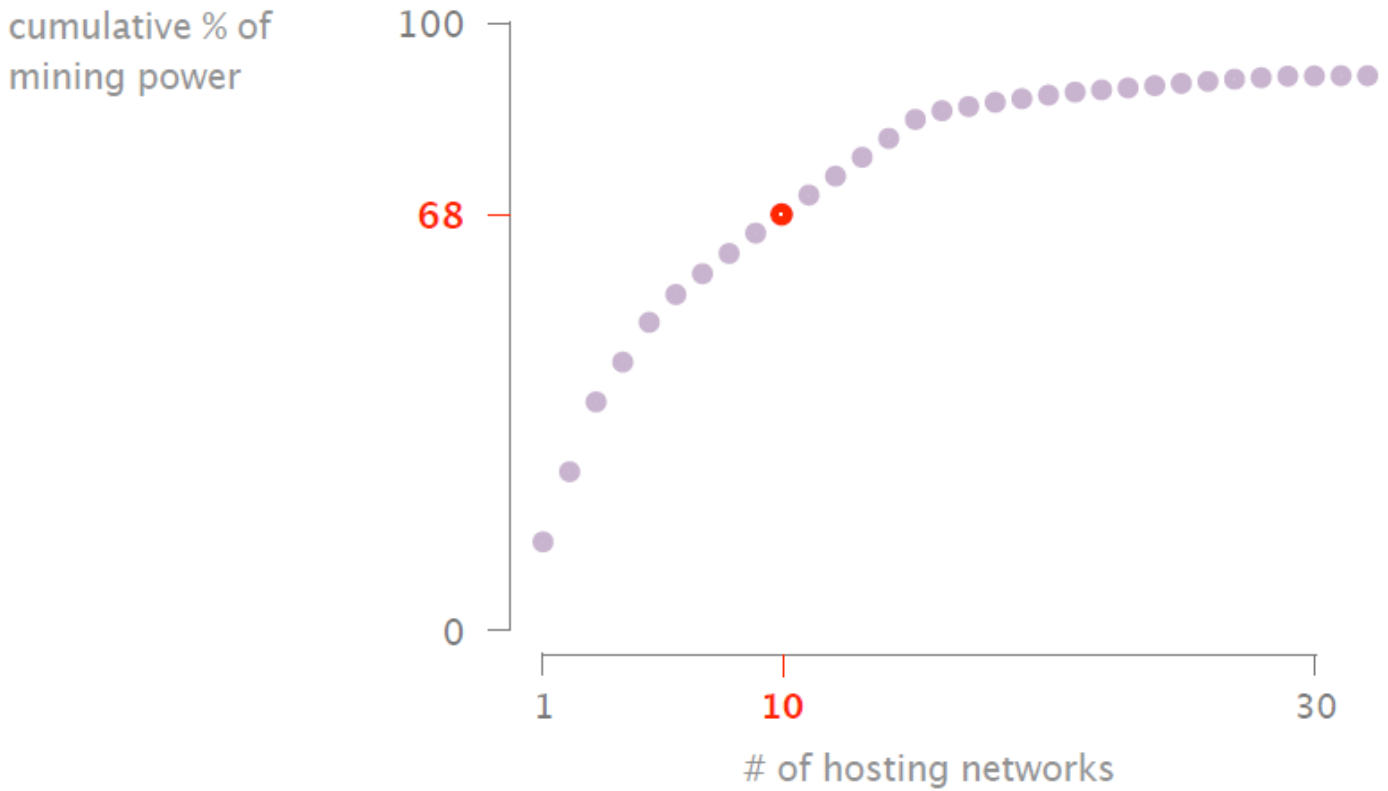


3 mining pools have 65% mining power*

*https://www.blockchain.com/explorer/charts/pools (2023.10.11)

Vulnerabilities (2) : Bitcoin is highly centralized

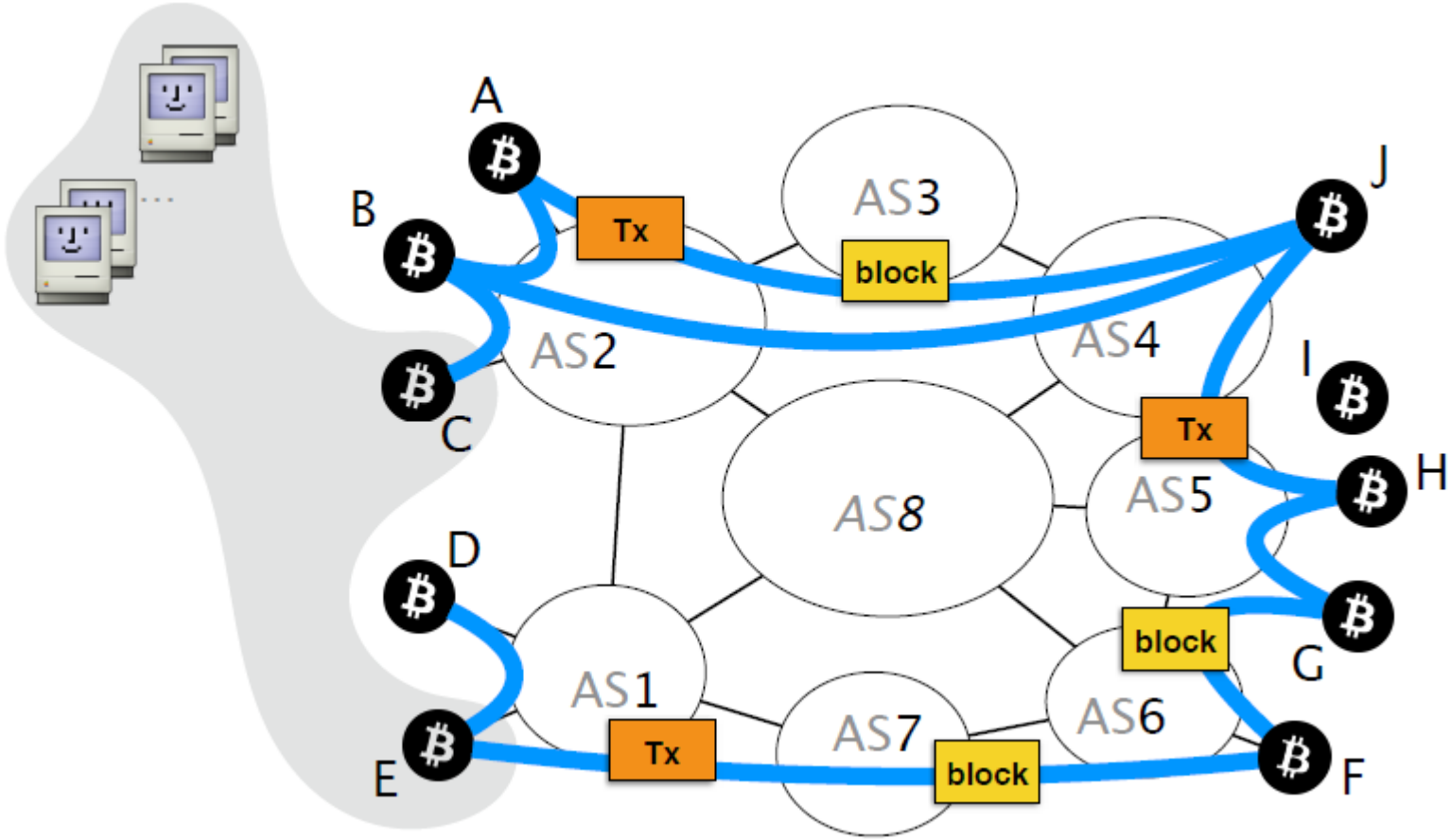
- Bitcoin is highly centralized both from routing and mining viewpoint



68% of mining power is hosted in 10 networks

Vulnerabilities (3) : Bitcoin Protocol Vulnerability

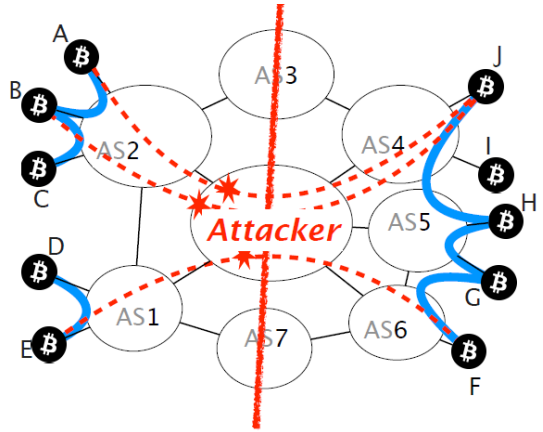
- Bitcoin messages are propagated without encryption & integrity guarantees



Exploitations (Attacks)

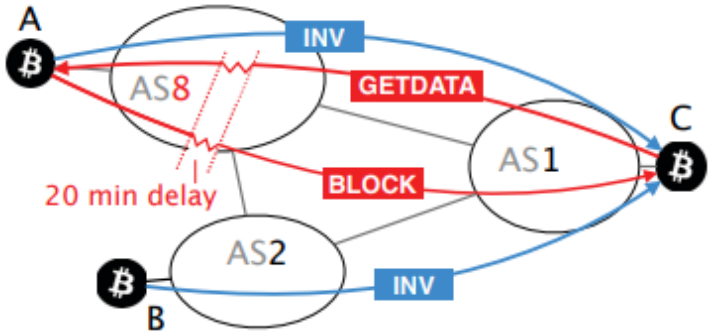
Exploitations

- Authors claim that two different types of routing attacks are possible due to Bitcoin's vulnerabilities



Partitioning attack:

- ✓ Visible
- ✓ Network-wide attack
- ➢ Exploiting significant centralization

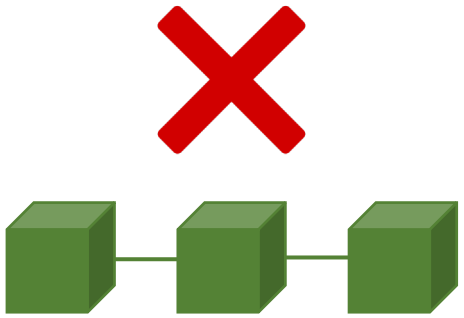


Delay attack:

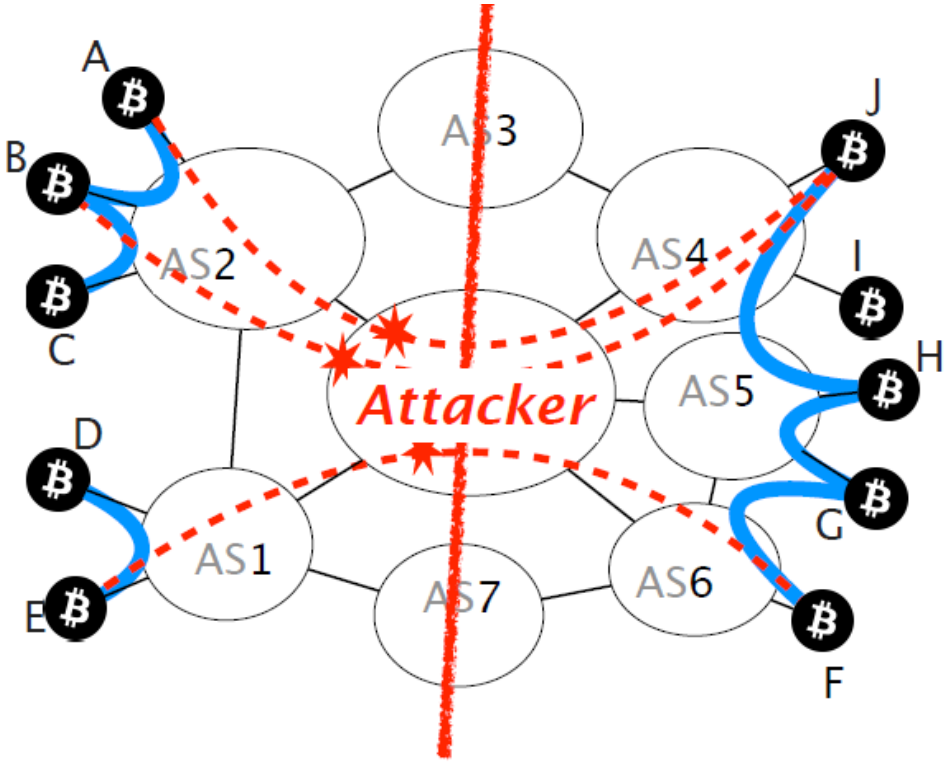
- ✓ Invisible
- ✓ Targeted attack
- ➢ Exploiting un-encryption & no integrity guarantee

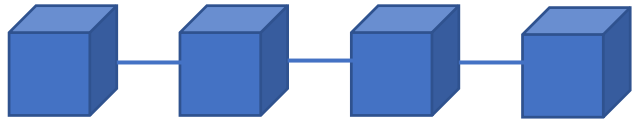
Exploitations (1) : Partitioning attack

- Goal: To split the bitcoin network into two disjoint components
- Impact: DoS, Revenue Loss, Double spending



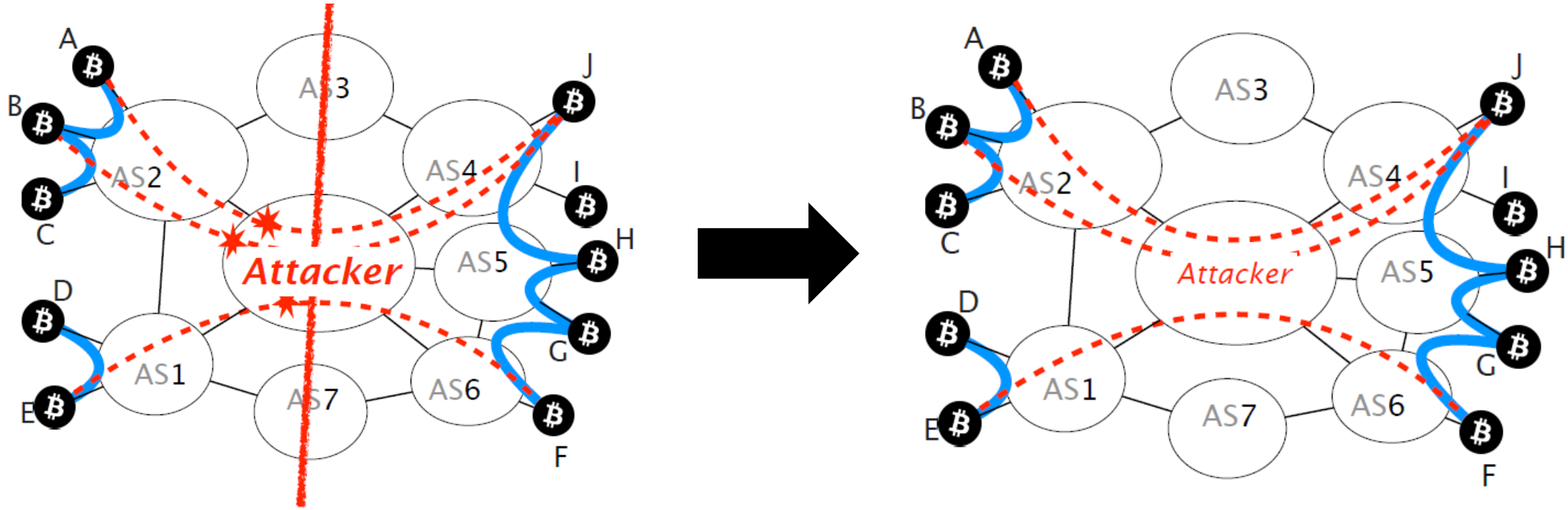
Shorter chain will be discarded
Tx becomes invalid





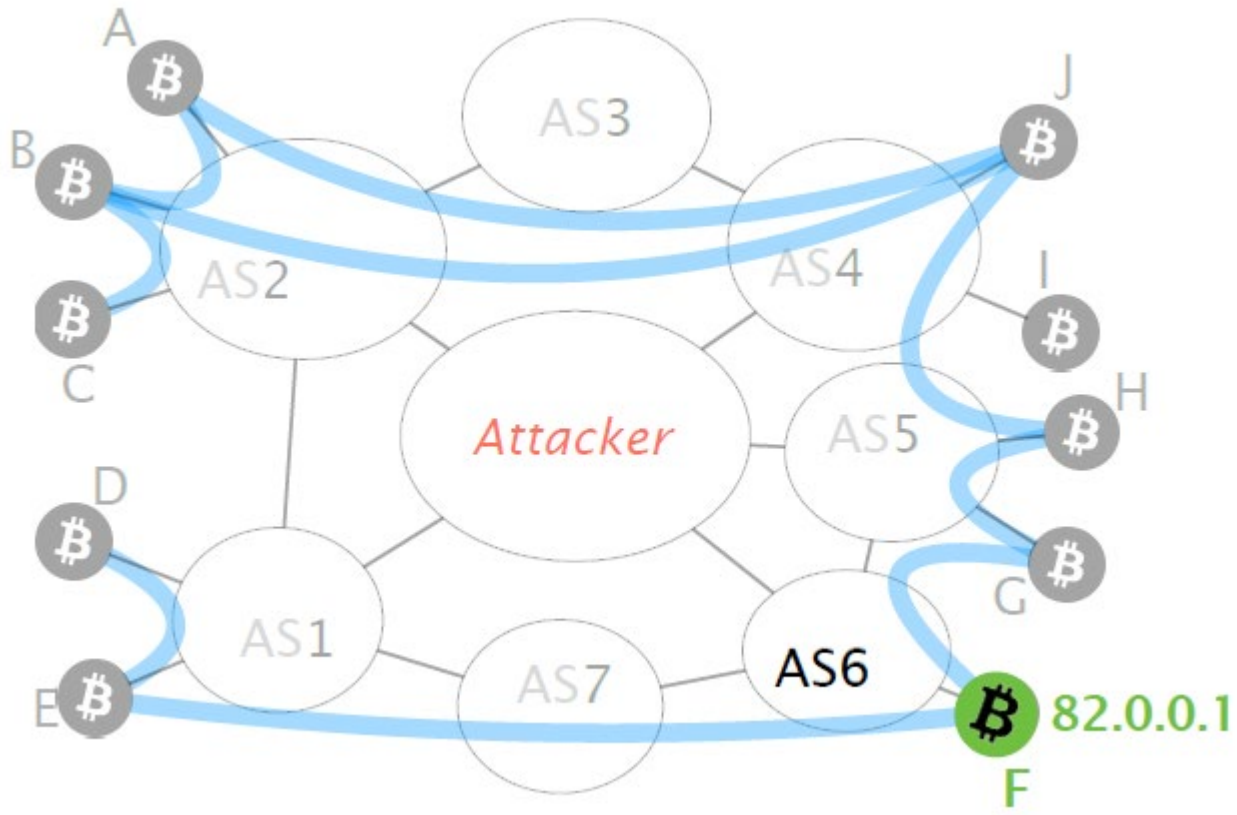
Exploitations (1) : Partitioning attack

- Let's say an attacker wants to partition the network into the left and right side
- For doing so, the attacker will manipulate BGP routes to intercept any traffic between two sides



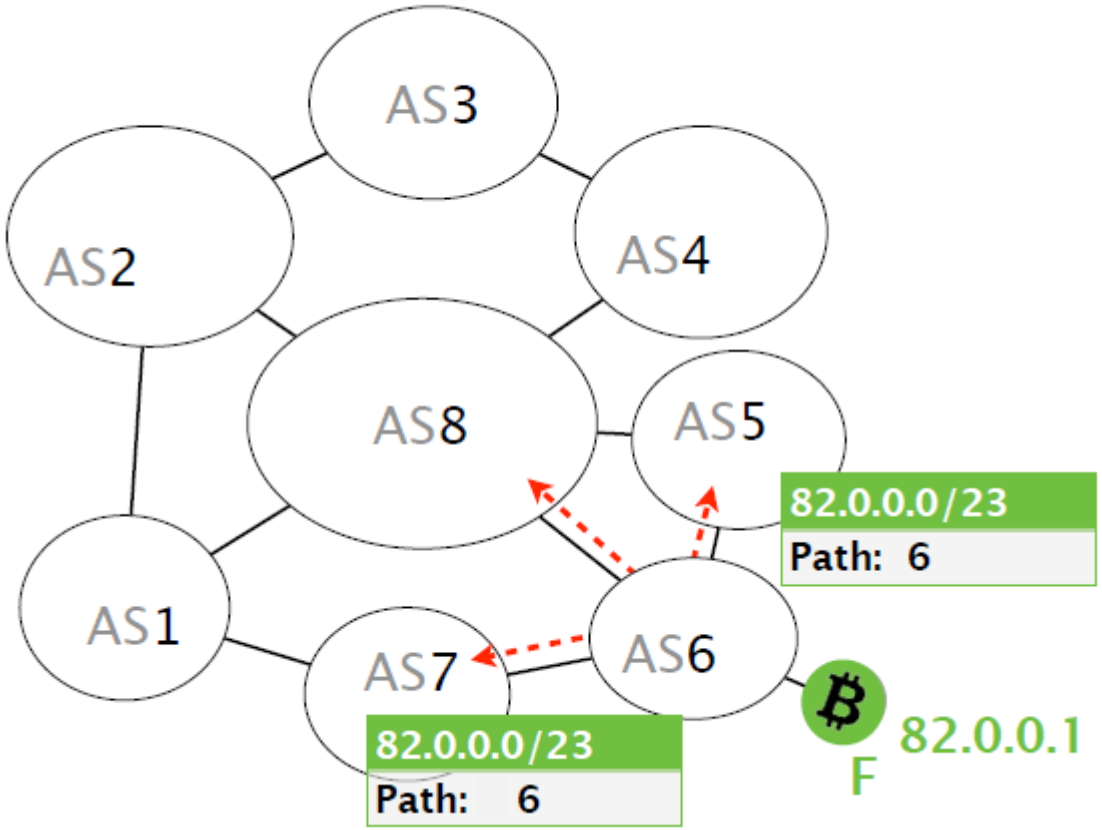
Exploitations (1) : Partitioning attack

- Let’s focus on F (hijacking victim) and AS6 (responsible for IP prefix)



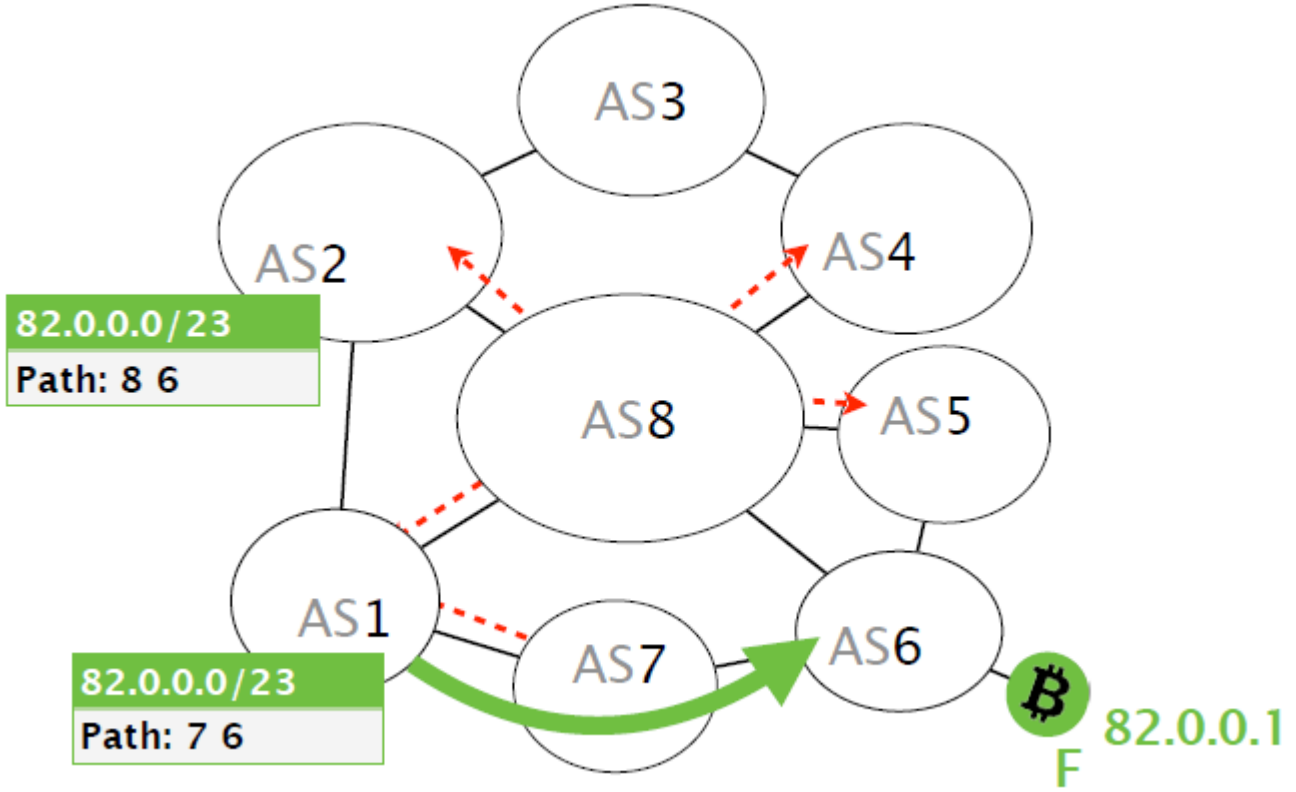
Exploitations (1) : Partitioning attack

- AS6 will create a BGP advertisement with /23 prefix



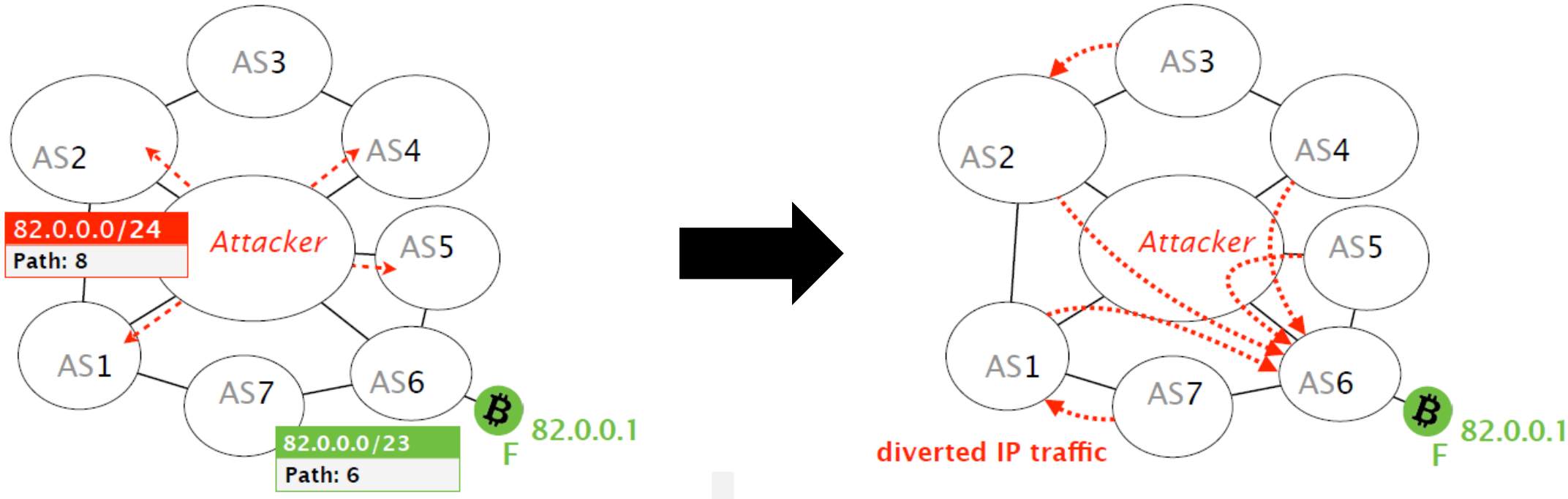
Exploitations (1) : Partitioning attack

- AS6's advertisement is propagated AS-by-AS until all ASes learn about it.
- Note: BGP does not check the validity of advertisements



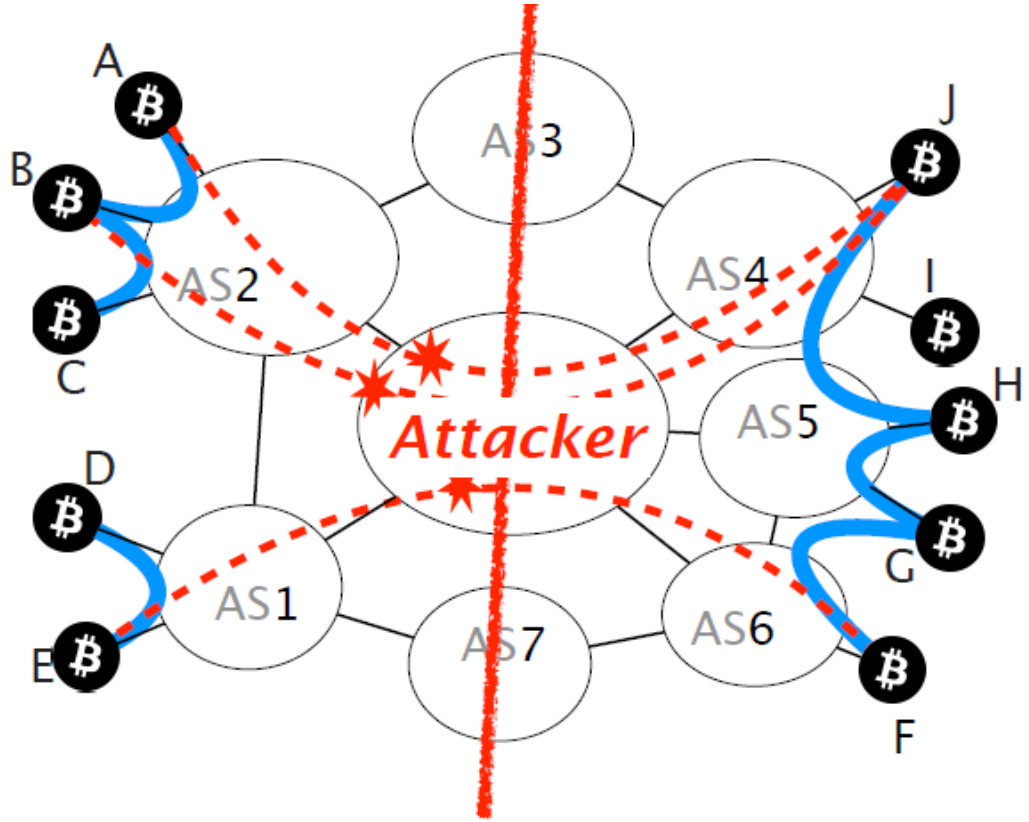
Exploitations (1) : Partitioning attack

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



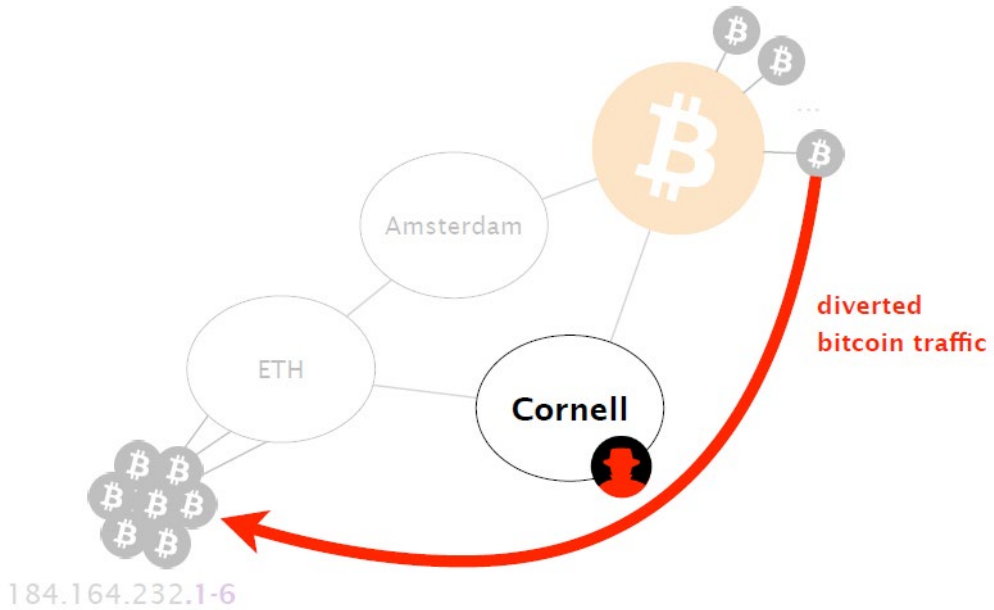
Exploitations (1) : Partitioning attack

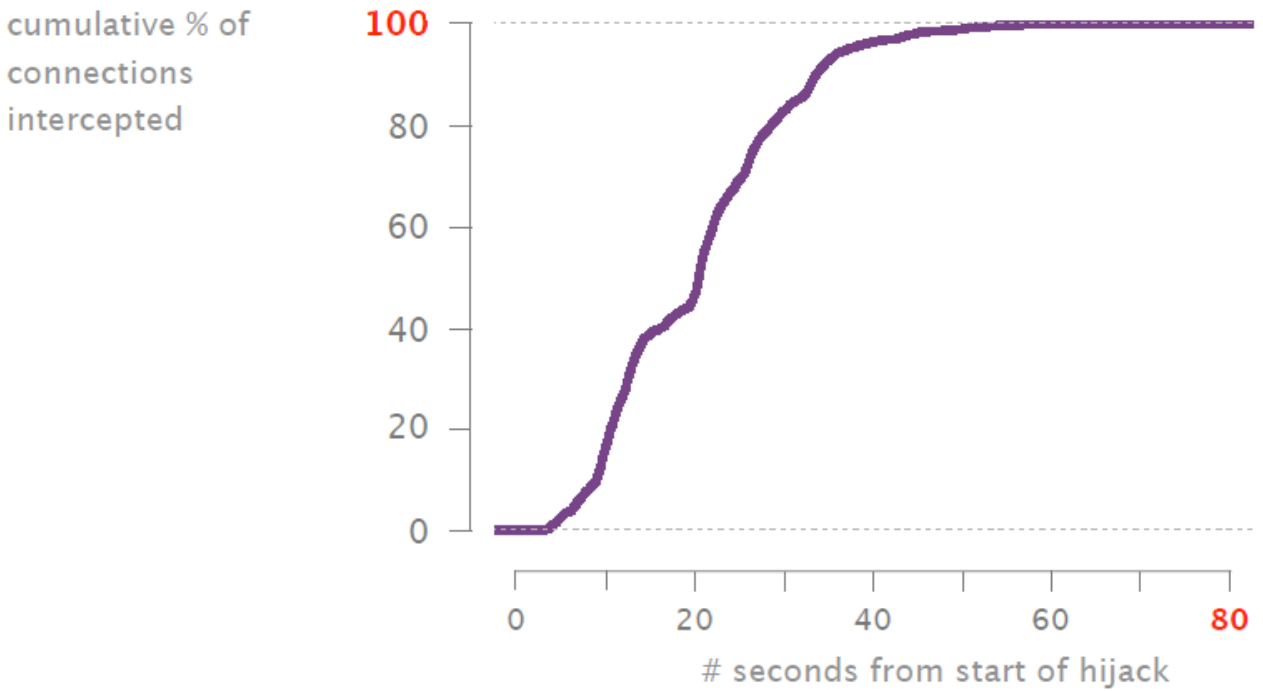
- By hijacking the IP prefixes pertaining to the right nodes, the attacker can intercept all their connection and drop it : partition created!



Exploitations (1): Partitioning attack - Evaluation

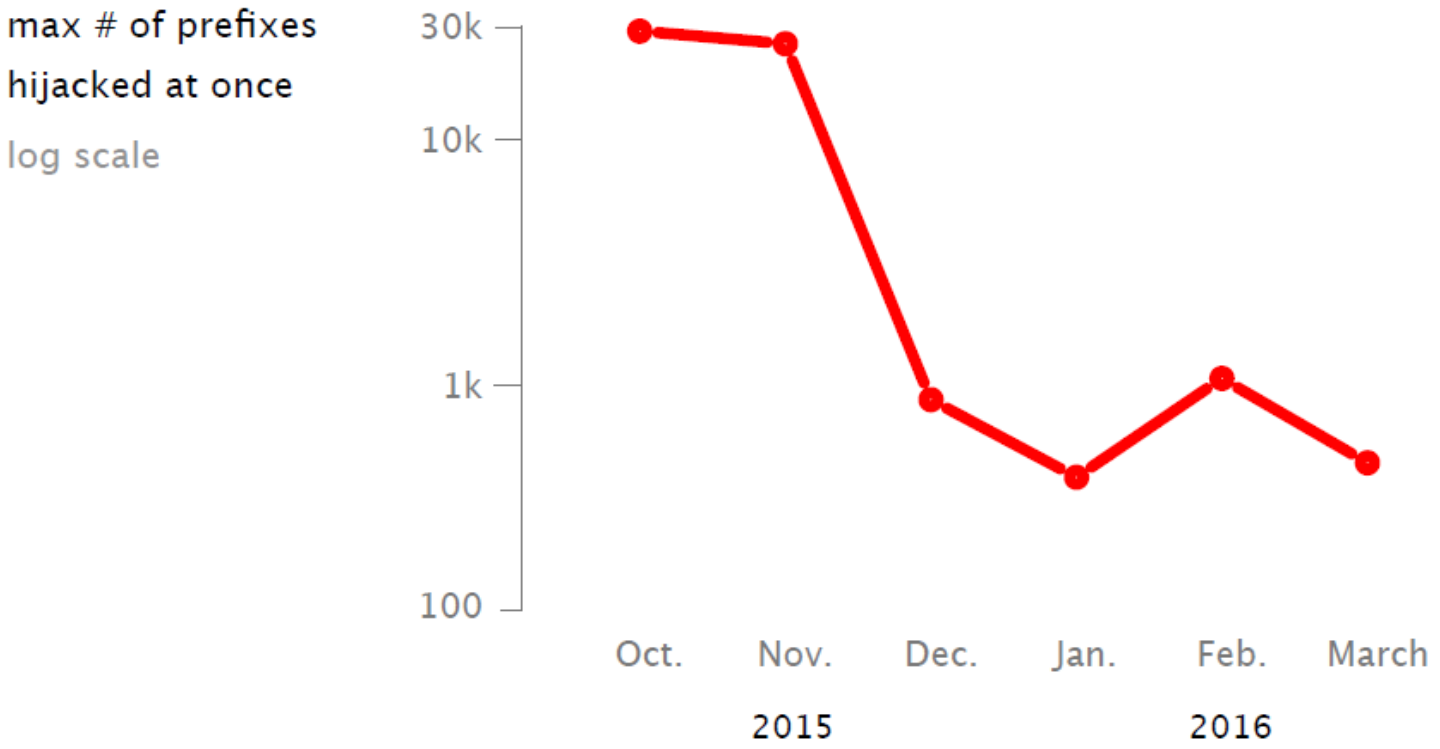
- **Time efficiency**: Took less than 2 minutes for the attacker to intercept all the connection





Exploitations (1): Partitioning attack - Evaluation

- **Practicality:** Splitting the mining power to half can be done by hijacking less than 100 prefixes



Exploitations (2): Delay attack

- Goal: To keep victim uninformed of the latest block

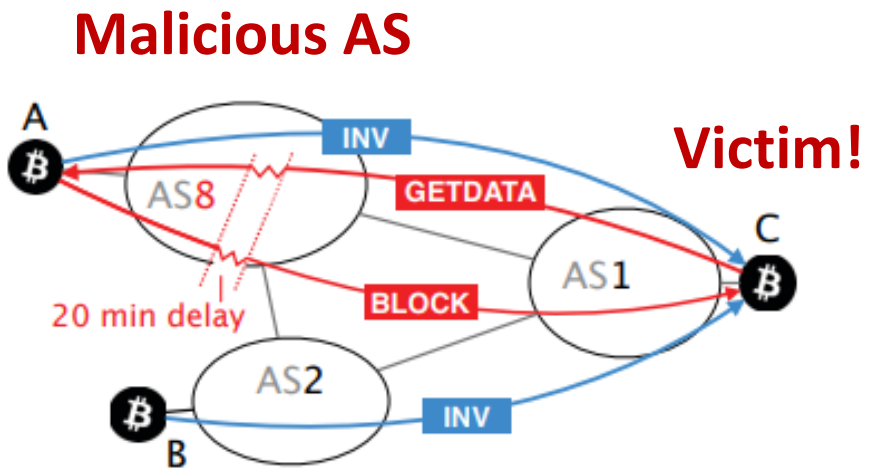


Fig. 2: Illustration of how an AS-level adversary (AS8) which naturally intercepts a part of the traffic can delay the delivery of a block for 20 minutes to a victim node (C).

Impact?

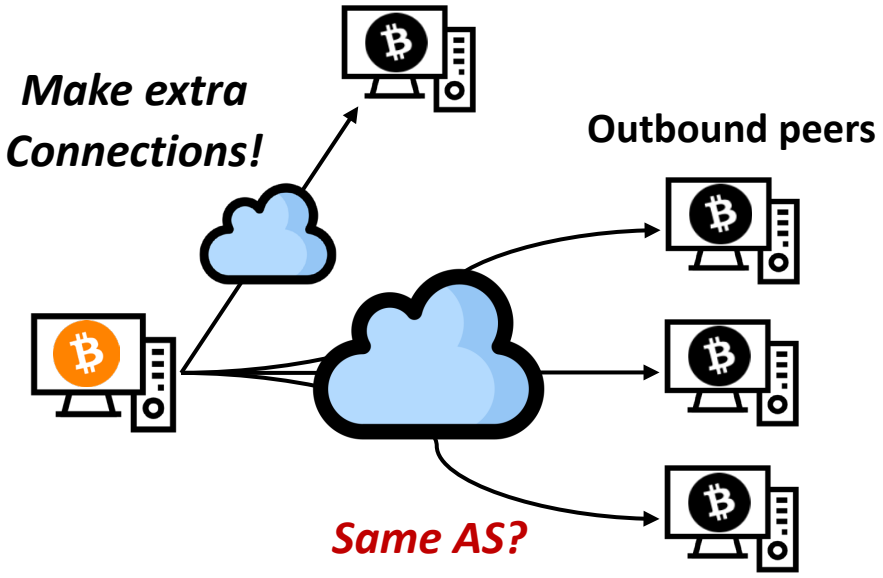
- Susceptible to be the victim of double-spending attacks
- Waste their mining power by mining on obsolete chain
- Unable to collaborate with p2p network

Countermeasures (Defenses)

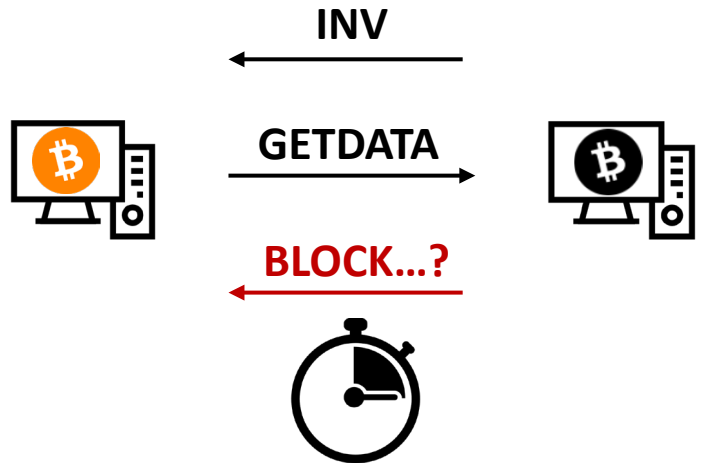
Countermeasures (1): Short-term

Short-term countermeasures

- Simple shifts in the Bitcoin clients (does not require protocol change)



Routing-aware peer selection

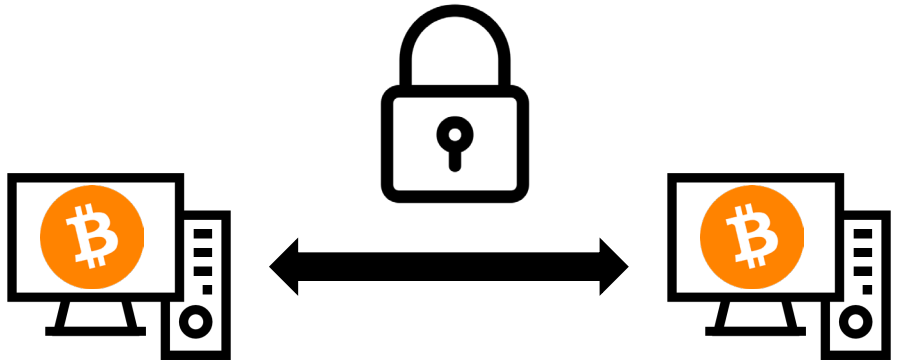


Monitoring anomalies

Countermeasures (2): Long-term

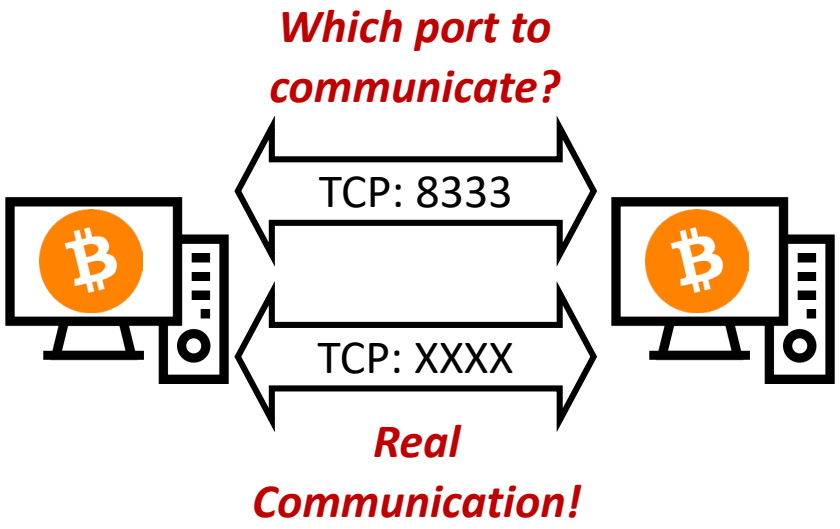
Long-term countermeasures

- Provide more guarantees, but require protocol or infrastructure changes



Use end-to-end encryption or MAC

(prevent delay attacks)

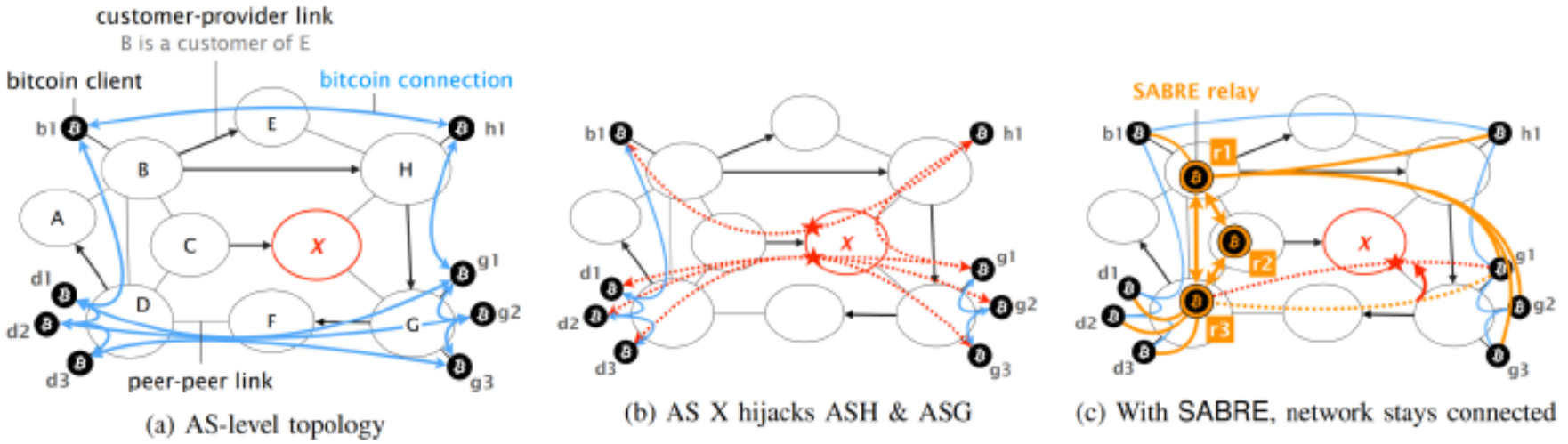


Use distinct control/data channels

(prevent partitioning attacks)

Countermeasures (3): SABRE

- Additional overlay network which allows communication, even when the Bitcoin network is partitioned
- Secure relay-to-relay connections
- Remains reachable by Bitcoin clients
- Relay blocks seamlessly



(a) AS-level topology

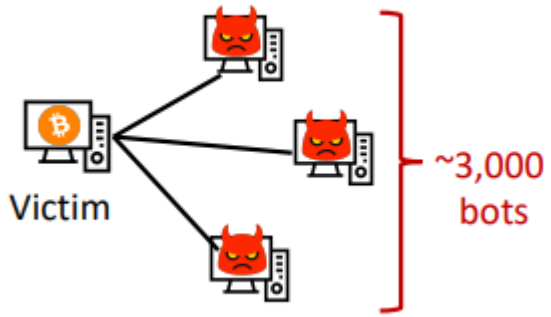
(b) AS X hijacks ASH & ASG

(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).

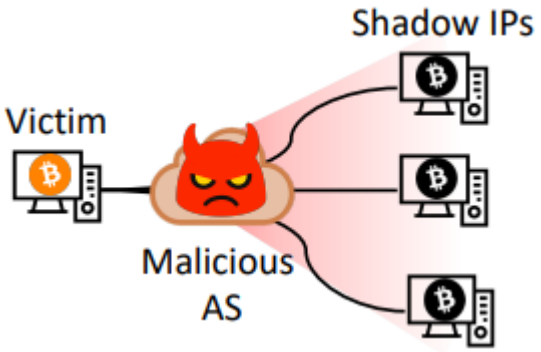
Related Works

Recent ***Partitioning attacks*** against Bitcoin



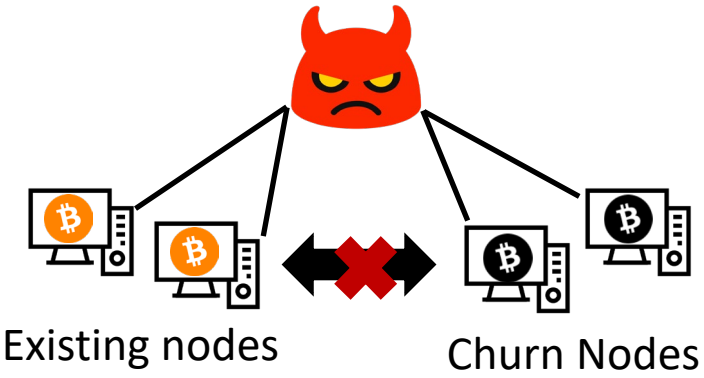
Botnet-based eclipse attack:

- ✓ E. Heilman et al. *[USENIX '15]*
- ➢ Connection starvation attack using botnets



EREBUS attack:

- ✓ M. Tran et al. *[IEEE S&P '20]*
- ➢ Stealthier MITM Routing attack exploiting the topological advantage



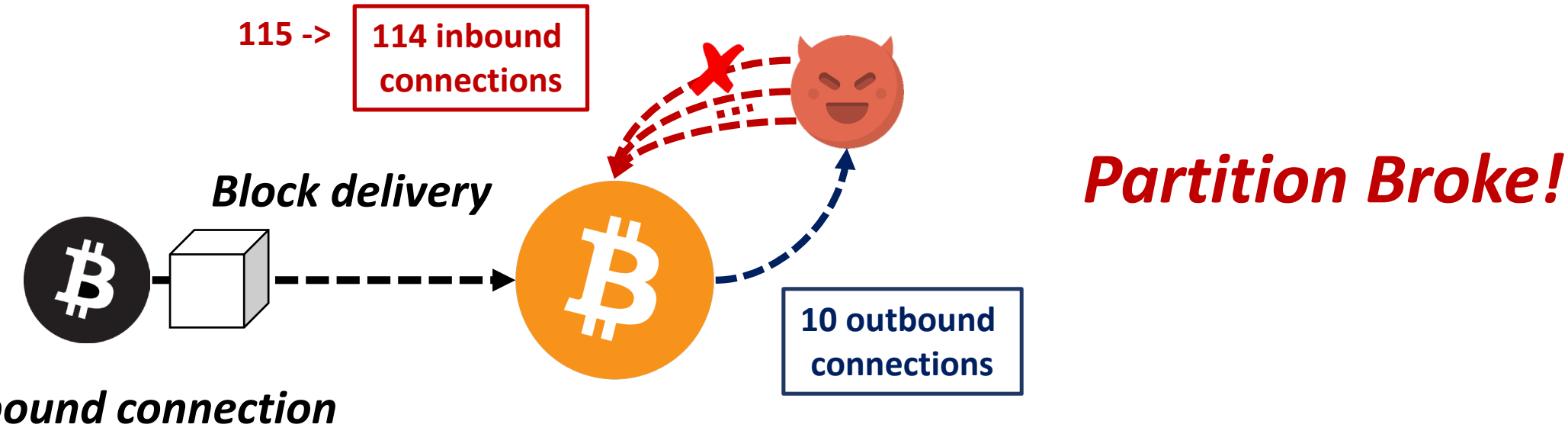
Sync attack:

- ✓ M. Saad et al. *[CCS '21]*
- ➢ Partitioning entire network by exploiting permission-less nature

NetS&P
Research Lab @ KAIST

Follow-up paper: Sustainability!

- **Jaehyun, Ha** et al: “On the Sustainability of Bitcoin Partitioning Attacks”, Financial Cryptography and Data Security 2023 (FC ’23)
- Claim: Bitcoin is safe from partitioning attacks, thanks to “***peer eviction mechanism***”



Conclusion

- Bitcoin is vulnerable to routing attacks both at the network and at the node level
- The potential impact on the currency is worrying, due to DoS, double spending, and loss of revenues, etc.
- Countermeasures were proposed to mitigate the routing attacks, but questions still remain for their practicality
- Another question remain about the attack feasibility
  - Which AS dares to partition the entire Bitcoin network, leaving clear skid marks in network layer?

Q&A Session

NetS&P
Research Lab @ KAIST

Q&A – Good Questions

윤태웅

To effectively execute a partitioning attack, how centralized should mining power be? Or, if large mining pools simply use different ASes, how much can this mitigate the effectiveness of the attack?

- Current state is centralized enough to launch partitioning attack
- Using more ASes will make the attack more costly

오성룡

I think this paper attacks networks based on the property of the bitcoin network, so the author seems to suggest randomness as defense. Is there a paper which randomness algorithm is better than others?

- A patch has been made after EREBUS attack is published (2020), now it is impossible for a node to connect to several nodes in a single AS. Same nodes from same ASes are now placed in the same bucket of client's peer table.

Q&A – Best Questions

이승현

Would using a rogue AS to attack Bitcoin be financially practical (/w shorting), given that BGP hijacking is likely to be detected?

- If the attack succeeds, it would be tremendously beneficial for attackers (Bitcoin market cap: 538B$)
- State-sponsored attackers are capable to hack some AS from other country, use for one-off attack

배한성, Zhixian Jin

Why encryptions weren't applied for messages in communication between Bitcoin nodes? Can it be regarded as realistic solution?

- There were some movements for communication encryption patch (BIP-151, BIP-342)
- Still vulnerable against routing attacks & partitioning attacks
- Key management in multi-hop routing becomes a big issue!

Thank You

Jaehyun Ha

jaehyunh1@kaist.ac.kr