# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

Laurent Vanbever

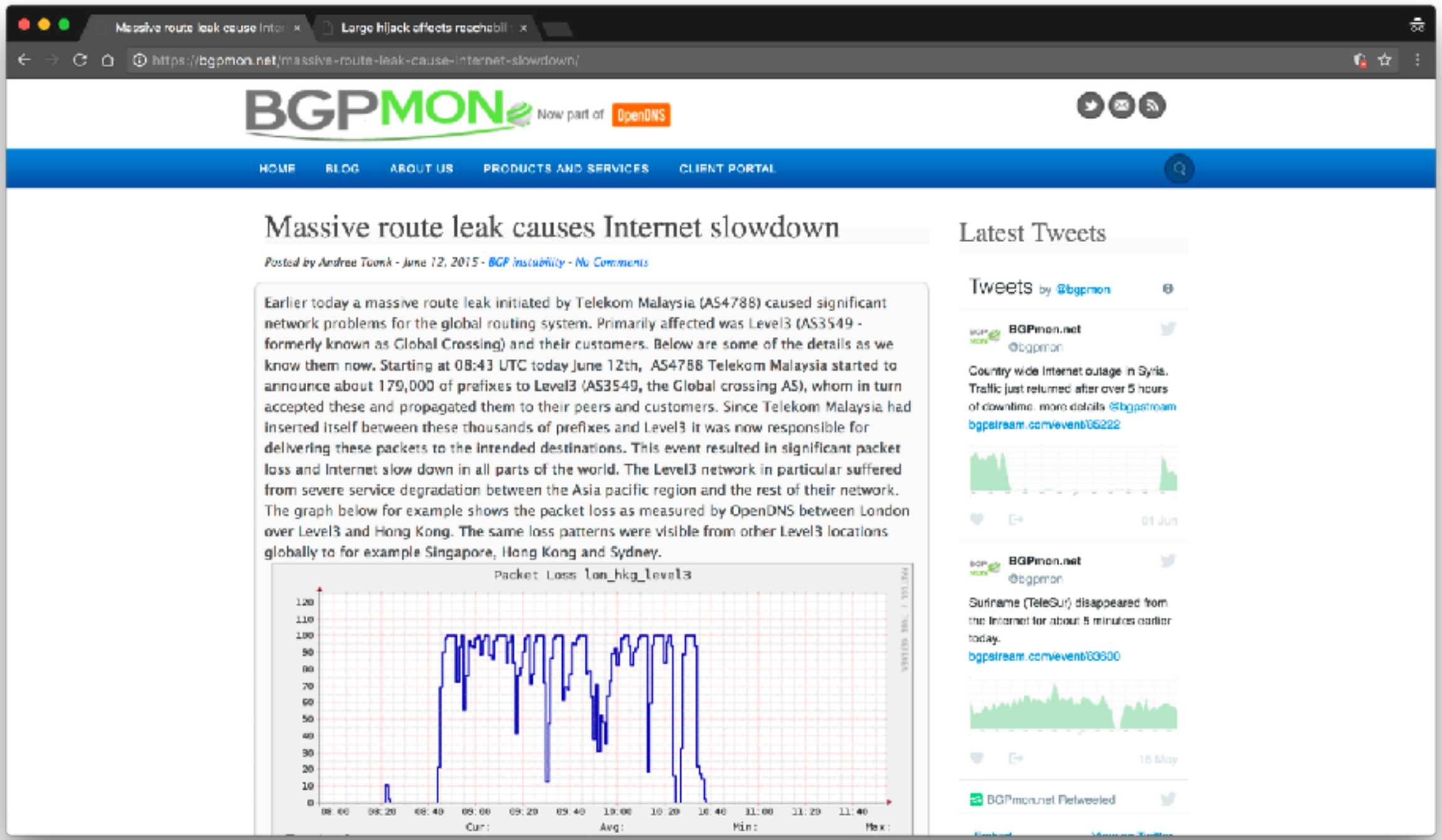
ETH Zürich

SuRI, EPFL

20 June 2017

Joint work with Maria Apostolaki and Aviv Zohar [S&P'2017]

# Millesime 2015




source: https://bgpmon.net/massive-route-leak-cause-internet-slowdown/

# Millesime 2016

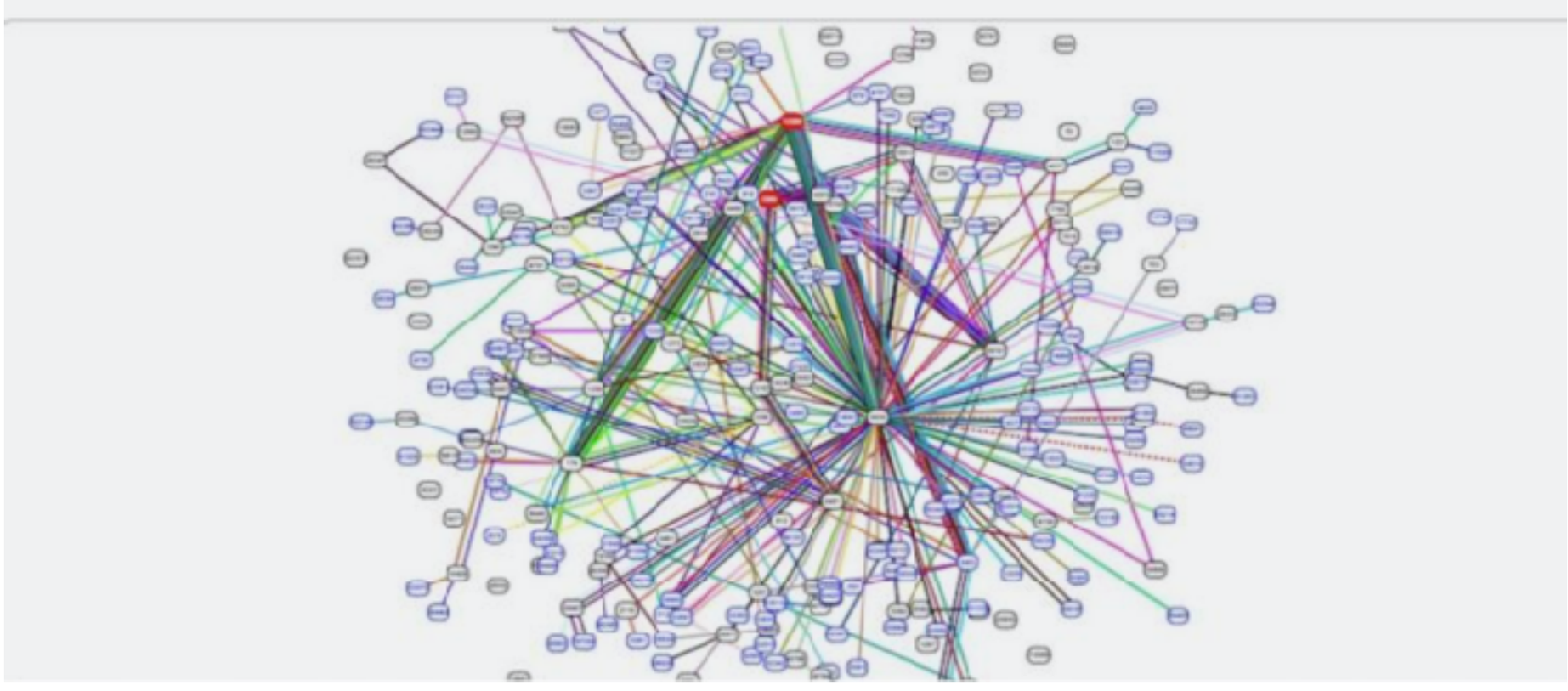

source: https://bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/

Millesime 2017

# Russian-controlled telecom hijacks financial services' Internet traffic

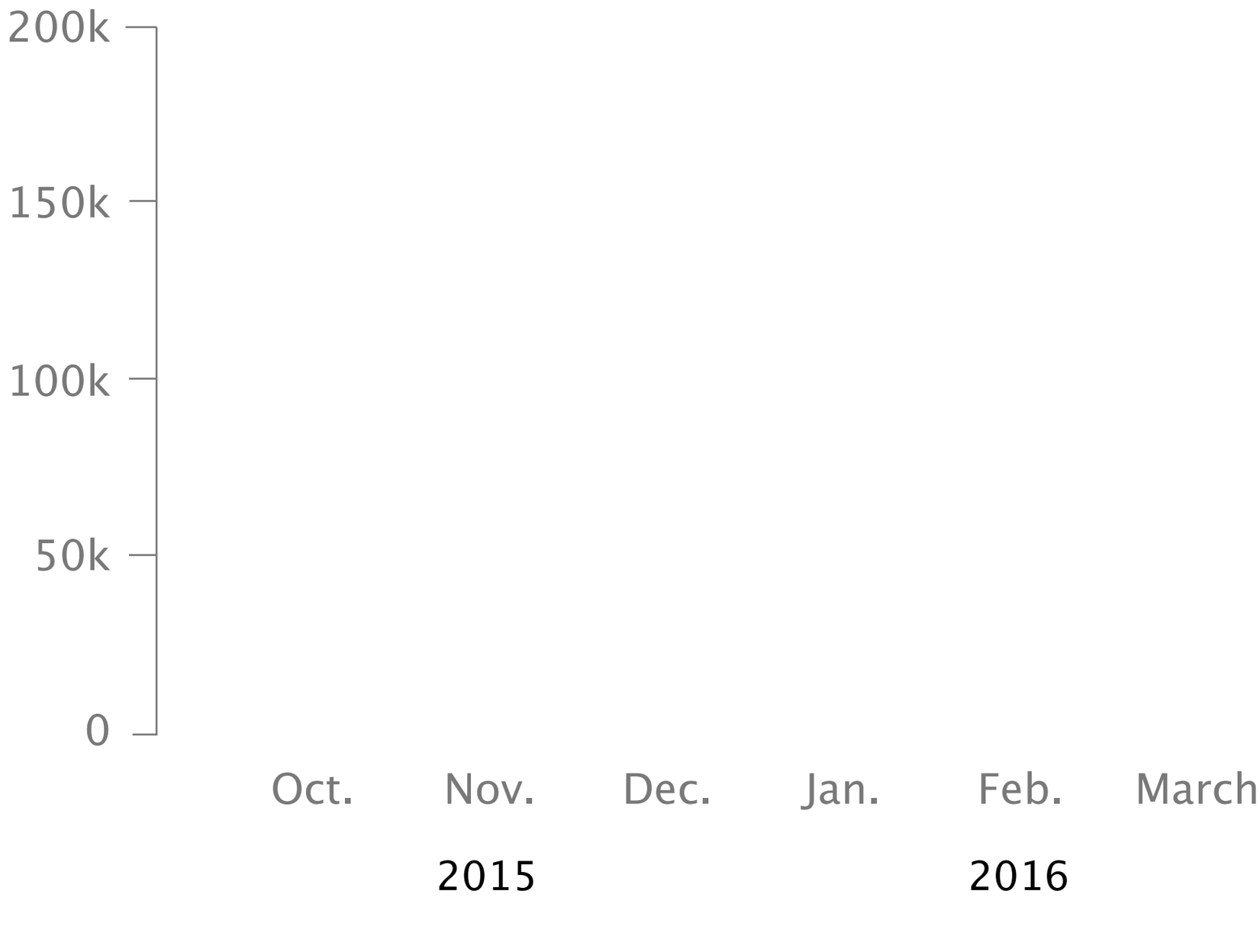
**Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.**

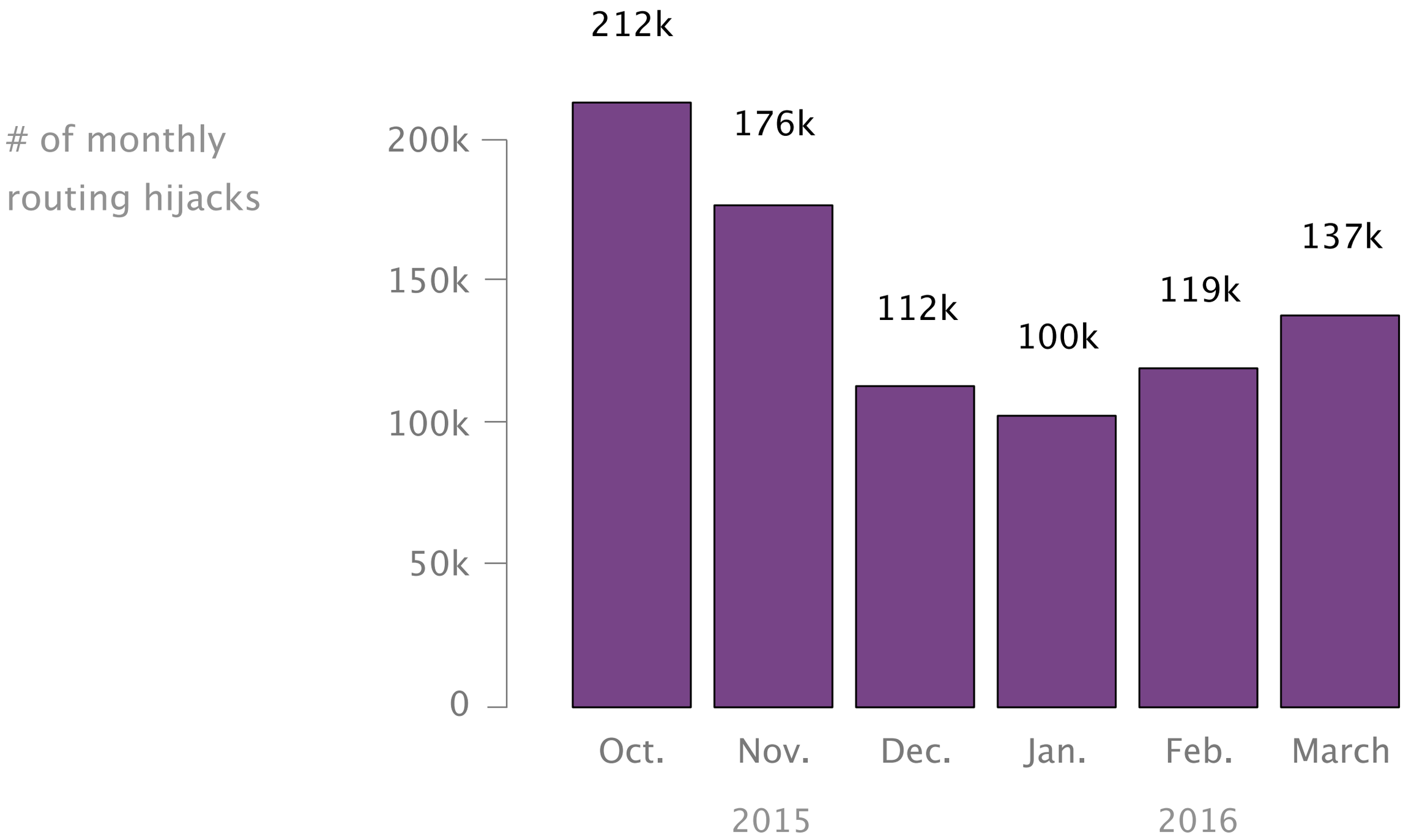
DAN GOODIN - 4/27/2017, 10:20 PM



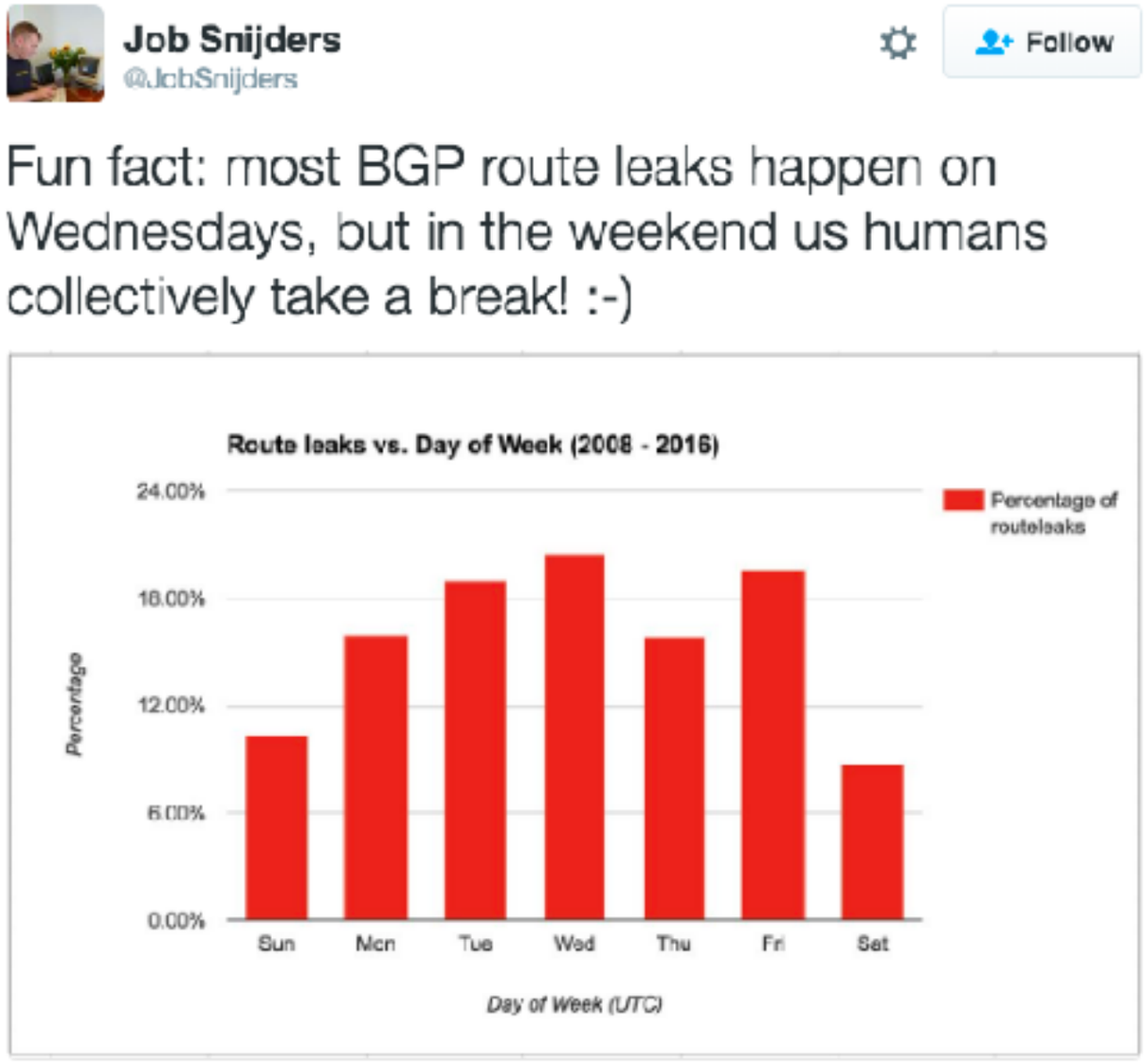
source: arstechnica.com

# of monthly routing hijacks




# of monthly routing hijacks
200k
150k
100k
50k
0
212k
176k
112k
100k
119k
137k
Oct.
Nov.
Dec.
Jan.
Feb.
March
2015
2016

# Most of these problems are human mistakes



# The Internet Under Crisis Conditions

## Learning from September 11

Committee on the Internet Under Crisis Conditions:
Learning from September 11

Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

National Research Council. The Internet Under Crisis Conditions: Learning from September 11

# The Internet Under Crisis Conditions

## Learning from September 11

Committee on the Internet Under Crisis Conditions:
Learning from September 11

Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
*OF THE NATIONAL ACADEMIES*

Internet advertisements rates

suggest that

The Internet was more stable

than normal on Sept 11


Internet advertisements rates

suggest that

The Internet was more stable

than normal on Sept 11

Information suggests that

operators were watching the news

instead of making changes

to their infrastucture

# Can such routing attacks impact Bitcoin?

Can such routing attacks impact Bitcoin?

**Yes.** And very much so.

THREAT LEVEL

# Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

BY ANDY GREENBERG 08.07.14 | 1:00 PM | PERMALINK



source: wired.com

In principle, Bitcoin should be highly decentralized
making it robust to routing attacks

Bitcoin nodes …

- are scattered all around the globe
- establish random connections
- use multihoming and extra relay networks

In principle, Bitcoin should be highly decentralized making it robust to routing attacks

In practice,

Bitcoin is highly centralized

Bitcoin’s centralization illustrates itself across three dimensions

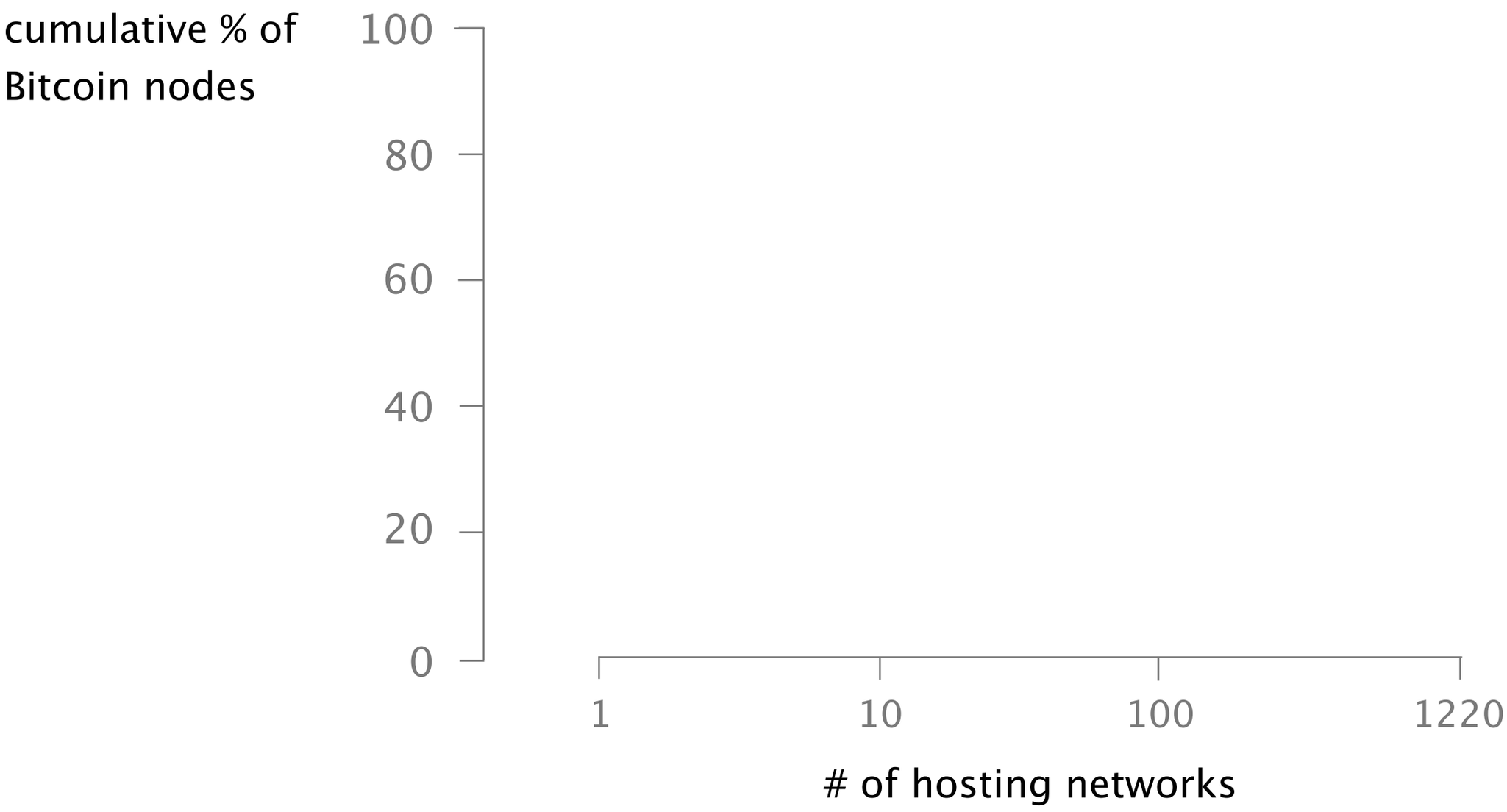
hosting

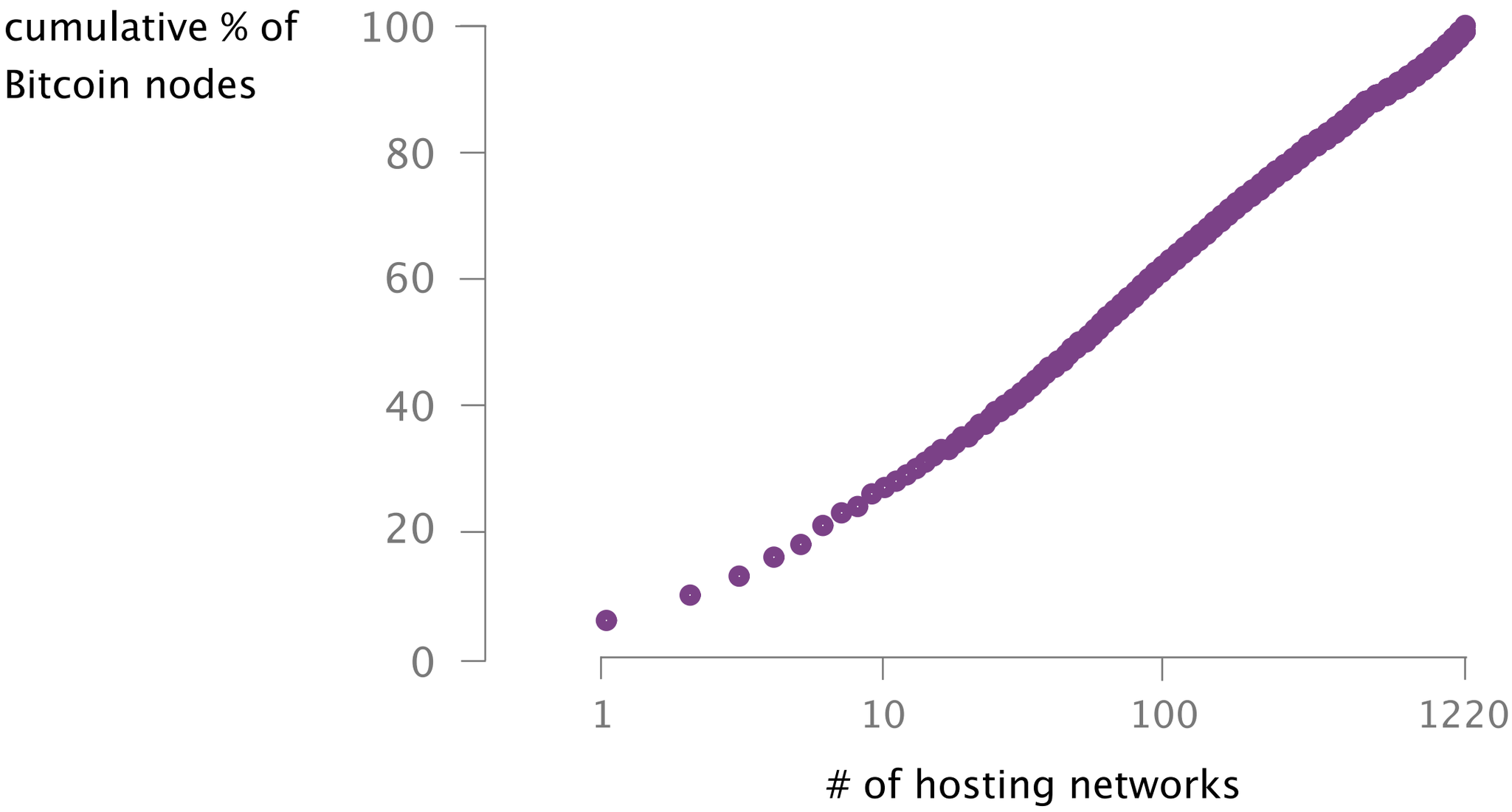
mining

transit

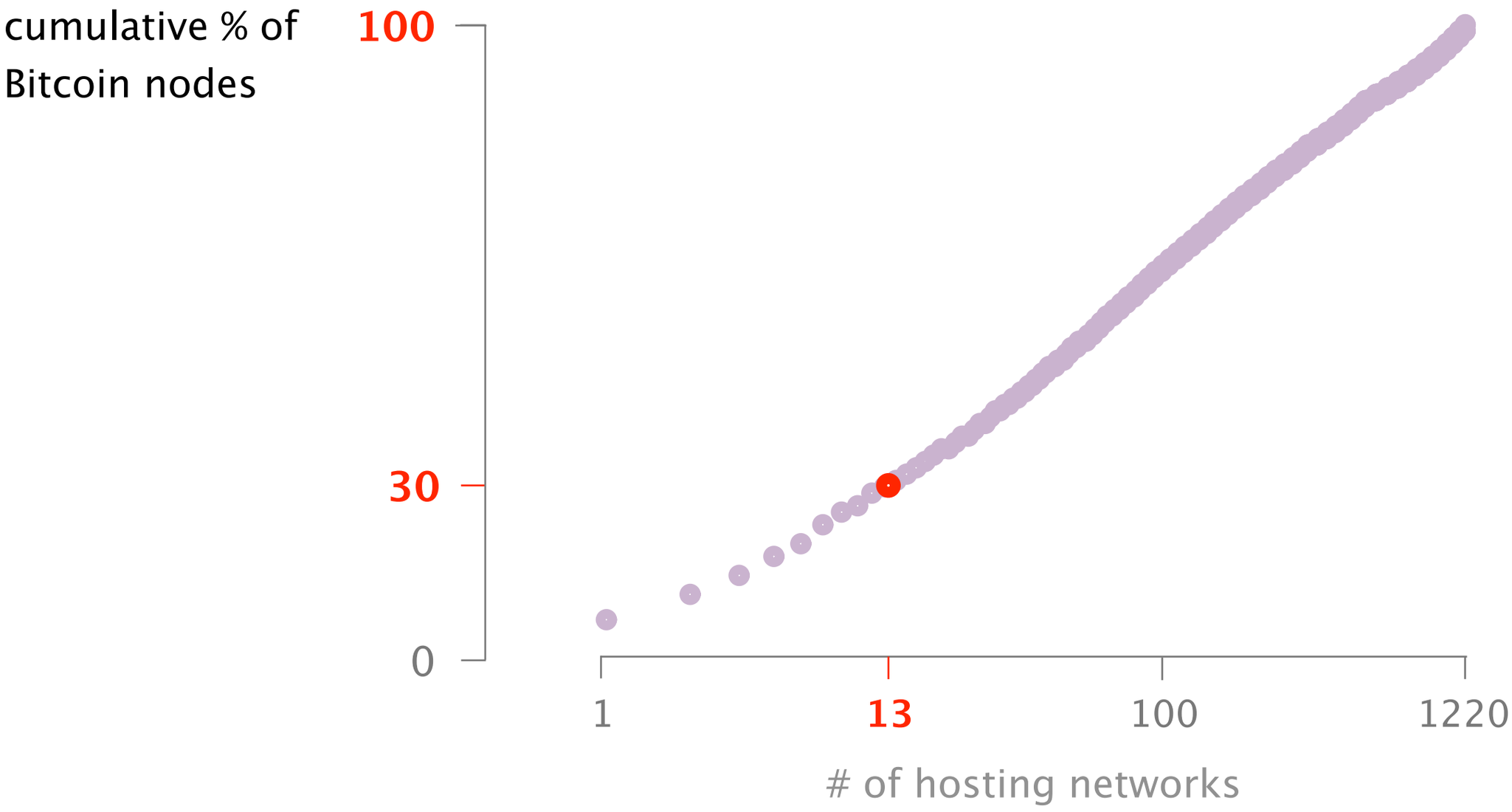
Bitcoin’s centralization illustrates itself across three dimensions

# Few networks host a large fraction of nodes


cumulative % of Bitcoin nodes
100
80
60
40
20
0
1
10
100
1220
# of hosting networks

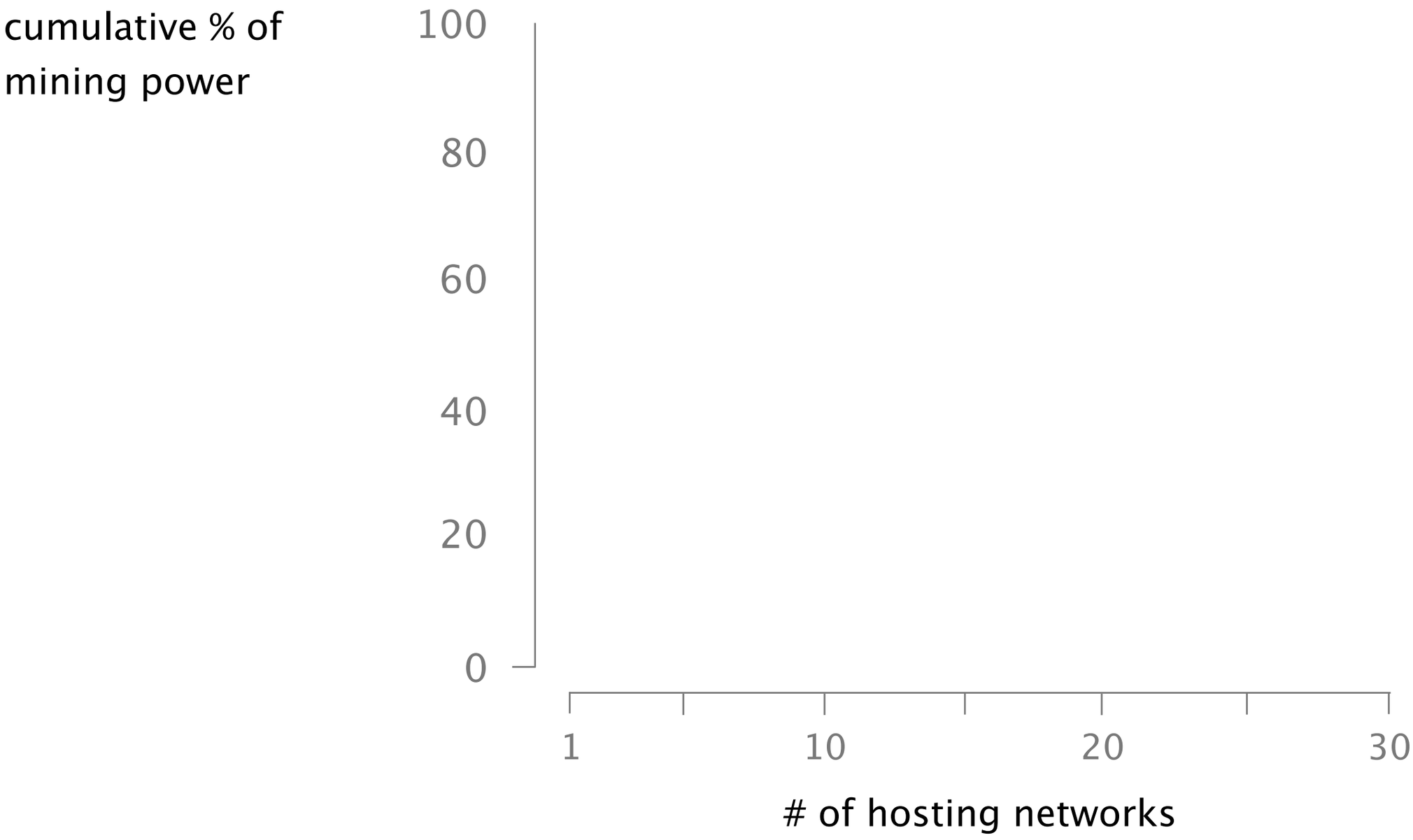

cumulative % of
Bitcoin nodes
100
80
60
40
20
0
1
10
100
1220
# of hosting networks

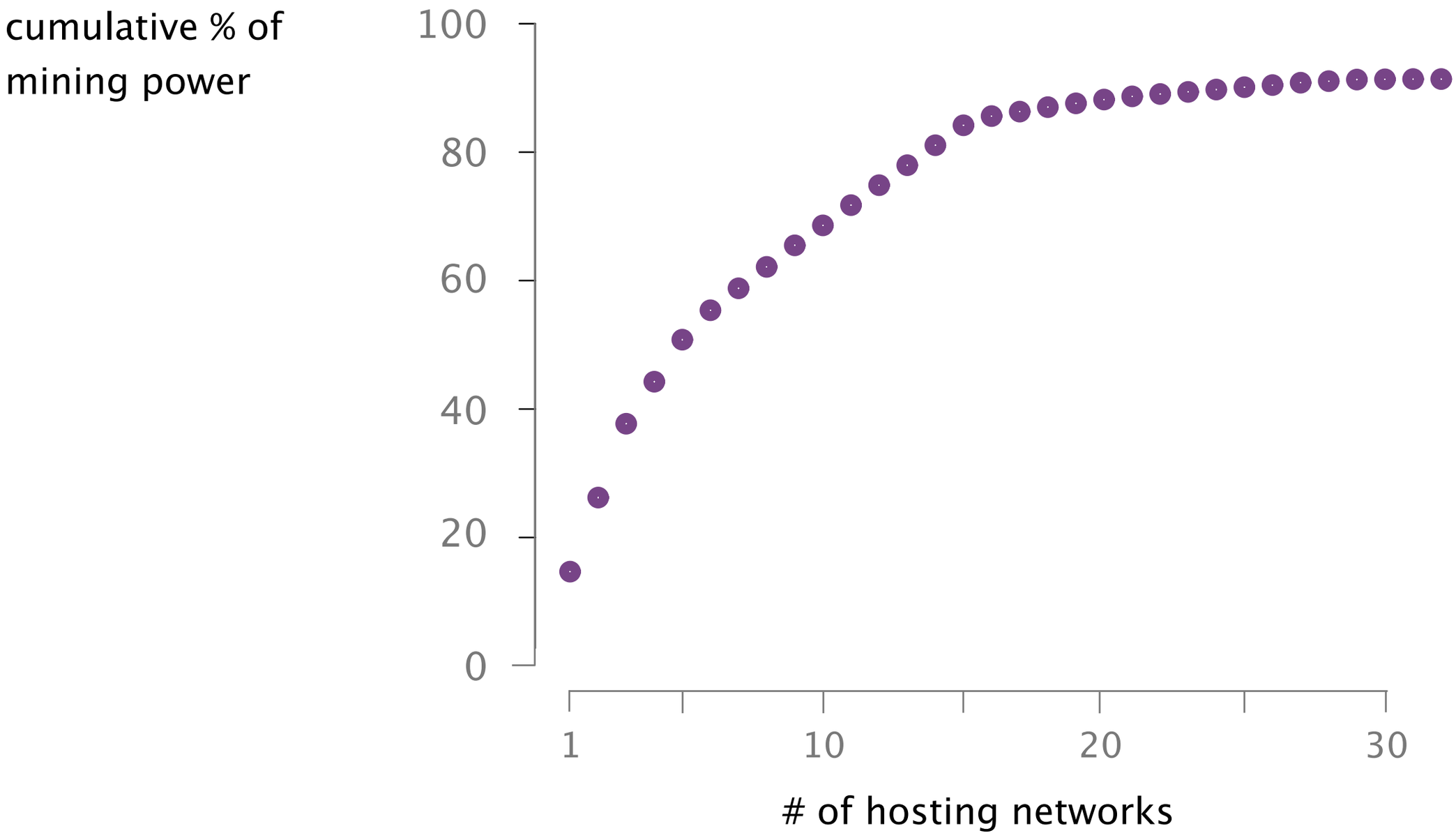
# 13 networks host 30% of all the nodes



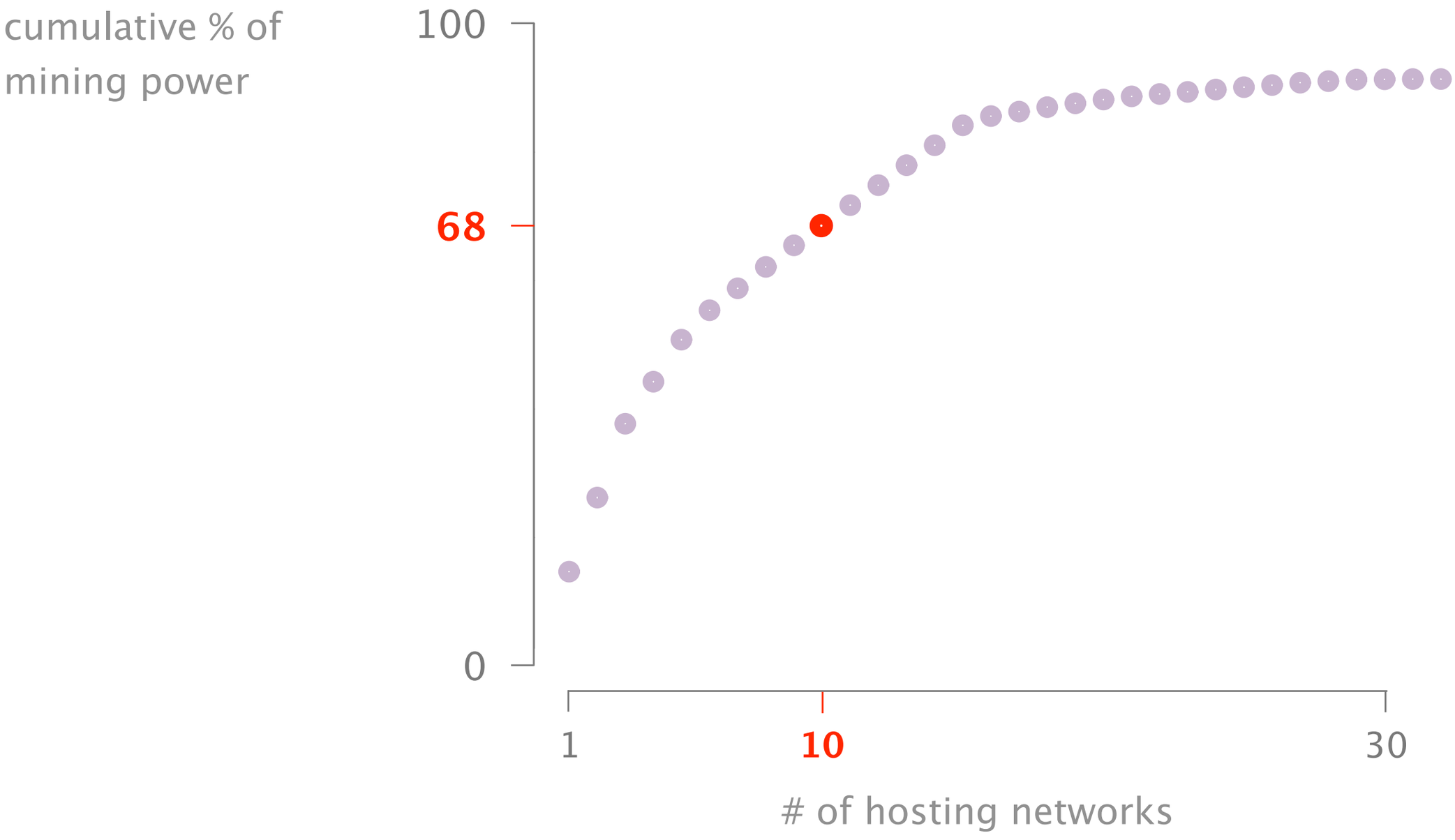
Bitcoin’s centralization illustrates itself across three dimensions

# Mining power is centralized to few hosting networks

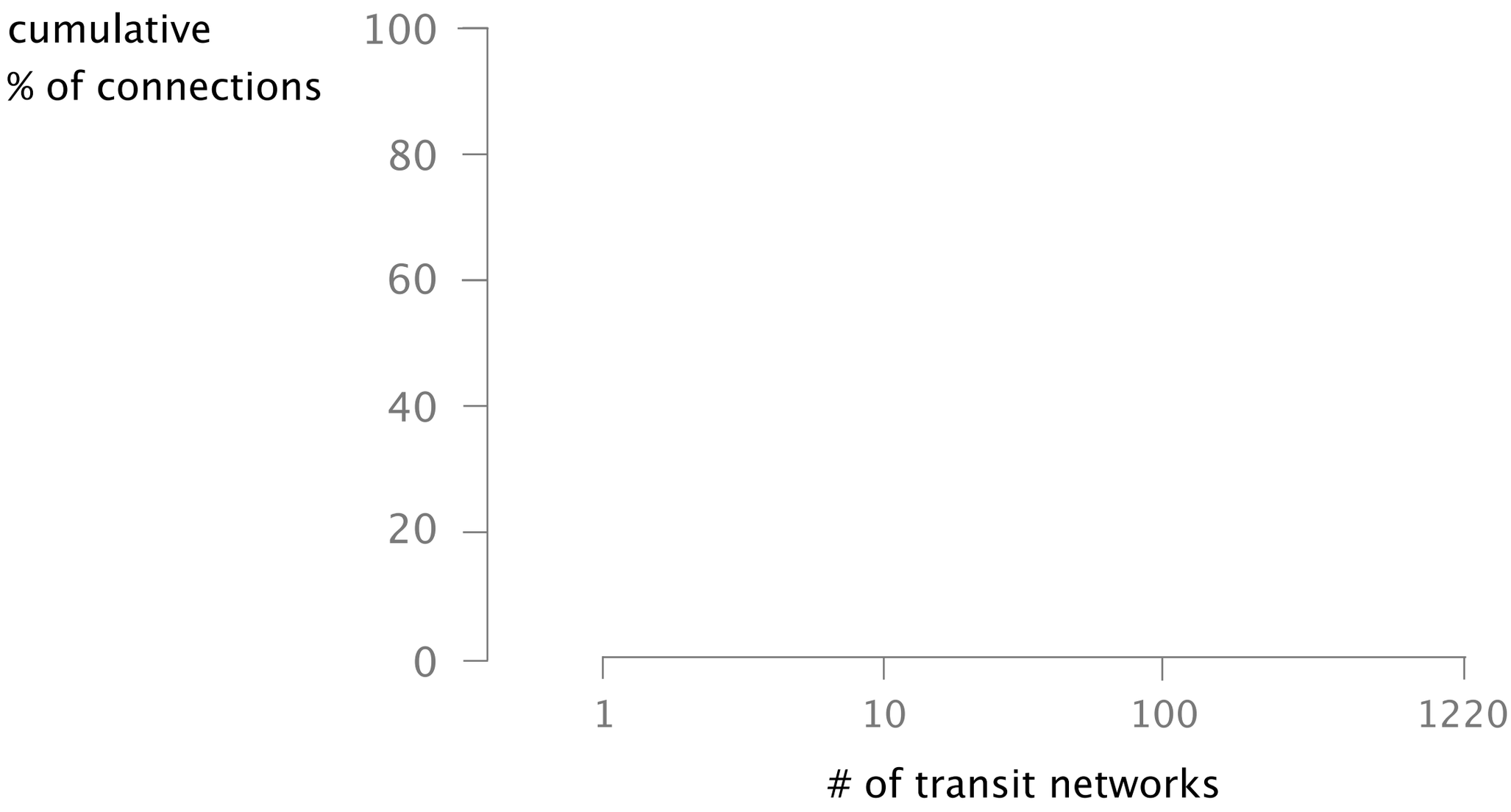

cumulative % of mining power
100
80
60
40
20
0
1
10
20
30
# of hosting networks


cumulative % of mining power
100
80
60
40
20
0
1
10
20
30
# of hosting networks

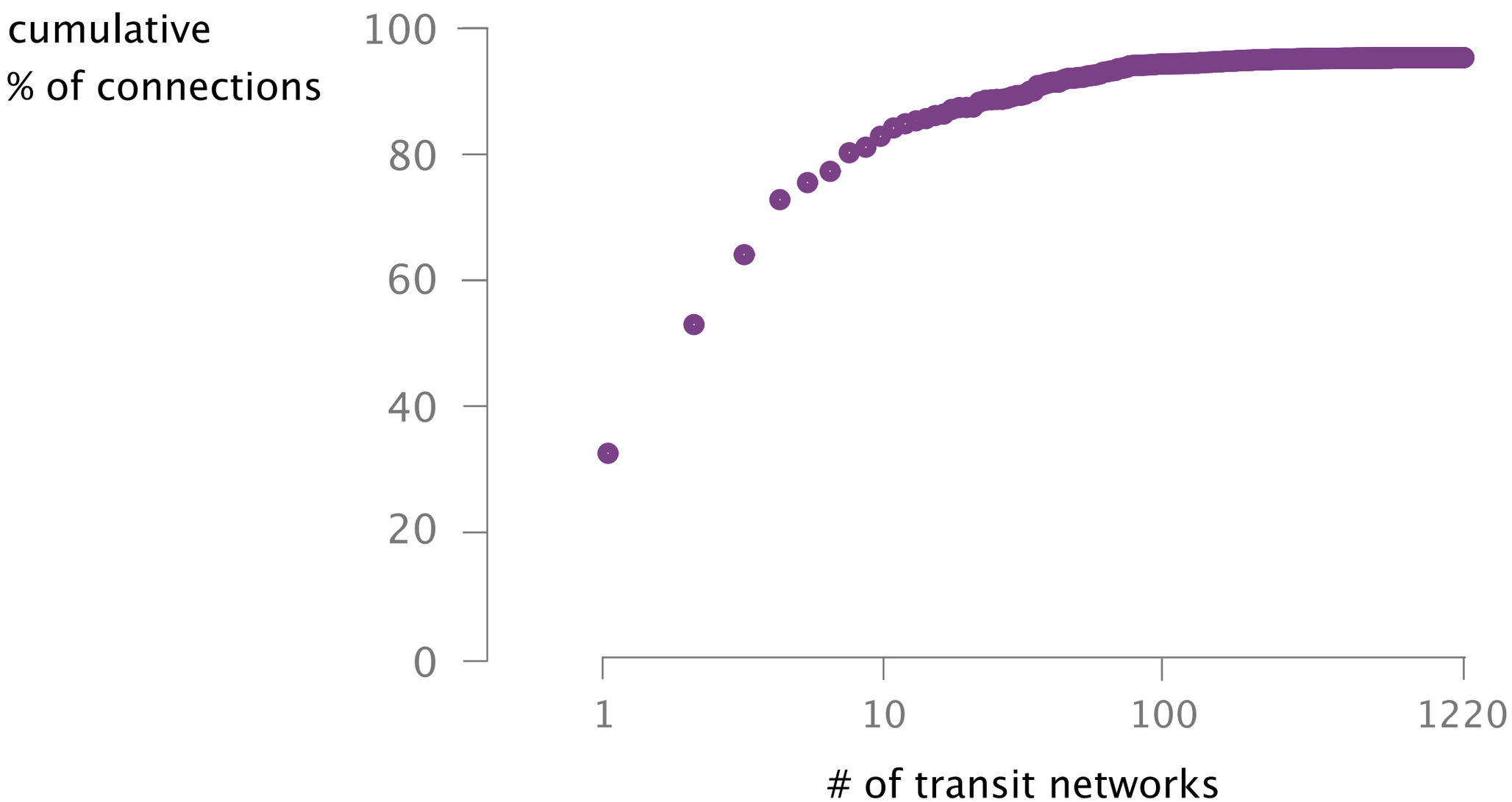
# 68% of the mining power is hosted in 10 networks only



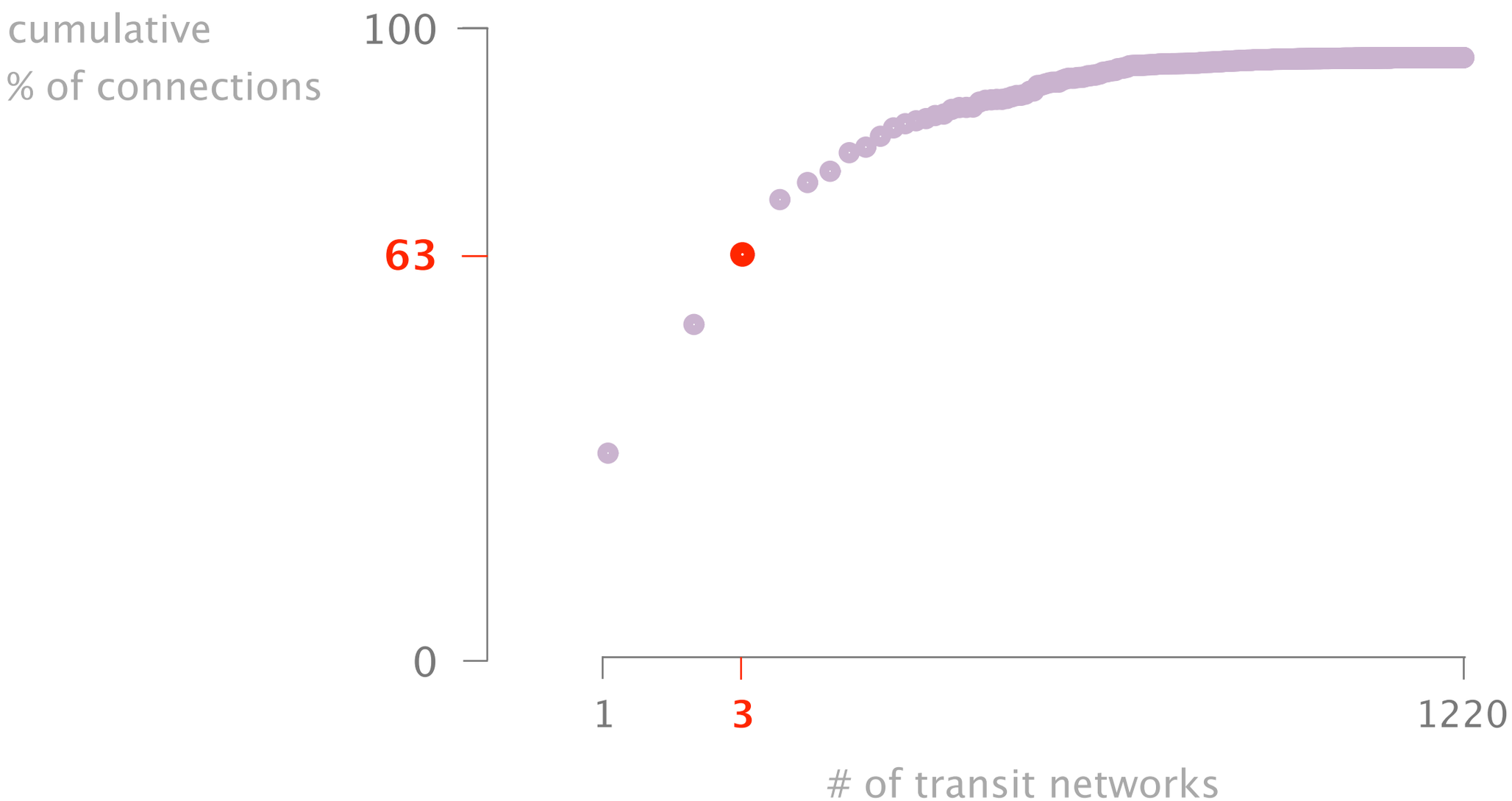
Bitcoin’s centralization illustrates itself across three dimensions


cumulative
% of connections
100
80
60
40
20
0
1
10
100
1220
# of transit networks

# Likewise, a few transit networks can intercept a large fraction of the Bitcoin connections



# 3 transit networks see more than 60% of all connections



Because of this centralization,

two routing attacks practical and effective today

Attack 1

Partitioning

Split the network in half

Attack 2

Delay

Delay block propagation

Each attack differs in terms of its visibility, impact, and targets

Attack 1

Partitioning

Delay

visible

network-wide attack

Each attack differs in terms of its

visibility, impact, and targets

Attack 2

Partitioning

Delay

invisible

targeted attack (set of nodes)

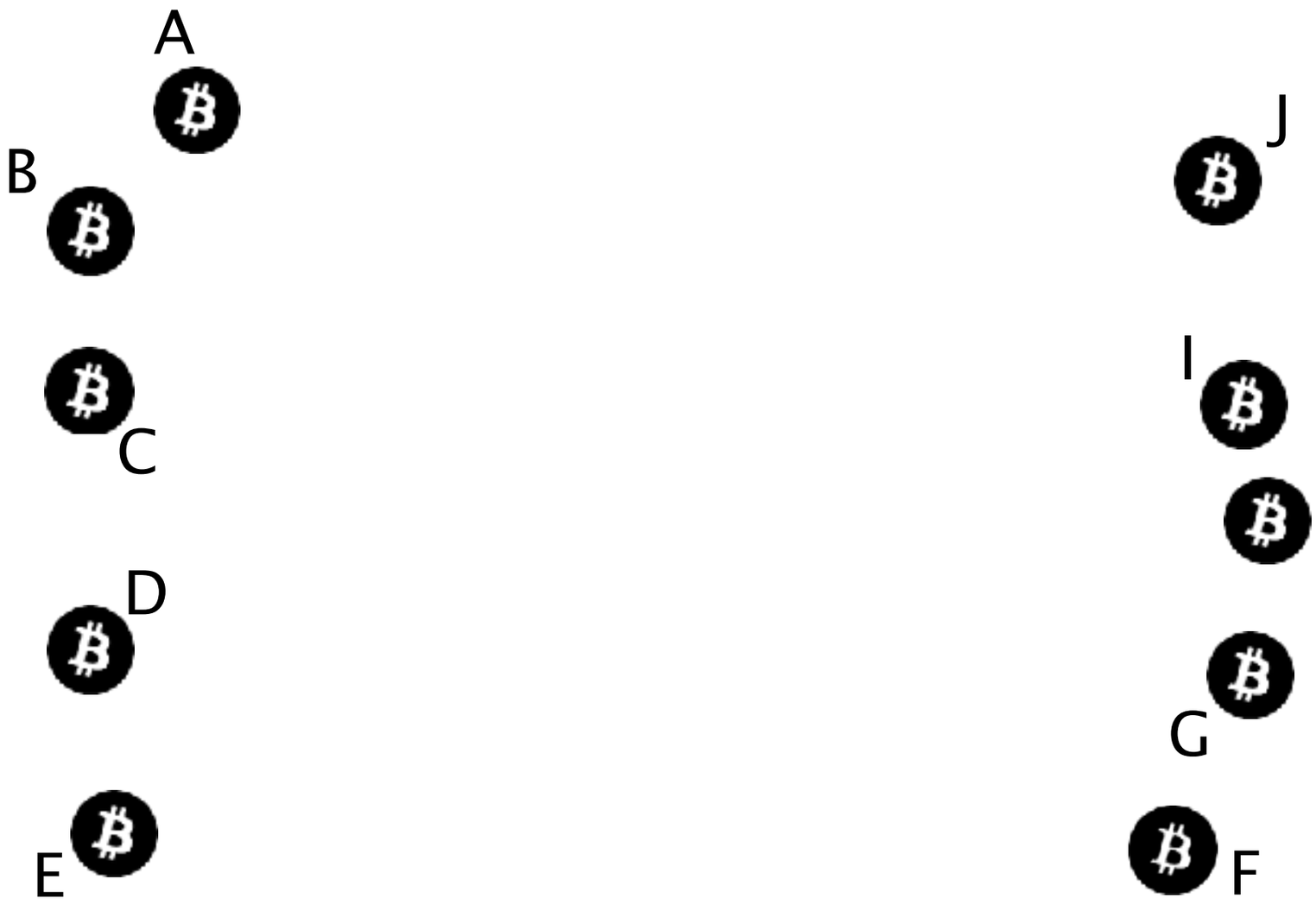
# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

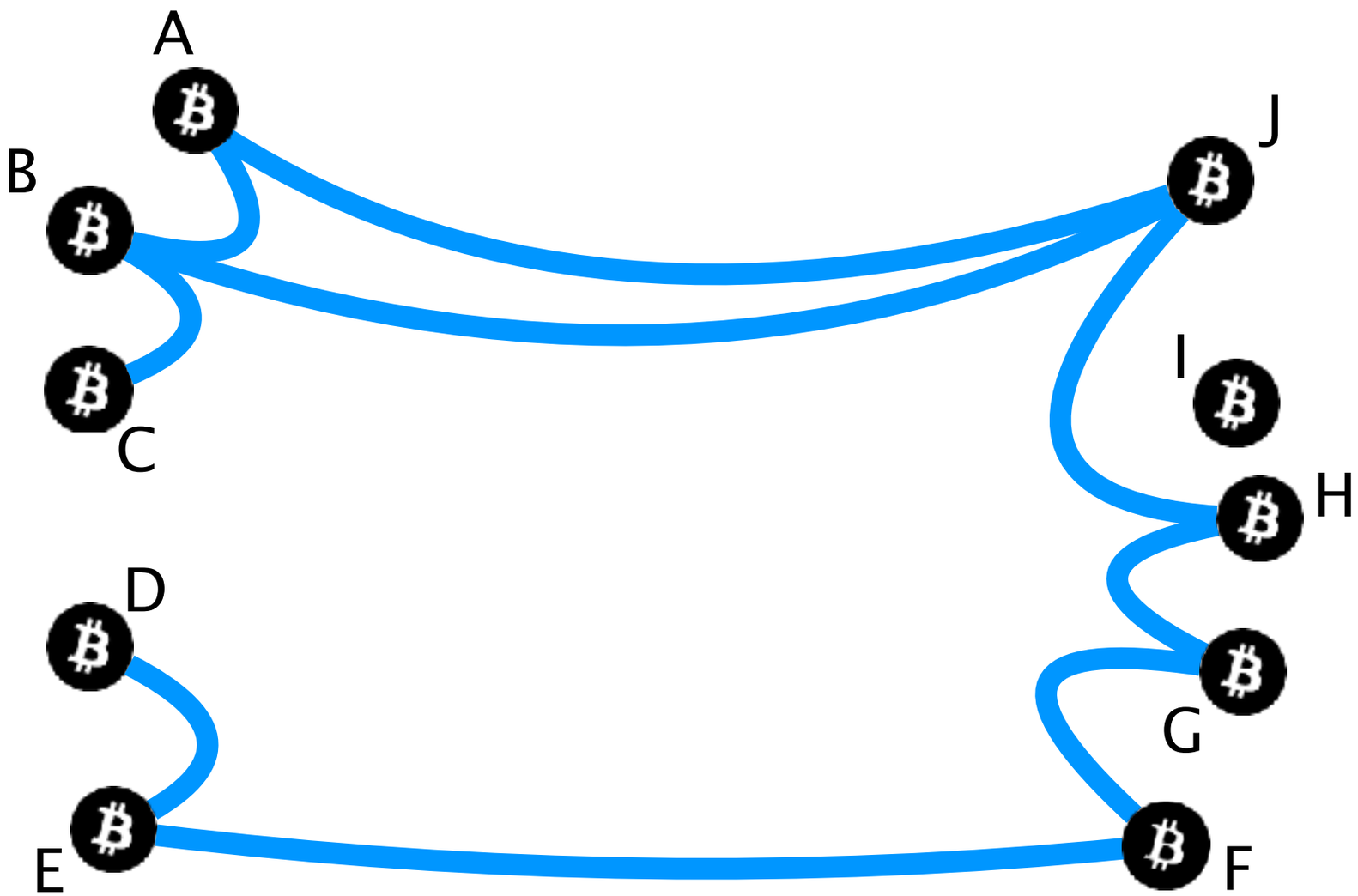
# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

Bitcoin is a distributed network of nodes



Bitcoin nodes establish random connections between each other



Each node keeps a ledger of all transactions ever performed: “the blockchain”

Tx a1a53743

Tx b5x89433

…

Tx x5f78432

Tx h1t91267

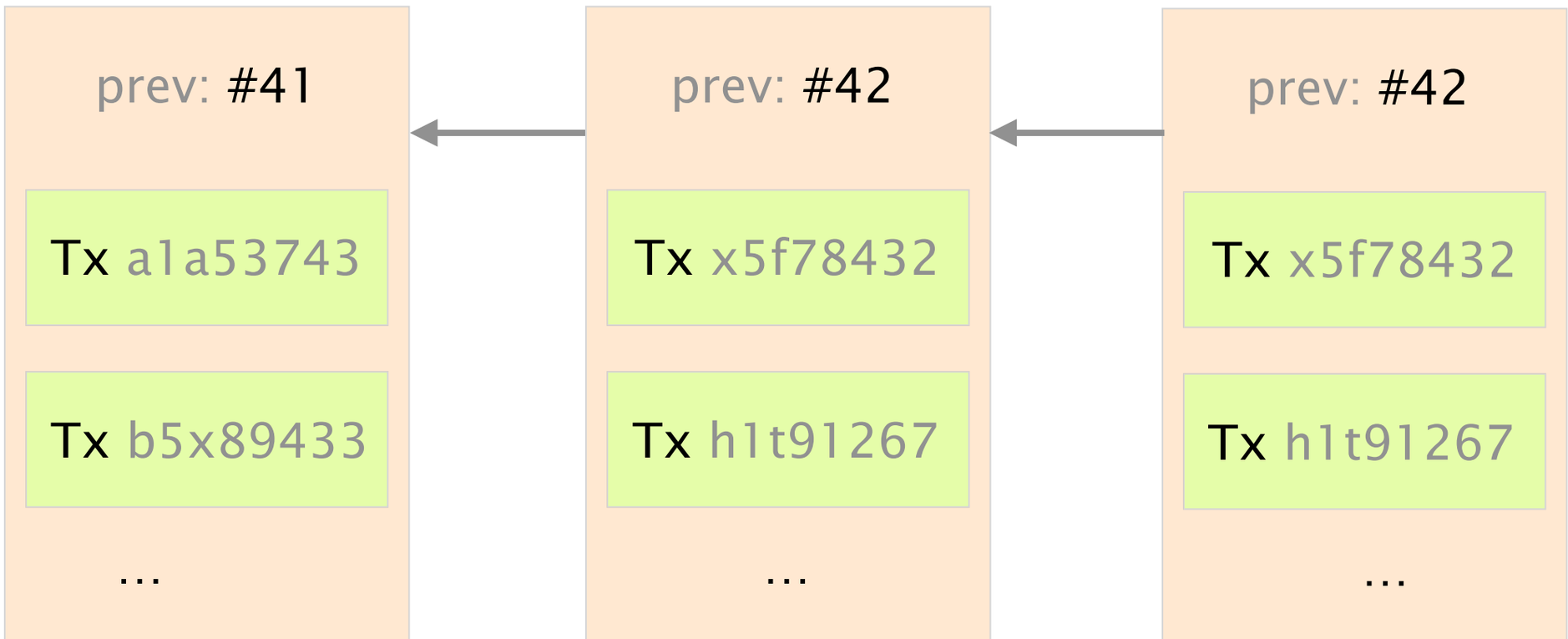
…

Tx x5f78432

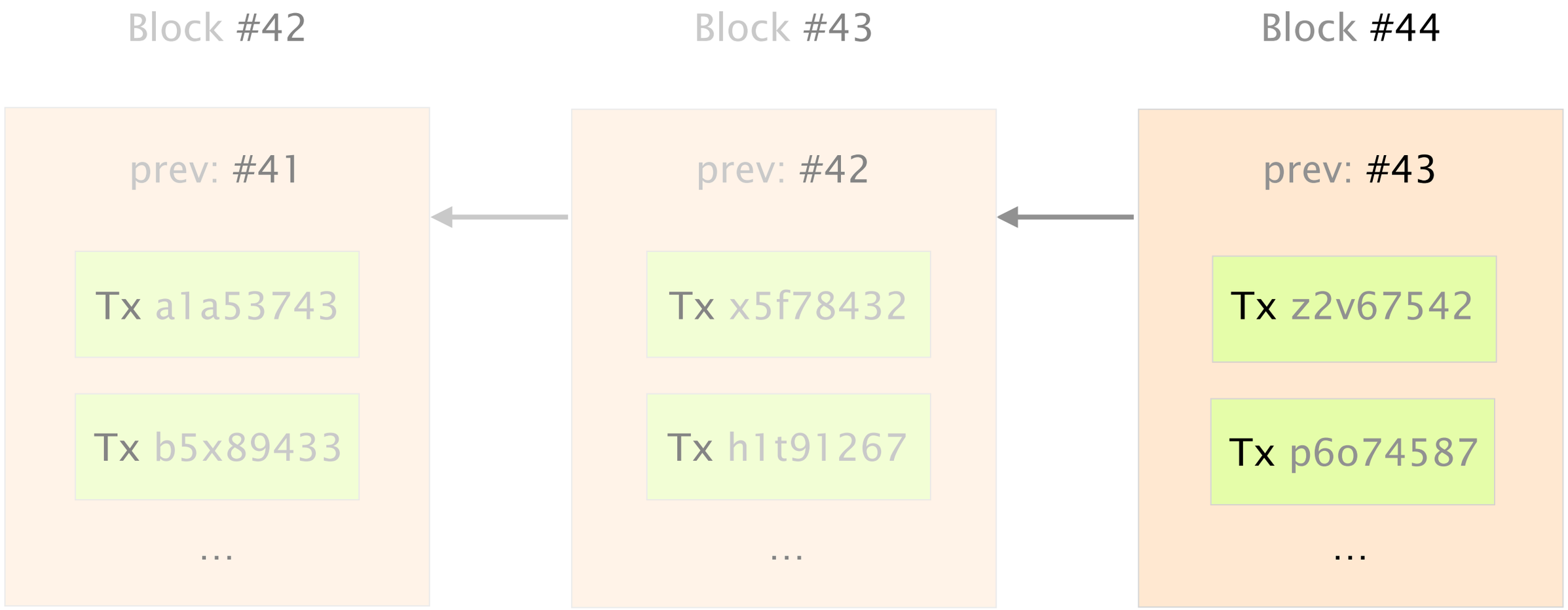
Tx h1t91267

…

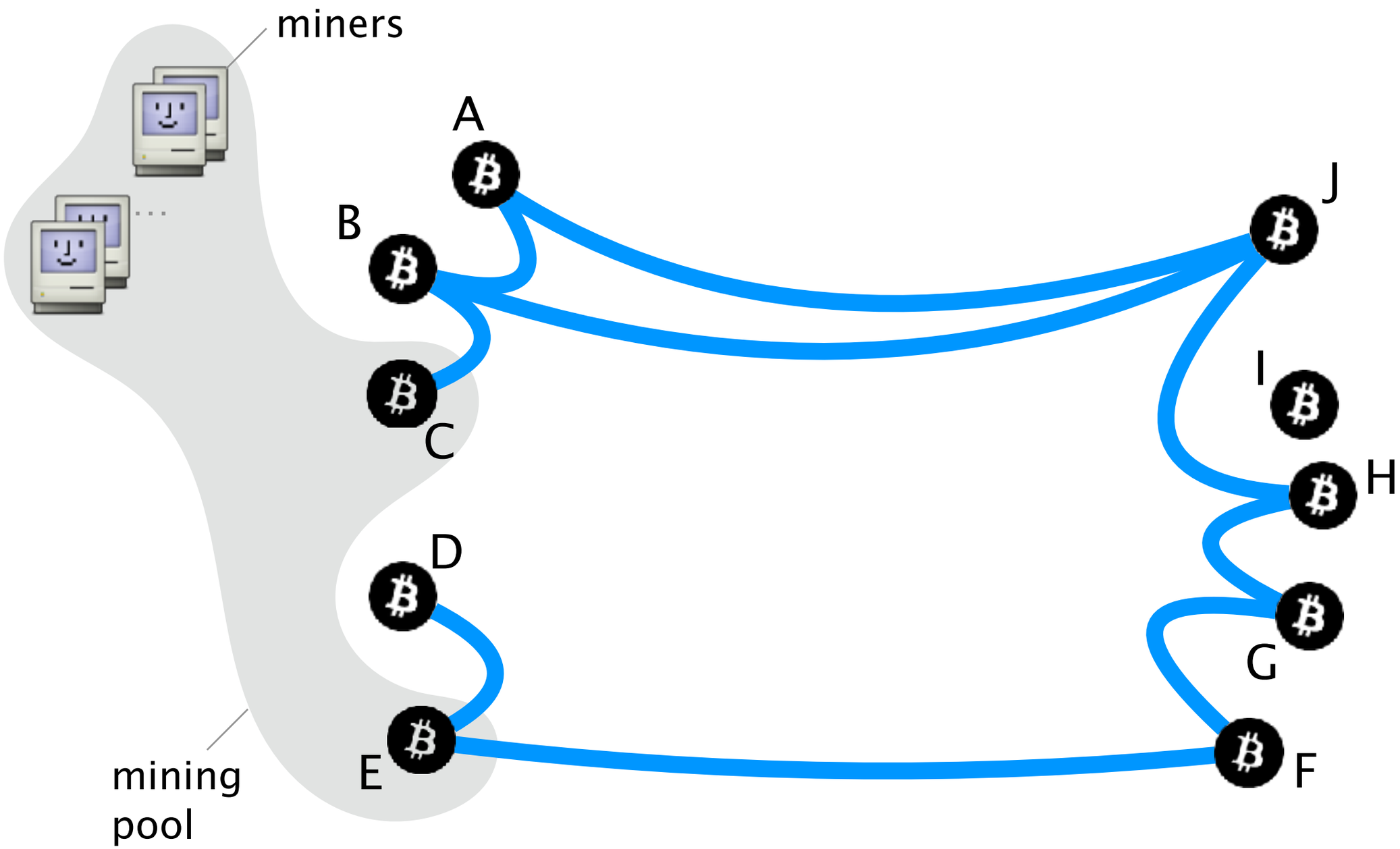
# The blockchain is a chain of blocks



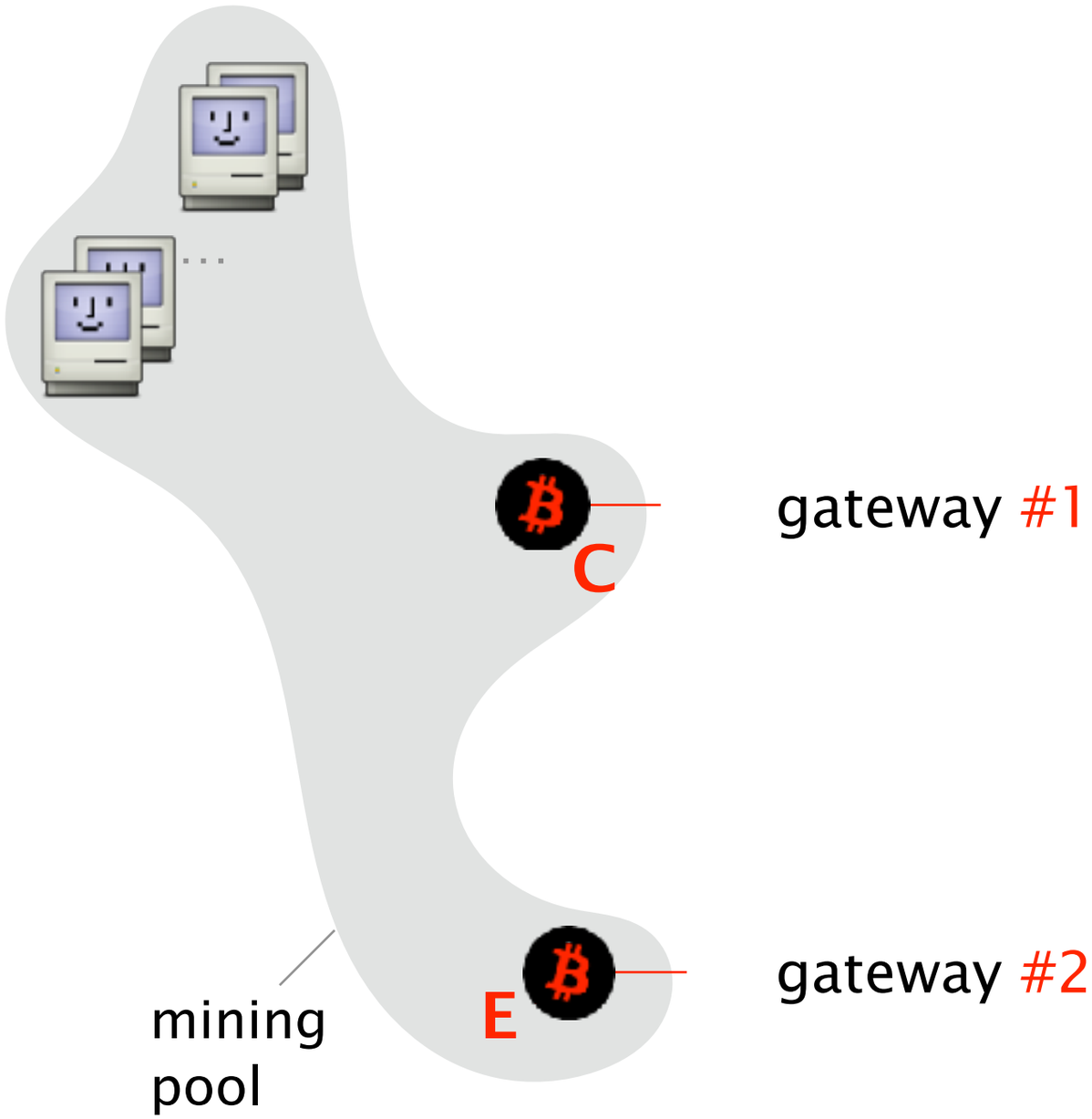
# The blockchain is extended by miners



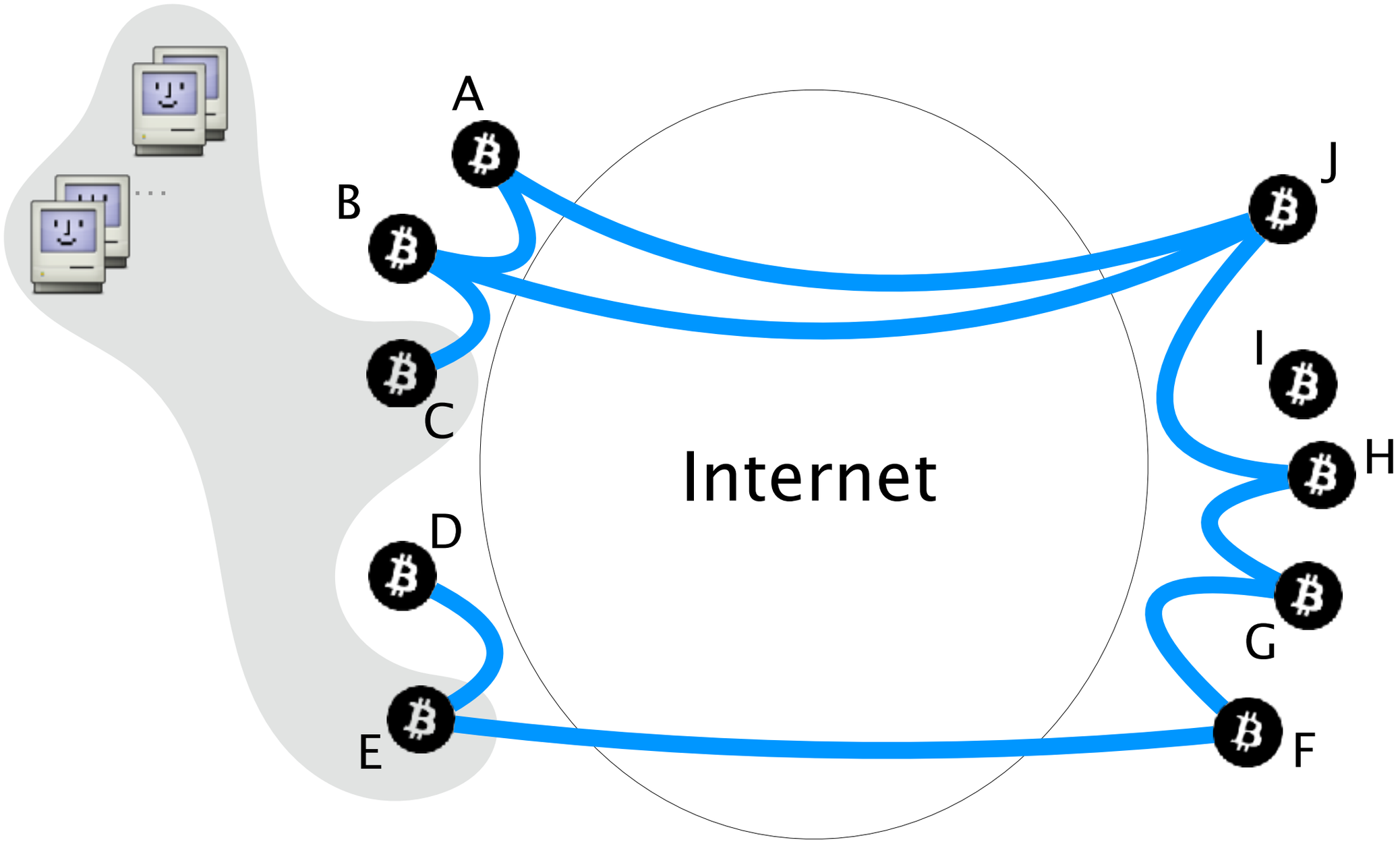
# Miners are grouped in mining pools



Mining pools connect to the Bitcoin network through multiple gateways

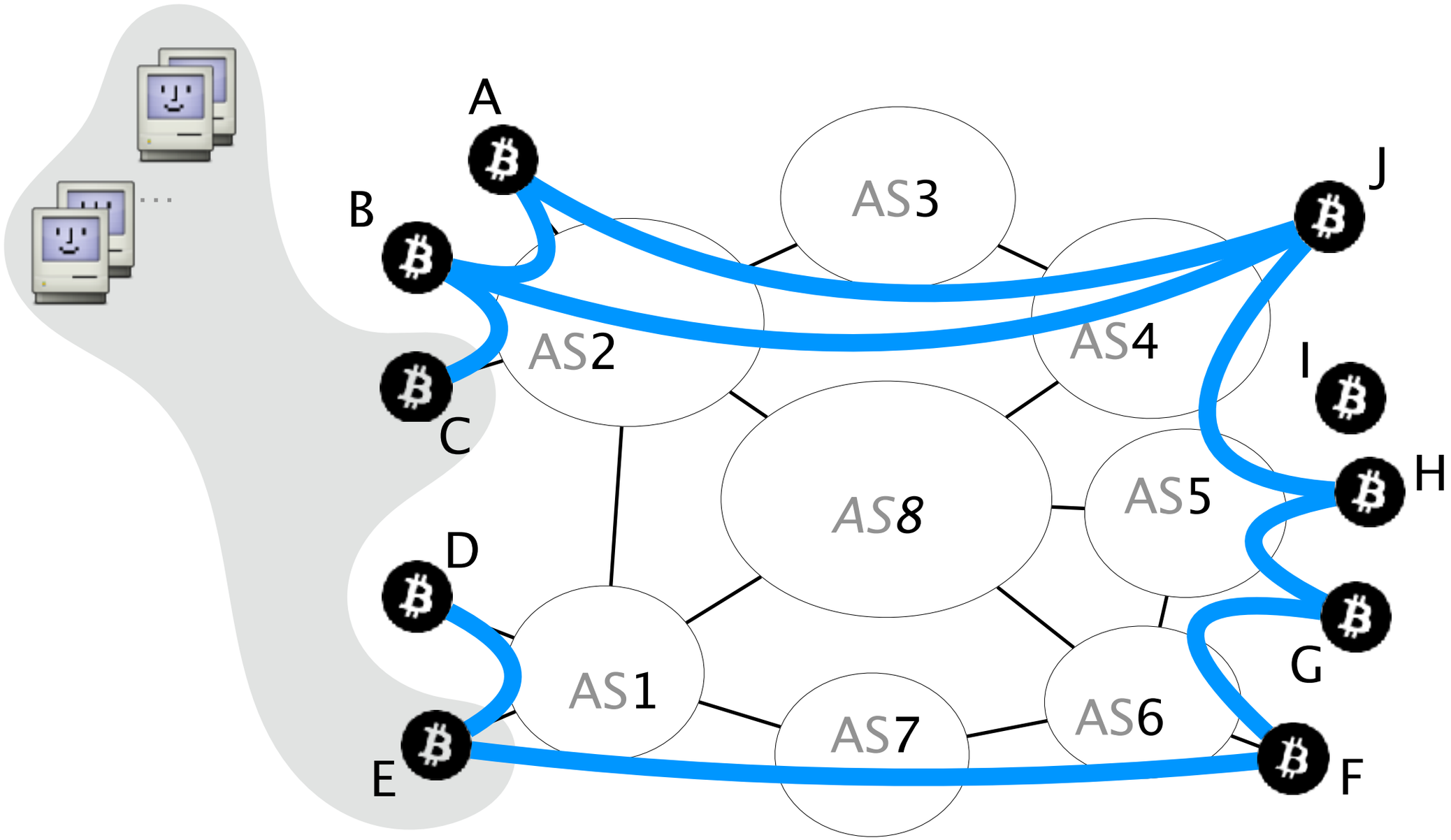


# Bitcoin connections are routed over the Internet

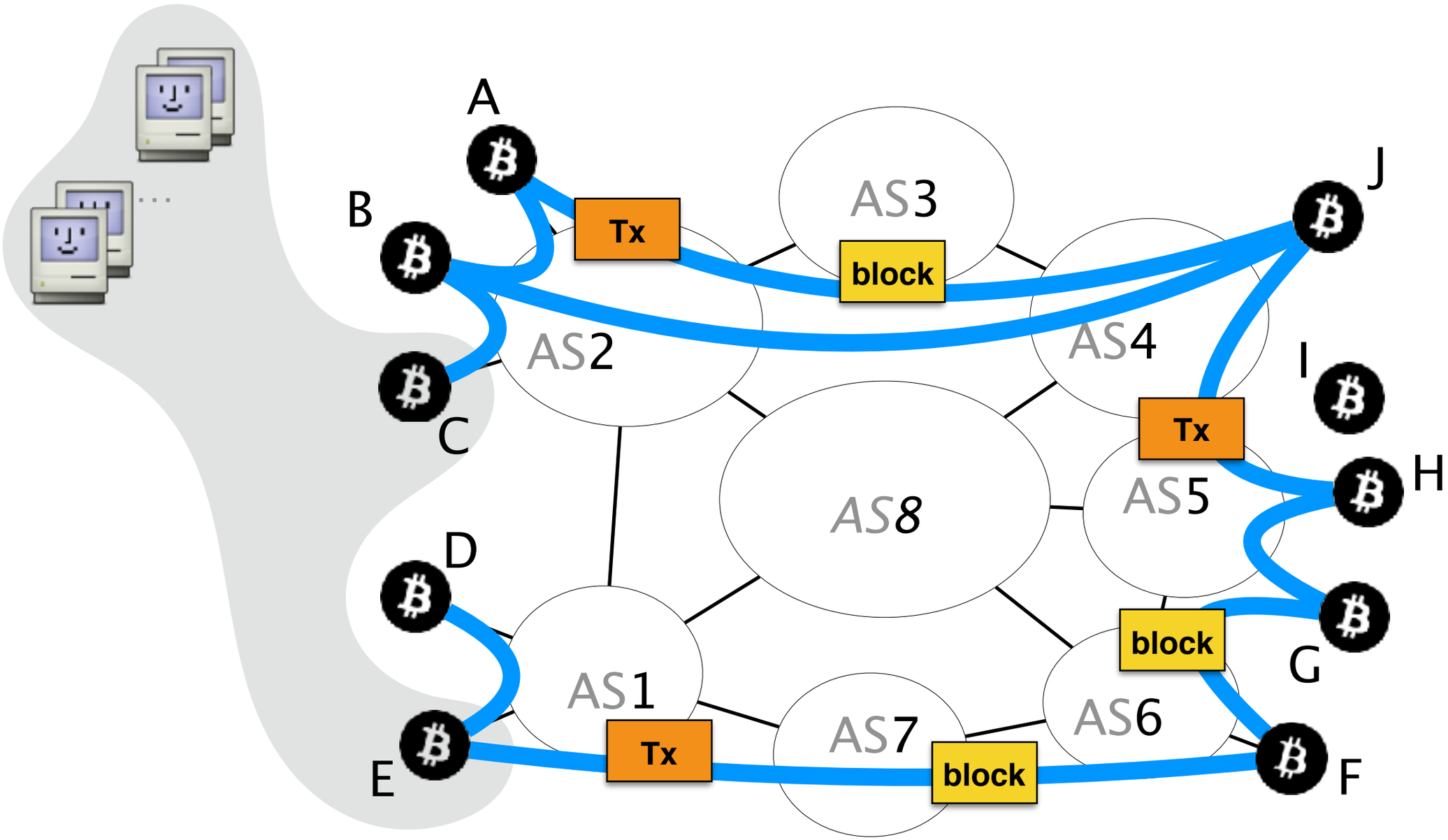


The Internet is composed of Autonomous Systems (ASes).

BGP computes the forwarding path across them



Bitcoin messages are propagated unencrypted and without any integrity guarantees



# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

The goal of a partitioning attack is to split
the Bitcoin network into two disjoint components

The impact of such an attack is worrying

Denial of Service

Revenue Loss

Double spending

# The impact of such an attack is worrying

Denial of Service

Bitcoin clients and wallets cannot secure or propagate transactions

Revenue Loss

Double spending

# The impact of such an attack is worrying

Denial of Service

Revenue Loss

Blocks in component with
less mining power are discarded

Double spending

The impact of such an attack is worrying

Denial of Service

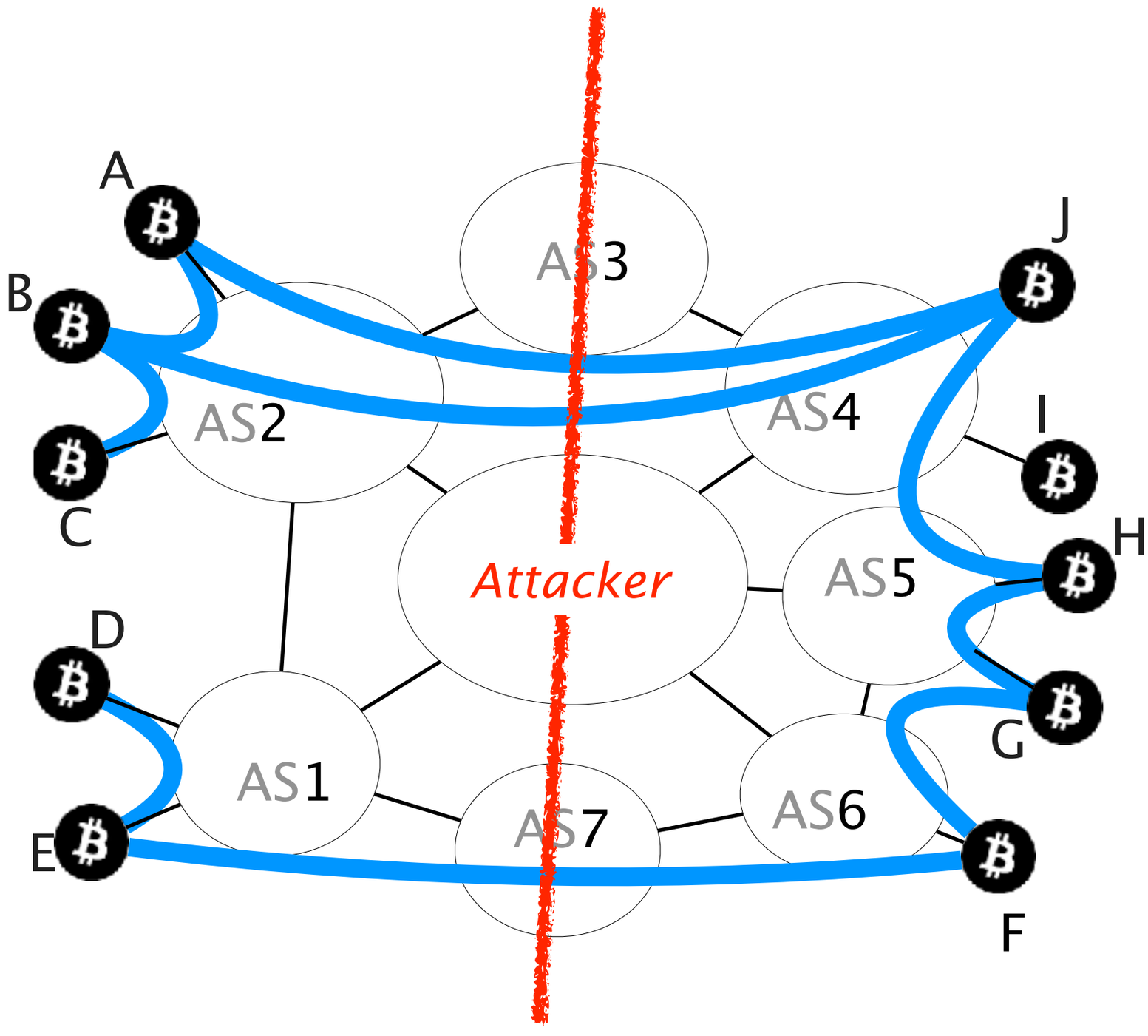
Revenue Loss

Double spending

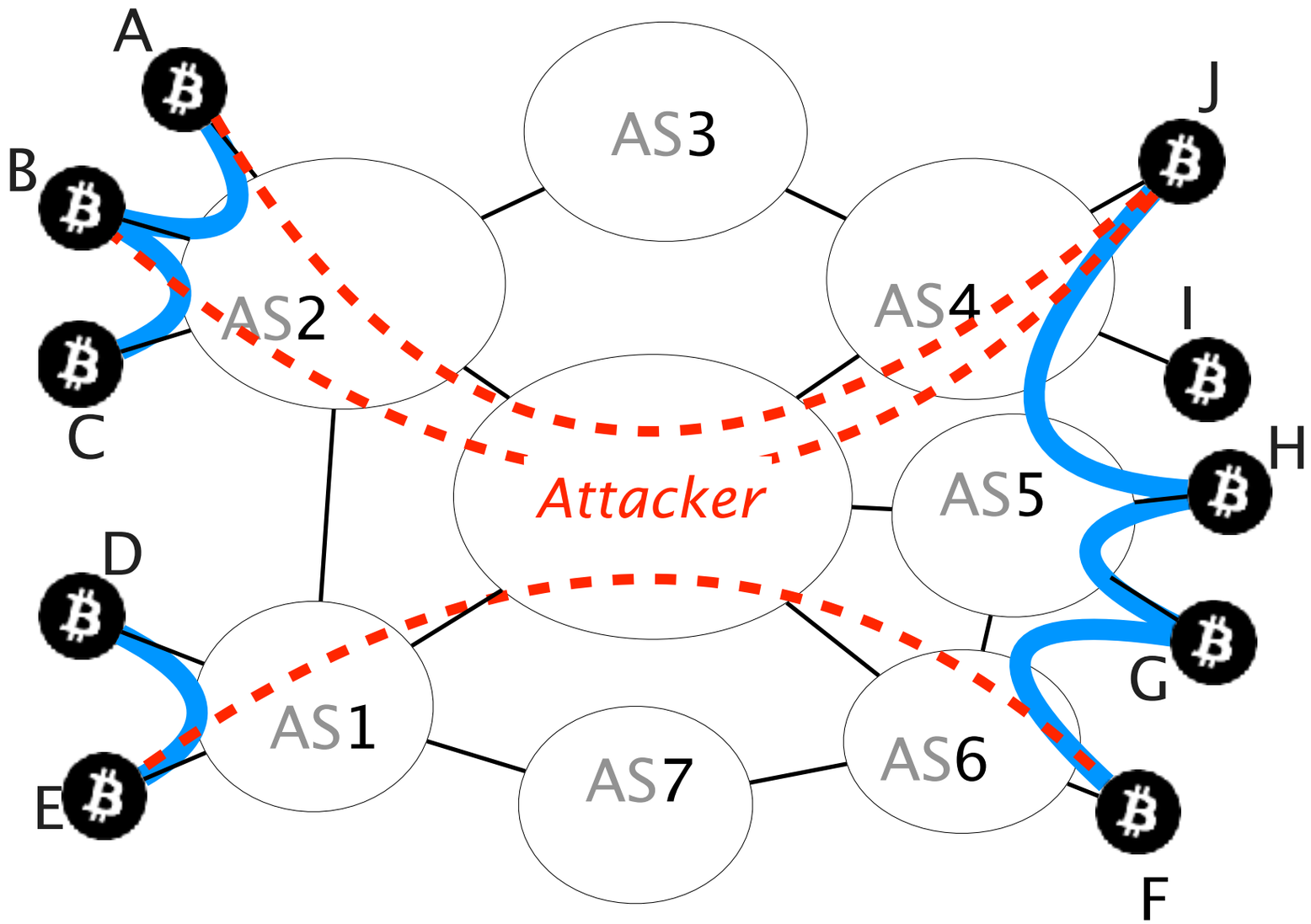
Transactions in components with less mining power can be reverted

# How does the attack work?

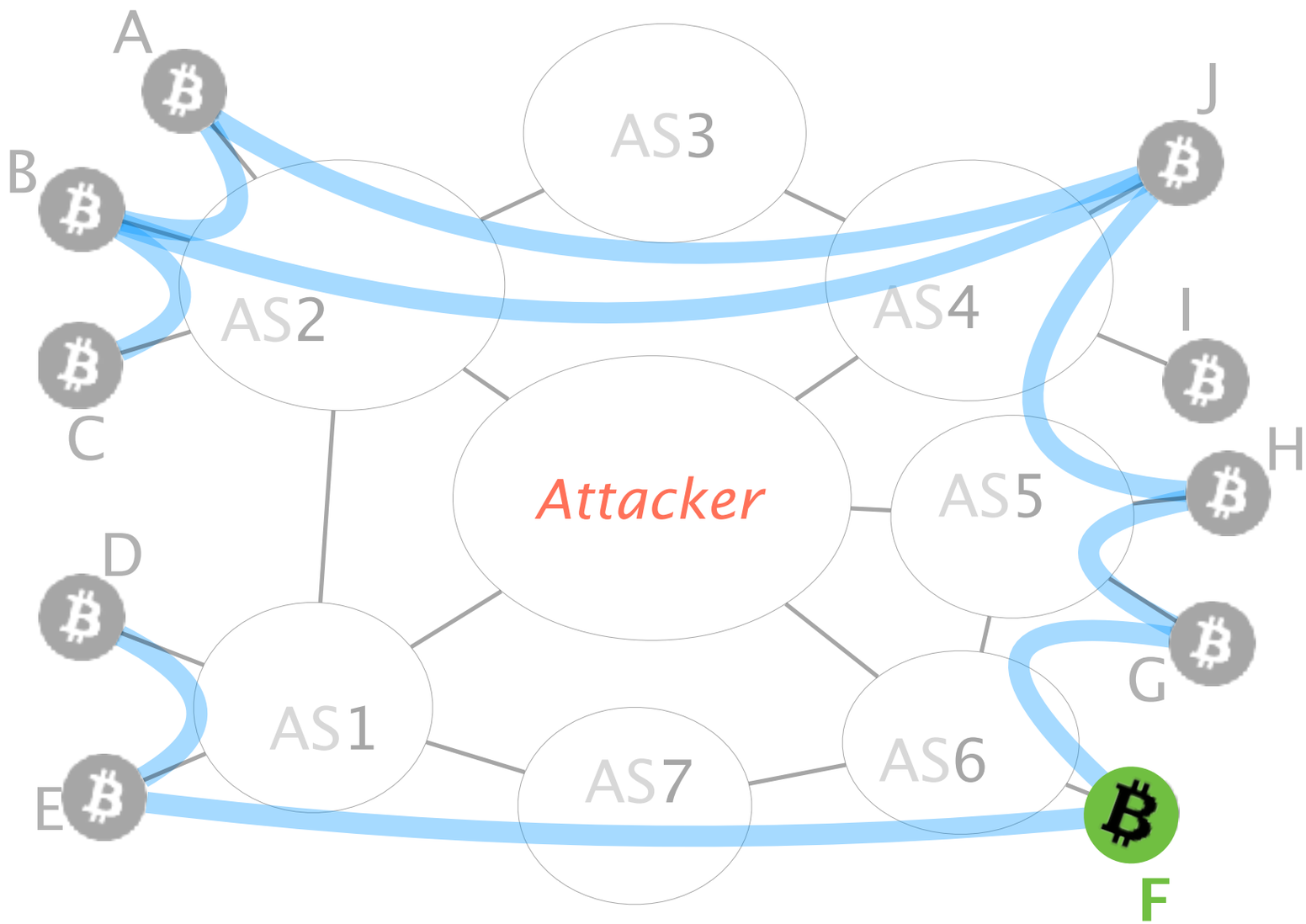
Let’s say an attacker wants to partition the network into the left and right side



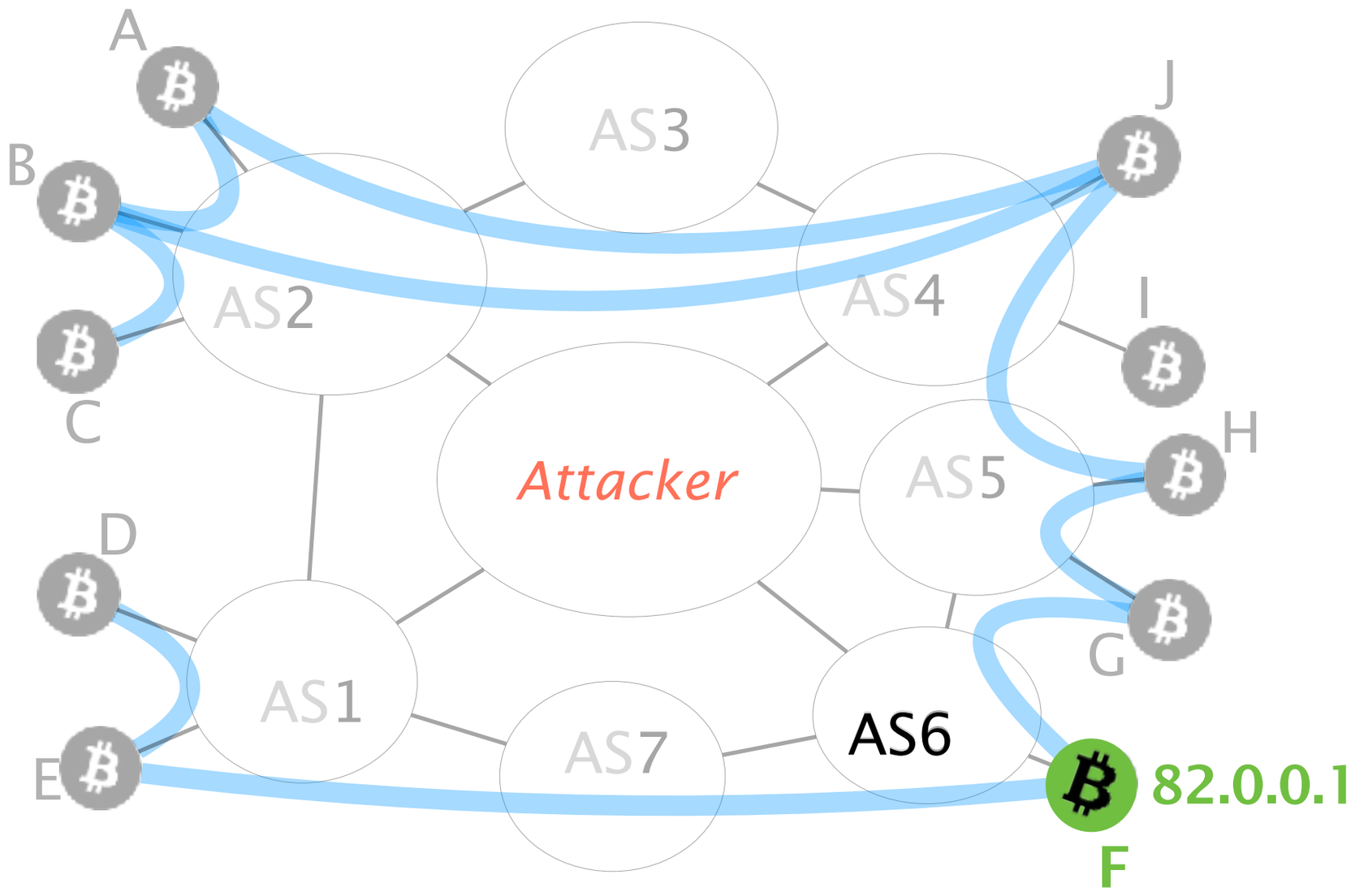
For doing so, the attacker will manipulate BGP routes to intercept any traffic to the nodes in the right



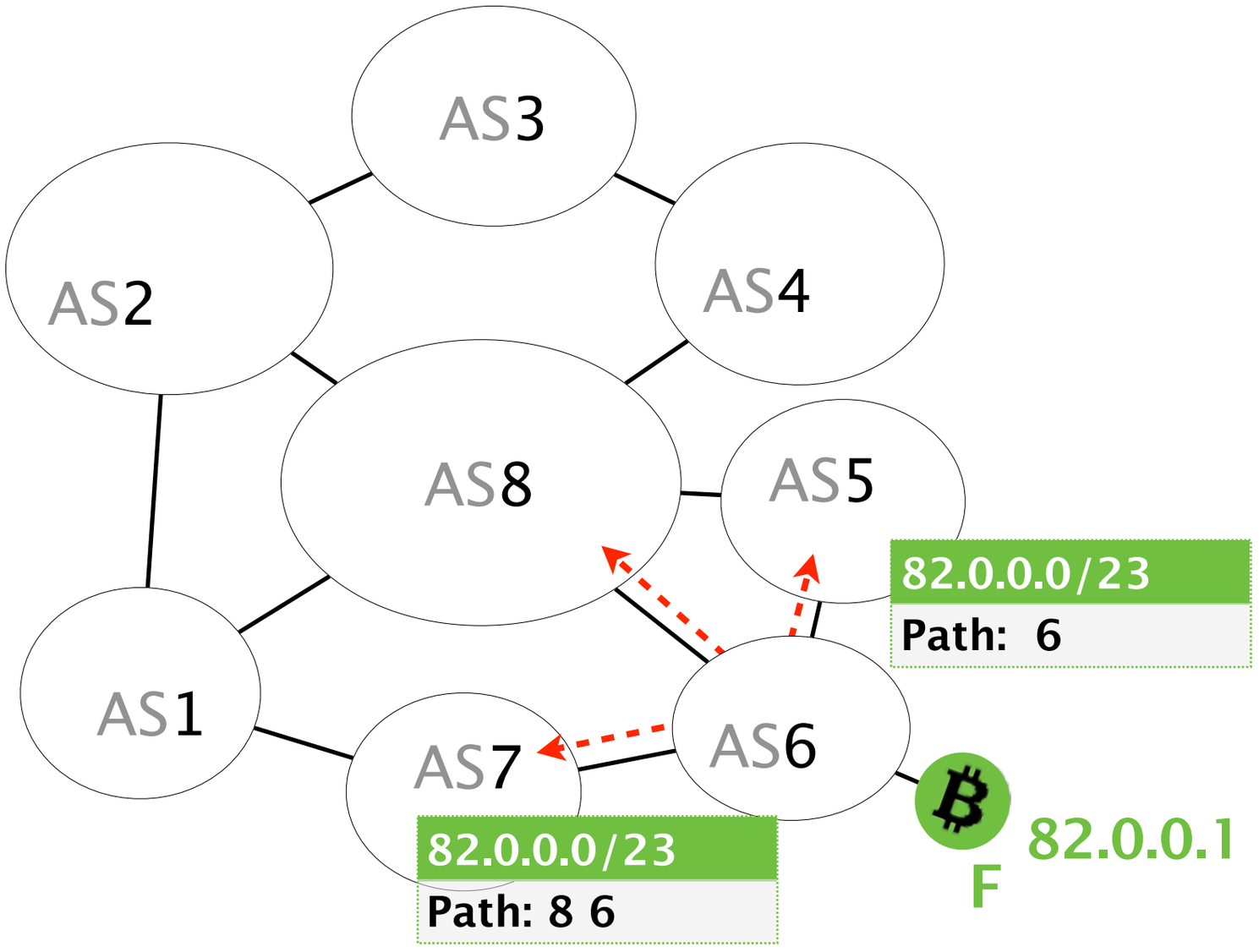
# Let us focus on node F



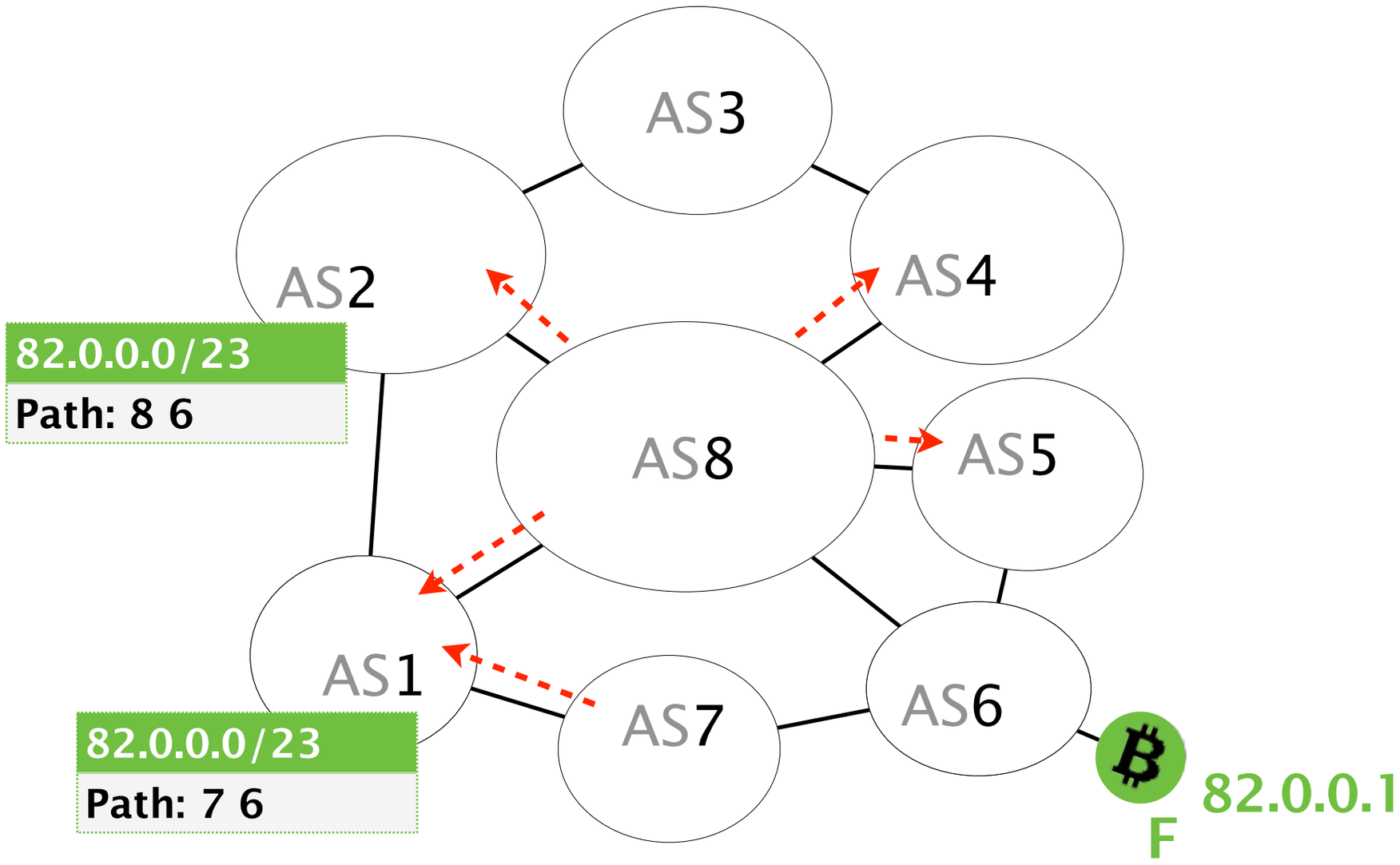
# F's provider (AS6) is responsible for IP prefix



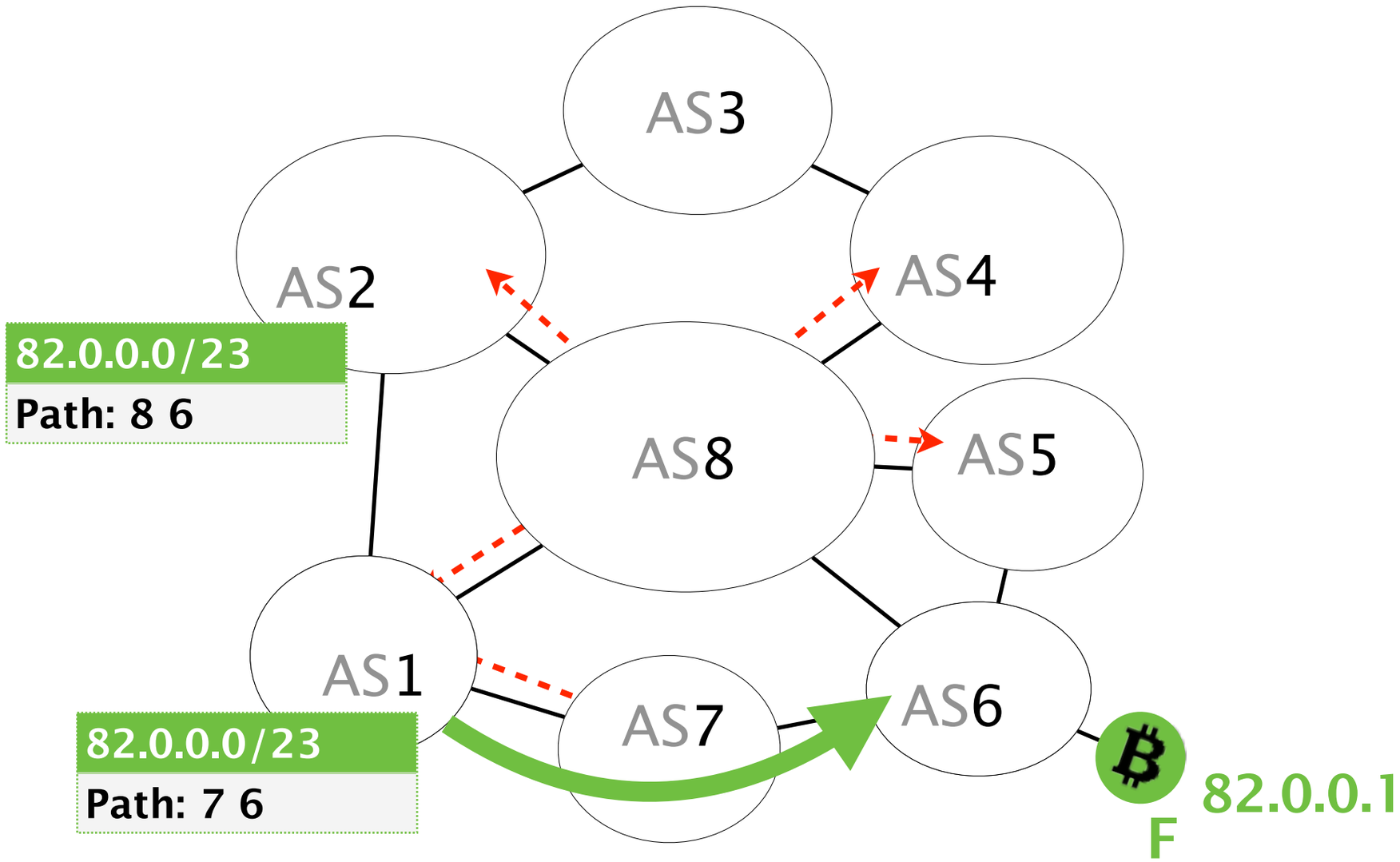
# AS6 will create a BGP advertisement



AS6's advertisement is propagated AS-by-AS until all ASes in the Internet learn about it



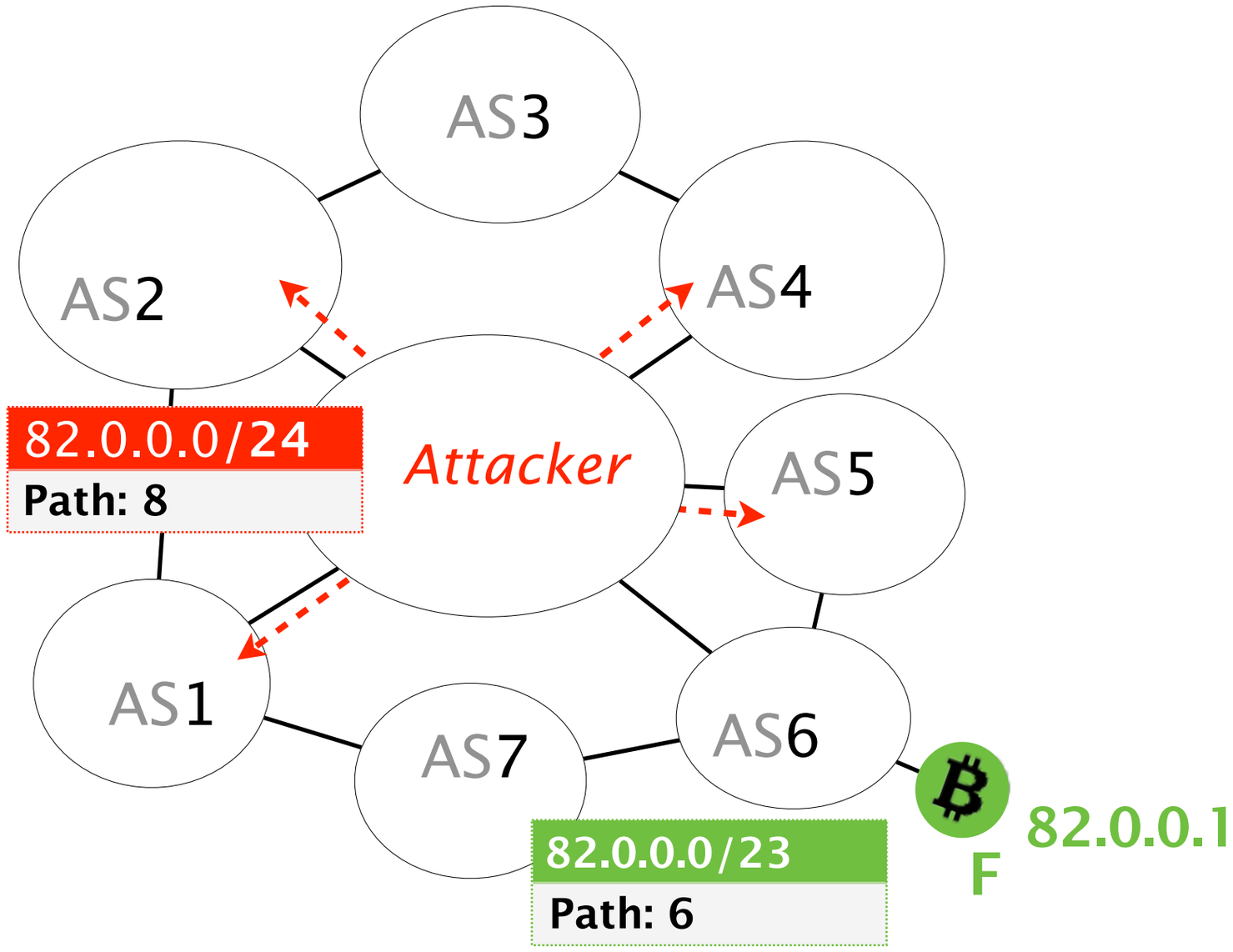
AS6's advertisement is propagated AS-by-AS until all ASes in the Internet learn about it



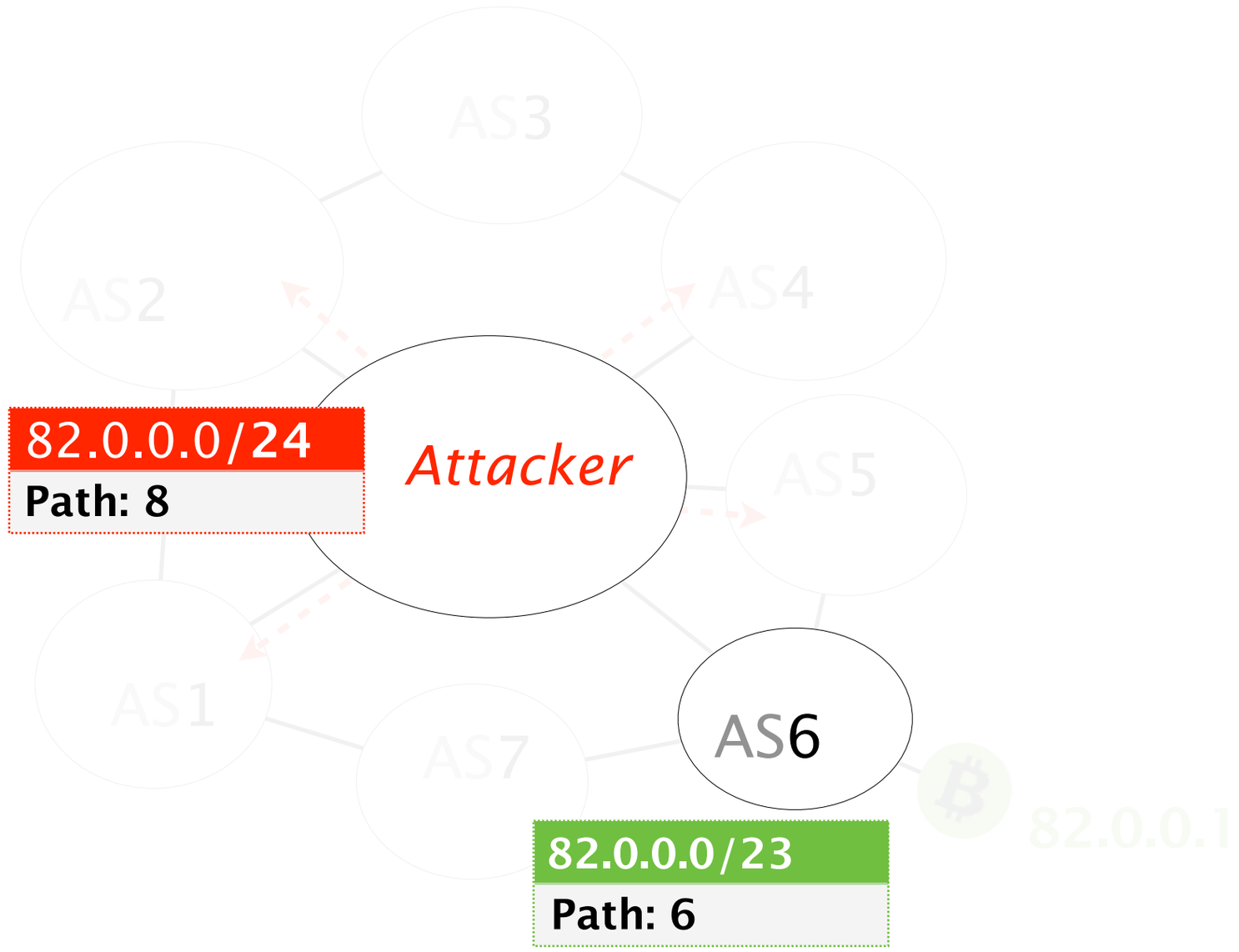
BGP does not check the validity of advertisements, meaning any AS can announce any prefix

Consider that the attacker advertises a more-specific prefix covering F's IP address

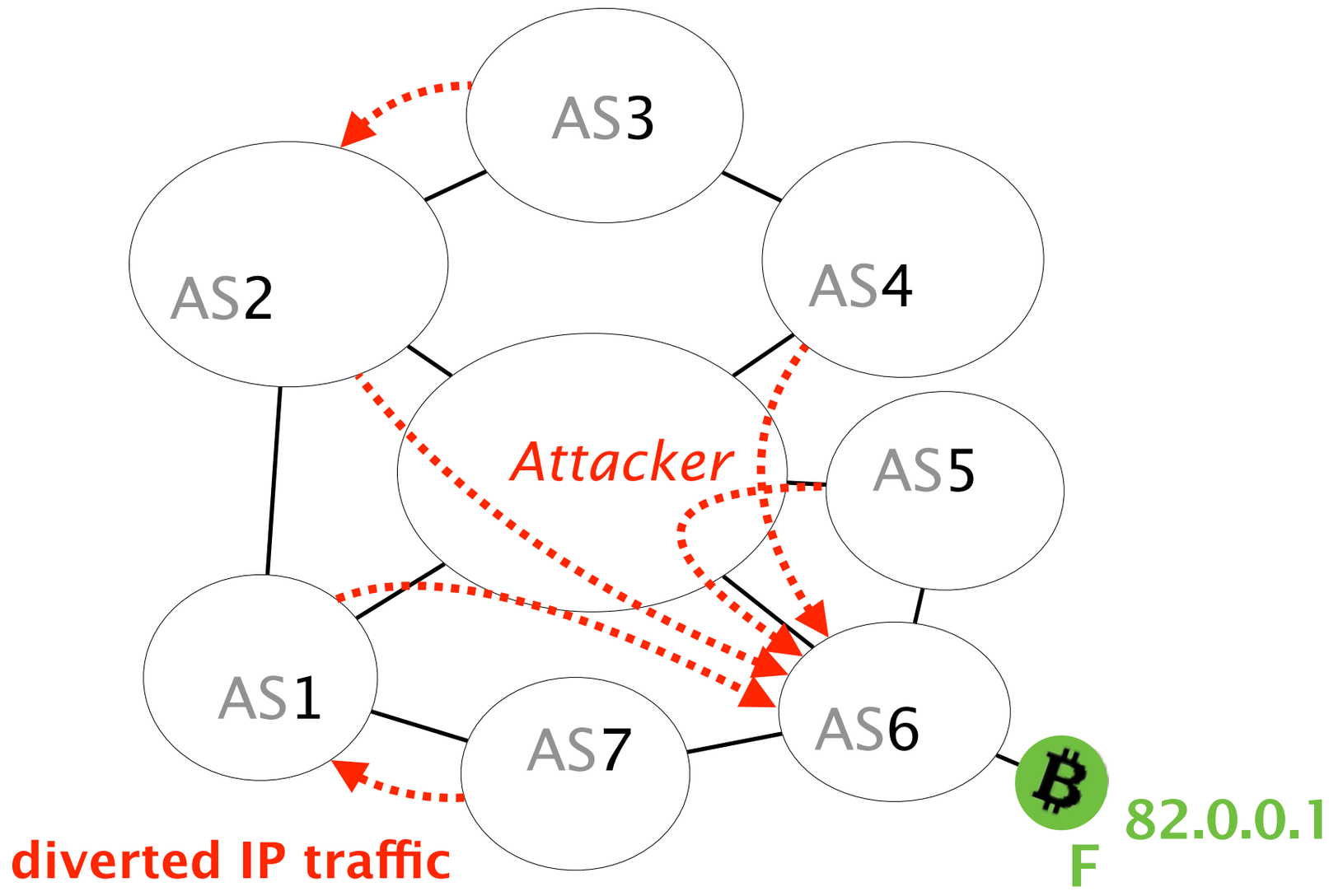
Consider that the attacker advertises a more-specific prefix covering F's IP address



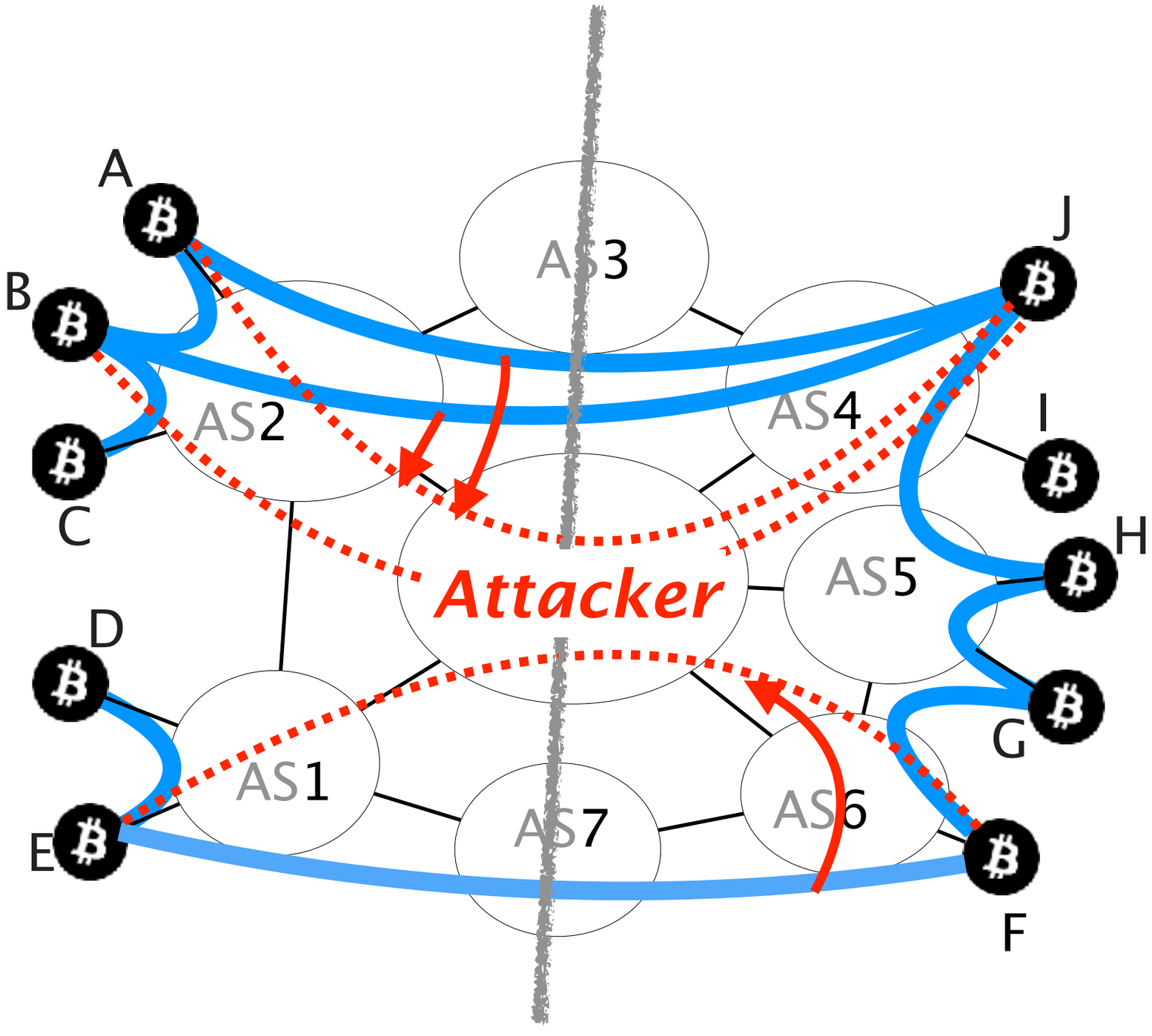
As IP routers prefer more-specific prefixes, the attacker route will be preferred



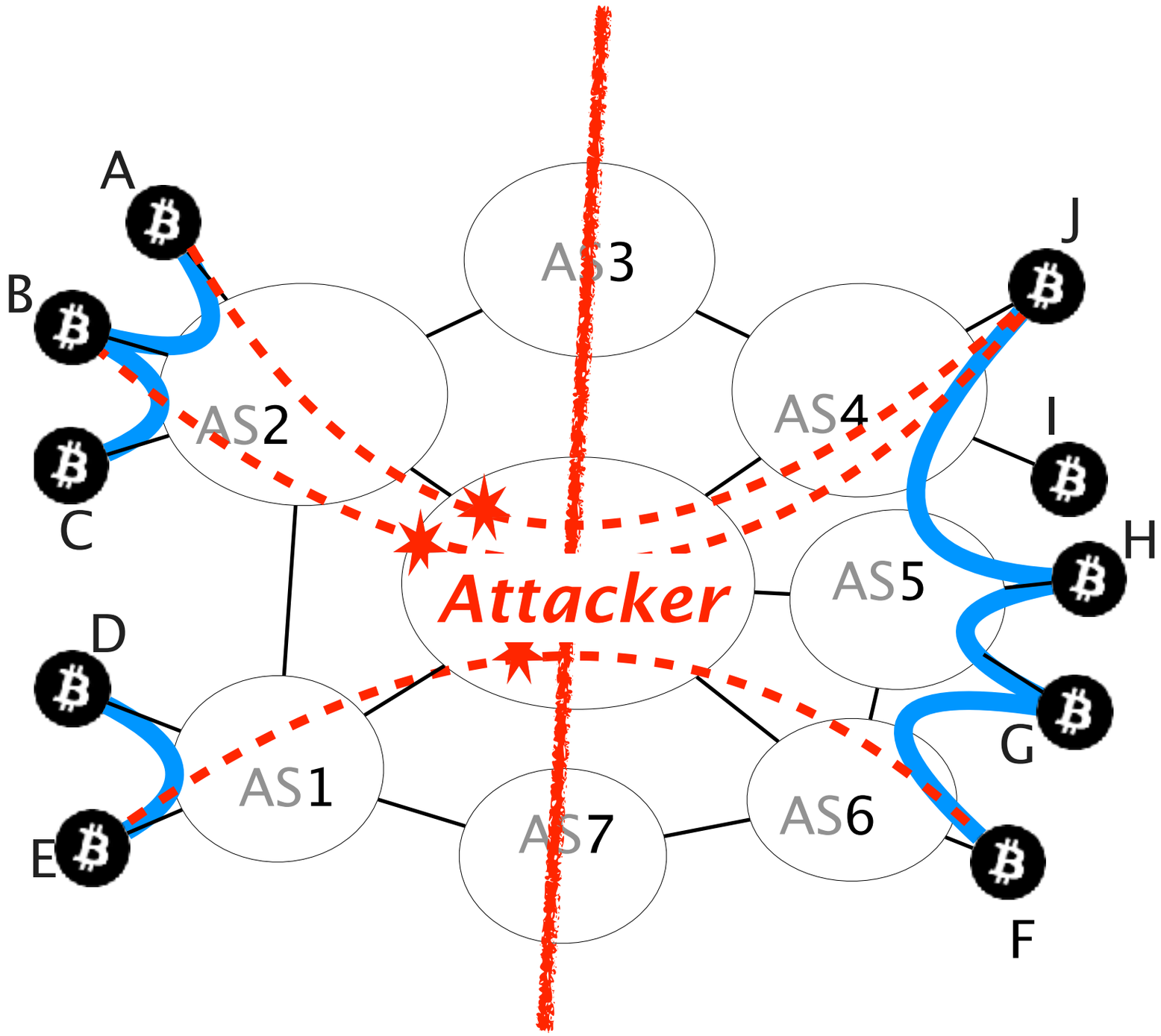
# Traffic to node F is hijacked



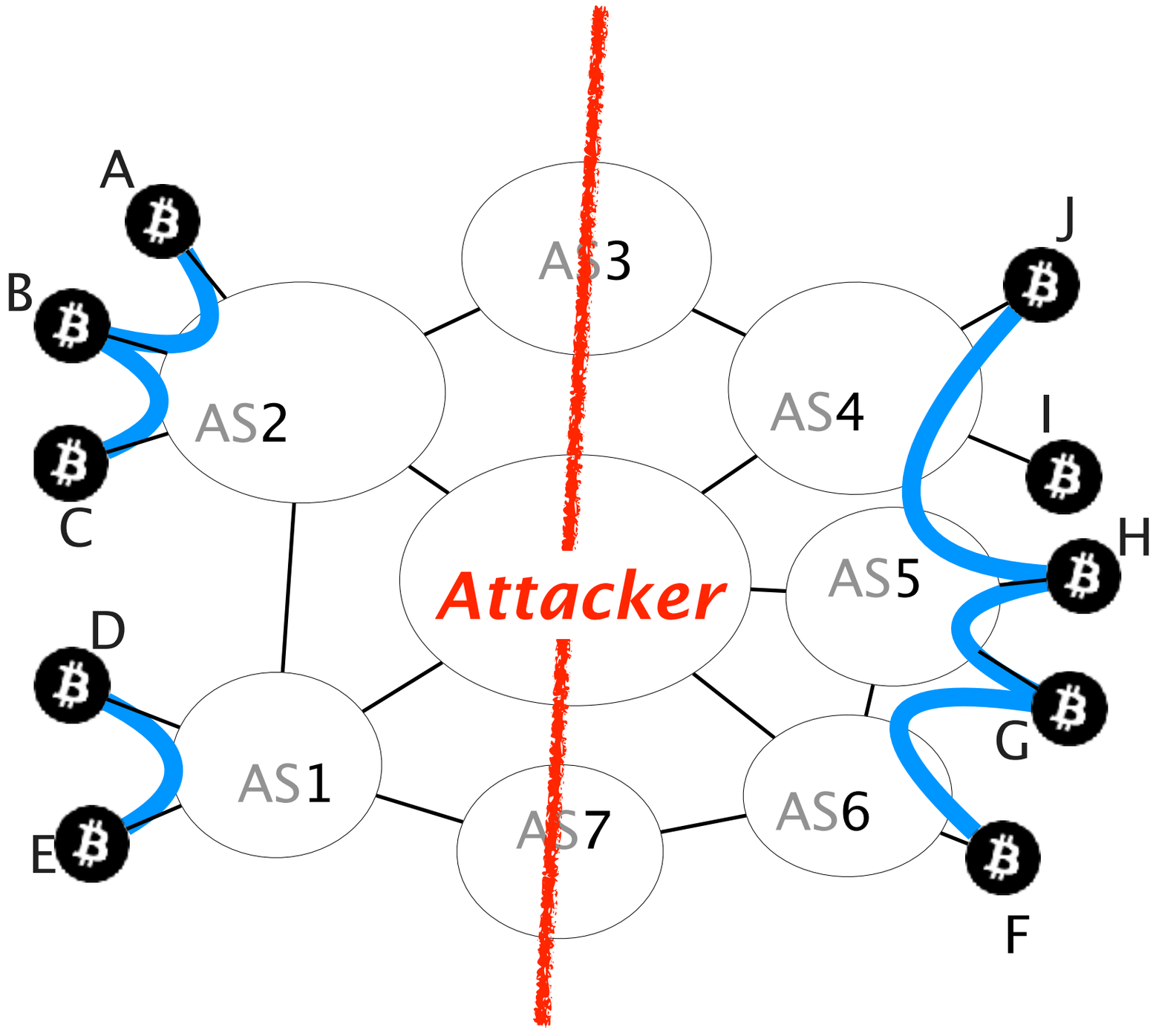
By hijacking the IP prefixes pertaining to the right nodes, the attacker can intercept all their connections



Once on-path, the attacker can drop all connections crossing the partition



# The partition is created



Not all partition are feasible in practice:
some connections cannot be intercepted

Bitcoin connections established…

- within a mining pool
- within an AS
- between mining pools

cannot be hijacked (usually)

Bitcoin connections established…

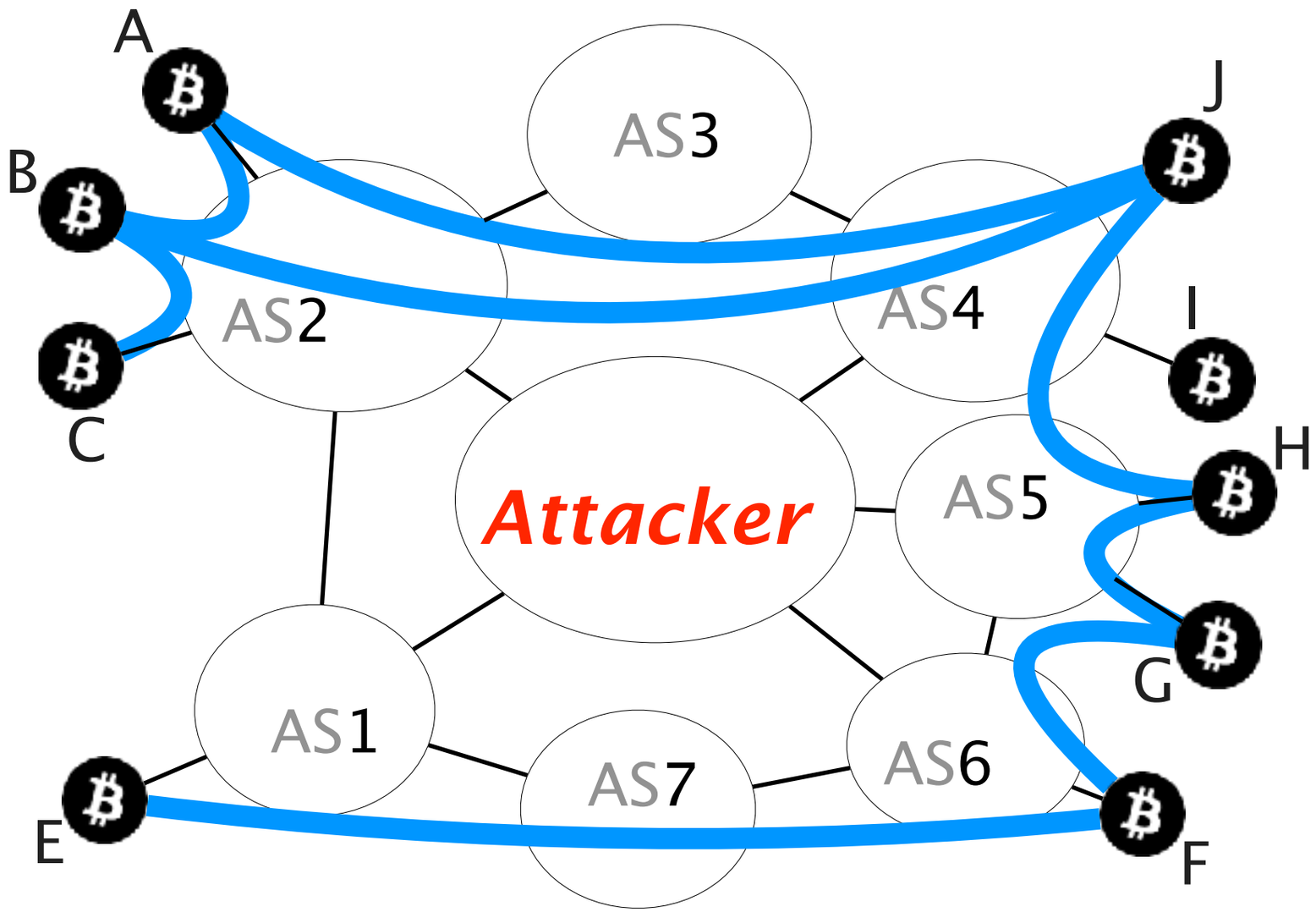
- within a mining pool
- within an AS
- between mining pools

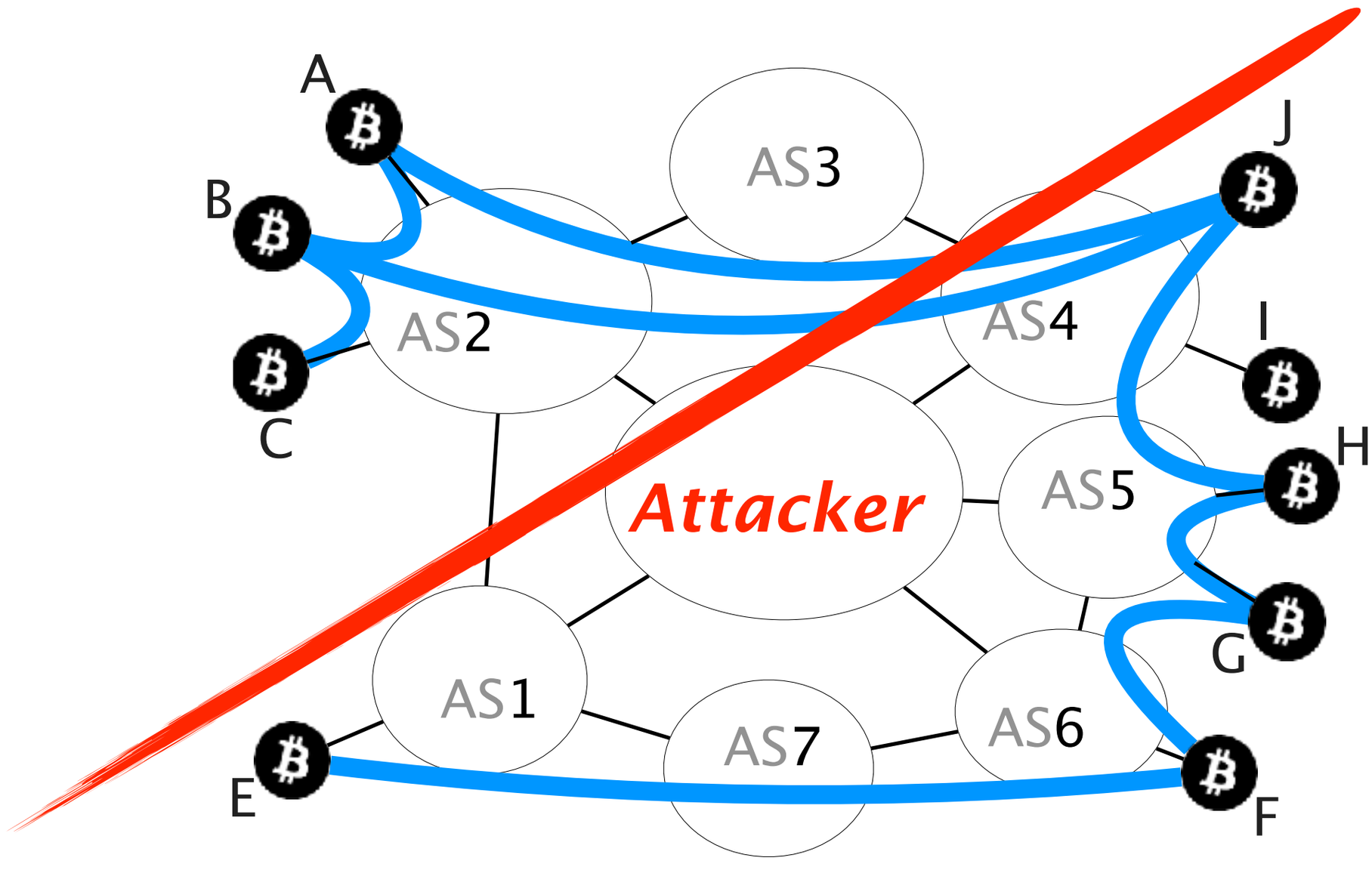
cannot be hijacked (usually)

*but* can be *detected* and *located* by the attacker

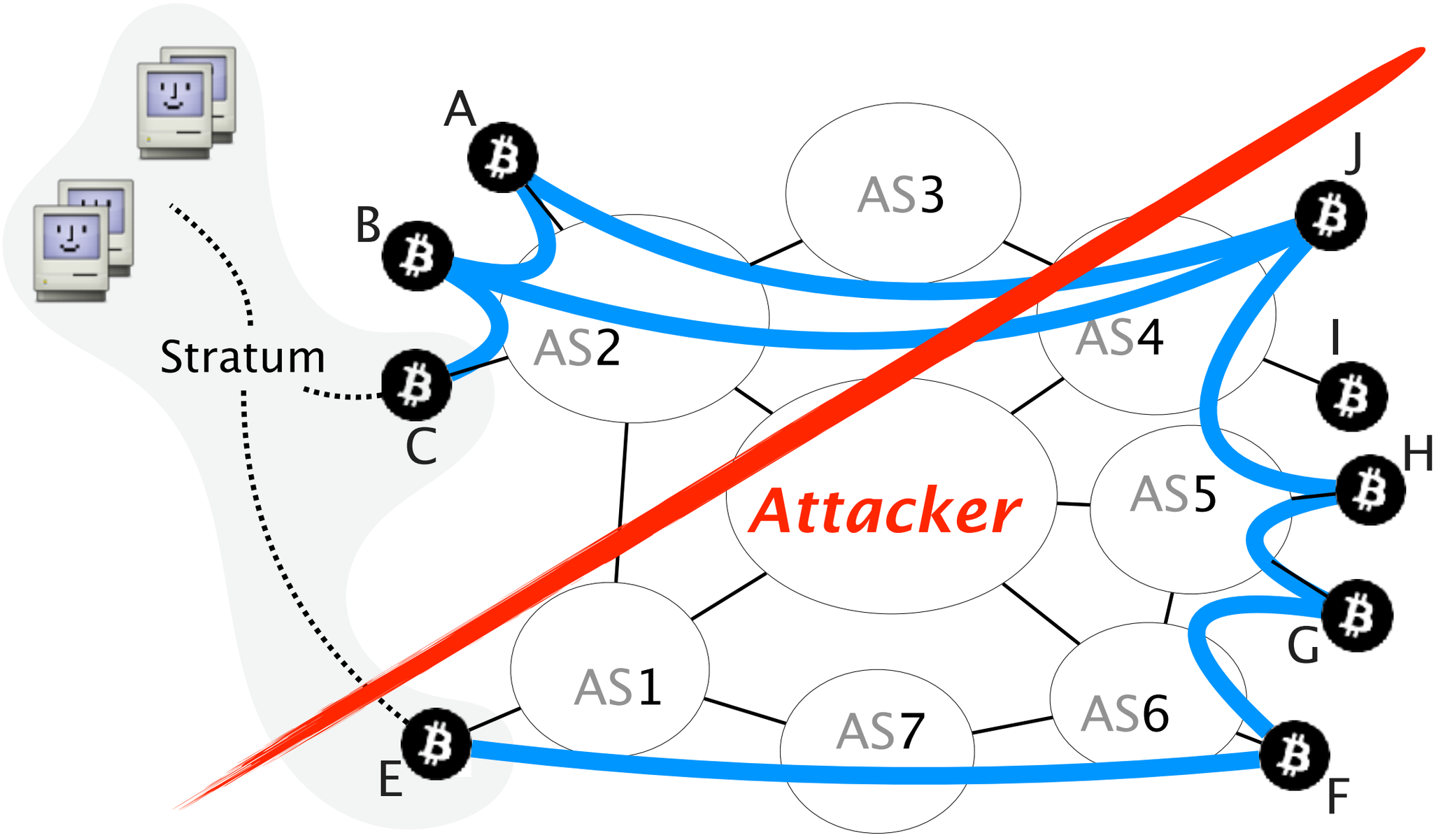
enabling her to build a similar but feasible partition

Let’s say the same attacker
wants to create another partition

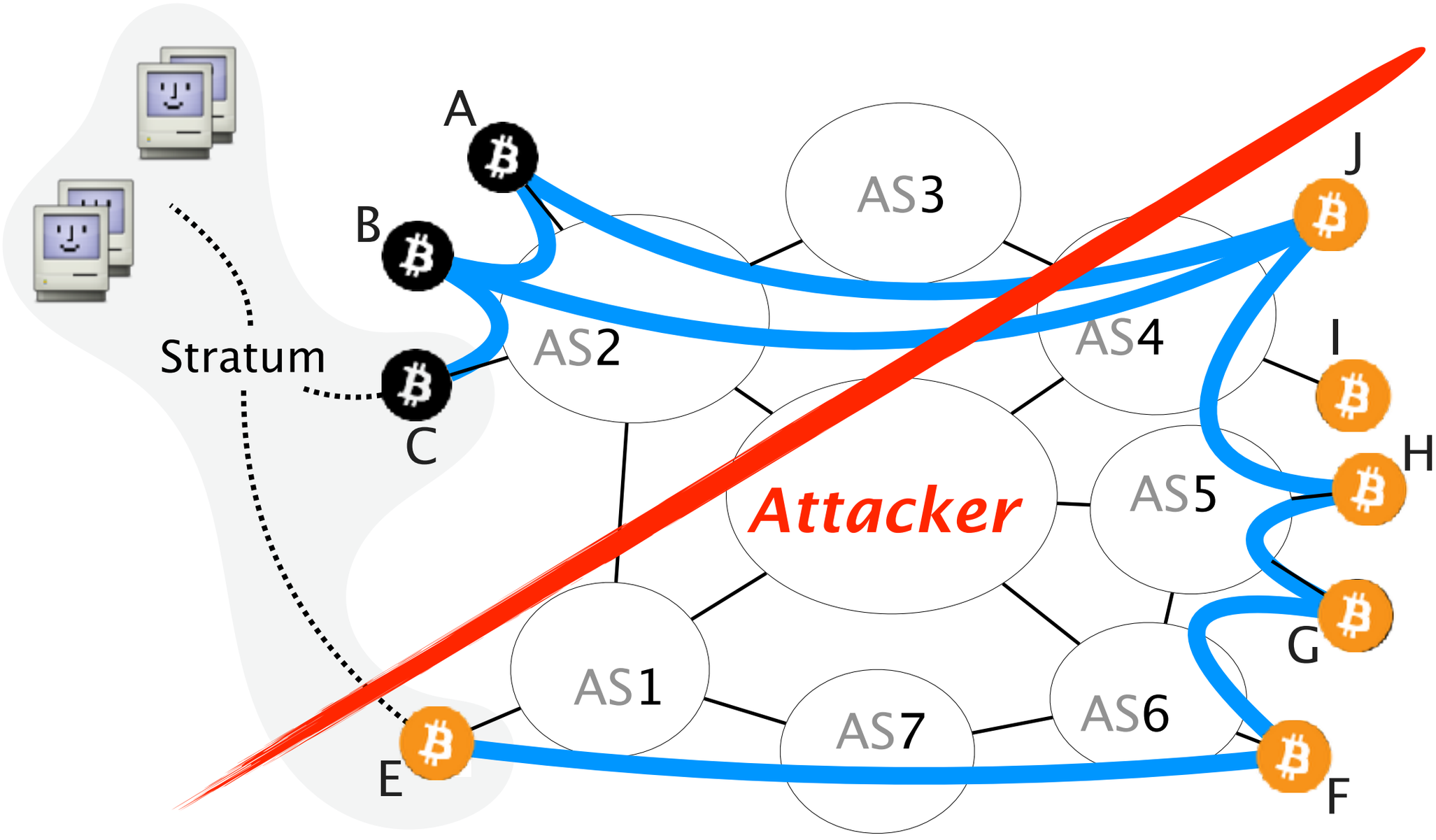


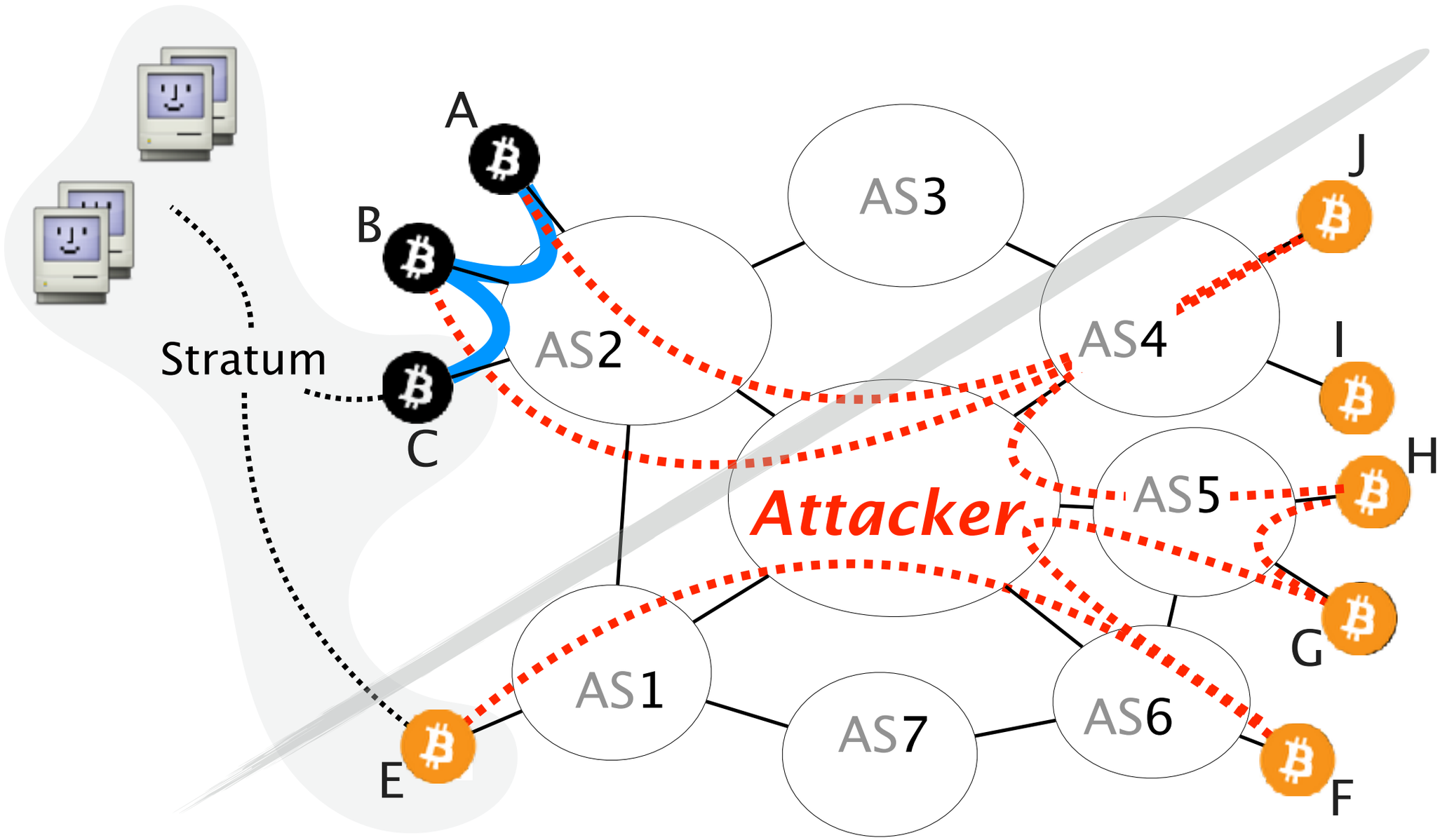

A
B
C
AS3
AS2
AS4
J
I
H
G
Attacker
AS5
AS1
AS7
AS6
E
F

# … with a mining pool in the middle

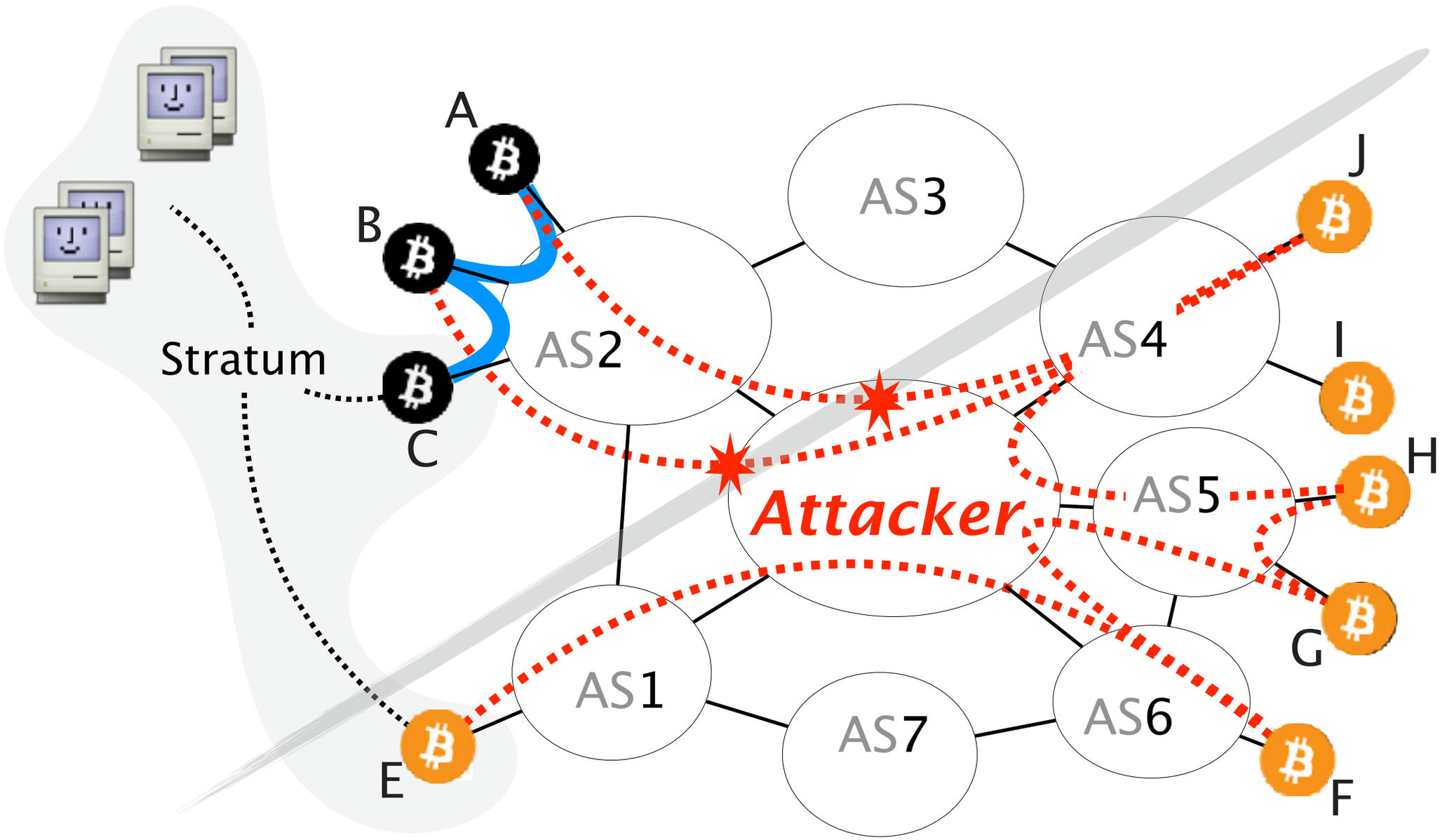


For this, the attacker hijacks all prefixes pertaining to the nodes located on the right-hand side

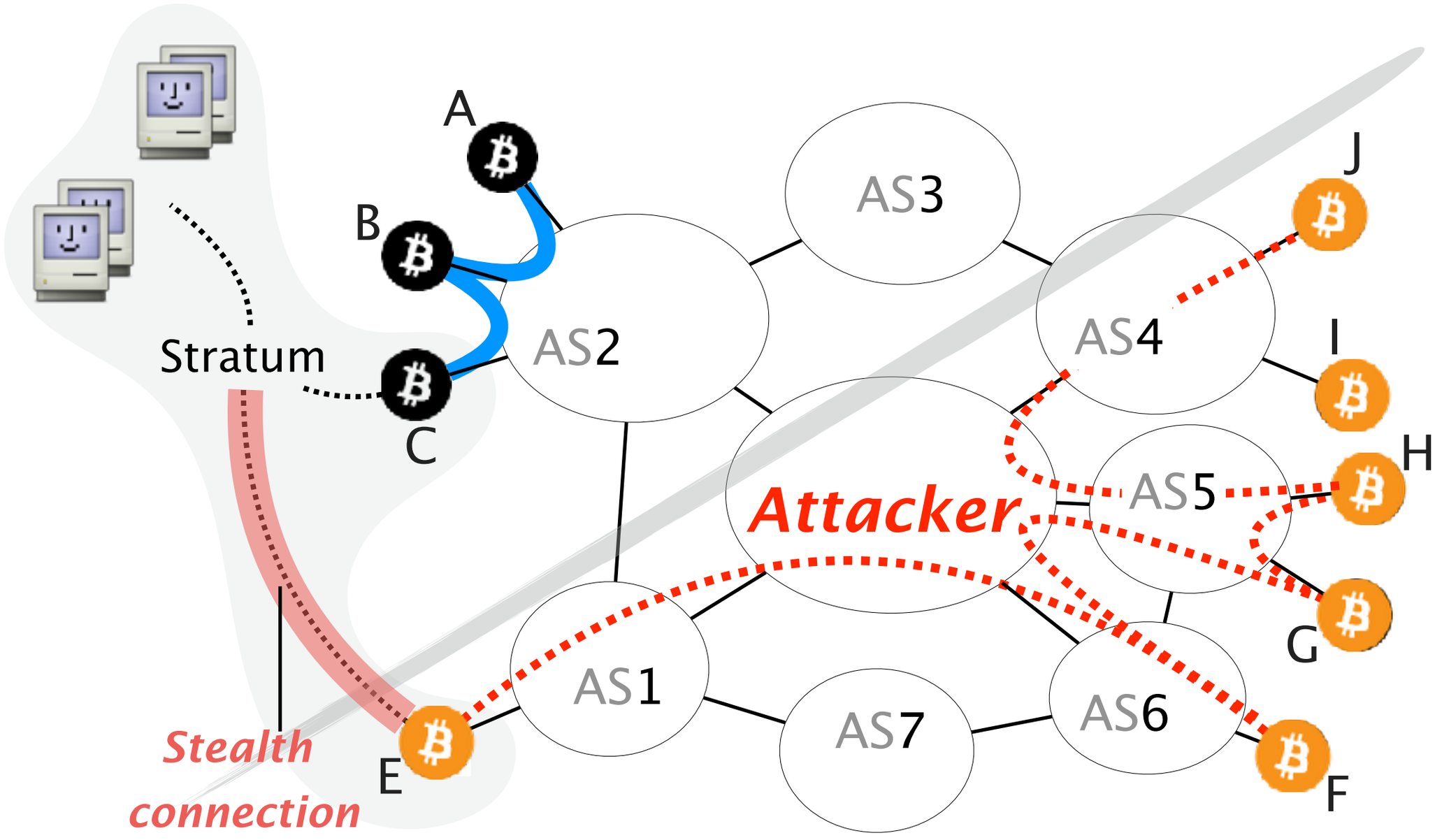



A
B
C
Stratum
AS2
AS3
AS4
J
I
H
G
F
Attacker
AS5
AS1
AS7
AS6
E

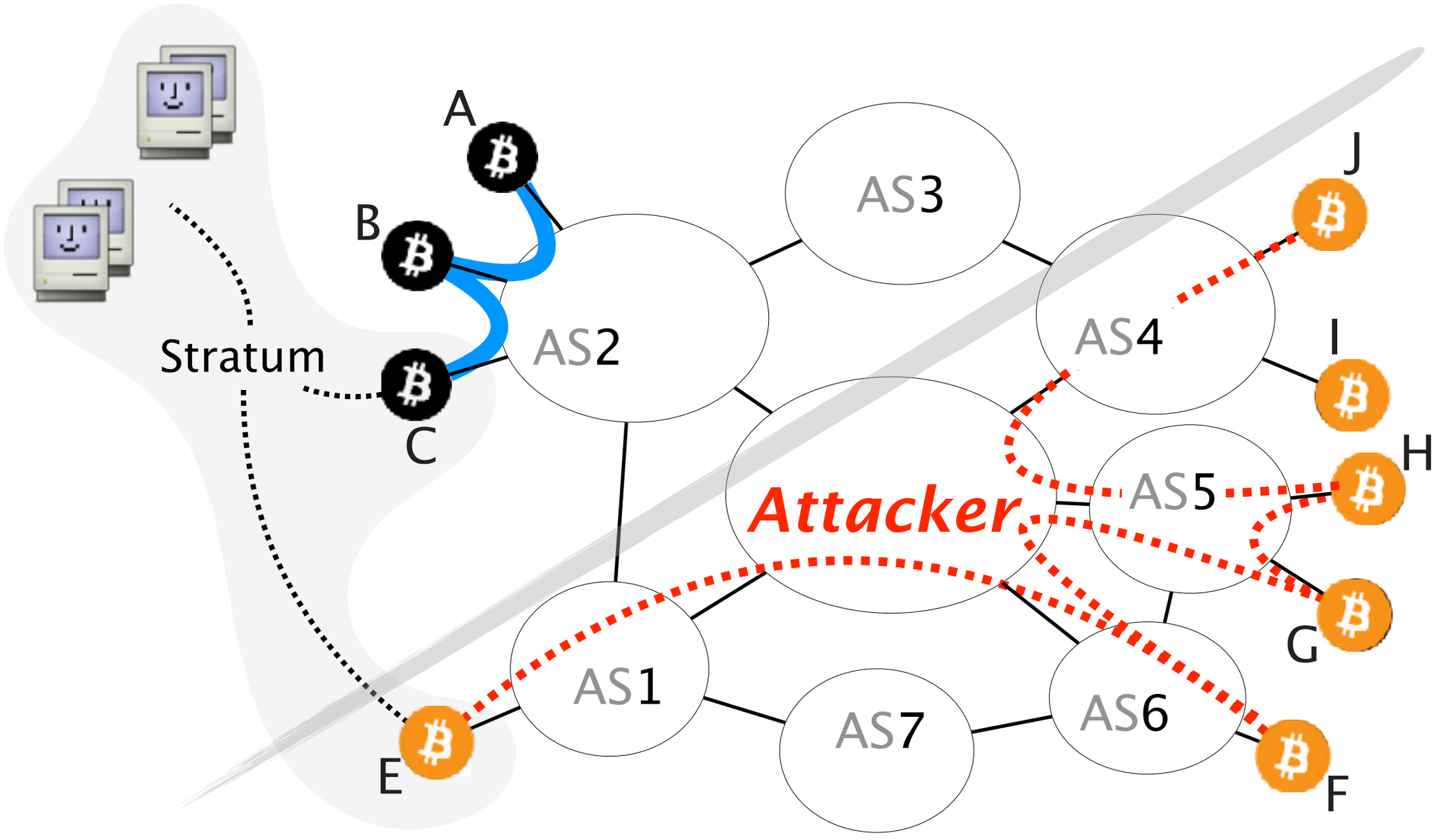
# The attacker then drops the connections



This partition is ineffective because of a stealth connection



Yet, by monitoring the connections, the attacker can figure out that there is a leakage



Theorem

Given a set of nodes to disconnect from the network, there exist a unique maximal subset that can be isolated and that the attacker will isolate.

see paper for proof

We evaluated the partition attack in terms of practicality and time efficiency

Practicality

Can it actually happen?

Time efficiency

How long does it take?

We evaluated the partition attack in terms of practicality and time efficiency

Practicality

Time efficiency

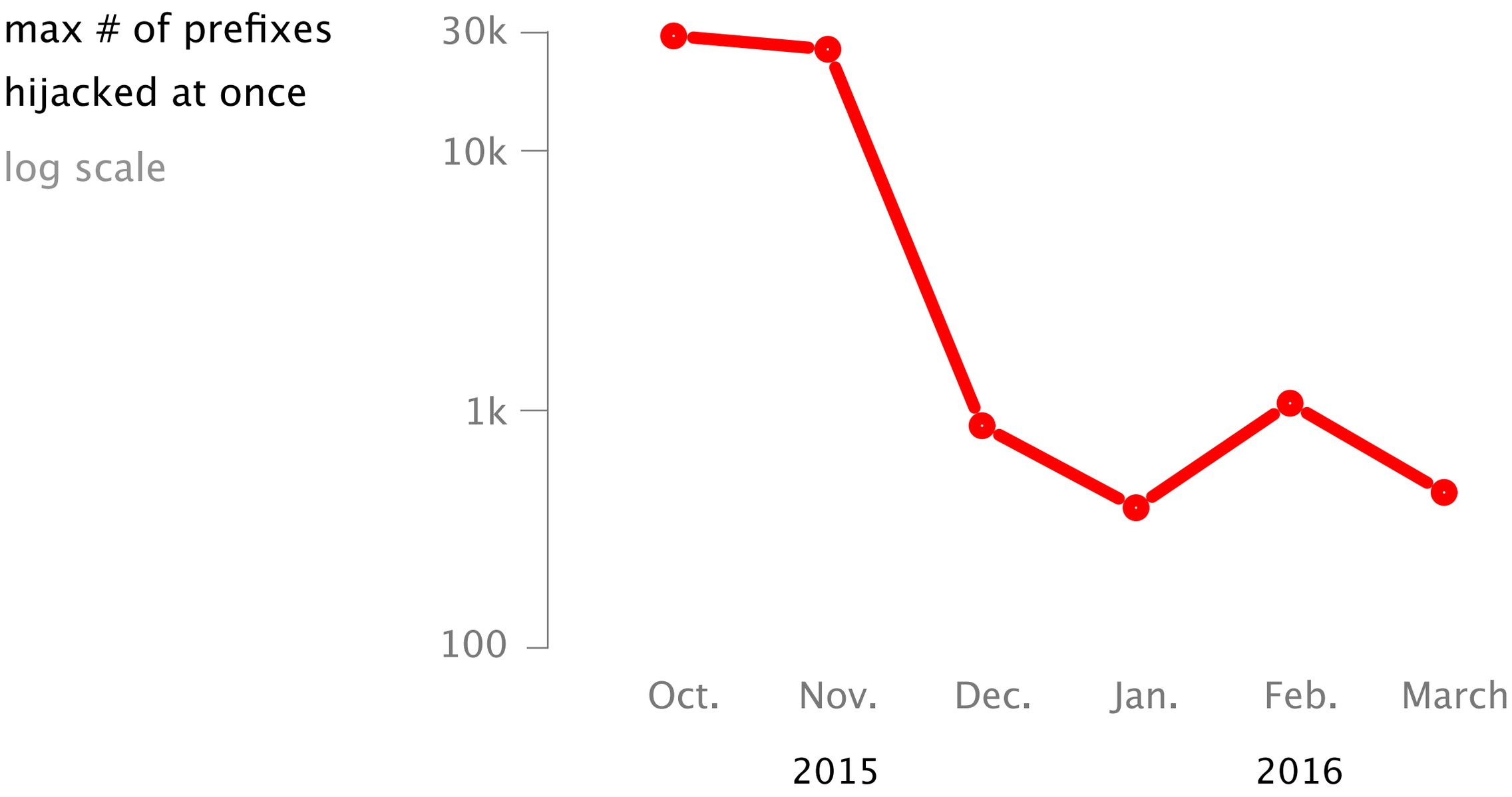
Can it actually happen?

Splitting the mining power even to half can be done by hijacking less than 100 prefixes

Splitting the mining power even to half can be done by hijacking less than 100 prefixes

*negligible* with respect to routinely observed hijacks

# Hijacks involving up to 1k of prefixes are frequently seen in the Internet today



We also evaluated the partition in terms of time efficiency

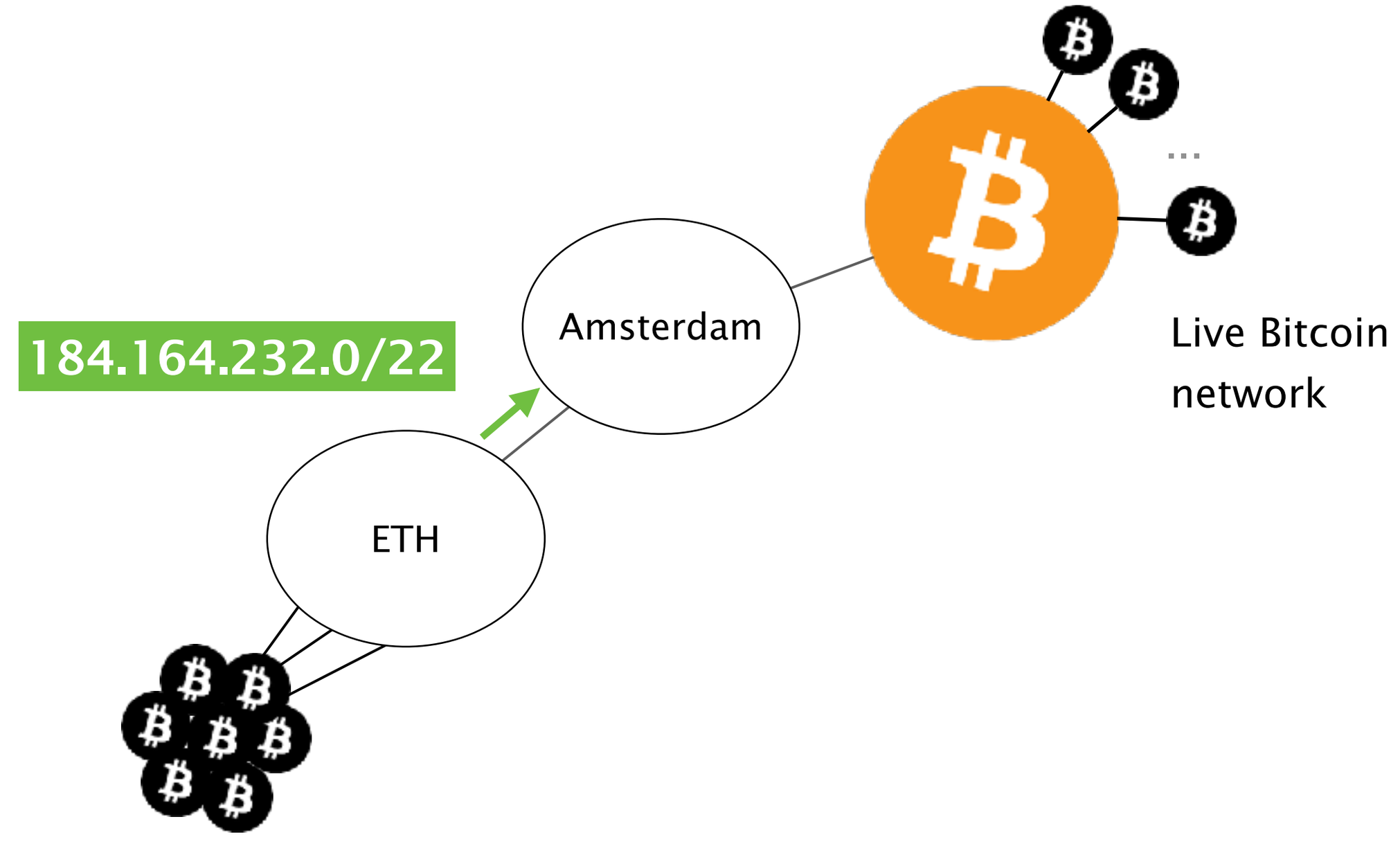
Practicality

Time efficiency

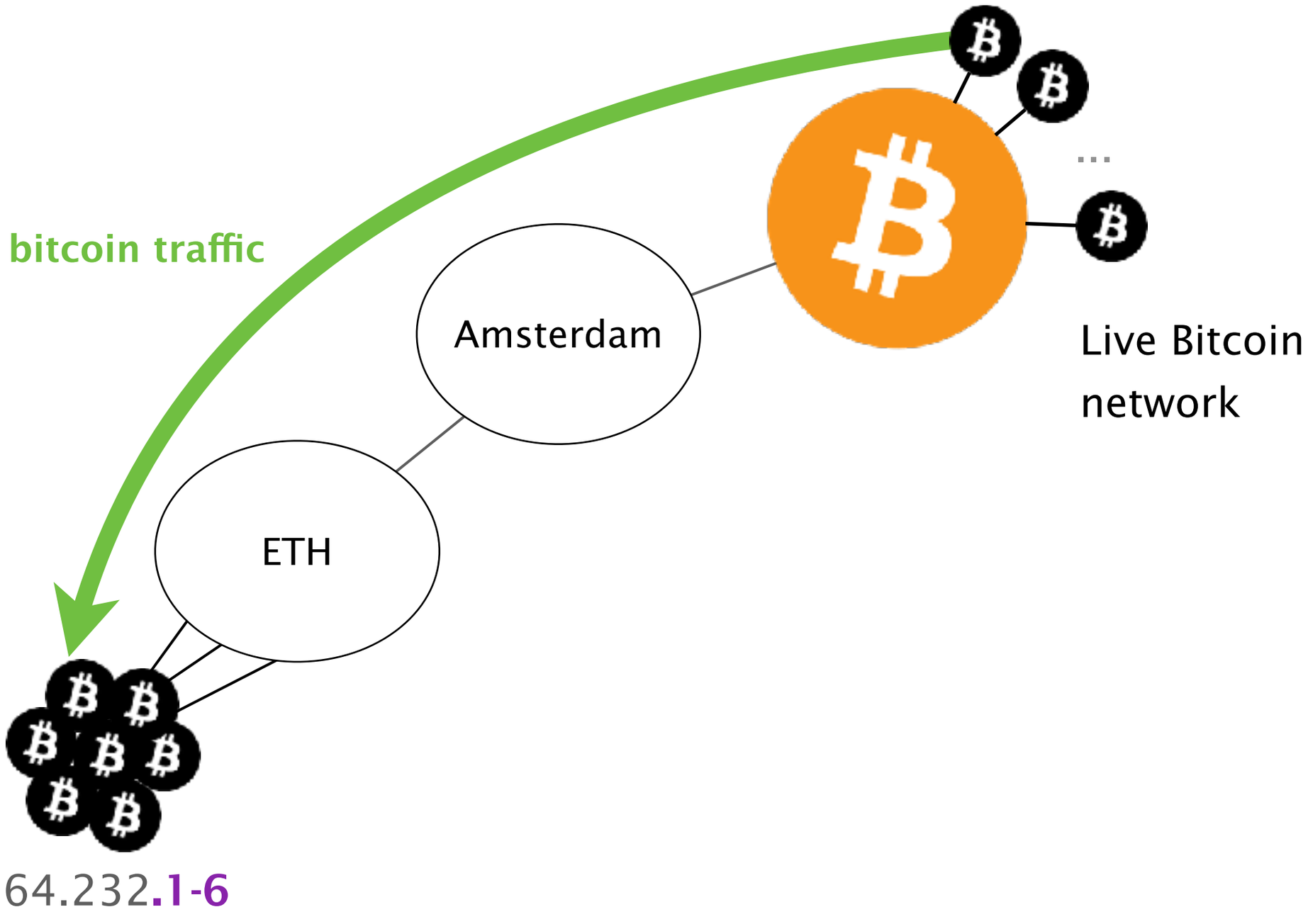
How long does it take?

We measured the time required to perform a partition attack by attacking our own nodes

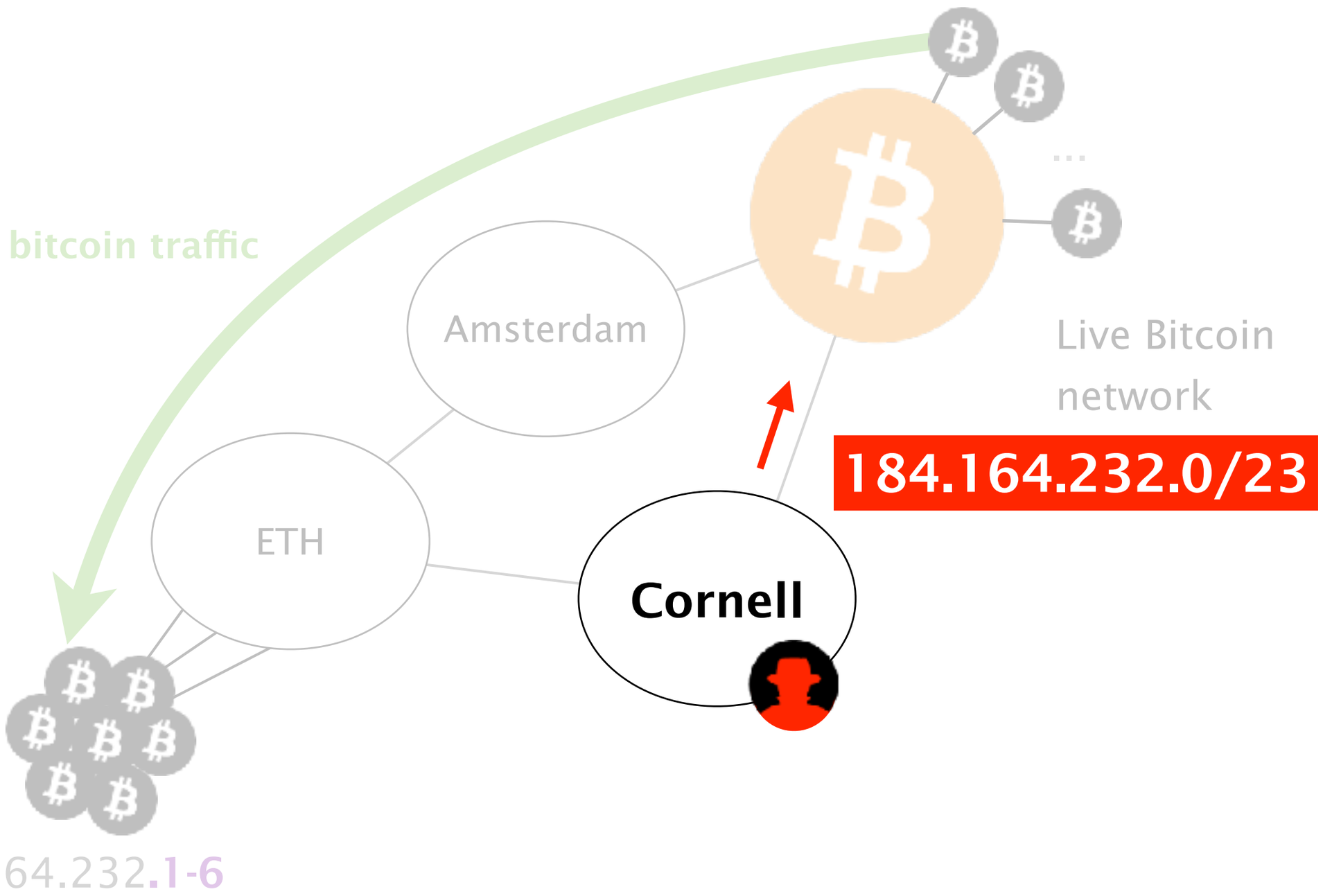
We hosted a few Bitcoin nodes at ETH and advertised a covering prefix via Amsterdam



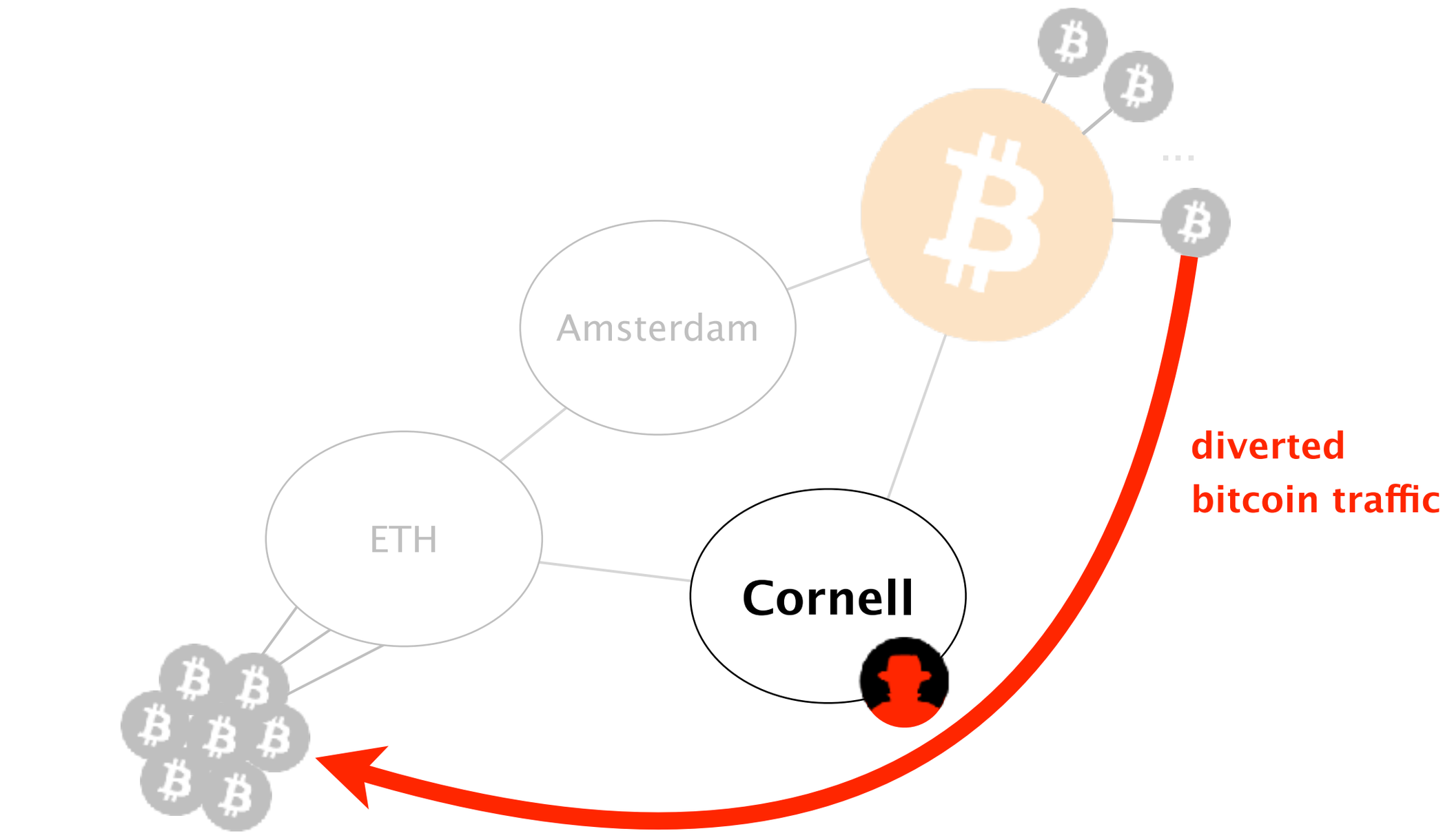
# Initially, all the traffic to our nodes transits via Amsterdam

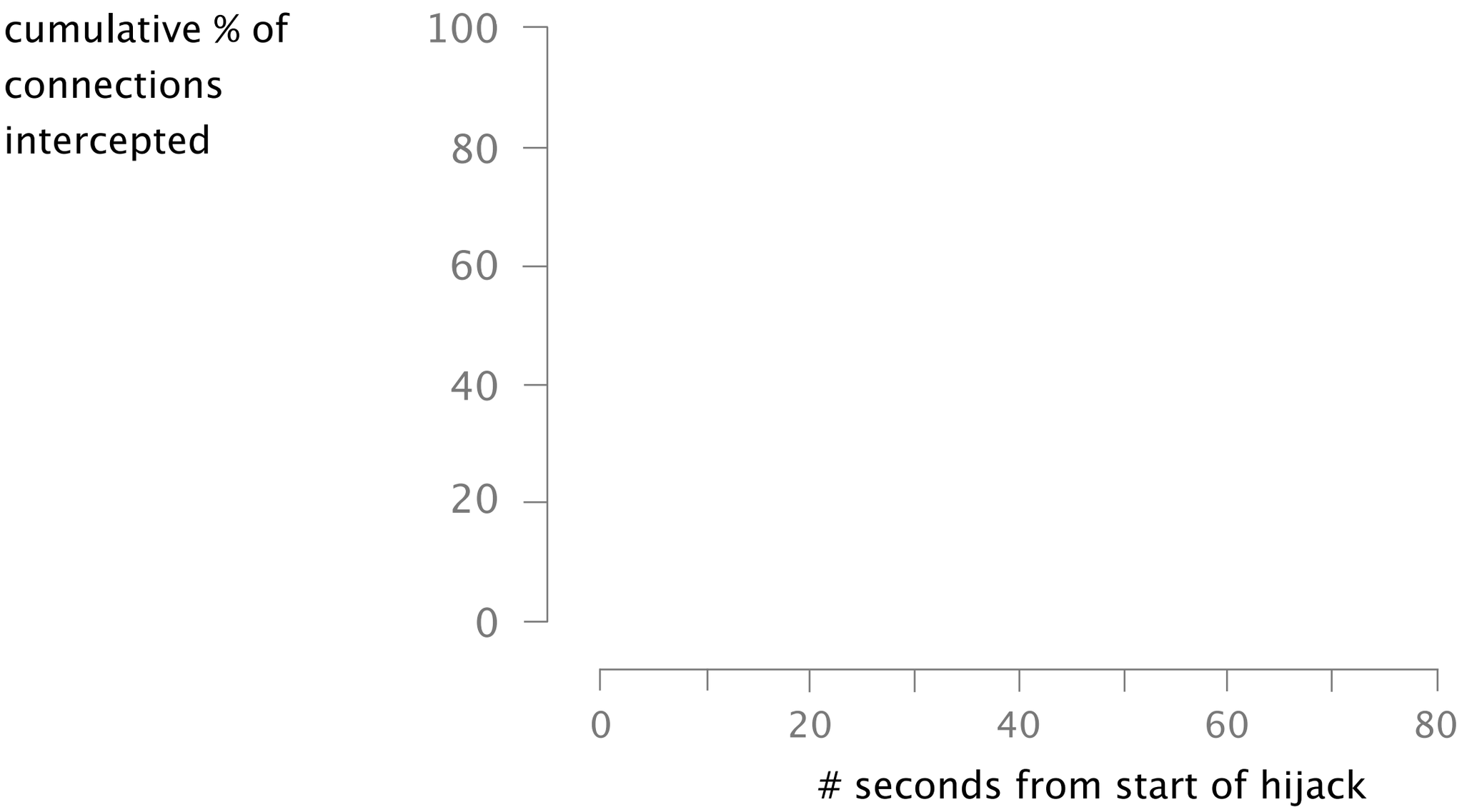


# We hijacked our nodes

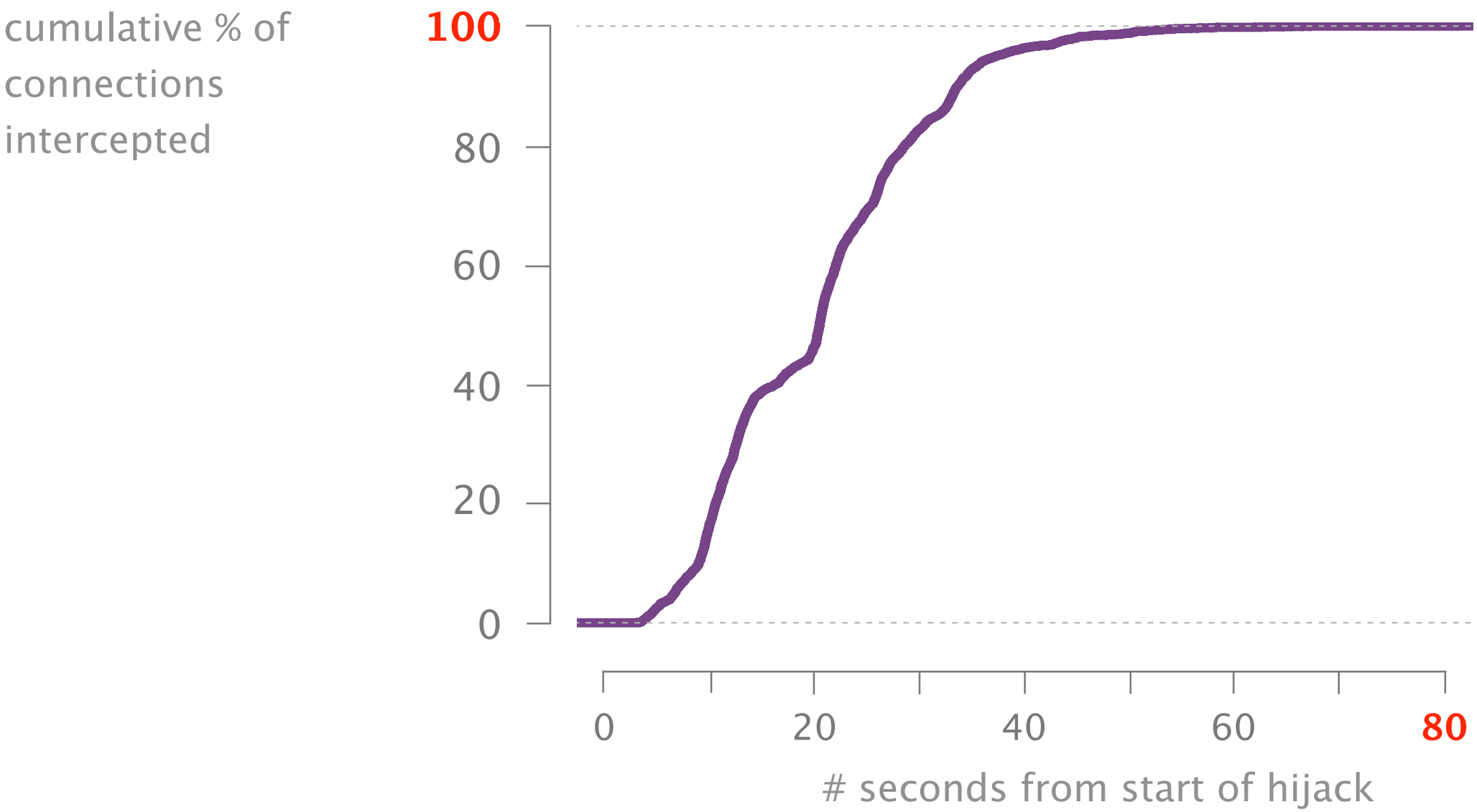


We measured the time required for a rogue AS to divert all the traffic to our nodes




cumulative % of connections intercepted
100
80
60
40
20
0
0
20
40
60
80
# seconds from start of hijack

# It takes less than 2 minutes for the attacker to intercept all the connections



Mitigating a hijack is a human-driven process,
as such it often takes hours to be resolved

Mitigating a hijack is a human-driven process,
as such it often takes hours to be resolved

It took Google close to 3h
to mitigate a large hijack in 2008 [6]

(same hold for more recent hijacks)

# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

The goal of a delay attack is to keep the victim uninformed of the latest Block

The impact of delay attacks is worrying and depends on the victim

Merchant

Mining pool

Regular node

# The impact of delay attacks is worrying and depends on the victim

Merchant

Mining pool

Regular node

susceptible to be the victim
of double-spending attacks

The impact of delay attacks is worrying and depends on the victim

Merchant

Mining pool

Regular node

waste their mining power by mining on an obsolete chain

# The impact of delay attacks is worrying and depends on the victim

Merchant

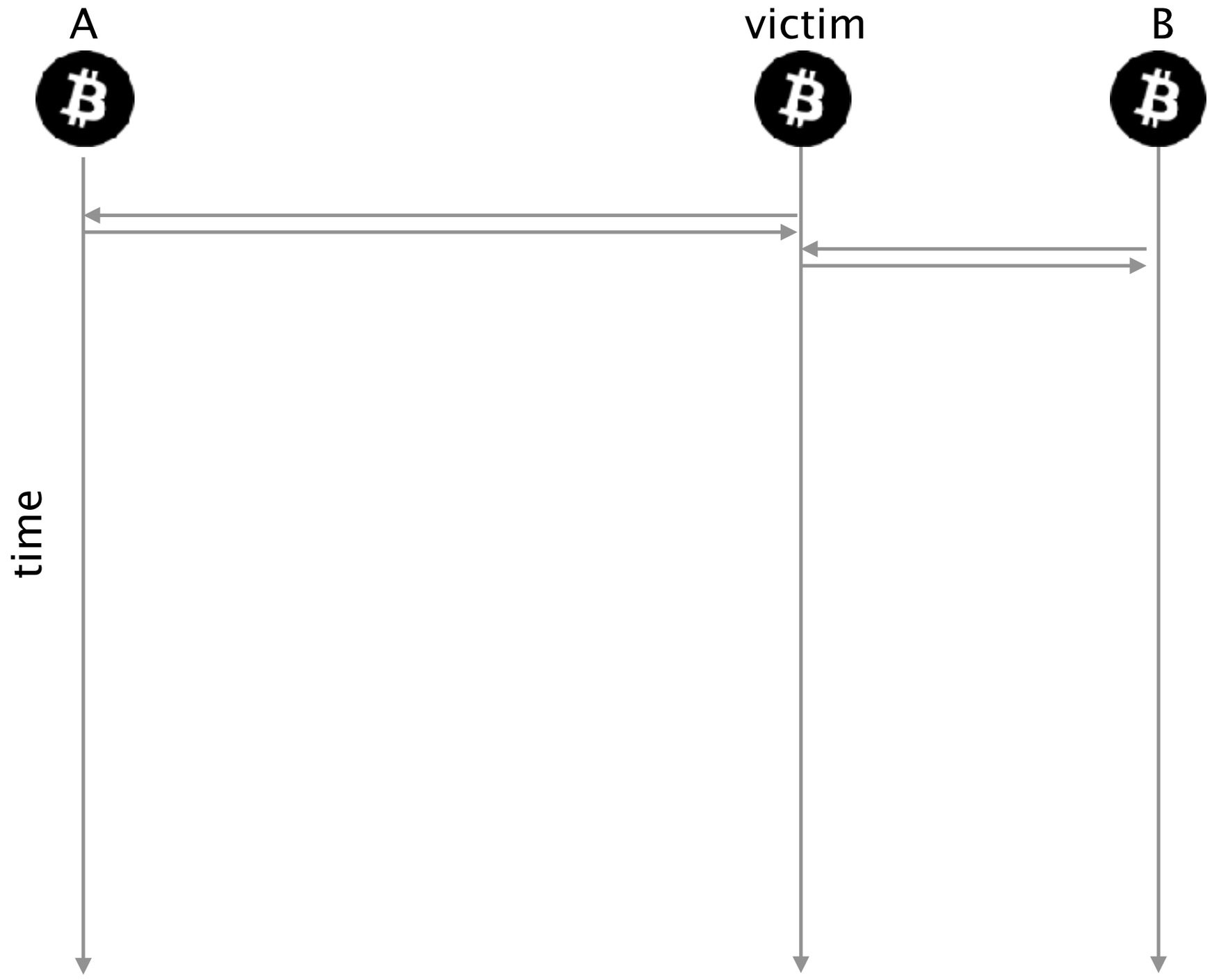
Mining pool

Regular node

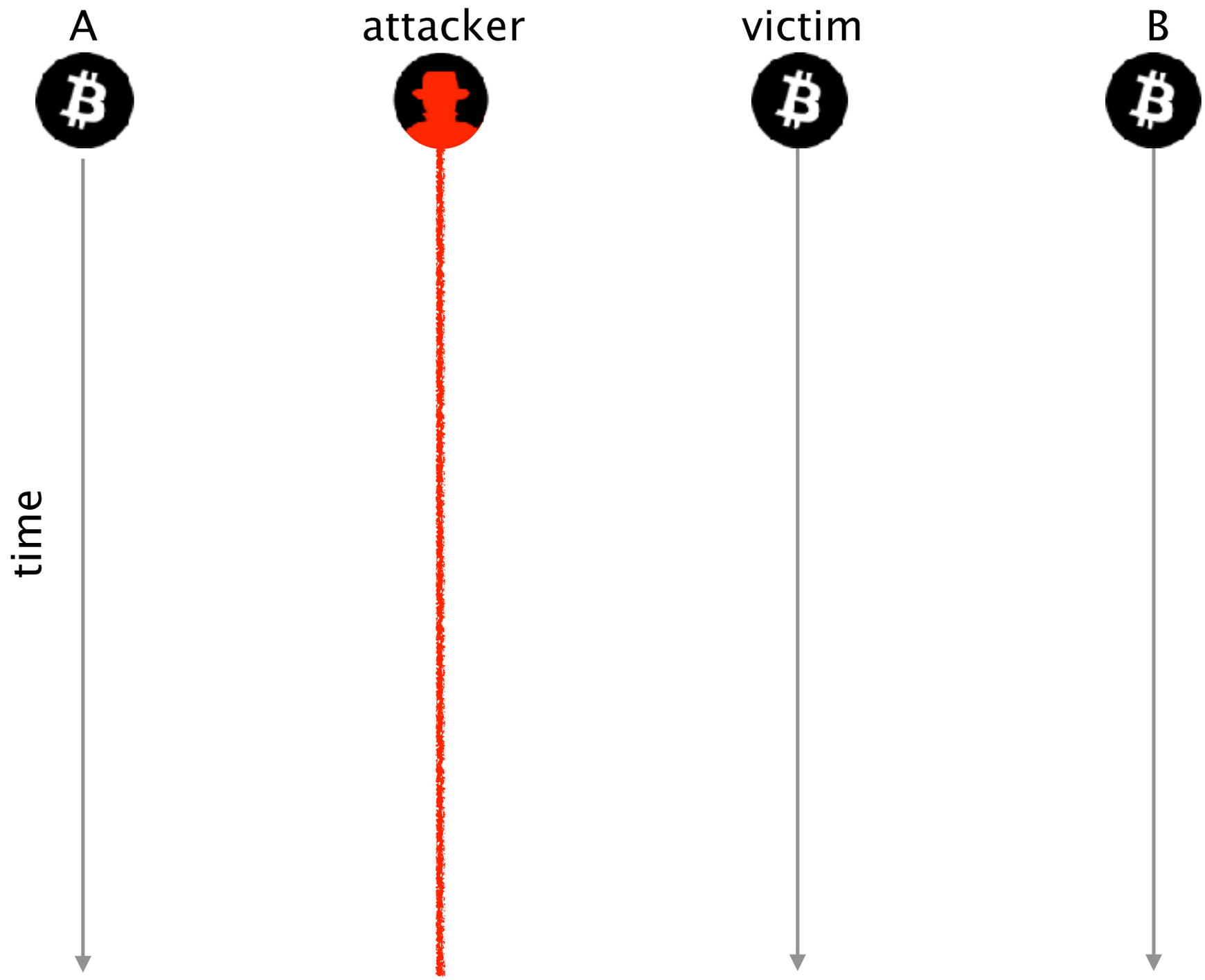
unable to collaborate to the peer-to-peer network

# How does a delay attack work?

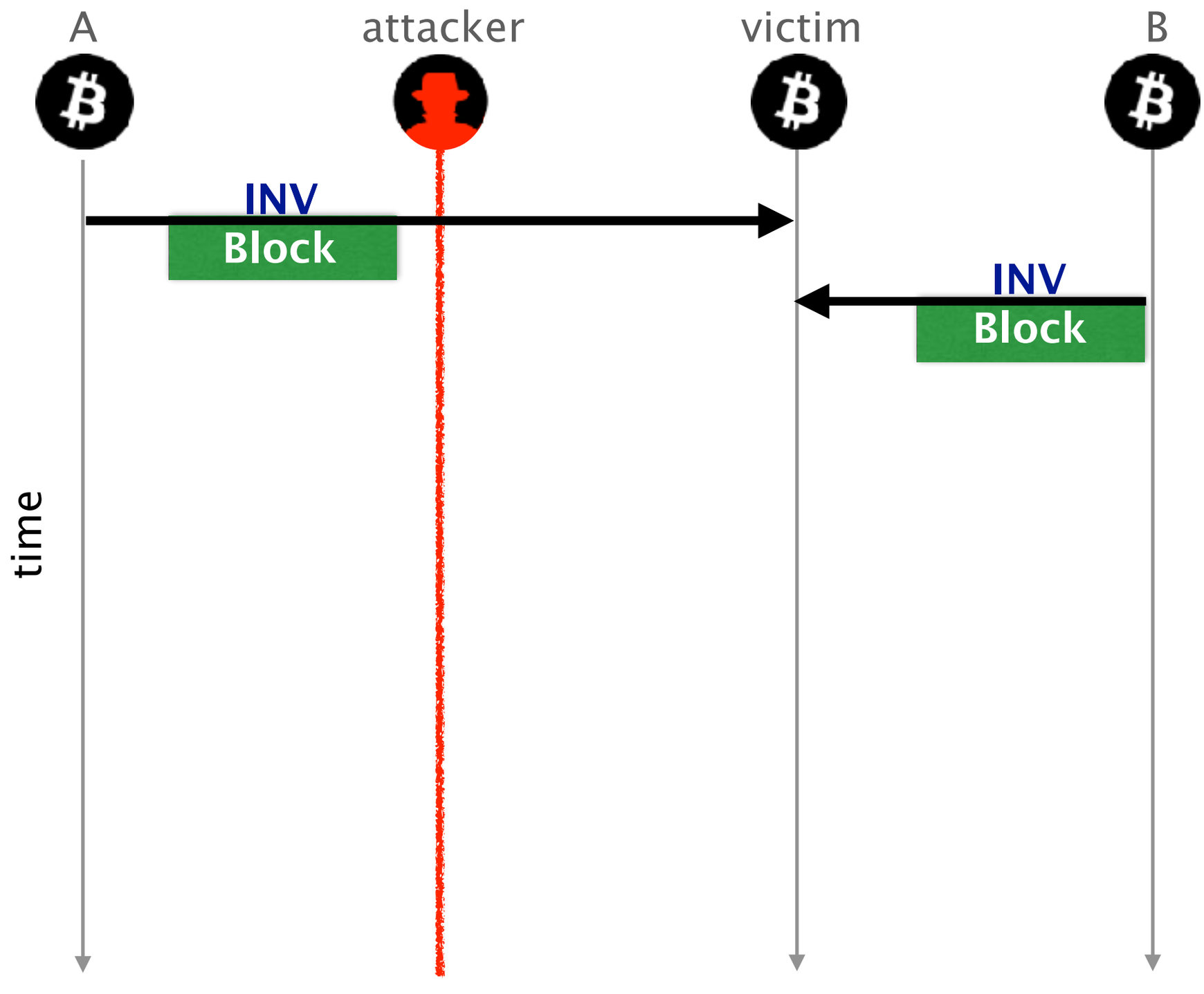
# Consider these three Bitcoin nodes



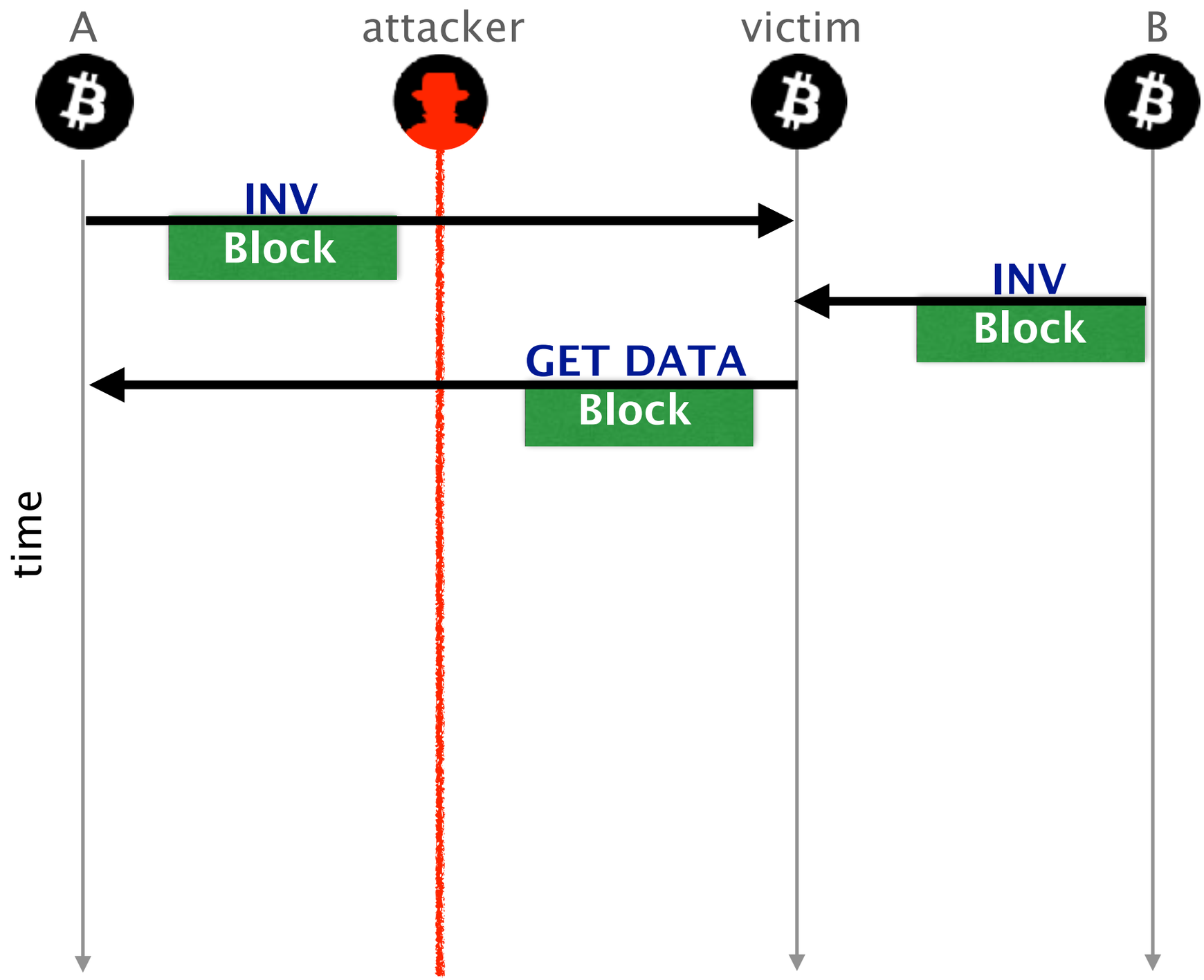
An attacker wishes to delay the block propagation towards the victim



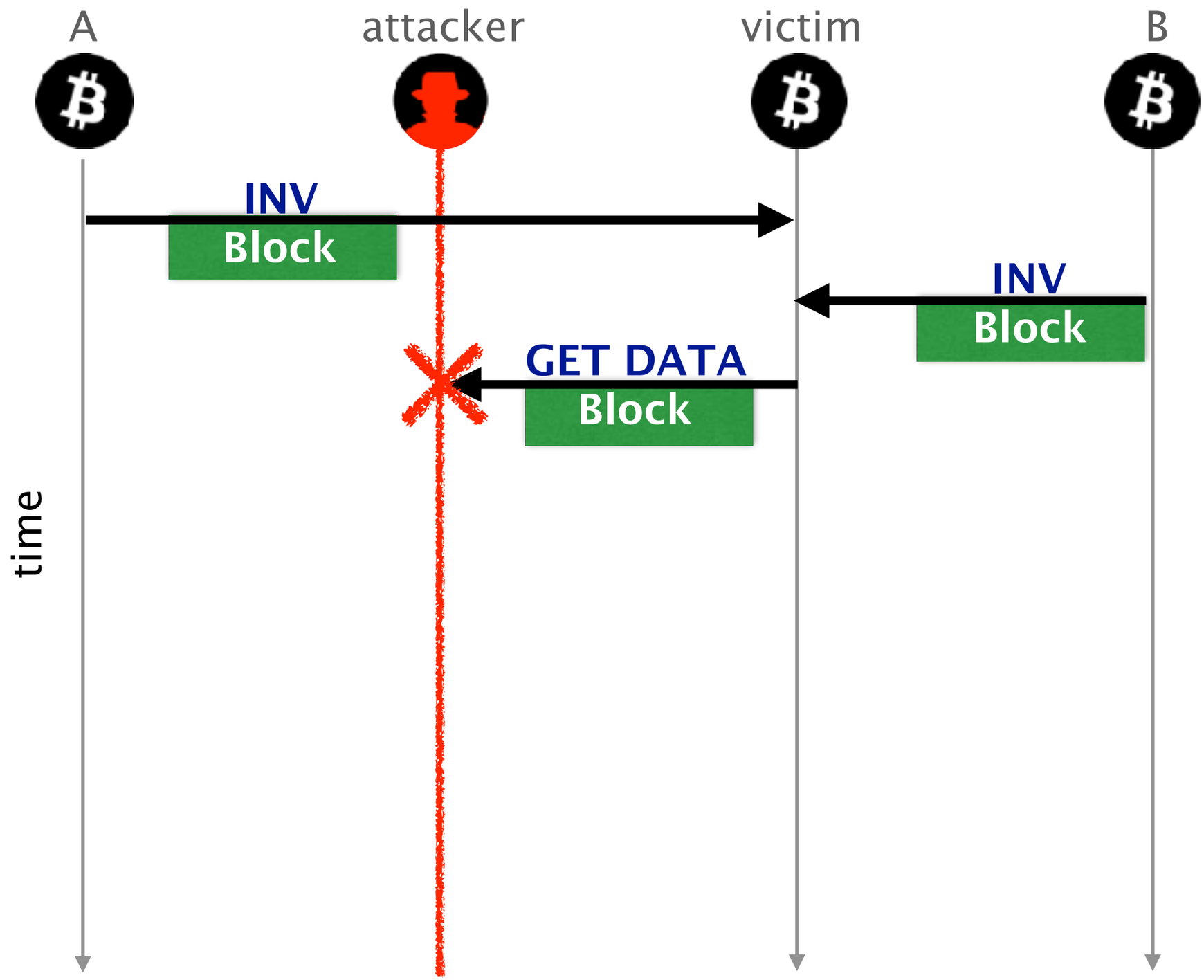
The victim receives two advertisement for the **block**



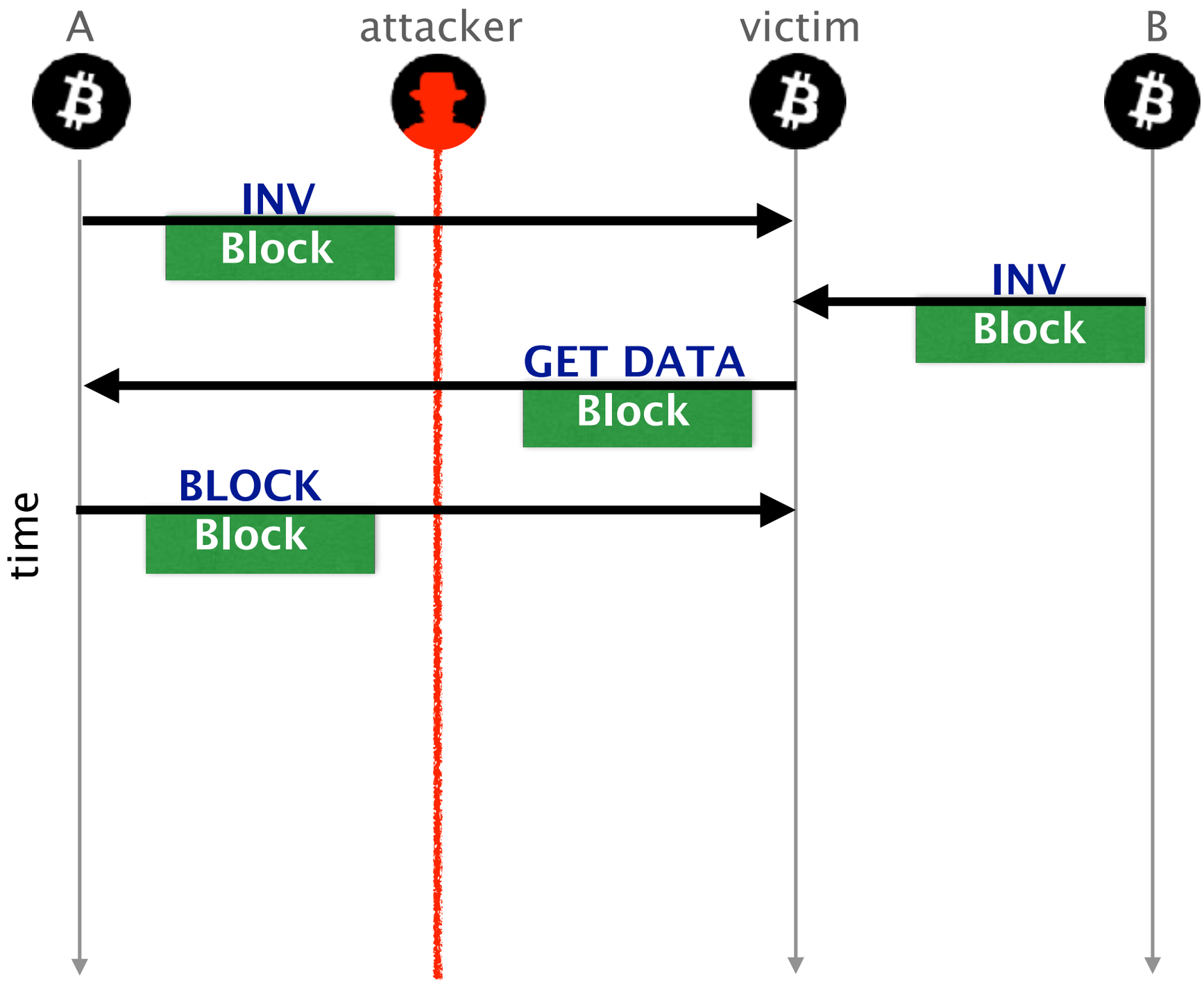
The victim requests the **block** to one of its peer, say A



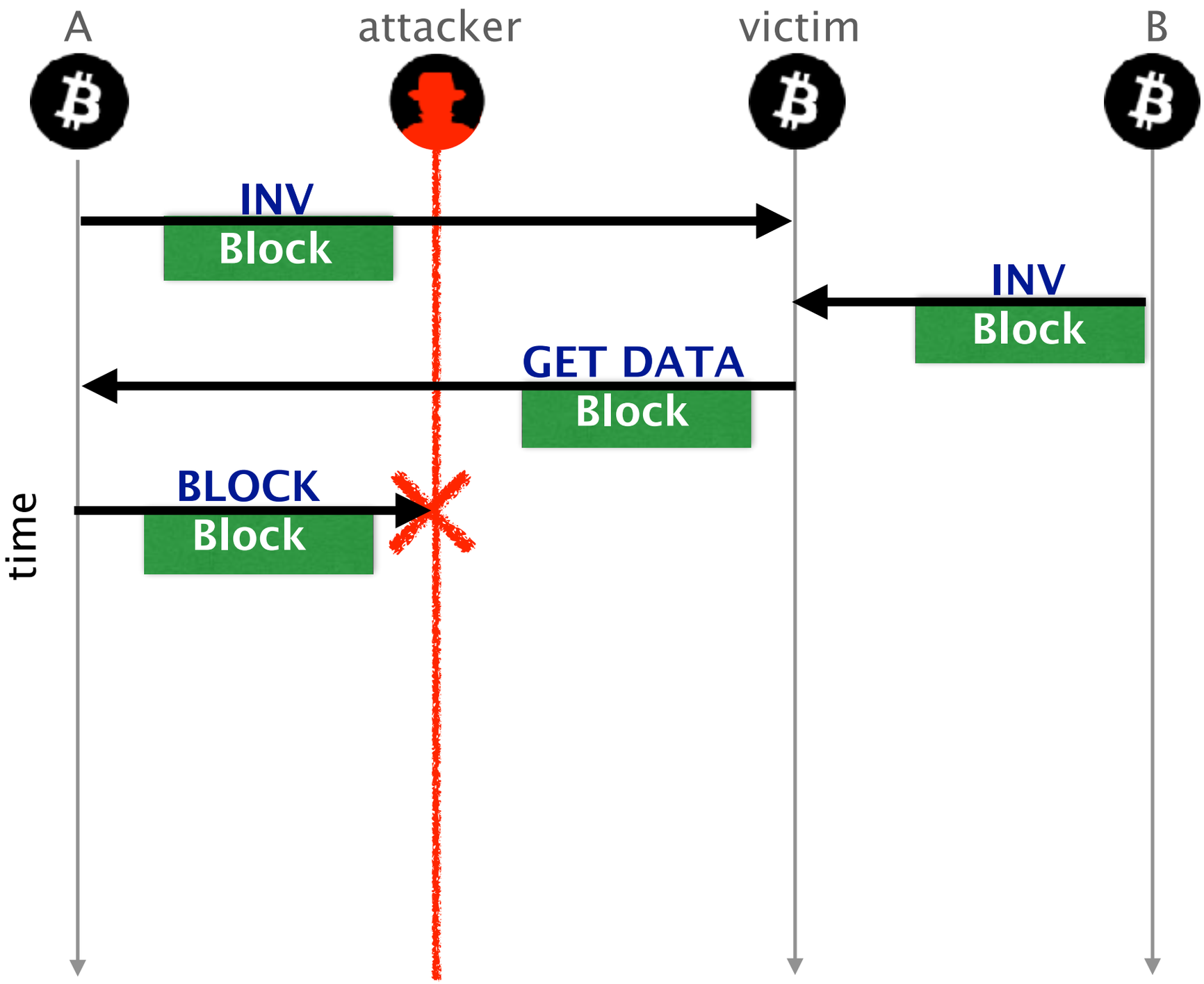
As a MITM, the attacker could drop the **GETDATA** message



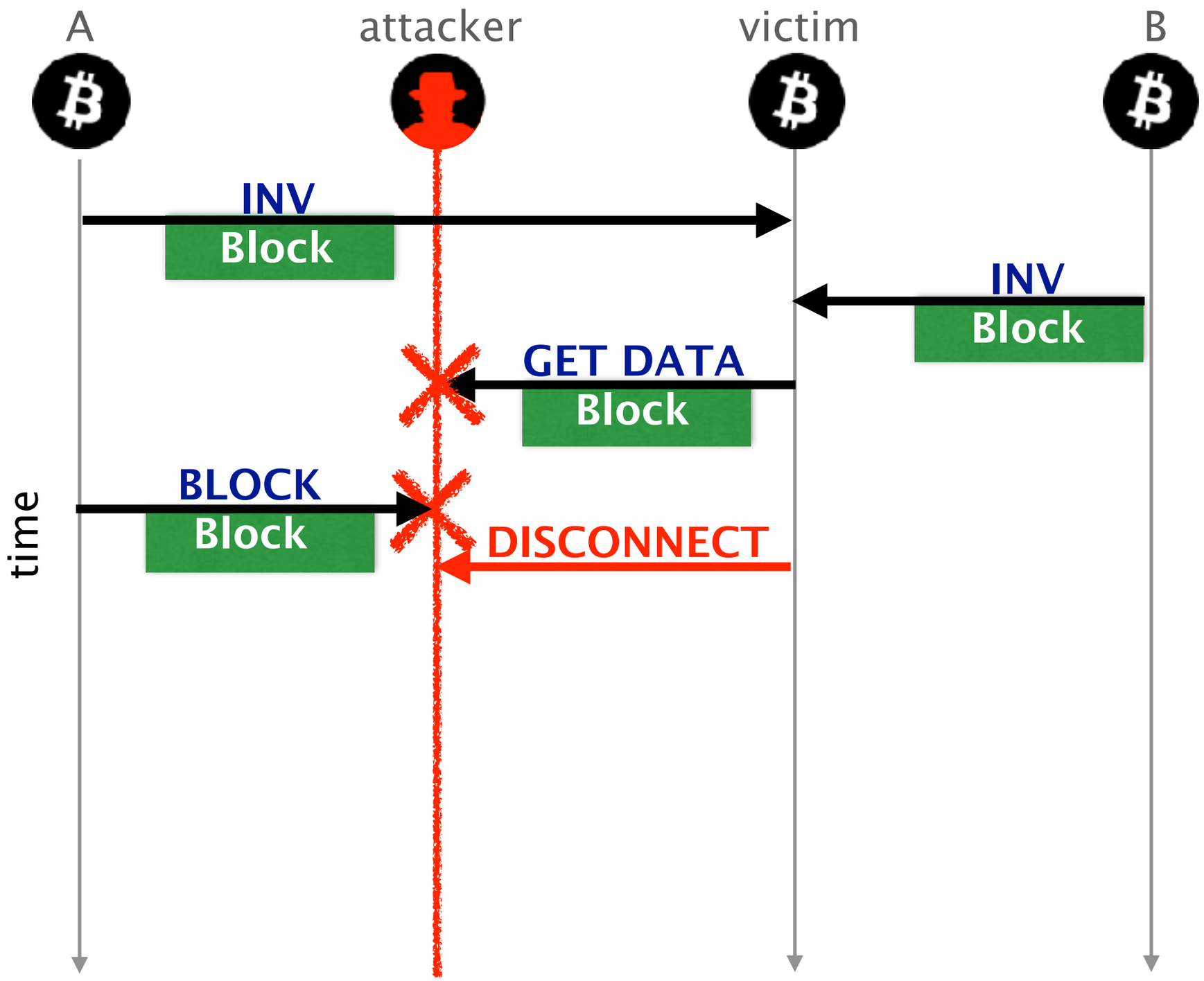
Similarly, the attacker could drop the delivery of the **block** message



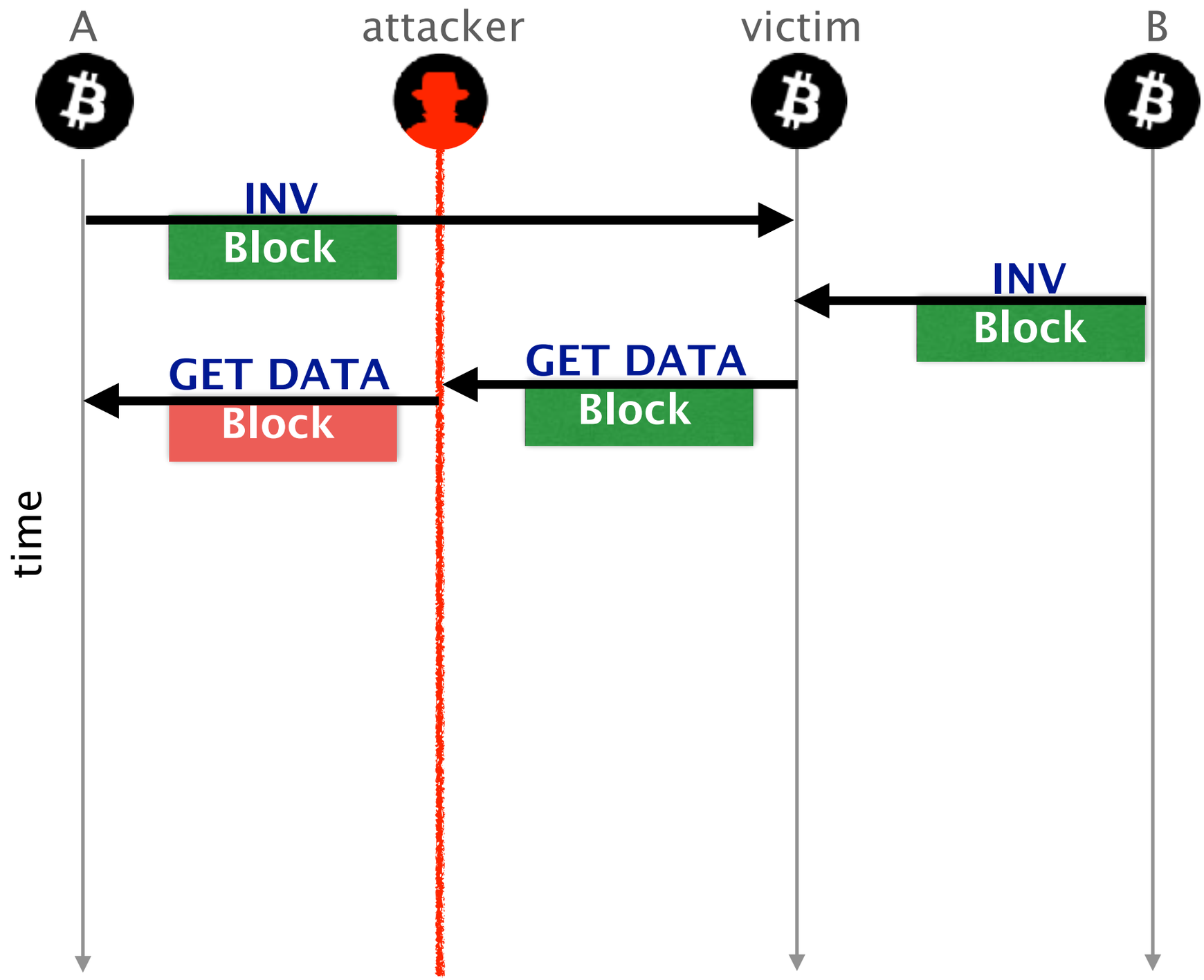
Similarly, the attacker could drop the delivery of the **block** message



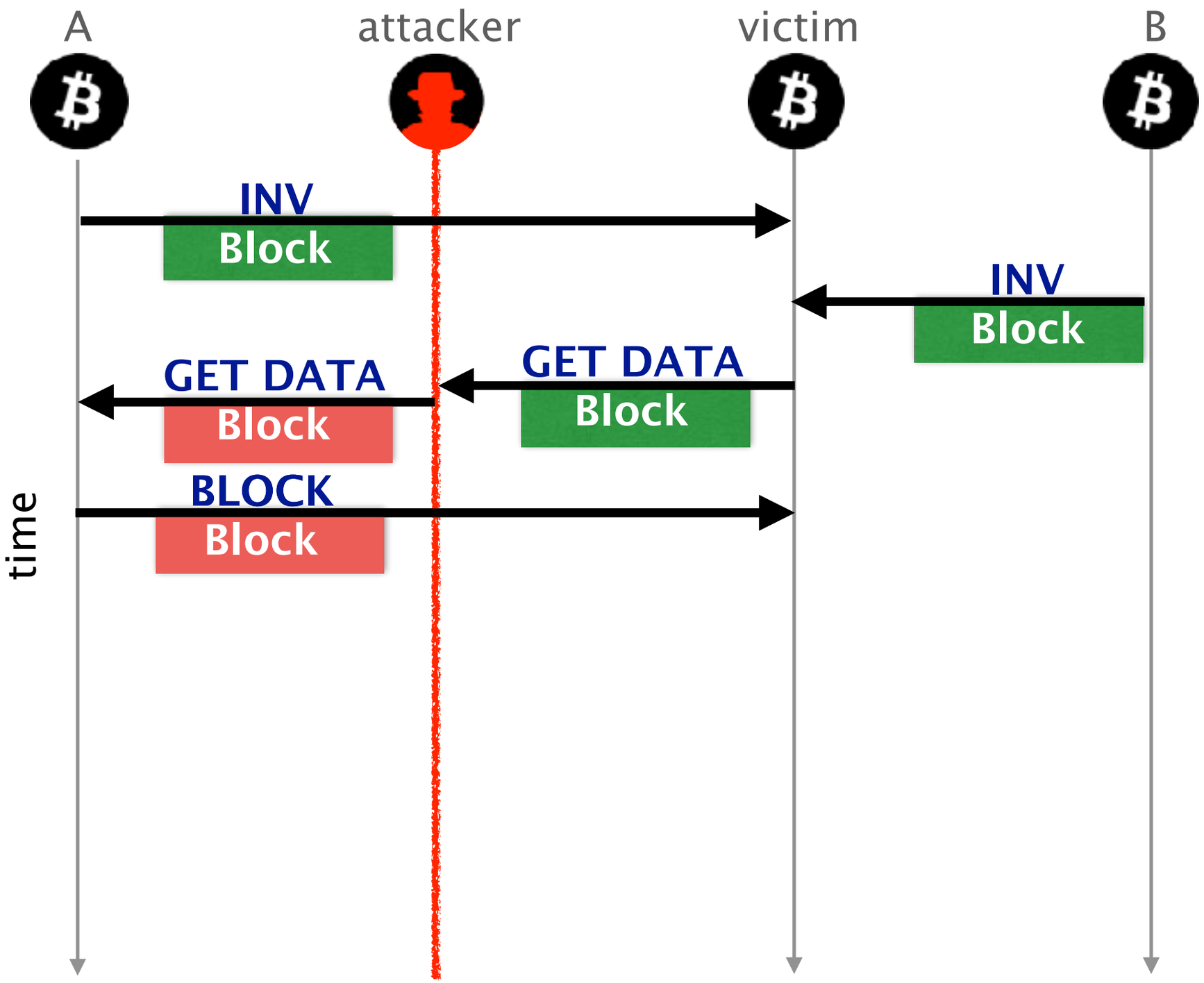
Yet, both cases will lead to the victim killing the connection (by the TCP stack on the victim)



Instead, the attacker could intercept the **GETDATA** and modifies its content

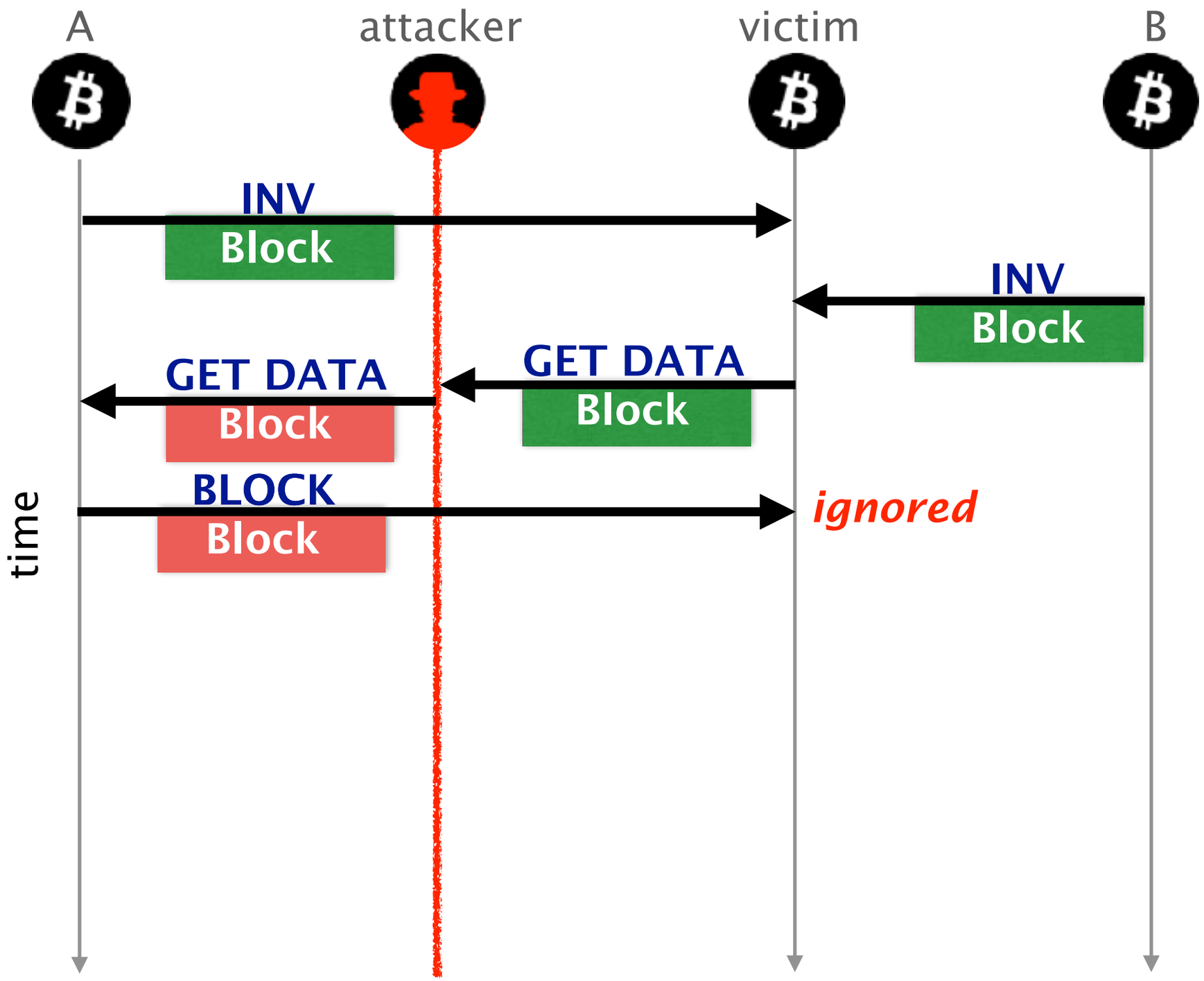


By modifying the ID of the requested block,
the attacker triggers the delivery of an older **block**

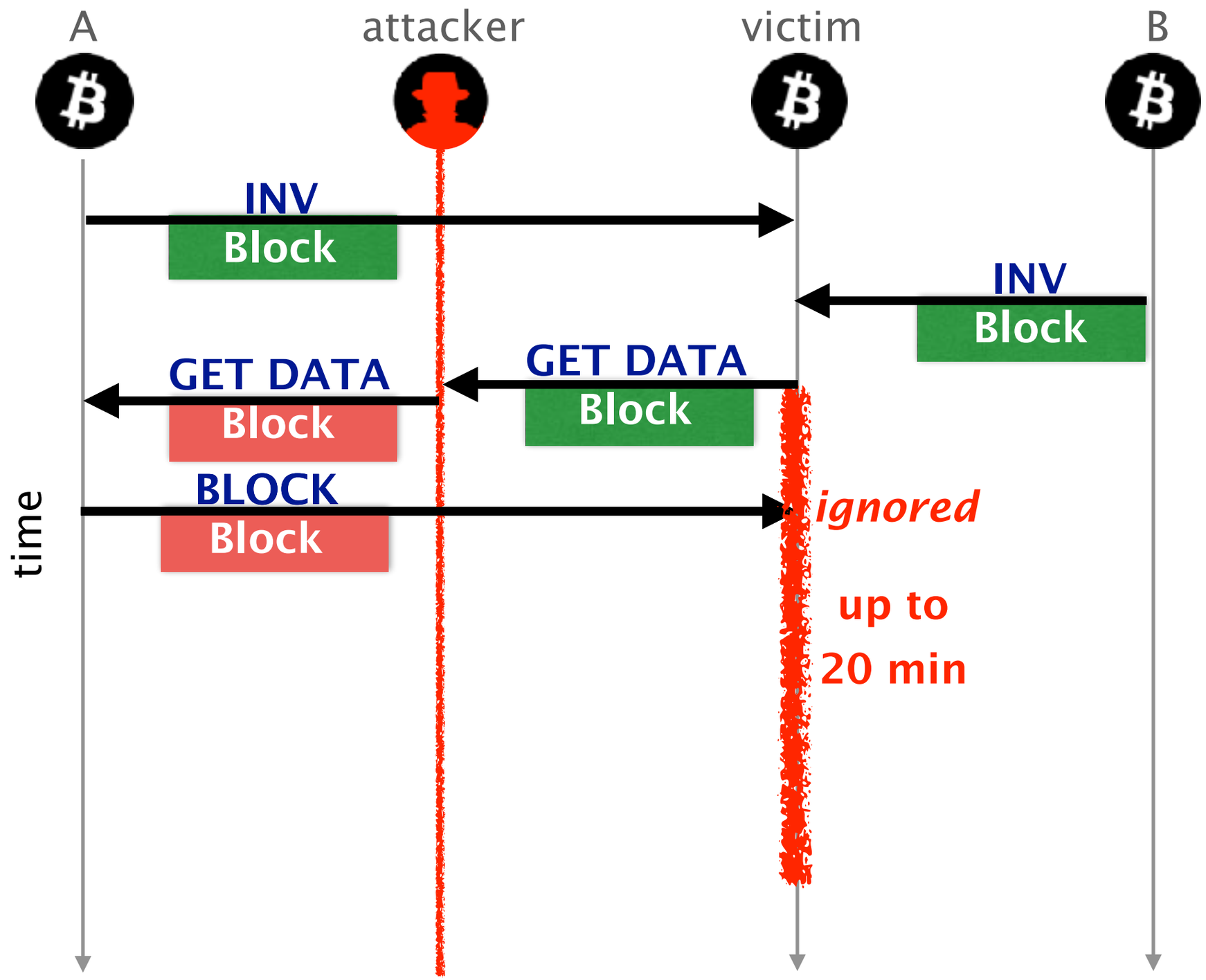


The delivery of an older block triggers

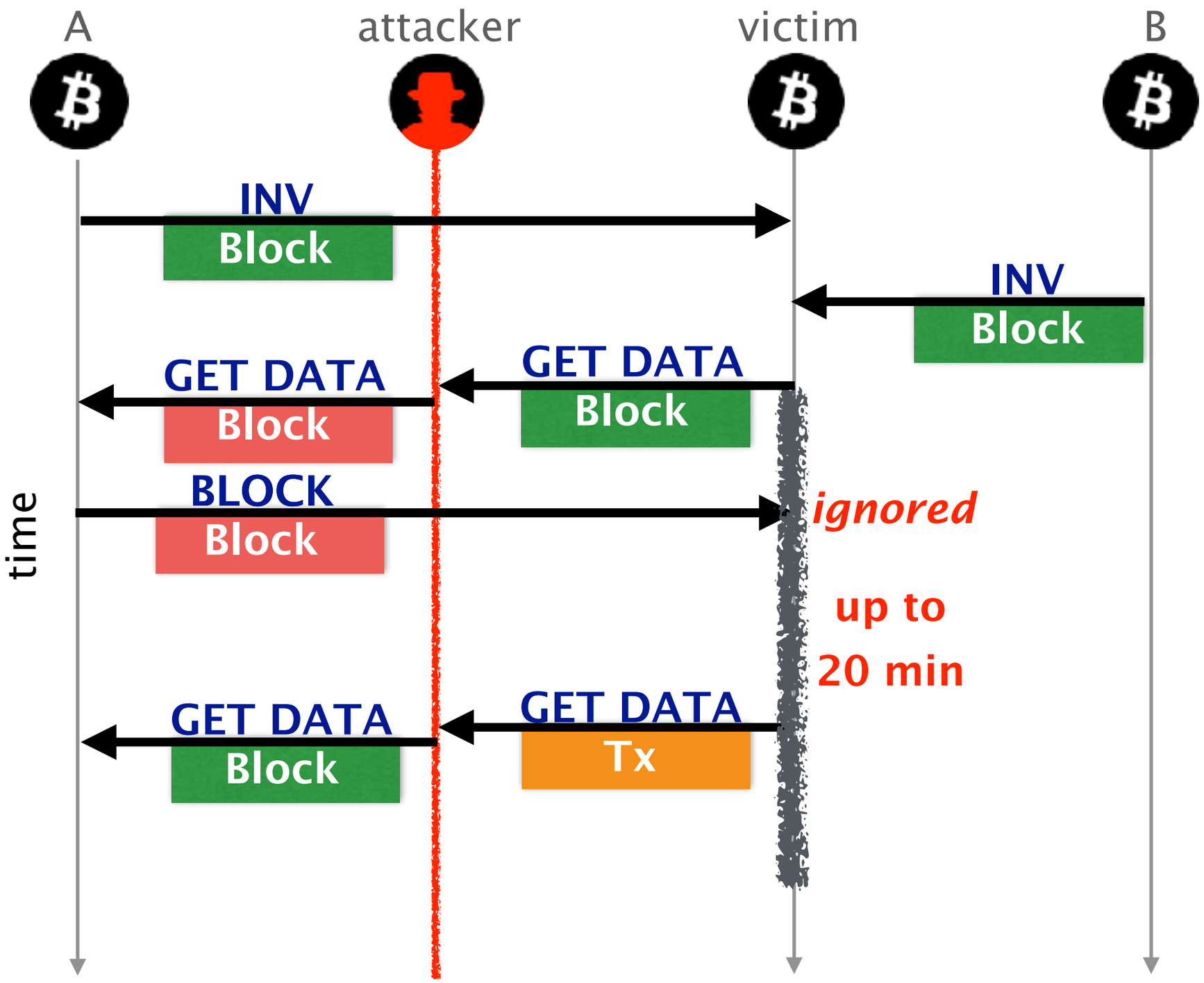
no error message at the victim



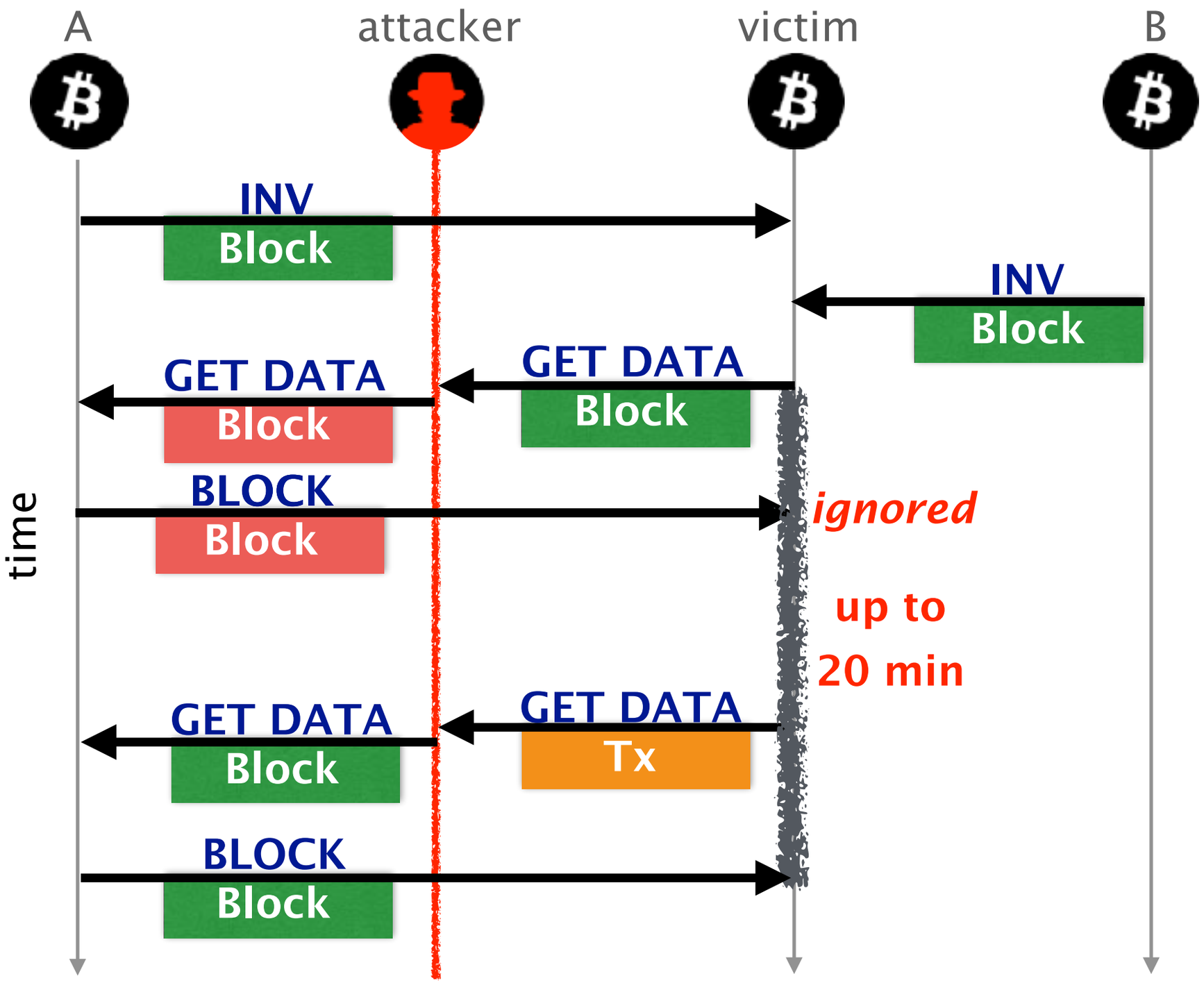
From there on, the victim will wait for 20 minutes for the actual block to be delivered



To keep the connection alive, the attacker can trigger the block delivery by modifying another **GETDATA** message



Doing so, the block is delivered before the timeout and the attack goes undetected (and could be resumed)



We evaluated the delay attack in terms of effectiveness and practicality

Effectiveness

How much time does the victim stay uniformed?

Practicality

Is it likely to happen?

We performed the attack
on a percentage of a node's connections (*)


(*) software available online: https://btc-hijack.ethz.ch/

The attacker can keep the victim uninformed
for most of its uptime while staying under the radar

The attacker can keep the victim uninformed

for most of its uptime while staying under the radar

even if the attacker intercepts

a fraction of the node connection

| | |
|---|---|
| % intercepted connections | 50% |

| | |
|---|---|
| % intercepted connections | 50% |
| % time victim does not have the most recent block | 63.2% |

| | |
|---|---|
| % intercepted connections | 50% |
| % time victim does not have the most recent block | 63.2% |
| % nodes vulnerable to attack | 67.9% |

While delay attacks are efficient against targeted nodes,

they are not so against the entire network

Observation

Large scale delay attacks are only possible

if the attacker is extremely powerful

e.g. *all* the US networks

see paper for details

# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

Both sort-term and long-term countermeasures exist

Short-term countermeasures can improve the resiliency of the Bitcoin network, with only software updates

Short-term

Routing-aware peer selection

reduce risk of having one ISP seeing all connections

Monitor changes in peer behavior, statistics, etc.

abnormal changes could be the sign of a partition

Longer-term countermeasures provide more guarantees but require protocol or infrastructure changes

Long-term

Use end-to-end encryption or MAC

prevent delay attacks (not partition attacks)

Deploy secure routing protocols

prevent partition attacks (not delay attacks)

# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

### Background

BGP & Bitcoin

### Partitioning attack

splitting the network

### Delay attack

slowing the network down

### Countermeasures

short-term & long-term

# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies


Bitcoin is vulnerable to routing attacks

both at the network and at the node level

The potential impact on the currency is worrying

DoS, double spending, loss of revenues, etc.

Countermeasures exist (we're working on it!)

some of which can be deployed today

# Hijacking Bitcoin

## Routing Attacks on Cryptocurrencies

Laurent Vanbever

https://btc-hijack.ethz.ch

SuRI, EPFL

20 June 2017

Joint work with Maria Apostolaki and Aviv Zohar [S&P'2017]