

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

Massive route leak cause Internet slowdown

Large hijack effects reachabil...

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

BGPmon

Now part of

OpenDNS

HOME BLOG ABOUT US PRODUCTS AND SERVICES CLIENT PORTAL

Massive route leak causes Internet slowdown

Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

Earlier today a massive route leak initiated by Telekom Malaysia (AS4788) caused significant network problems for the global routing system. Primarily affected was Level3 (AS3549 - formerly known as Global Crossing) and their customers. Below are some of the details as we know them now. Starting at 08:43 UTC today June 12th, AS4788 Telekom Malaysia started to announce about 179,000 of prefixes to Level3 (AS3549, the Global crossing AS), whom in turn accepted these and propagated them to their peers and customers. Since Telekom Malaysia had inserted itself between these thousands of prefixes and Level3 it was now responsible for delivering these packets to the intended destinations. This event resulted in significant packet loss and Internet slow down in all parts of the world. The Level3 network in particular suffered from severe service degradation between the Asia pacific region and the rest of their network. The graph below for example shows the packet loss as measured by OpenDNS between London over Level3 and Hong Kong. The same loss patterns were visible from other Level3 locations globally to for example Singapore, Hong Kong and Sydney.

Packet Loss lon_hkg_level3

Time	Cur (%)	Avg (%)	Min (%)	Max (%)
08:00	0	0	0	0
08:20	0	0	0	0
08:40	0	0	0	0
08:43	100	100	100	100
09:00	100	100	100	100
09:20	100	100	100	100
09:40	100	100	100	100
10:00	100	100	100	100
10:20	100	100	100	100
10:40	100	100	100	100
11:00	100	100	100	100
11:20	100	100	100	100
11:40	0	0	0	0

Latest Tweets

Tweets by @bgpmon

BGPmon.net

@bgpmon

Country wide Internet outage in Syria. Traffic just returned after over 5 hours of downtime. more details @bgpstream [bgpstream.com/event/66222](#)

01 Jun

BGPmon.net

@bgpmon

Suriname (TeleSur) disappeared from the Internet for about 5 minutes earlier today. [bgpstream.com/event/66300](#)

15 May

BGPmon.net Retweeted

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

Millesime 2016

The screenshot shows a web browser window with two tabs. The active tab is titled 'Large hijack affects reachability of high traffic destinations' and shows the URL 'https://bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/'. The page features the BGPmon logo, which includes the text 'Now part of OpenDNS'. The navigation bar contains links for HOME, BLOG, ABOUT US, PRODUCTS AND SERVICES, and CLIENT PORTAL. The main article title is 'Large hijack affects reachability of high traffic destinations', posted by Andree Toonk on April 22, 2016. The article text describes a large-scale routing incident affecting hundreds of Autonomous systems, with a focus on high-traffic prefixes like those of Google, Amazon, and Twitter. It mentions that the incident was caused by AS200759 'innofield AG' and lists the peers through which the hijack was announced: 20634 'Telecom Liechtenstein AG', 6939 'Hurricane Electric, Inc.', and 16265 'LeaseWeb Network B.V.'. The article also includes a timeline of events and a list of affected prefixes. To the right of the article is a 'Latest Tweets' section showing two tweets from BGPmon.net (@bgpmon) dated June 01 and May 15, 2016, discussing internet outages in Syria and Suriname.

Massive route leak cause Inter x Large hijack affects reachability of high traffic destinations

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

BGPmon Now part of **OpenDNS**

HOME BLOG ABOUT US PRODUCTS AND SERVICES CLIENT PORTAL

Large hijack affects reachability of high traffic destinations

Posted by Andree Toonk - April 22, 2016 - Hijack - 10 Comments

April 23, Update: [NOC Team at innofield posted an explanation of the incident in the comments section below.](#) Starting today at 17:09 UTC our systems detected a large scale routing incident affecting hundreds of Autonomous systems. Many BGPmon users have received an email informing them of this change. Our initial investigation shows that the scope of this incident is widespread and affected 576 Autonomous systems and 3431 prefixes. Amongst the networks affected are high traffic prefixes including those of Google, Amazon, Twitter, Apple, Akamai, Time Warner Cable Internet and more. All these events have either AS200759 "innofield AG" or private AS 65021 as the origin AS. In the cases where AS65021 appears as the origin AS, AS200759 is again the next-hop AS. AS200759 "innofield AG" is a provider based out of Switzerland and normally only announces one IPv4 and one IPv6 prefix. These are 2 example events: Prefix: 66.220.152.0/21 is normally announced by Facebook AS32934 and during this event was announced by AS200759 as a more specific /22 Detected prefix: 66.220.152.0/22 Example aspath: 4608 24130 7545 6939 200759 And AS origin: 65021 behind AS 200759 Detected prefix: 66.220.152.0/22 Example aspath: 133812 23948 4788 6939 200759 65021

We saw the announcements via the following peers of AS200759 "innofield AG":

- 20634 "Telecom Liechtenstein AG"
- 6939 "Hurricane Electric, Inc."
- 16265 "LeaseWeb Network B.V."

Not surprisingly, as HE is a major provider most of our probes (BGPmon peers) detected this path via their provider HE (6939). It appears things have been resolved as of 17:30 UTC. This event affected the reachability of many high traffic destinations, some good examples are

Latest Tweets

Tweets by @bgpmon

BGPmon.net @bgpmon
Country wide Internet outage in Syria. Traffic just returned after over 5 hours of downtime. more details [@bgpstream](#) [bgpstream.com/event/06222](#)

BGPmon.net @bgpmon
Suriname (TeleSur) disappeared from the Internet for about 5 minutes earlier today. [bgpstream.com/event/06000](#)

BGPmon.net Retweeted

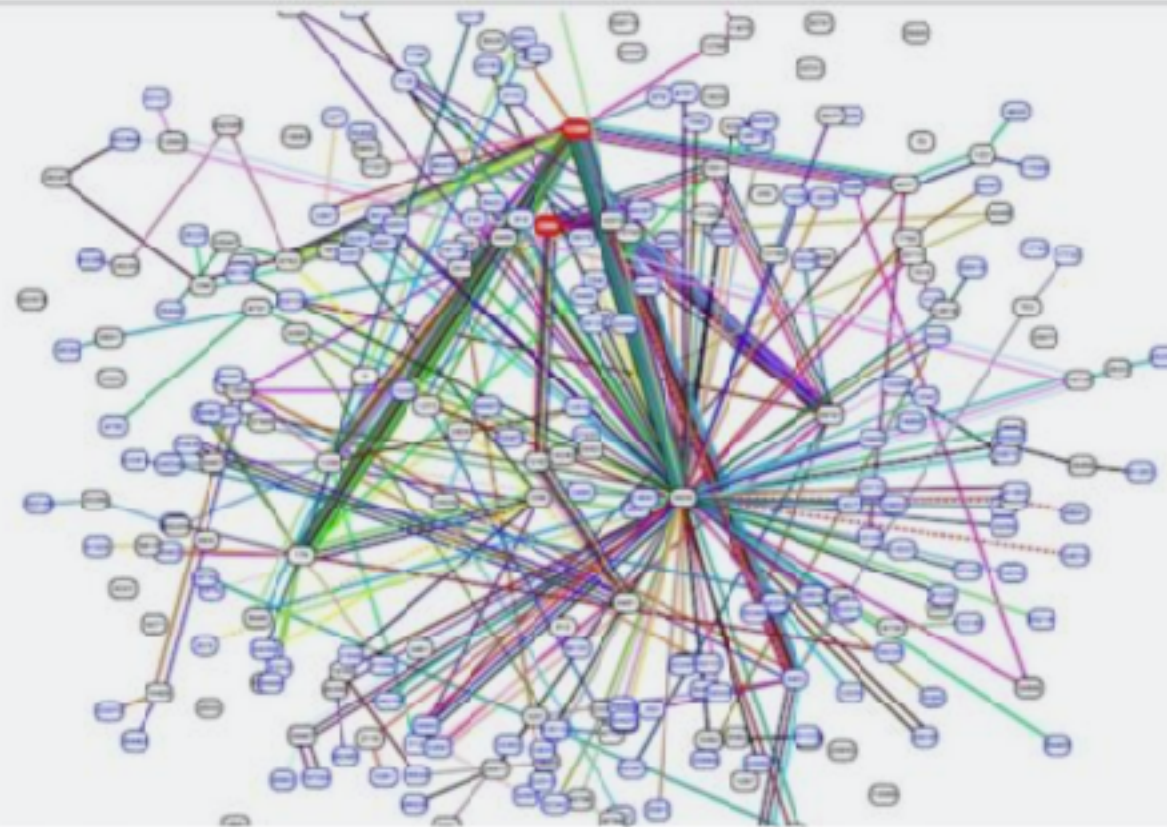
source: <https://bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/>

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

200k

150k

100k

50k

0

Oct.

Nov.

Dec.

Jan.

Feb.

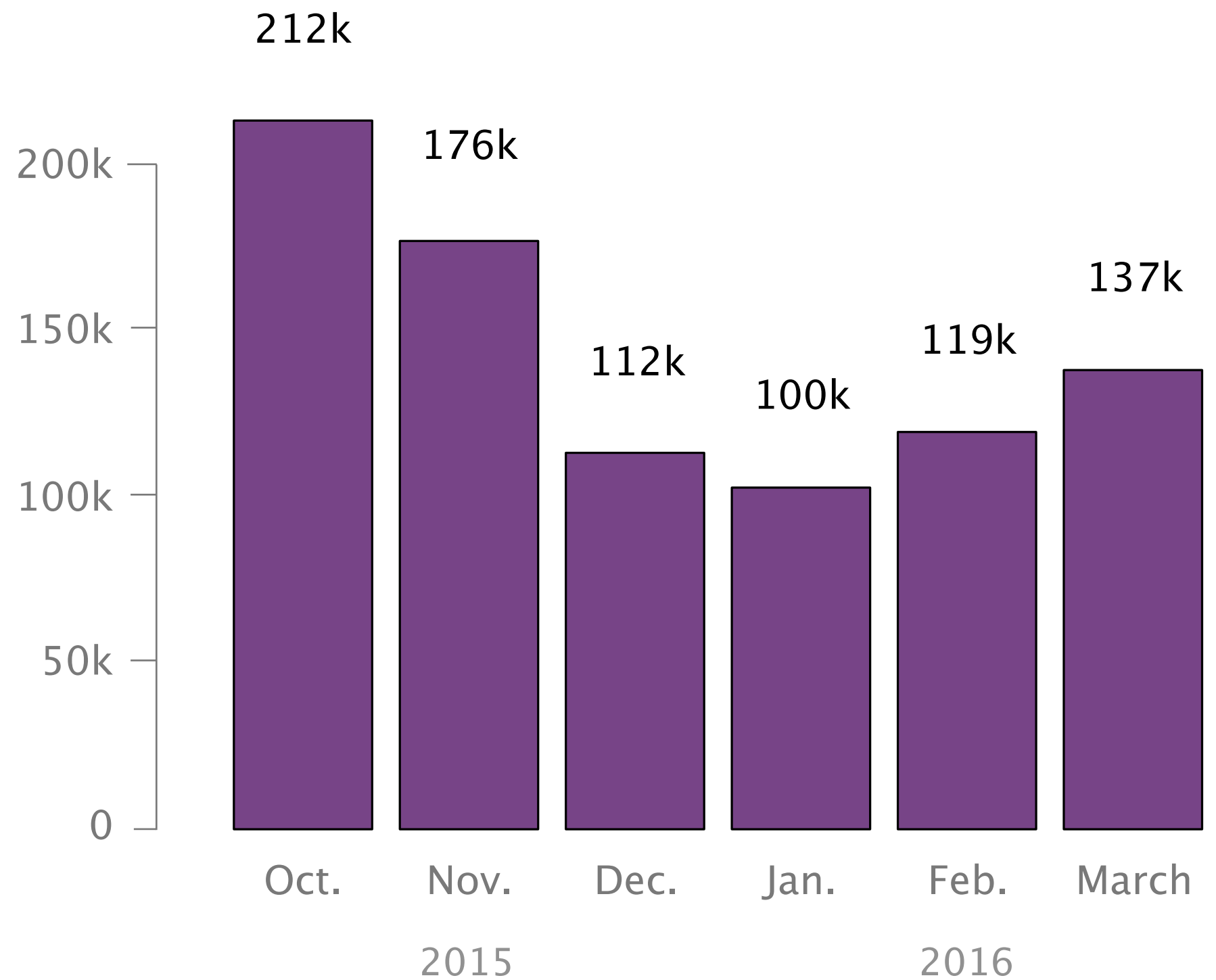
March

2015

2016



of monthly
routing hijacks



Most of these problems are human mistakes

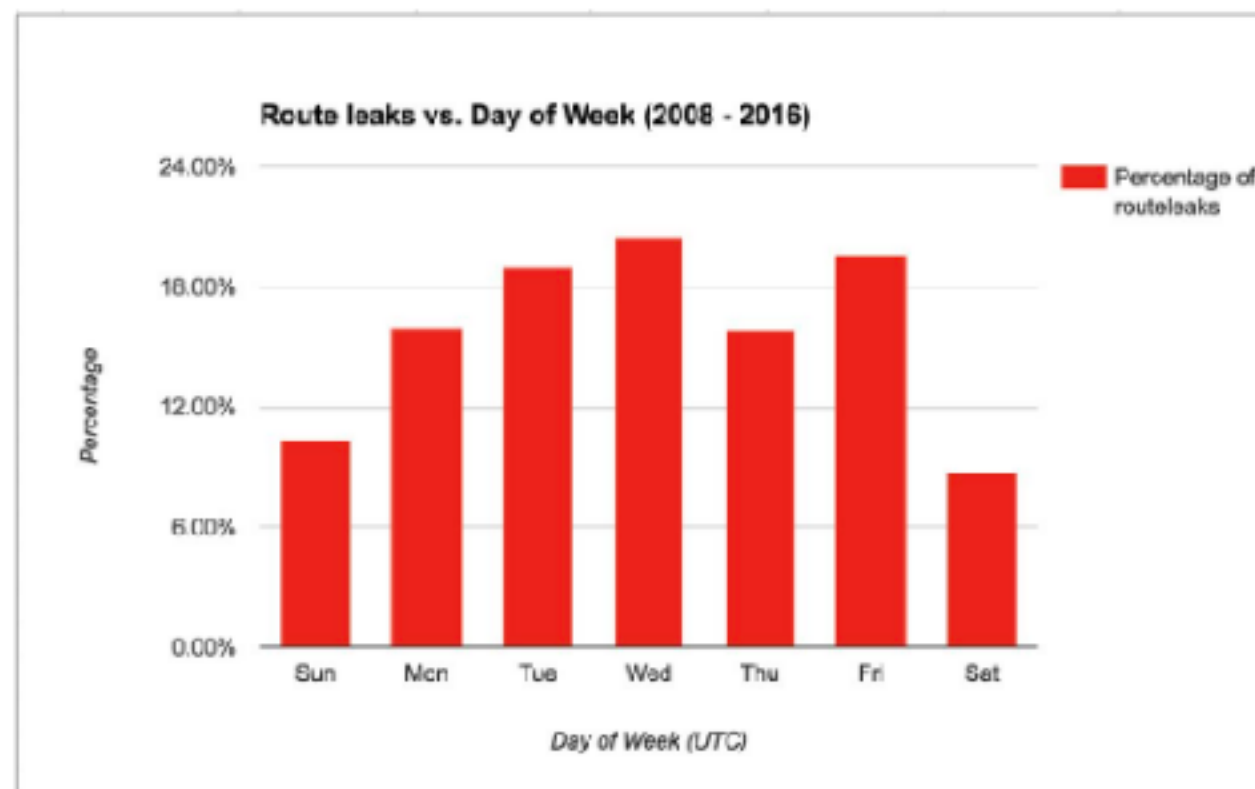


Job Snijders
@JobSnijders



 Follow

Fun fact: most BGP route leaks happen on Wednesdays, but in the weekend us humans collectively take a break! :-)



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

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**

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

Information suggests that
operators were **watching the news**
instead of making changes
to their infrastructure

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](#)

[f Share](#) 1.0k [t Tweet](#) 1,464 [g+1](#) 213 [in Share](#) 512 [Pin it](#)

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



hosting

The diagram consists of three rectangular boxes arranged horizontally. The first box on the left is light green and contains the word 'hosting'. The second box in the middle is light orange and contains the word 'mining'. The third box on the right is also light orange and contains the word 'transit'. All boxes have a thin grey border.

mining

transit

Few networks host a large fraction of nodes

cumulative % of
Bitcoin nodes

100

80

60

40

20

0

1

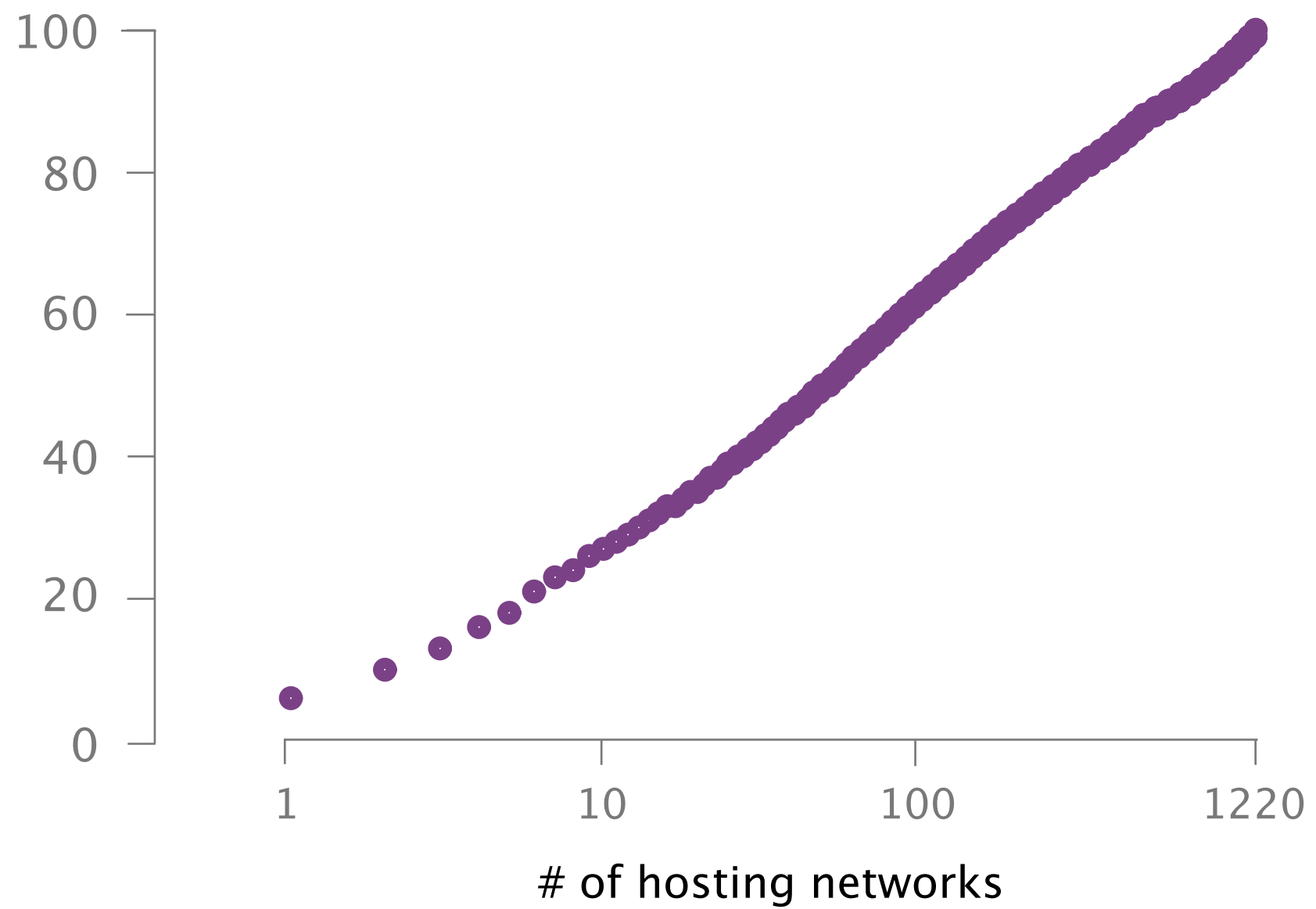
10

100

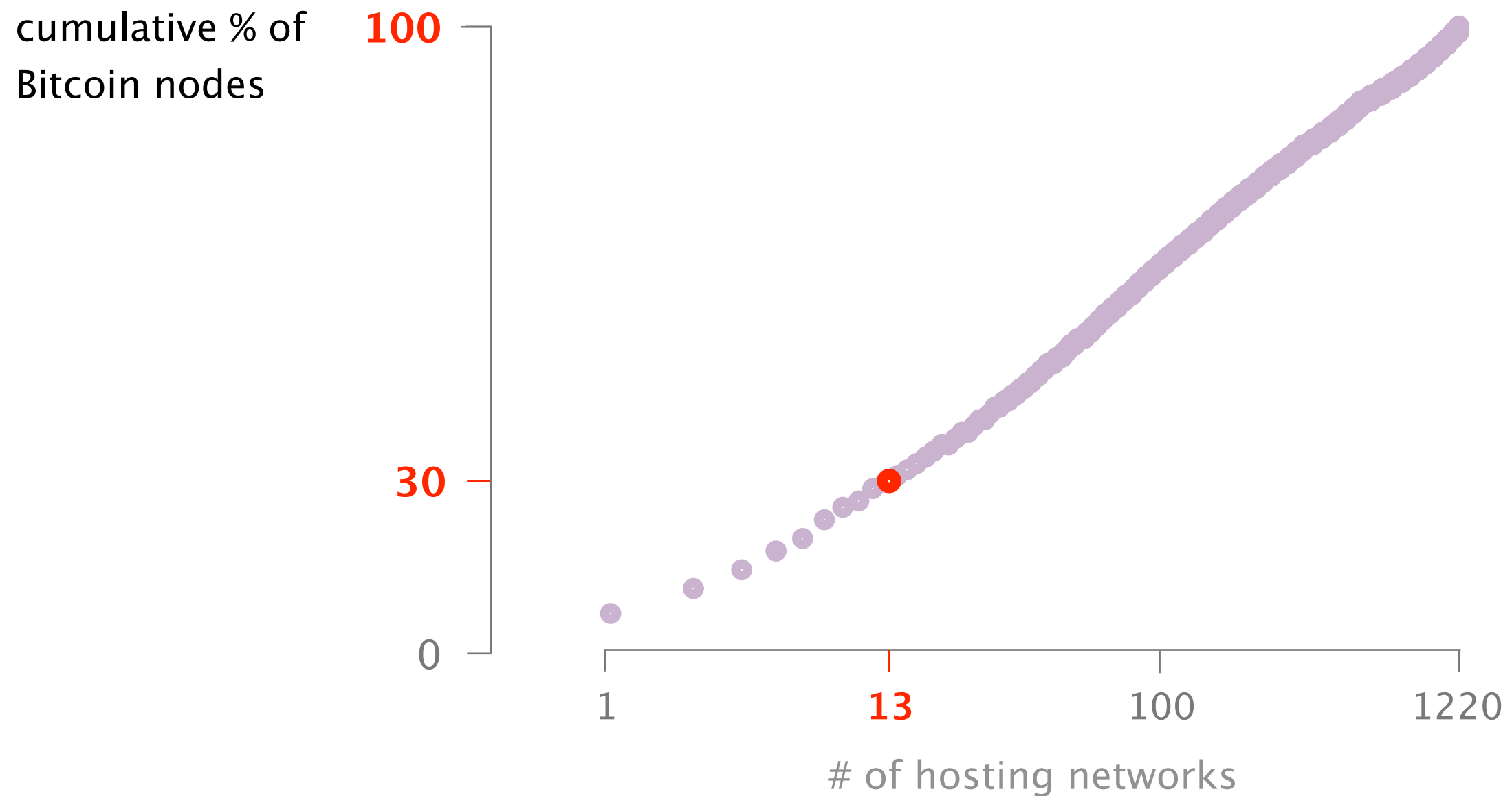
1220

of hosting networks

cumulative % of
Bitcoin nodes



13 networks host 30% of all the nodes



Bitcoin's centralization illustrates itself across three dimensions



hosting

The diagram consists of three rectangular boxes arranged horizontally. The first box on the left is light orange and contains the word 'hosting'. The middle box is light green and contains the word 'mining'. The third box on the right is light orange and contains the word 'transit'. All boxes have a thin black border.

mining

transit

Mining power is centralized to few hosting networks

cumulative % of
mining power

100

80

60

40

20

0

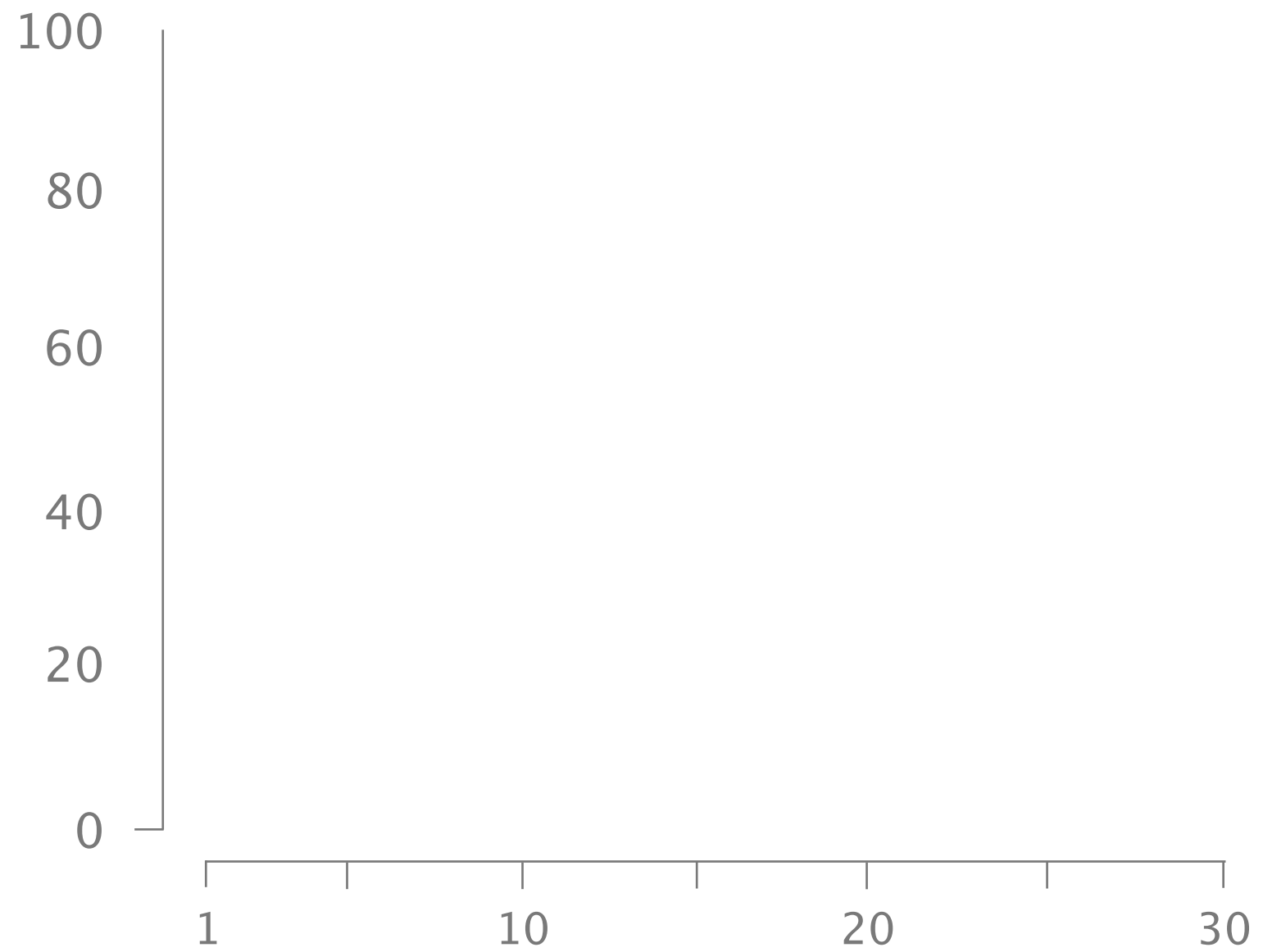
1

10

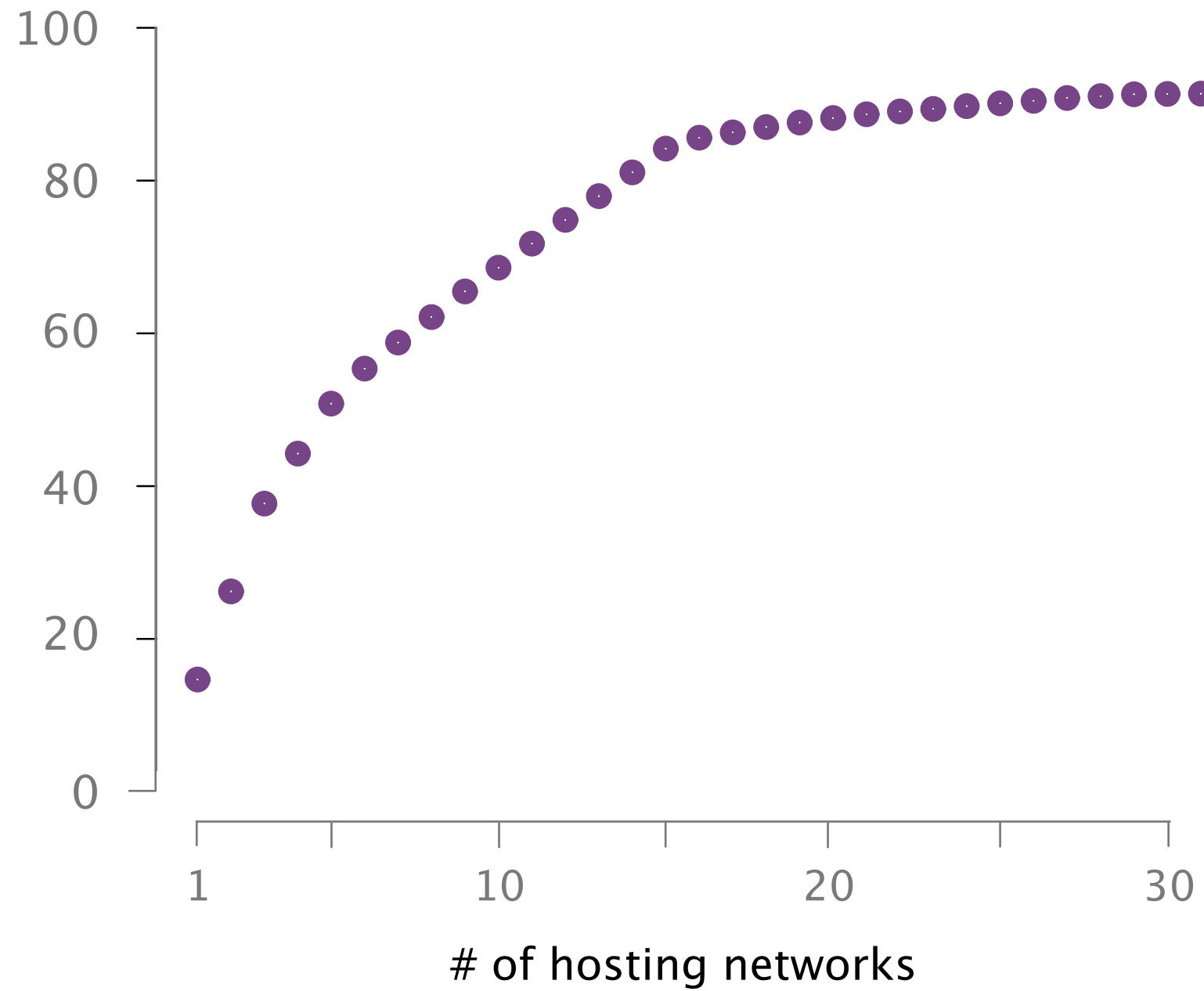
20

30

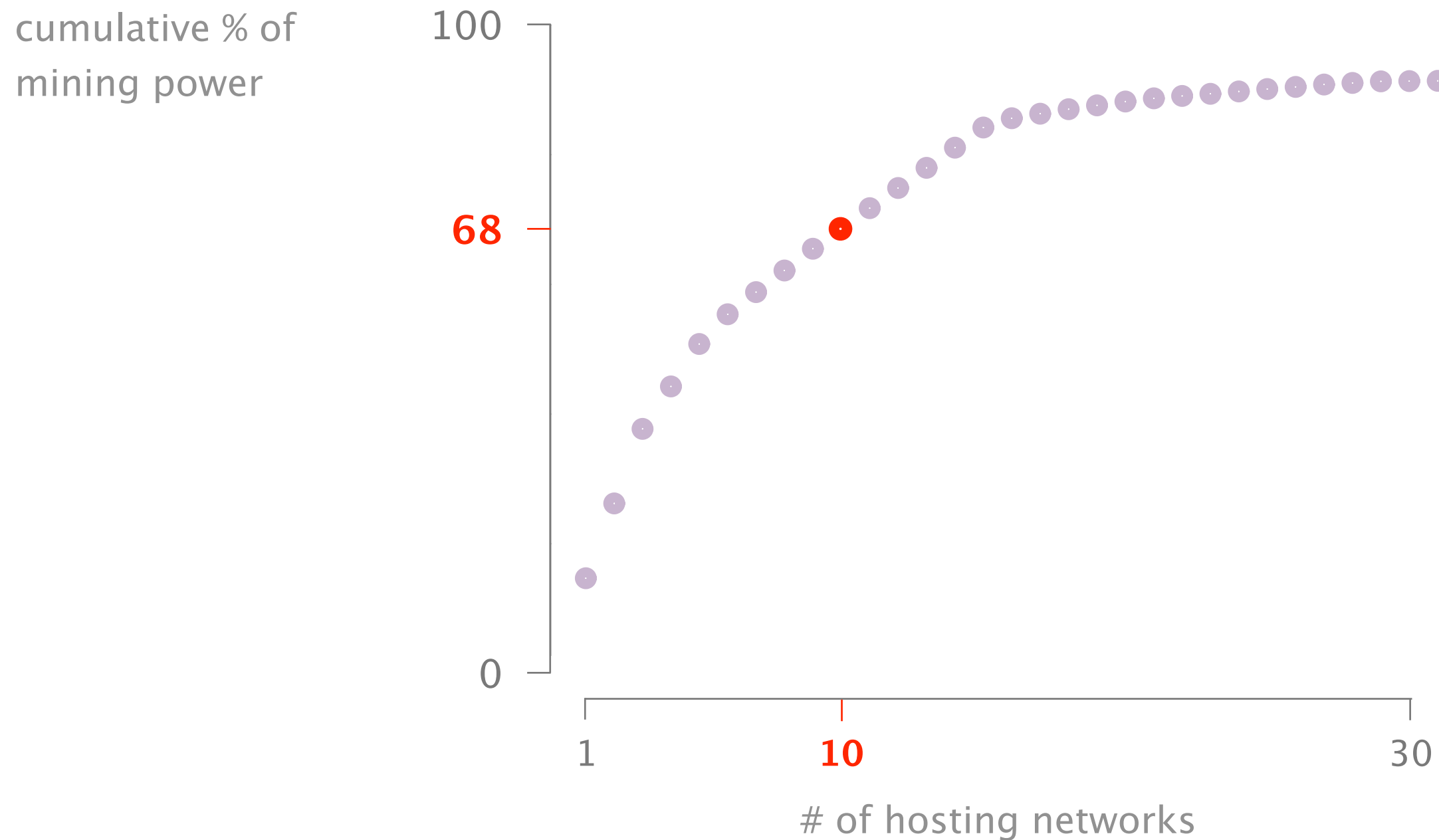
of hosting networks



cumulative % of
mining power



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



Bitcoin's centralization illustrates itself across three dimensions



hosting

The diagram consists of three rectangular boxes arranged horizontally. The first two boxes, labeled 'hosting' and 'mining', are light orange. The third box, labeled 'transit', is light green. All boxes have a thin grey border.

mining

transit

cumulative
% of connections

100

80

60

40

20

0

1

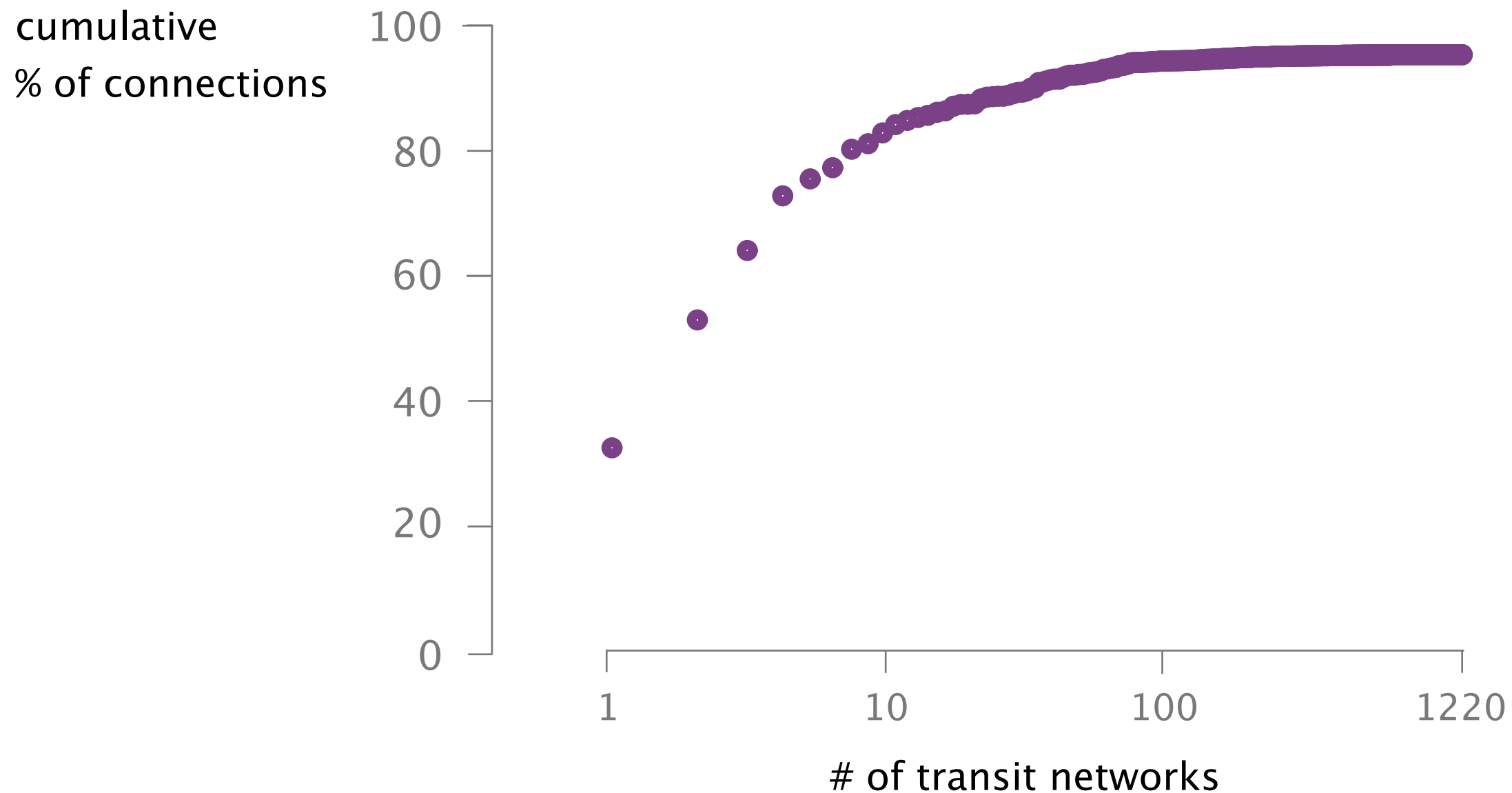
10

100

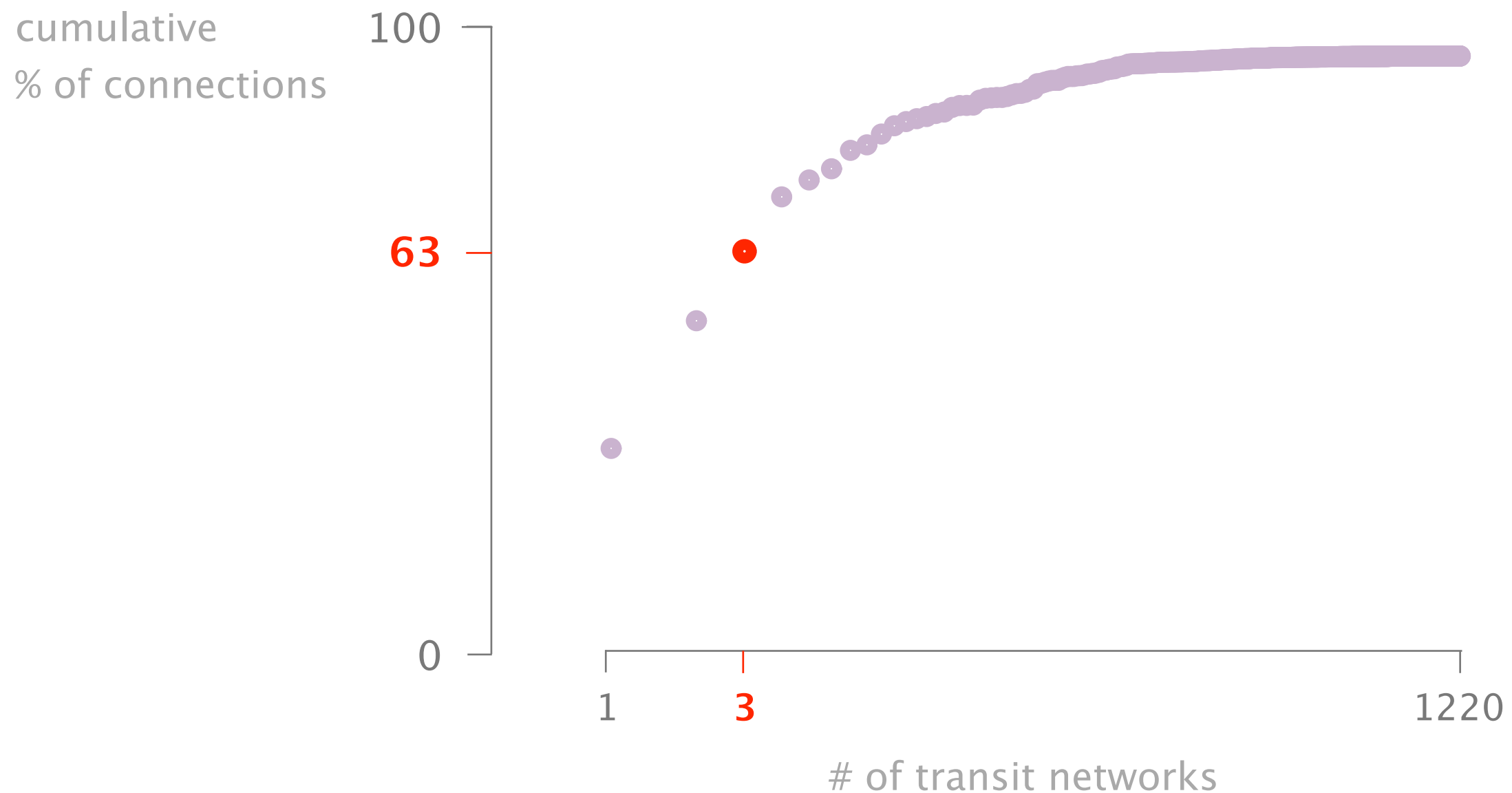
1220

of transit networks

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

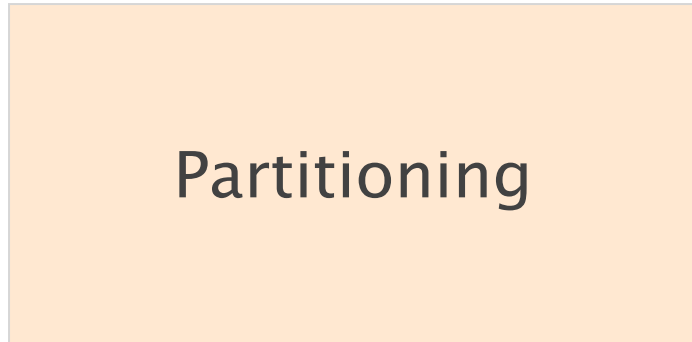


3 transit networks see more than 60% of all connections



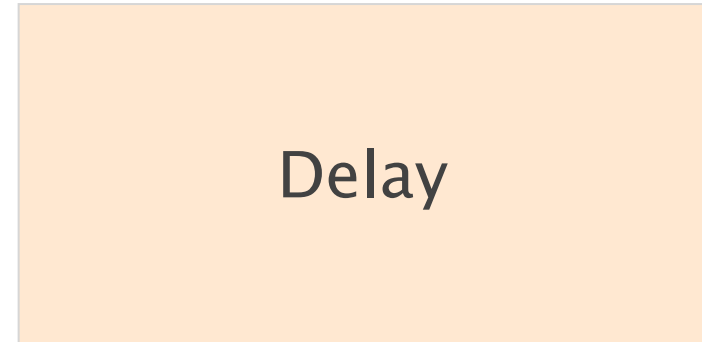
Because of this centralization,
two routing attacks practical and effective today

Attack 1



Split the network in half

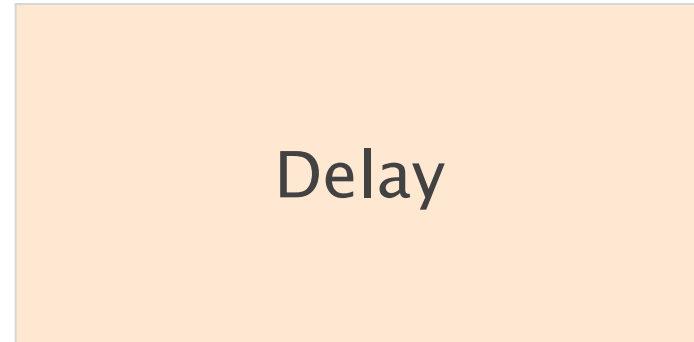
Attack 2



Delay block propagation

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

Attack 1



visible
network-wide attack

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



Partitioning

Attack 2



Delay

invisible

targeted attack (set of nodes)

Hijacking Bitcoin

Routing Attacks on Cryptocurrencies



- 1 **Background**
BGP & Bitcoin
- 2 **Partitioning attack**
splitting the network
- 3 **Delay attack**
slowing the network down
- 4 **Countermeasures**
short-term & long-term

Hijacking Bitcoin

Routing Attacks on Cryptocurrencies



1

Background

BGP & Bitcoin

Partitioning attack

splitting the network

Delay attack

slowing the network down

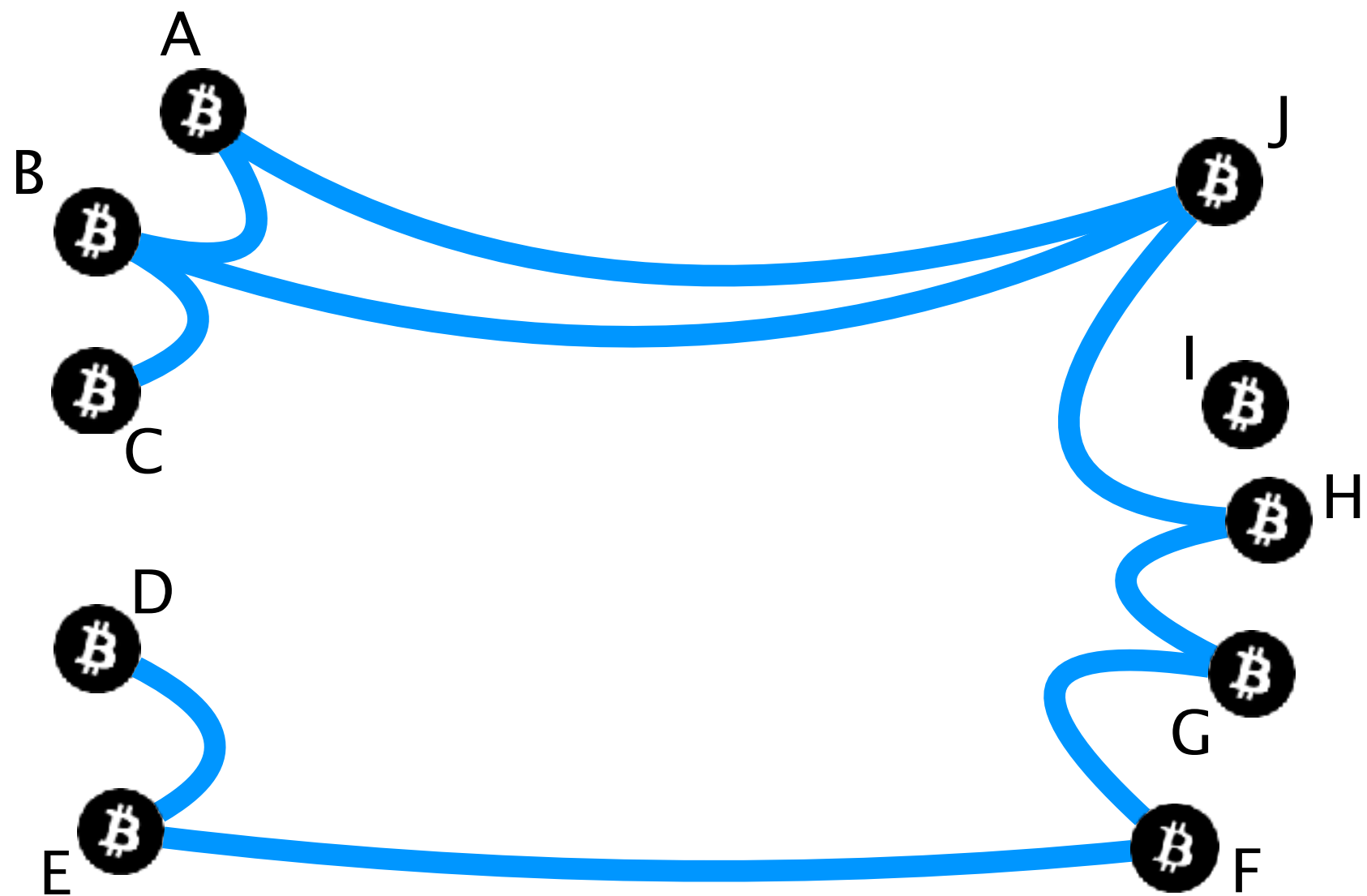
Countermeasures

short-term & long-term

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 x5f78432

Tx x5f78432

Tx b5x89433

Tx h1t91267

Tx h1t91267

...

...

...

The blockchain is a chain of blocks

Block #42

Block #43

Block #44

prev: #41

Tx a1a53743

Tx b5x89433

...

prev: #42

Tx x5f78432

Tx h1t91267

...

prev: #42

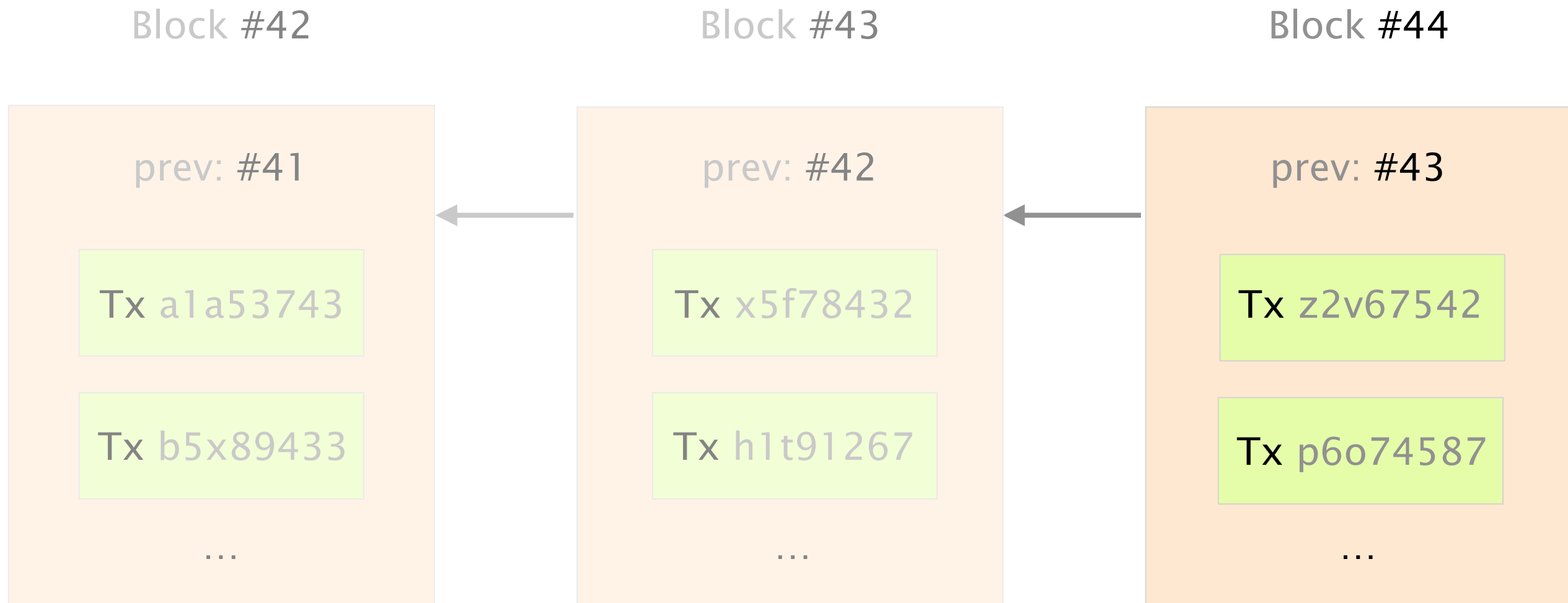
Tx x5f78432

Tx h1t91267

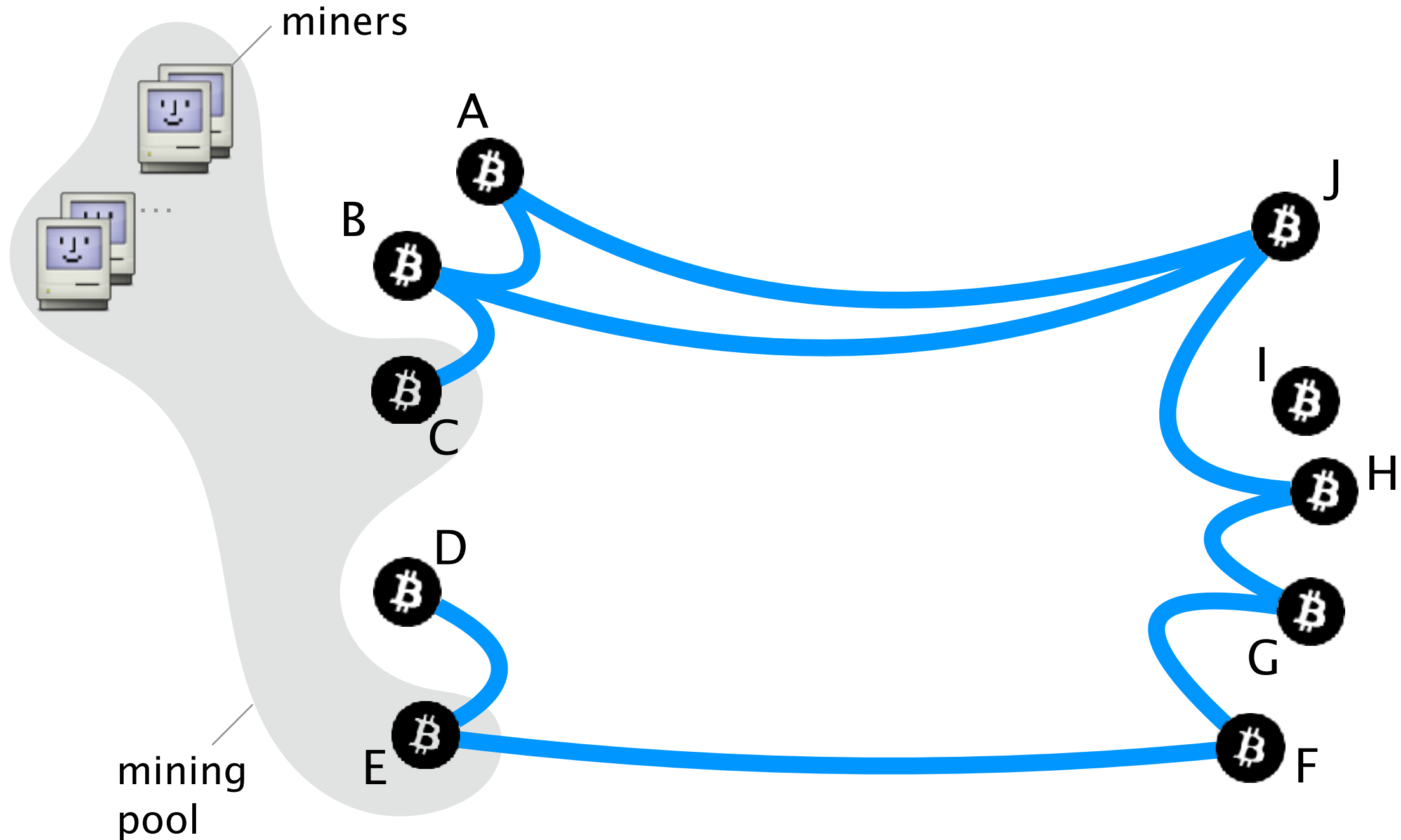
...



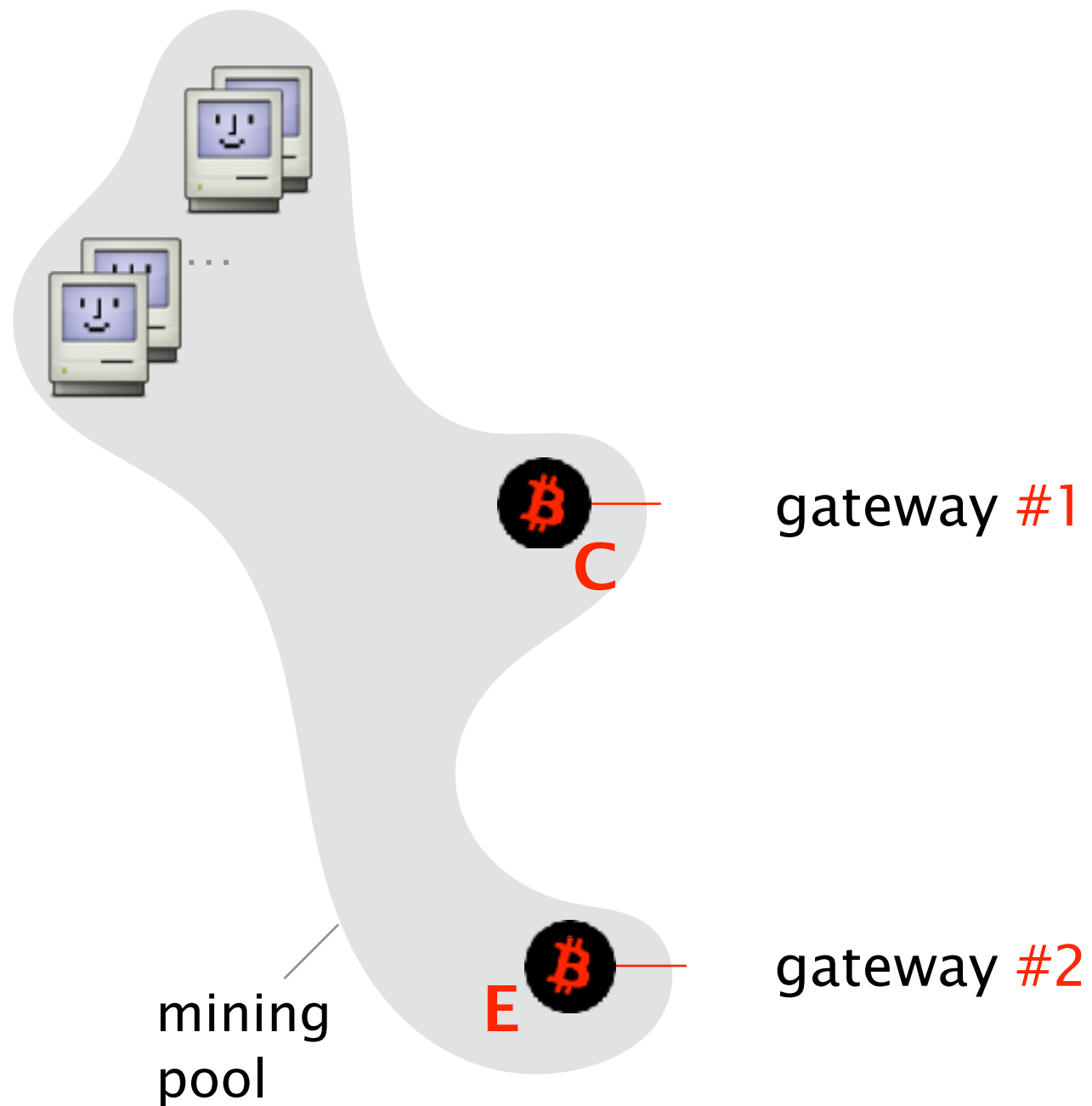
The blockchain is extended by miners



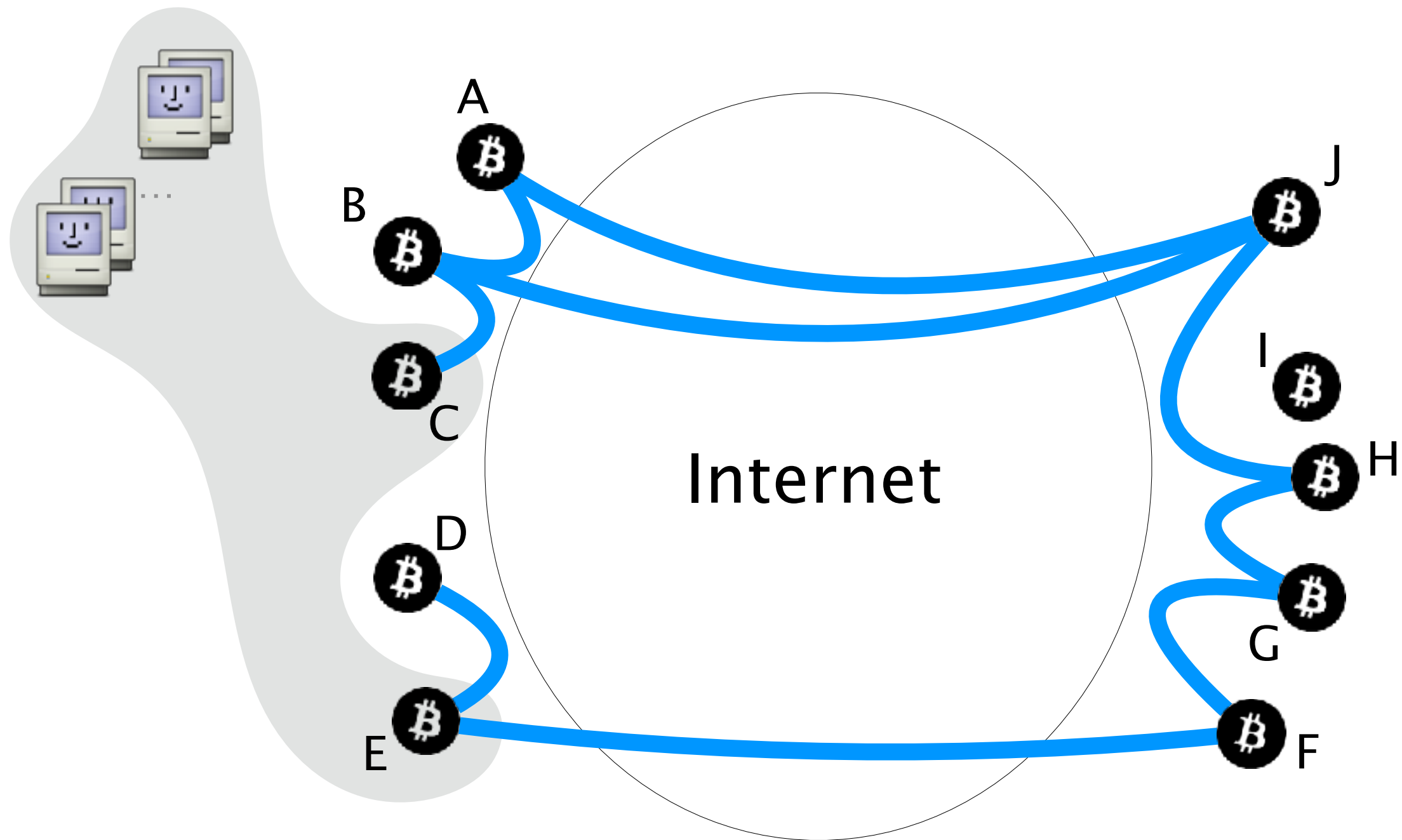
Miners are grouped in **mining pools**



Mining pools connect to the Bitcoin network through **multiple gateways**

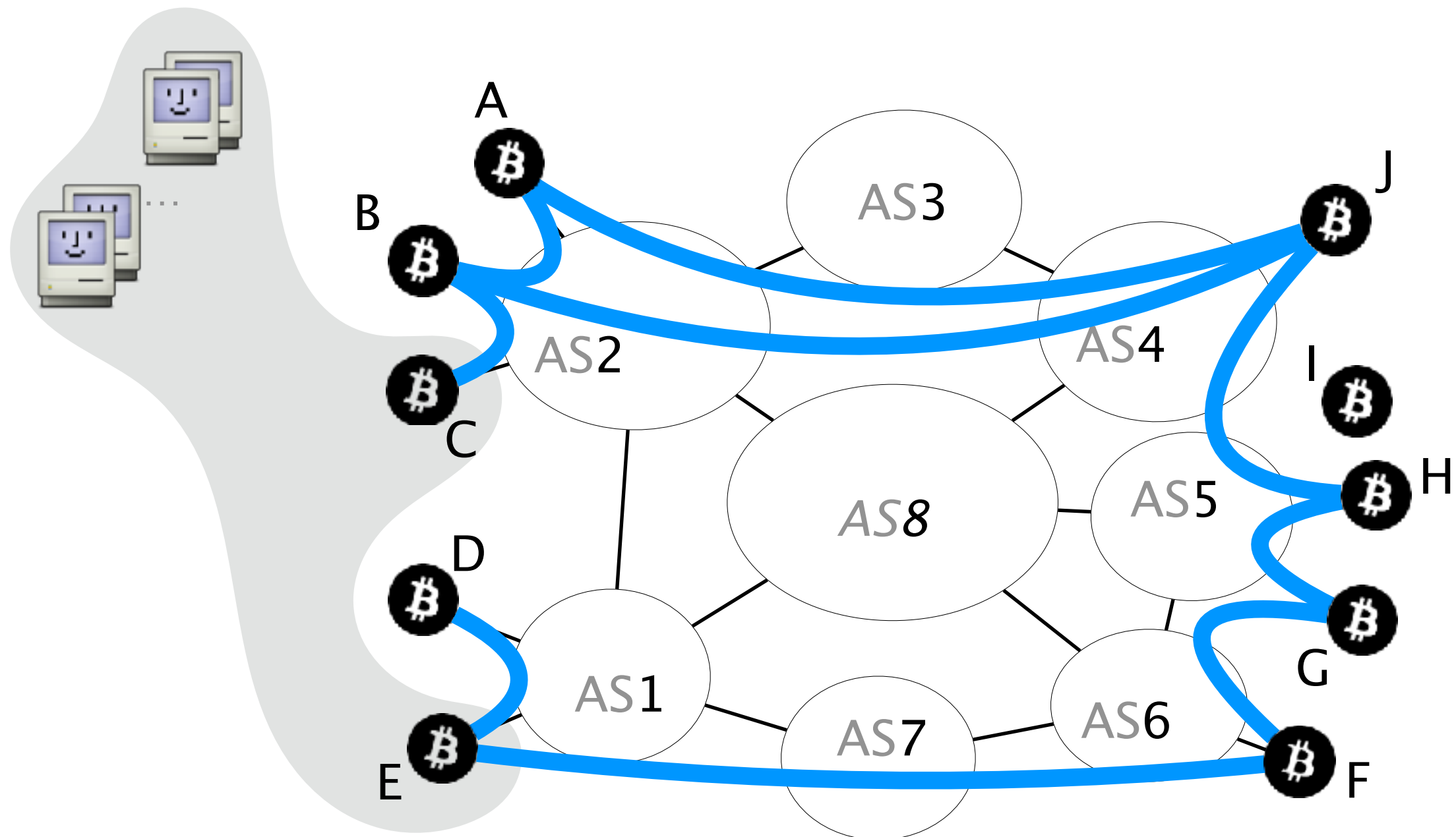


Bitcoin connections are routed over the Internet

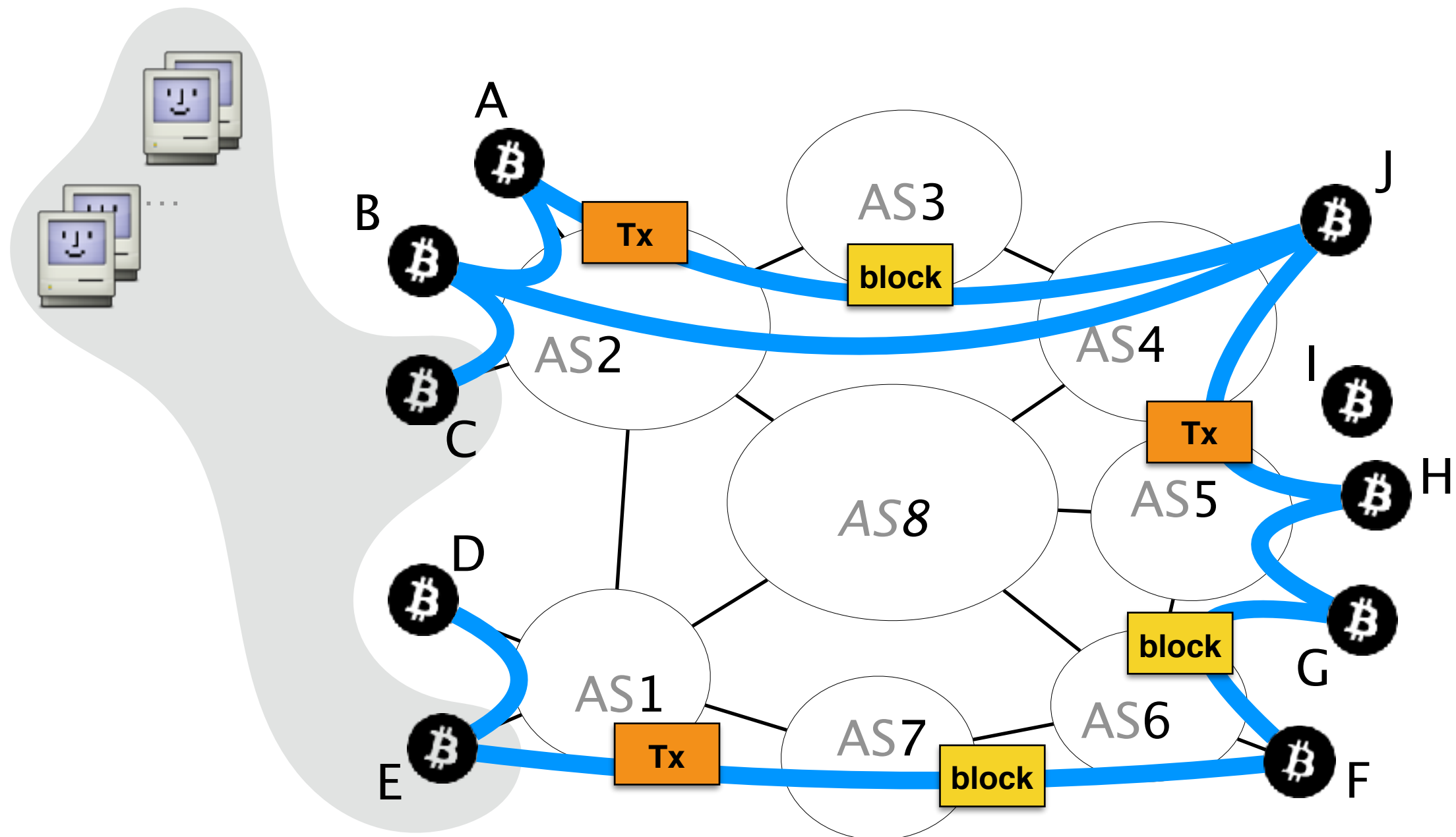


The Internet is composed of Autonomous Systems (ASes).

BGP computes the forwarding path across them



Bitcoin messages are propagated **unencrypted**
and **without any integrity guarantees**



Hijacking Bitcoin

Routing Attacks on Cryptocurrencies



Background

BGP & Bitcoin

2

Partitioning attack

splitting the network

Delay attack

slowing the network down

Countermeasures

short-term & long-term

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

Double spending



Blocks in component with
less mining power are discarded

The impact of such an attack is worrying

Denial of Service

Revenue Loss

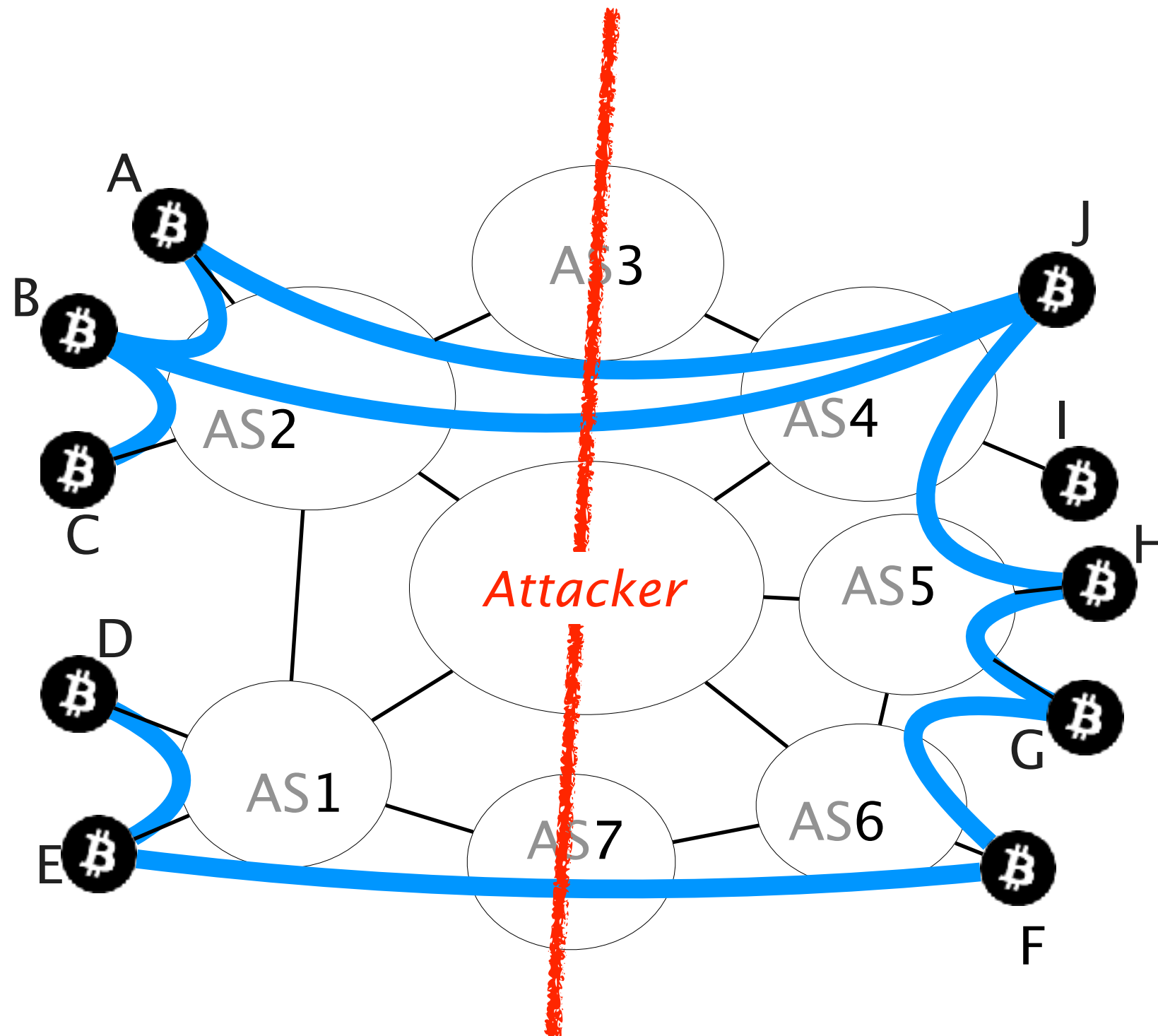
Double spending



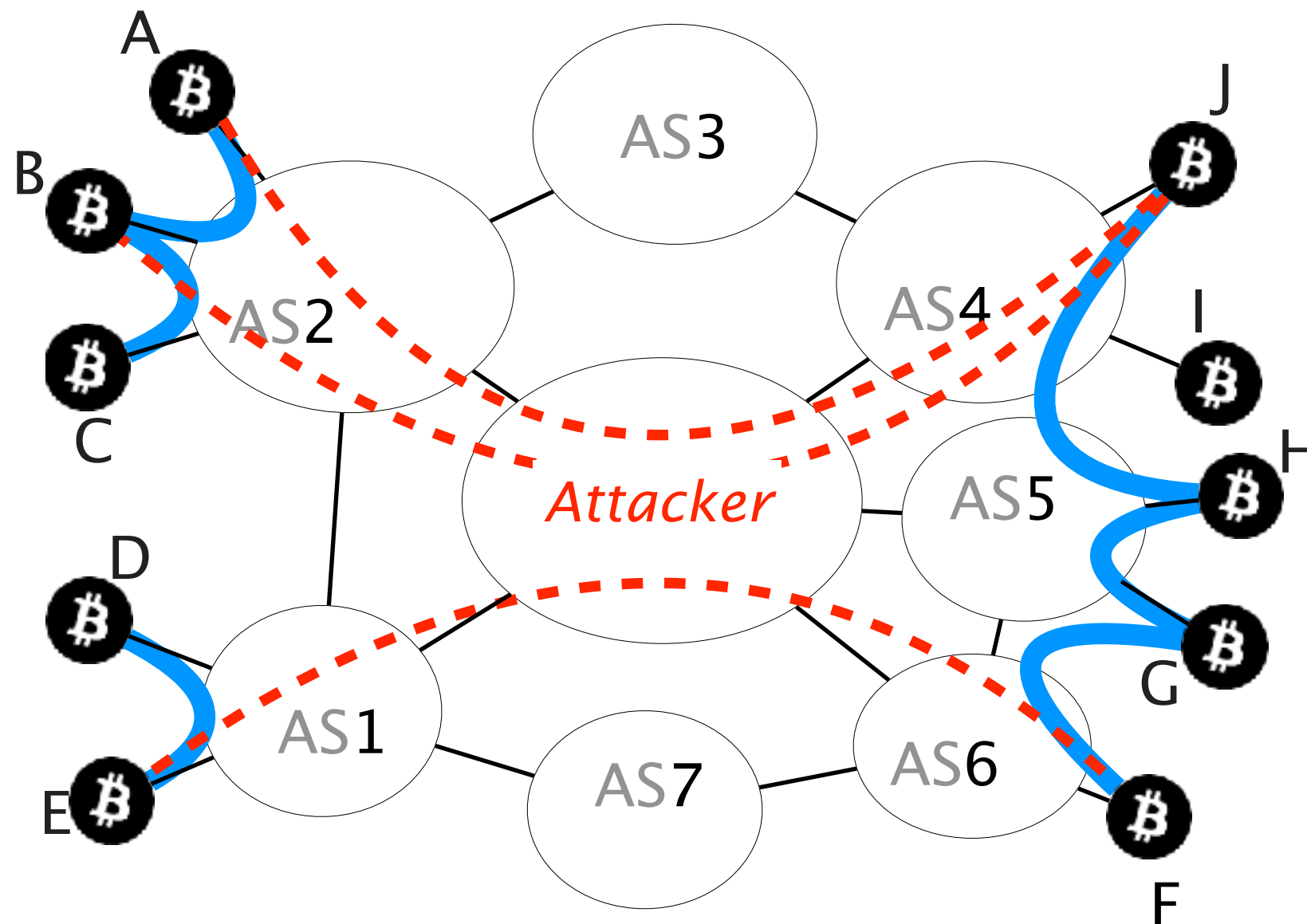
Transactions in components with less mining power can be reverted

How does the attack work?

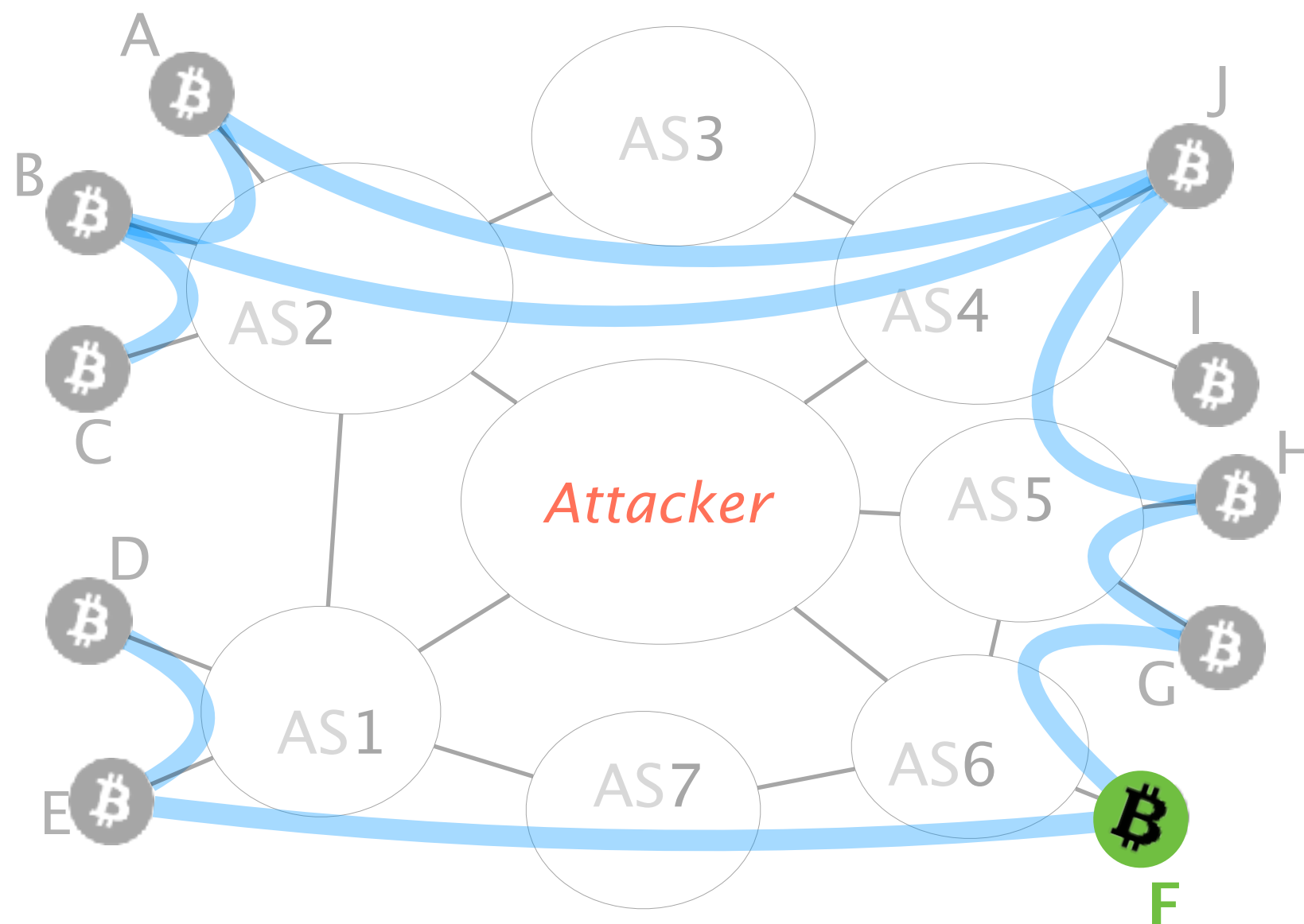
Let's say an attacker wants to **partition** the network into the **left** and **right** side



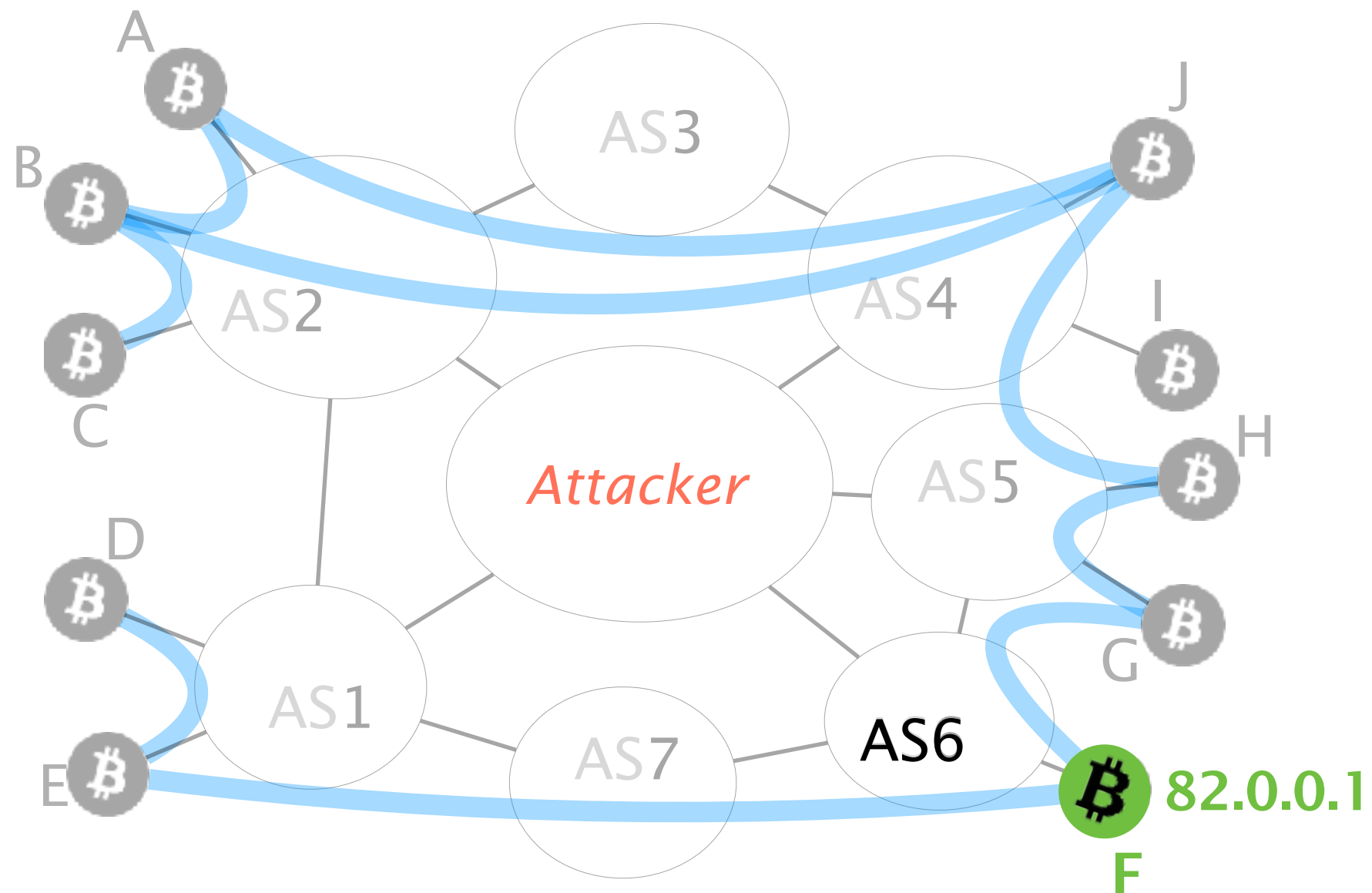
For doing so, the attacker will manipulate BGP routes to intercept any traffic to the nodes in the right



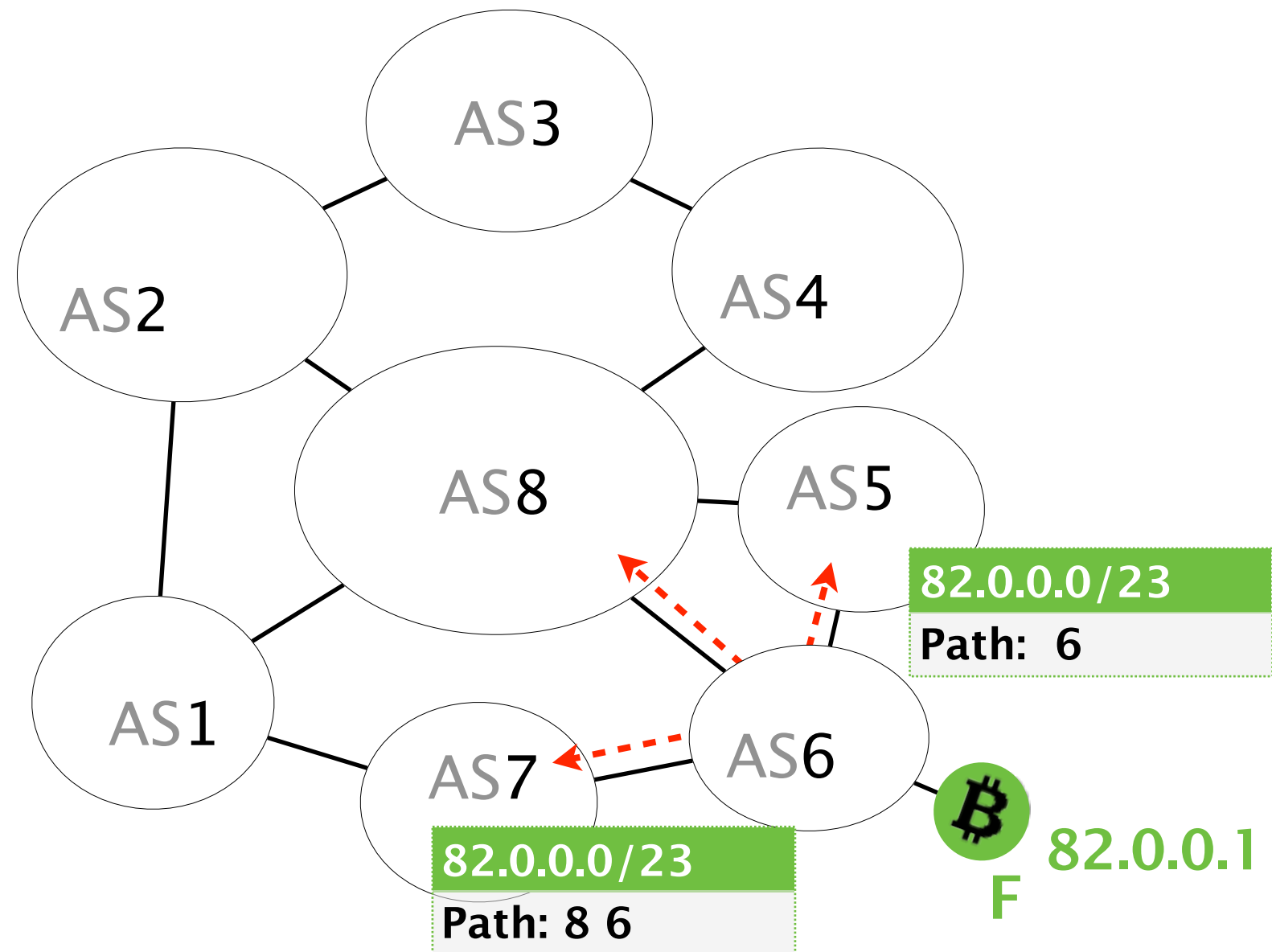
Let us focus on node **F**



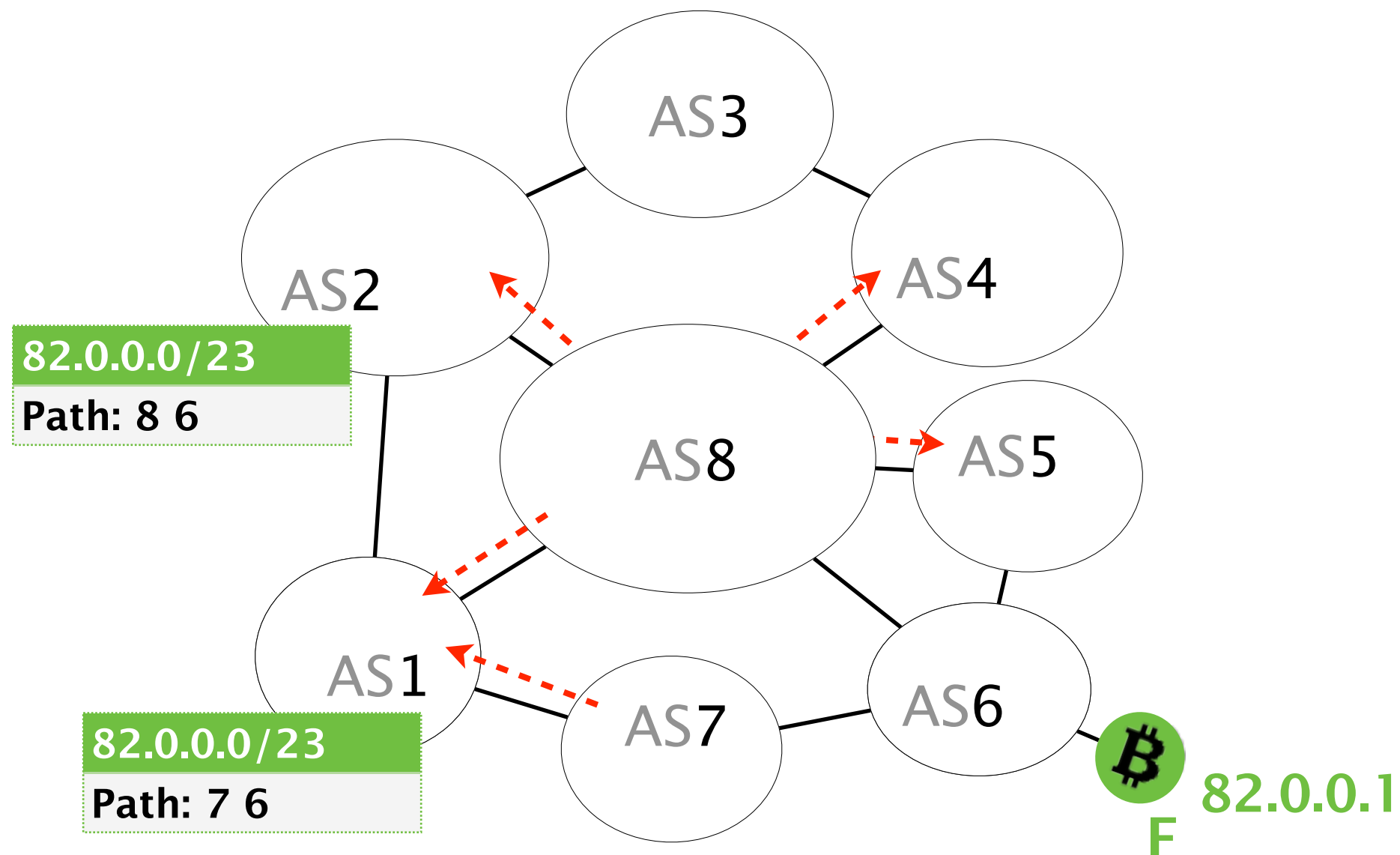
F's provider (AS6) is responsible for IP prefix



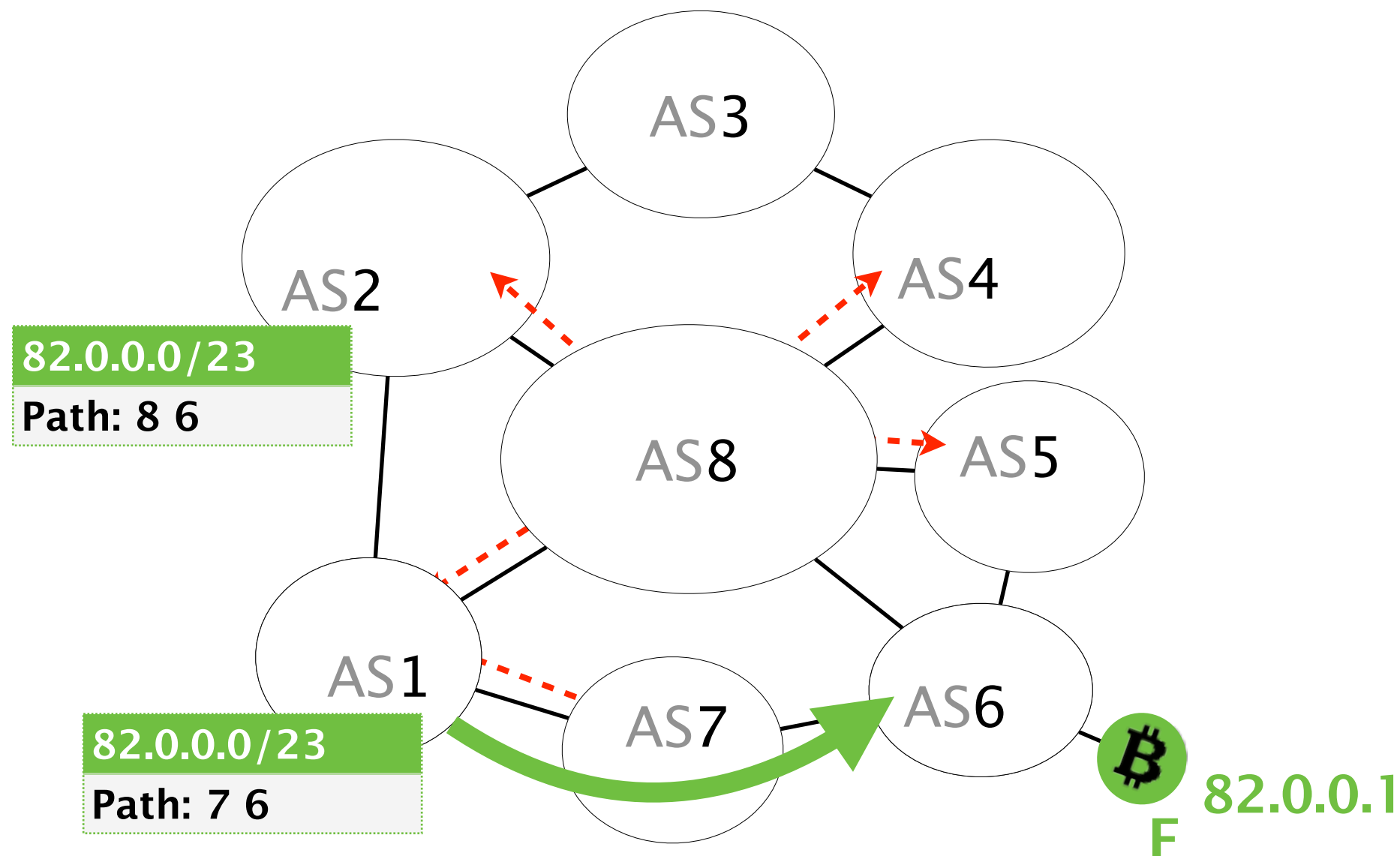
AS6 will create a BGP advertisement



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



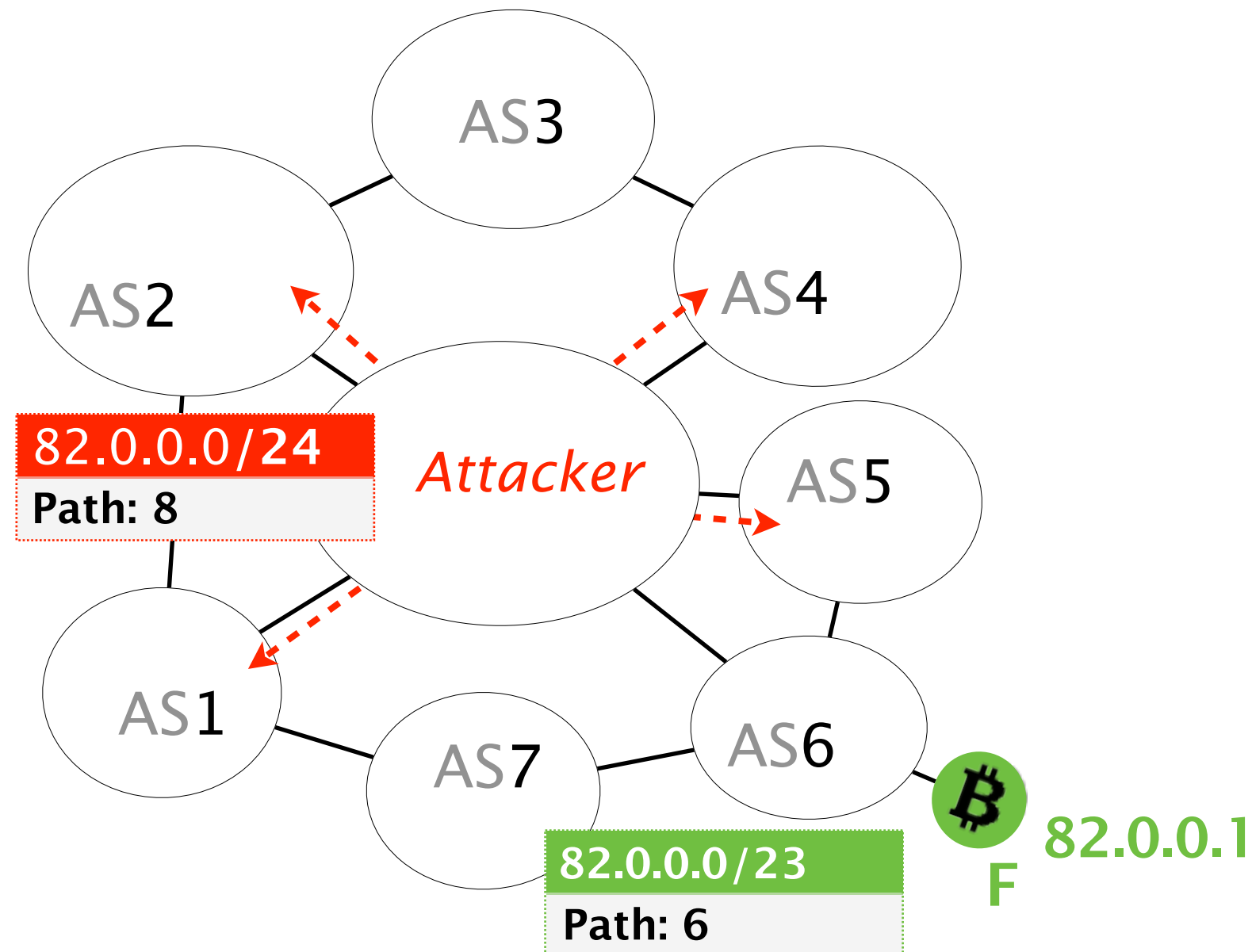
AS6's advertisement is propagated AS-by-AS until all ASes in the Internet learn about it



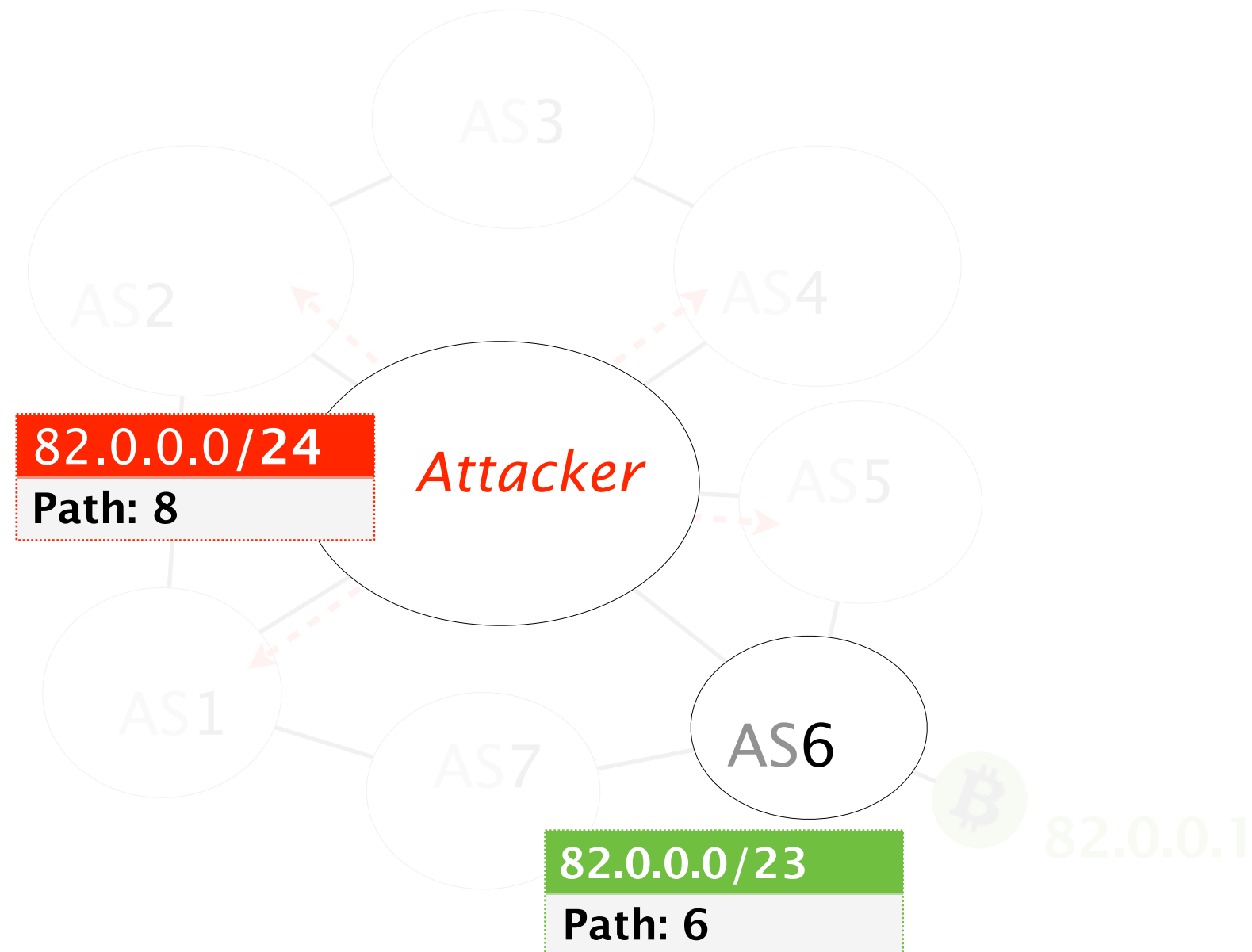
BGP **does not check the validity** of advertisements,
meaning any AS can announce any prefix

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

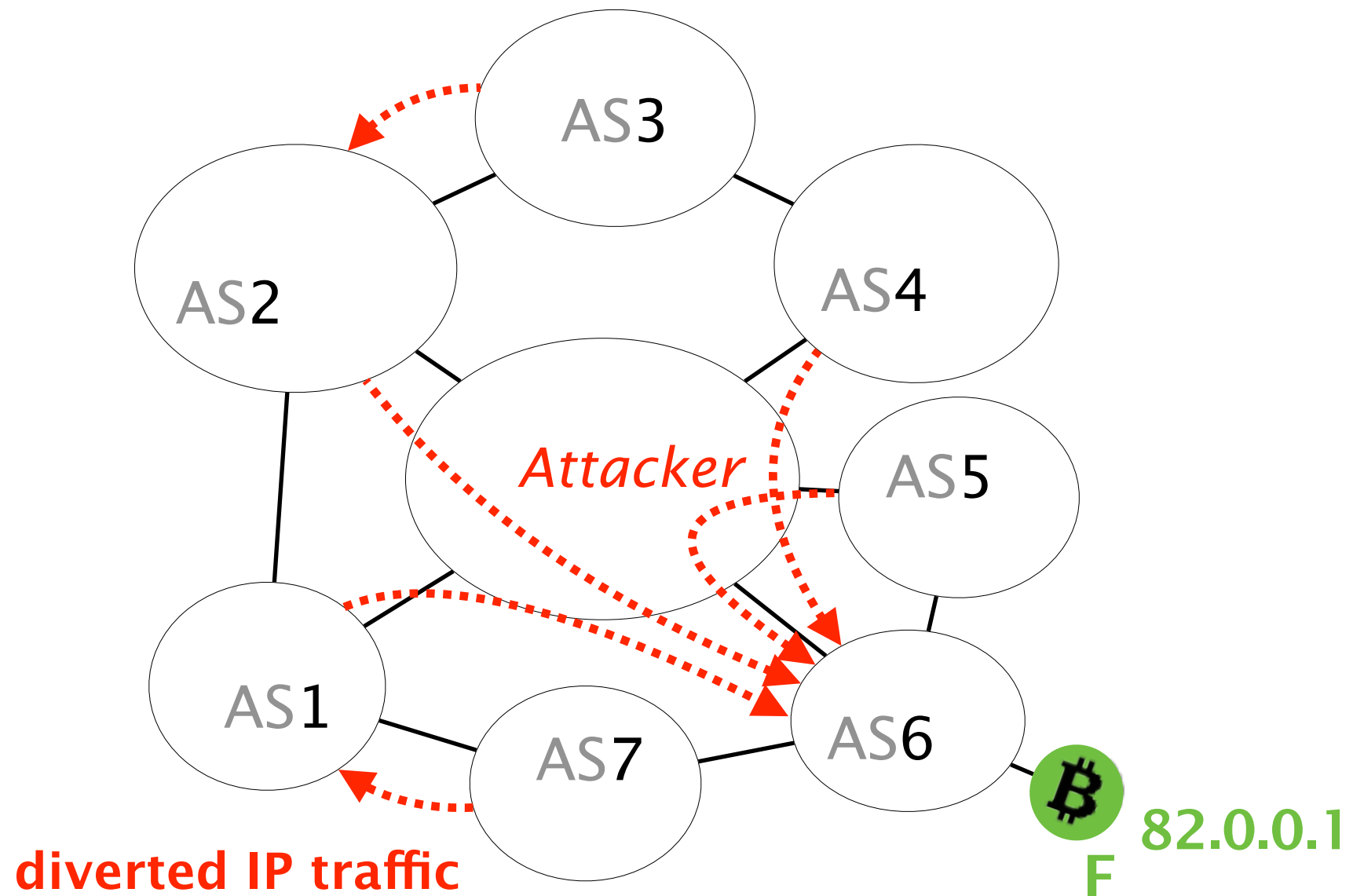
Consider that the attacker advertises a **more-specific prefix** covering F's IP address



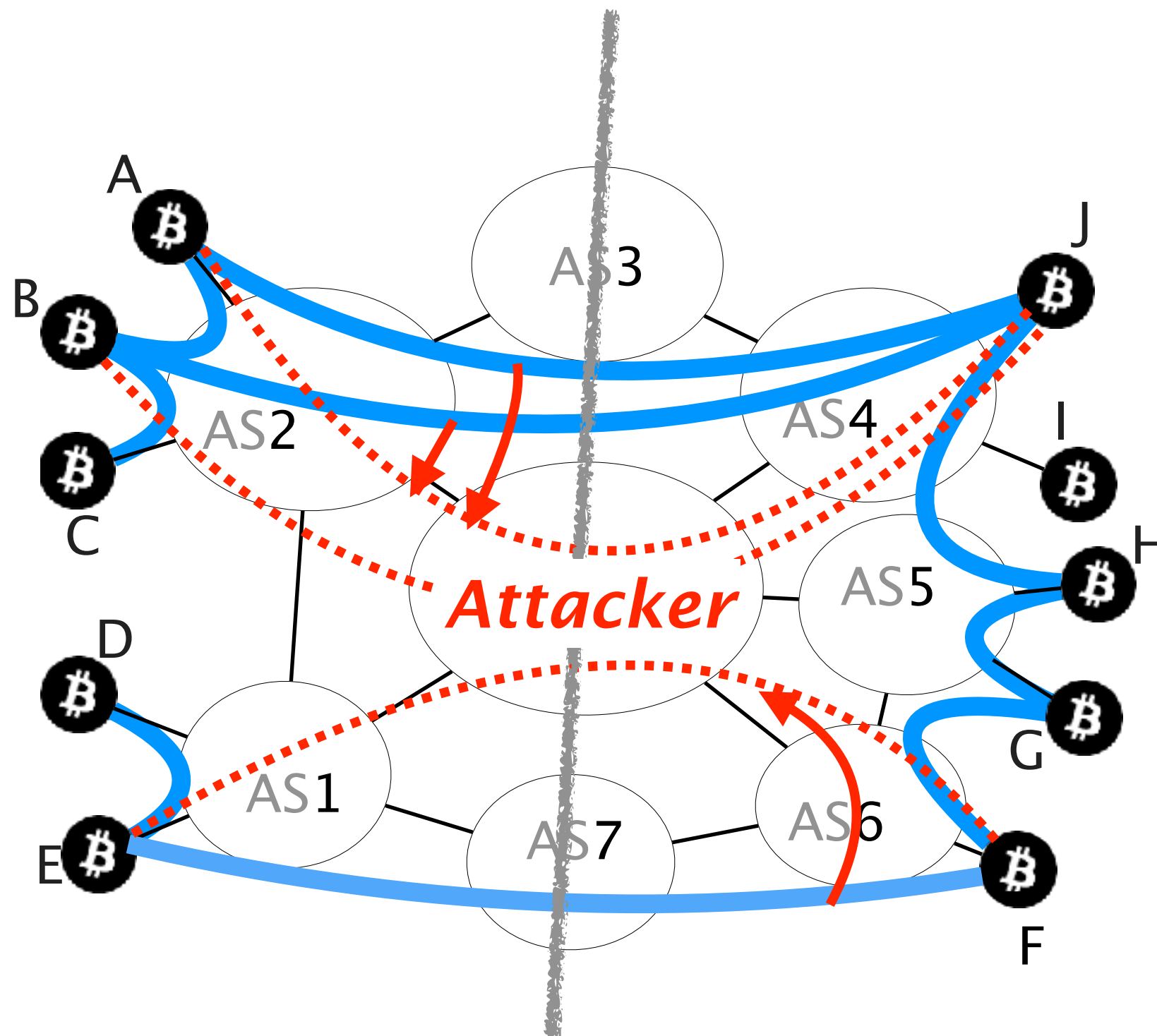
As IP routers prefer more-specific prefixes, the attacker route will be preferred



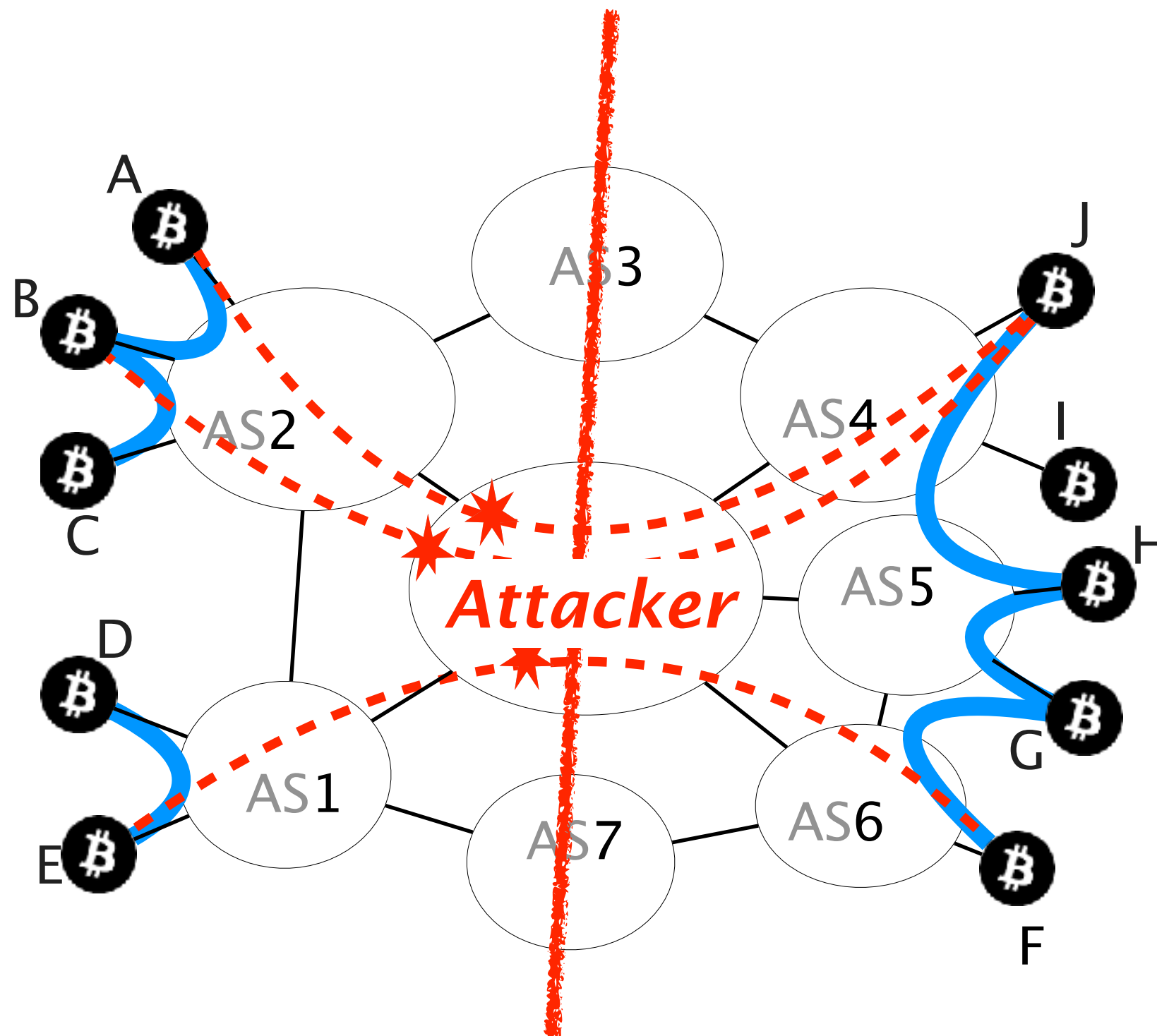
Traffic to node F is **hijacked**



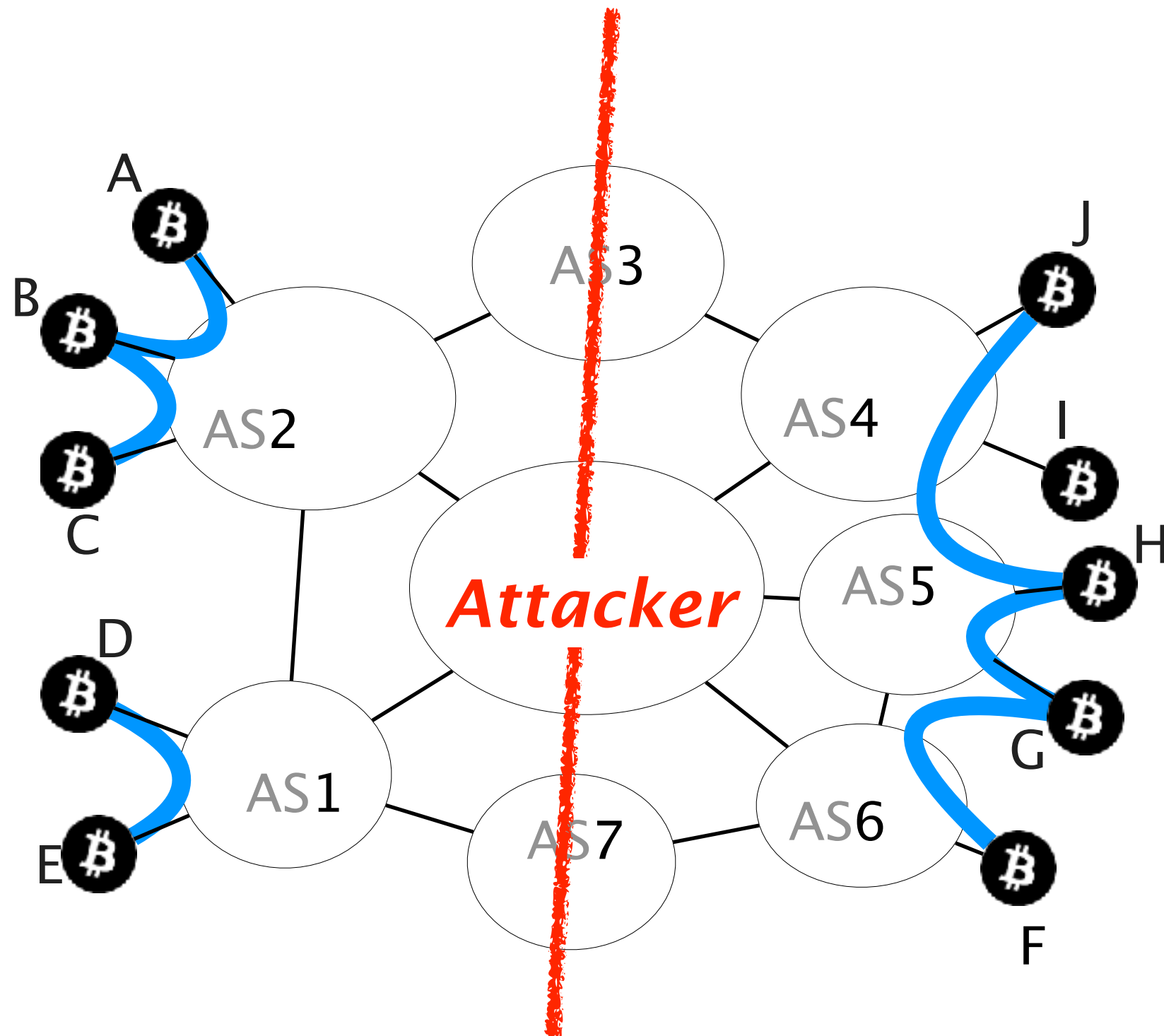
By hijacking the IP prefixes pertaining to the right nodes, the attacker can intercept all their connections



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)

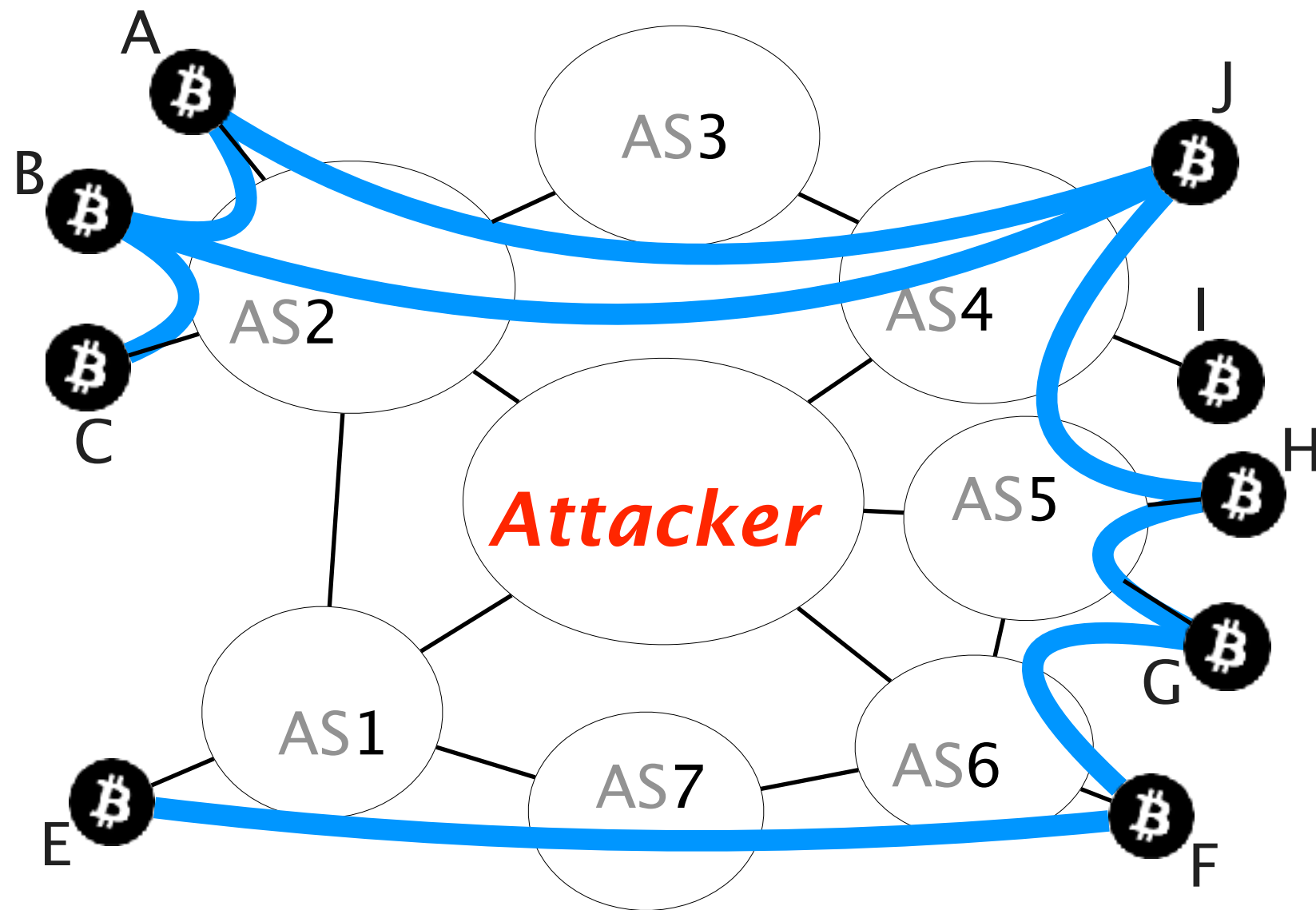
Bitcoin connections established...

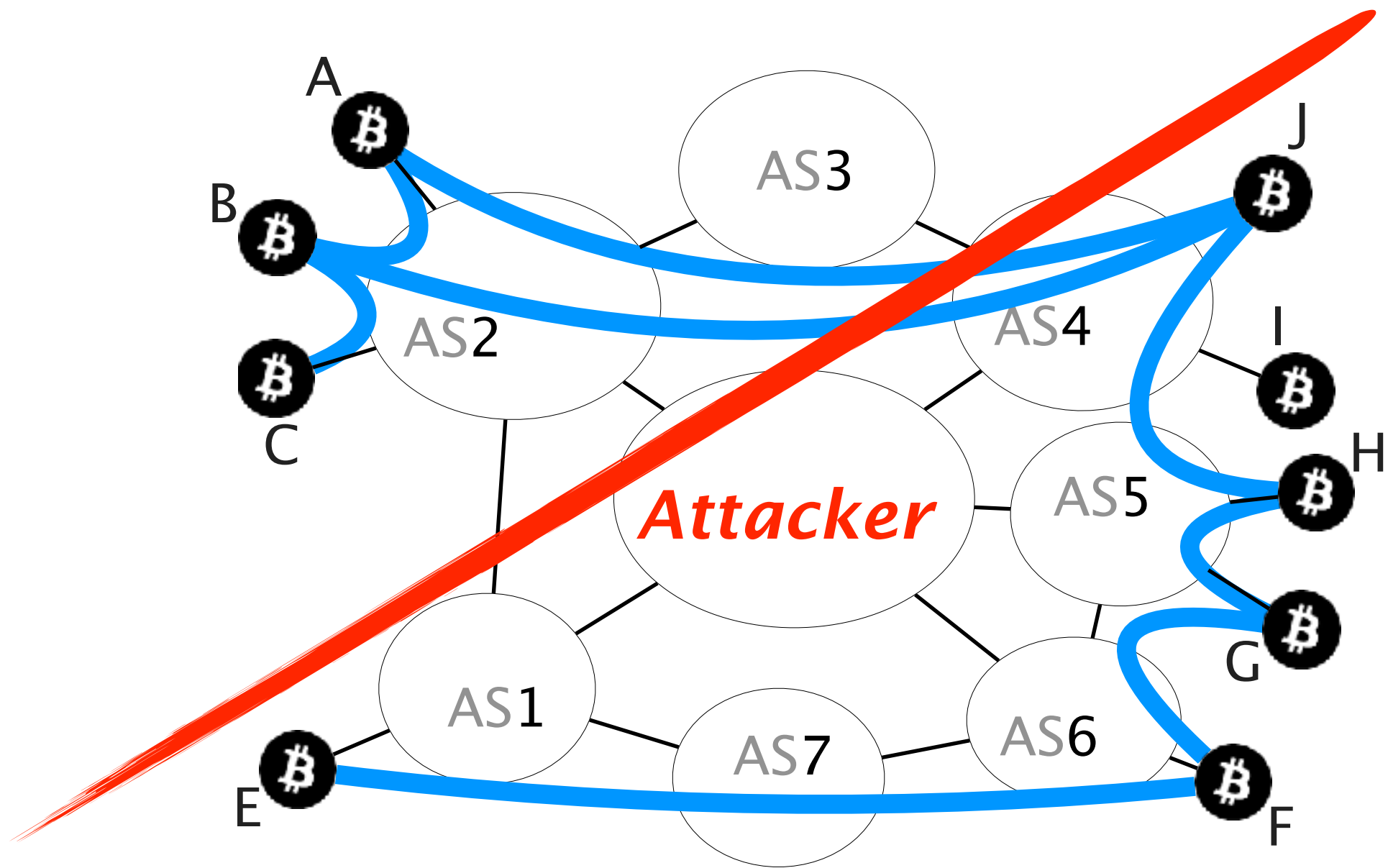
- within a mining pool
- within an AS
- between mining pools

cannot be hijacked (usually)

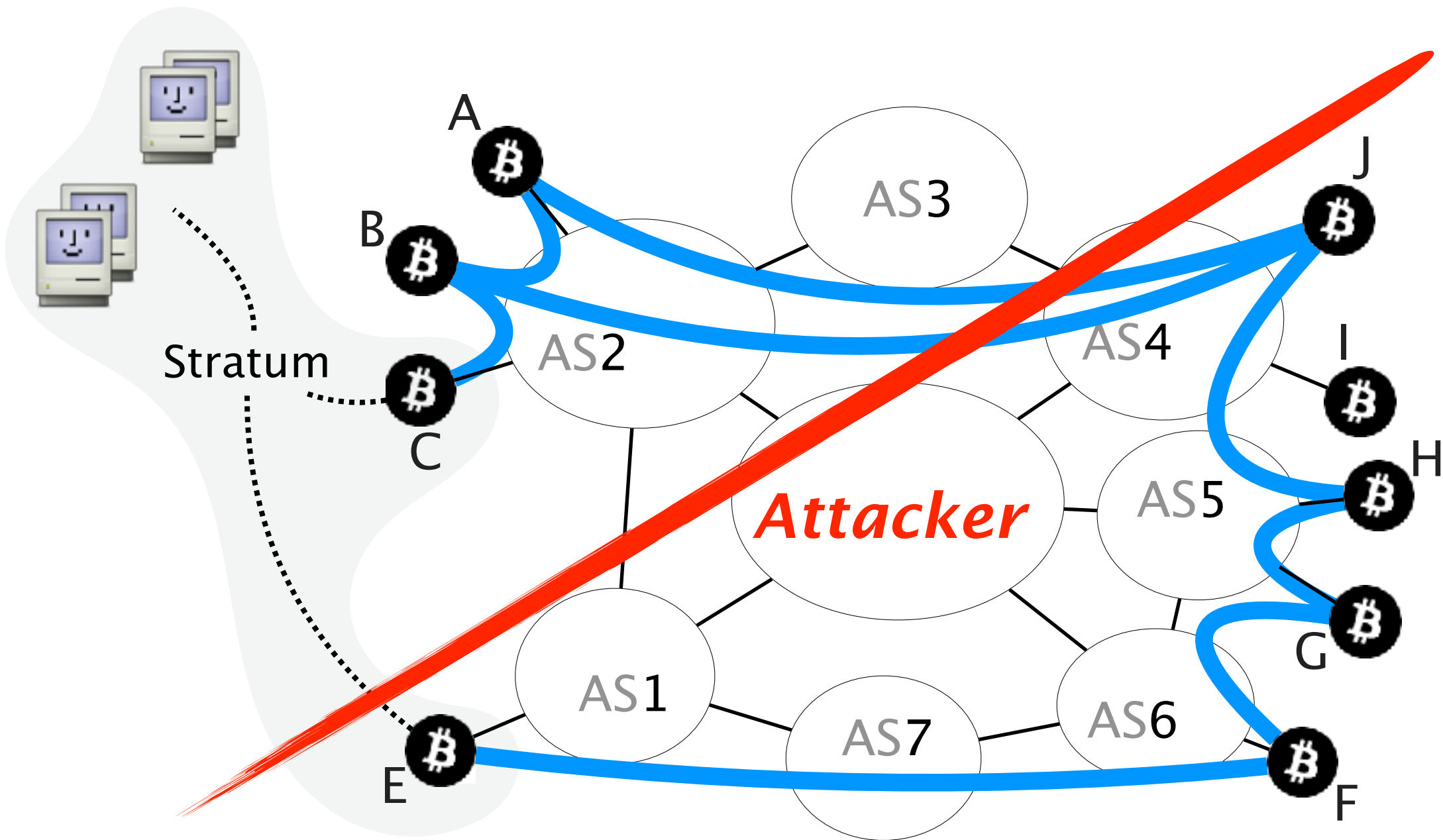
but can be *detected* and *located* by the attacker
enabling her to build a similar but feasible partition

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

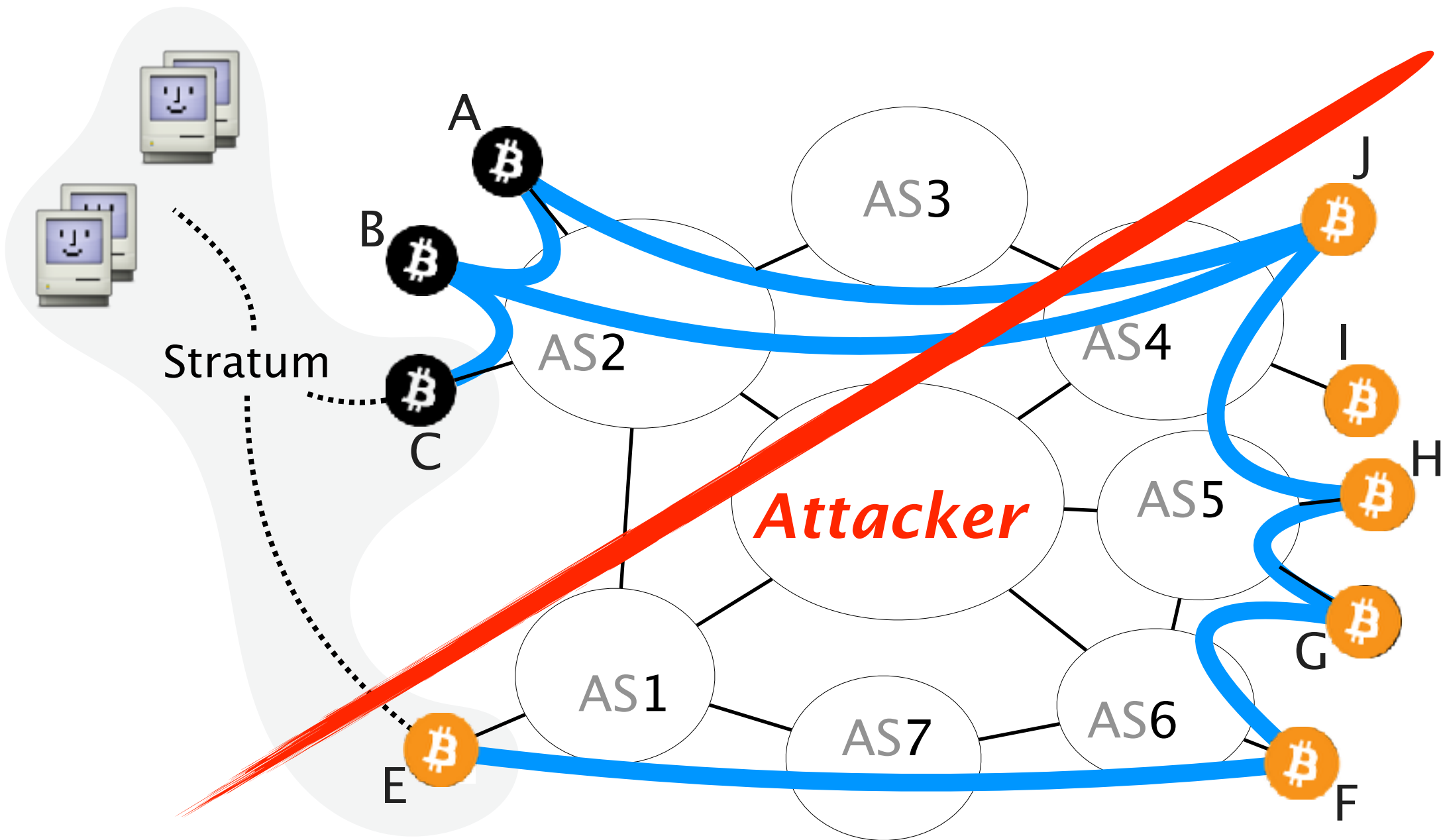


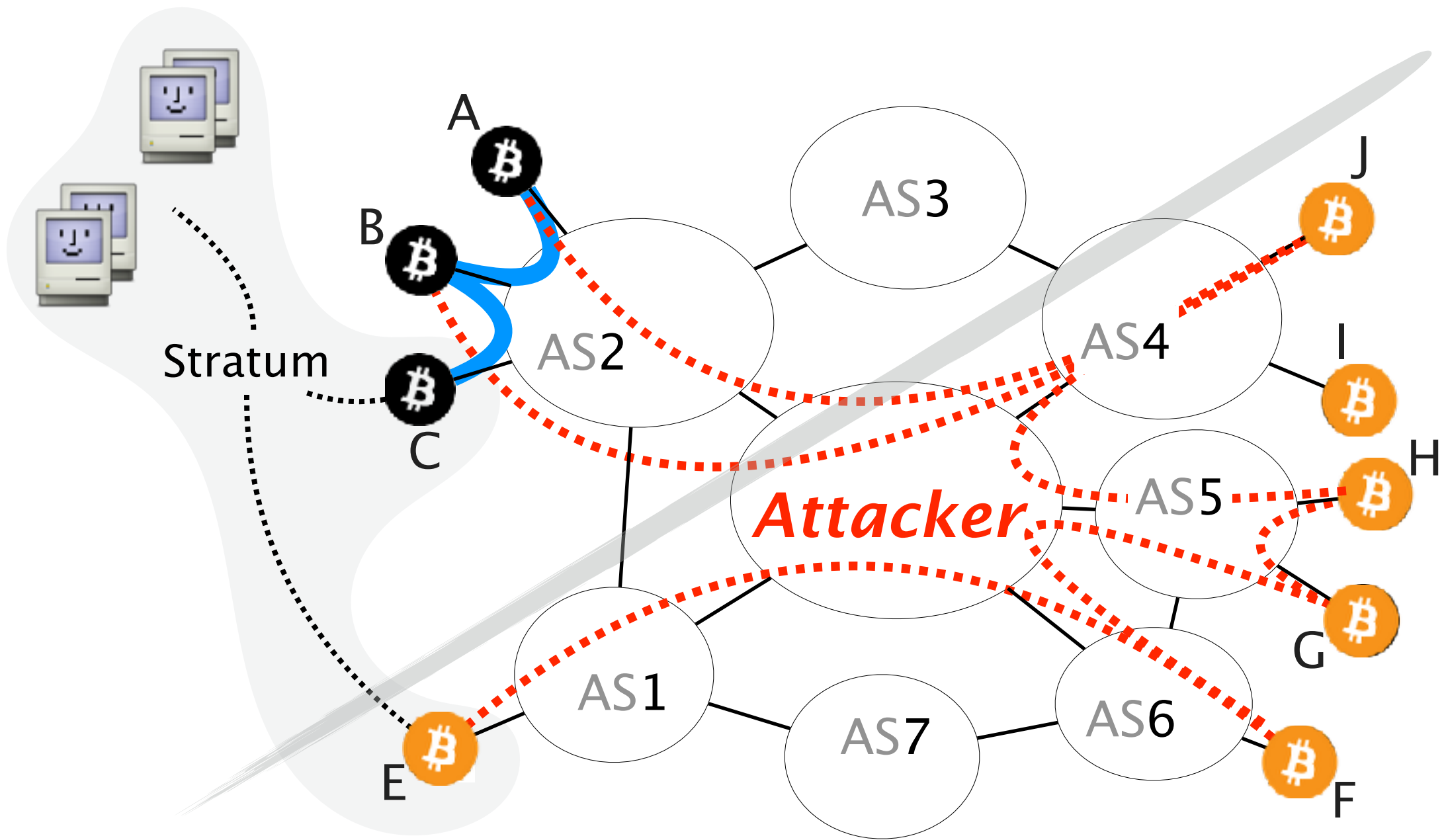


... with a mining pool in the middle

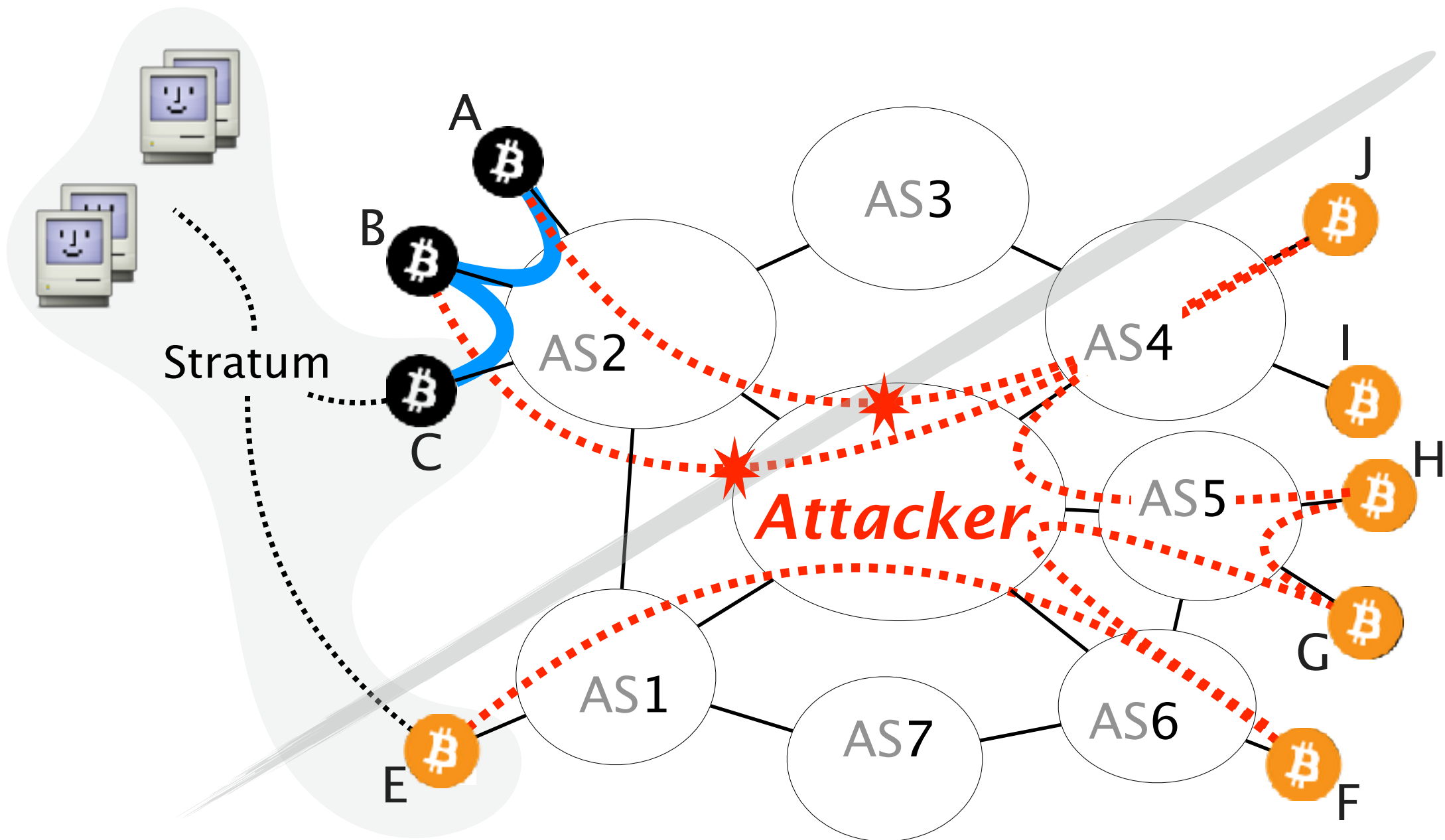


For this, the attacker hijacks all prefixes pertaining to the nodes located on the right-hand side

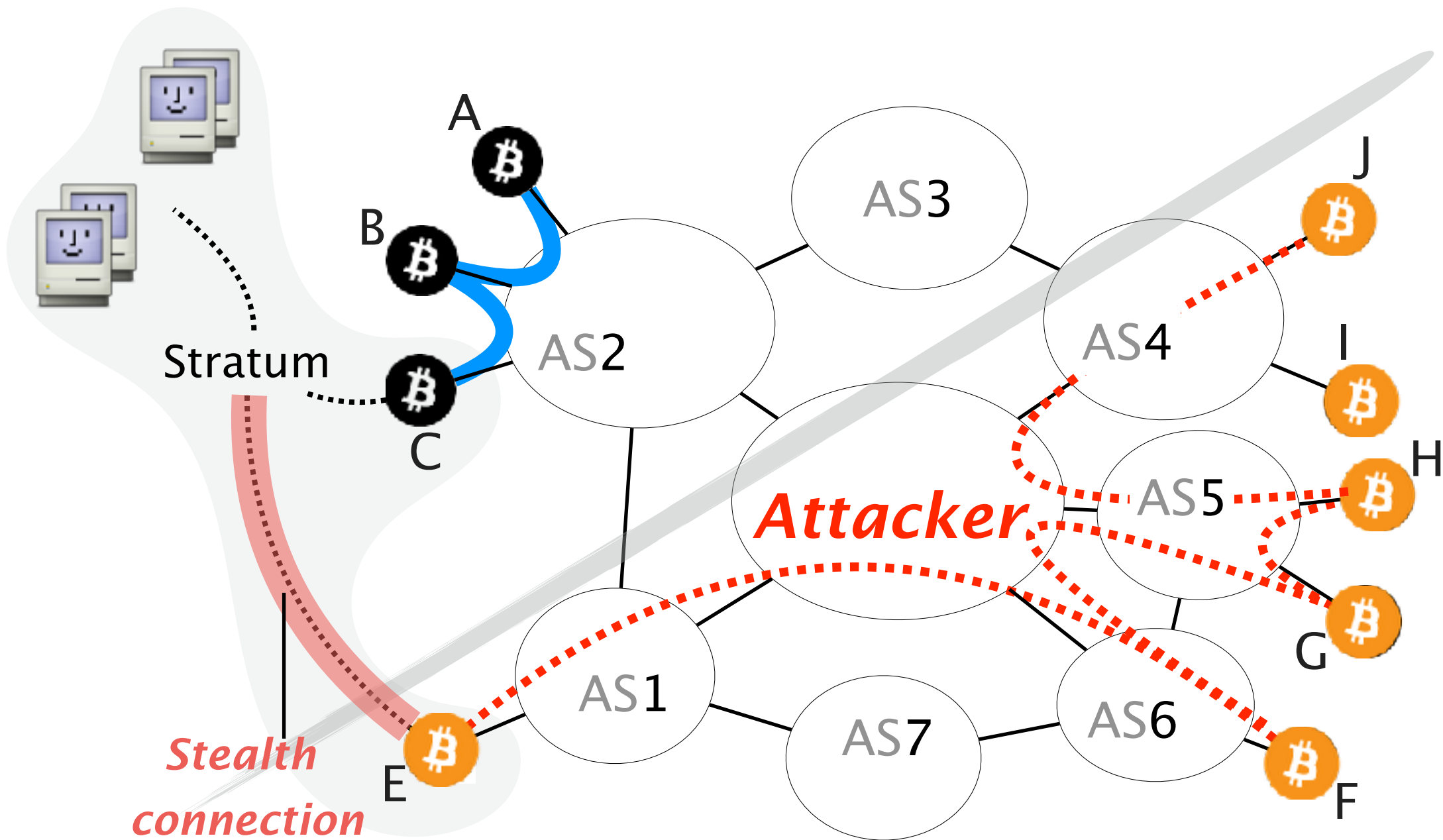




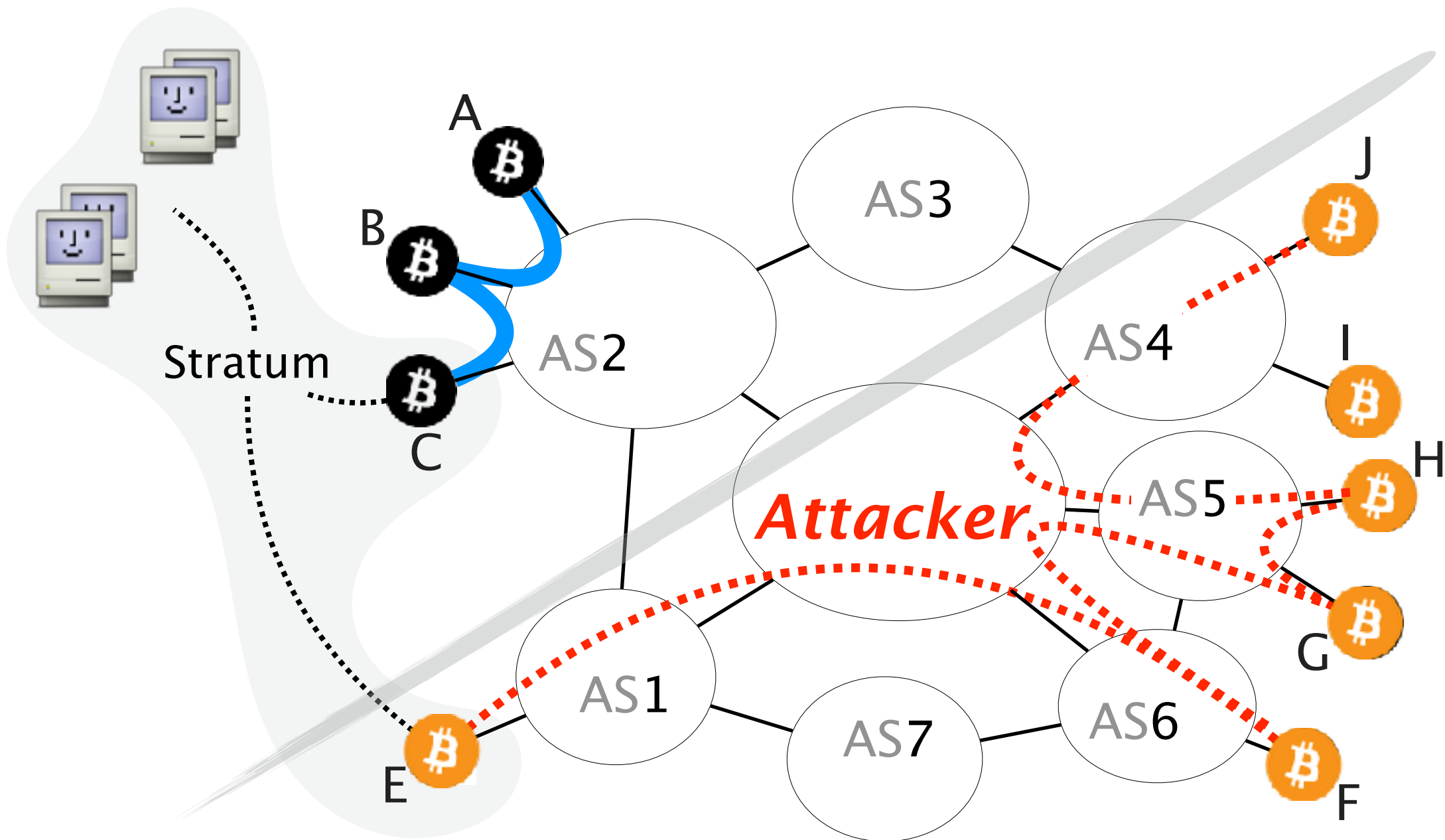
The attacker then drops the connections



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?

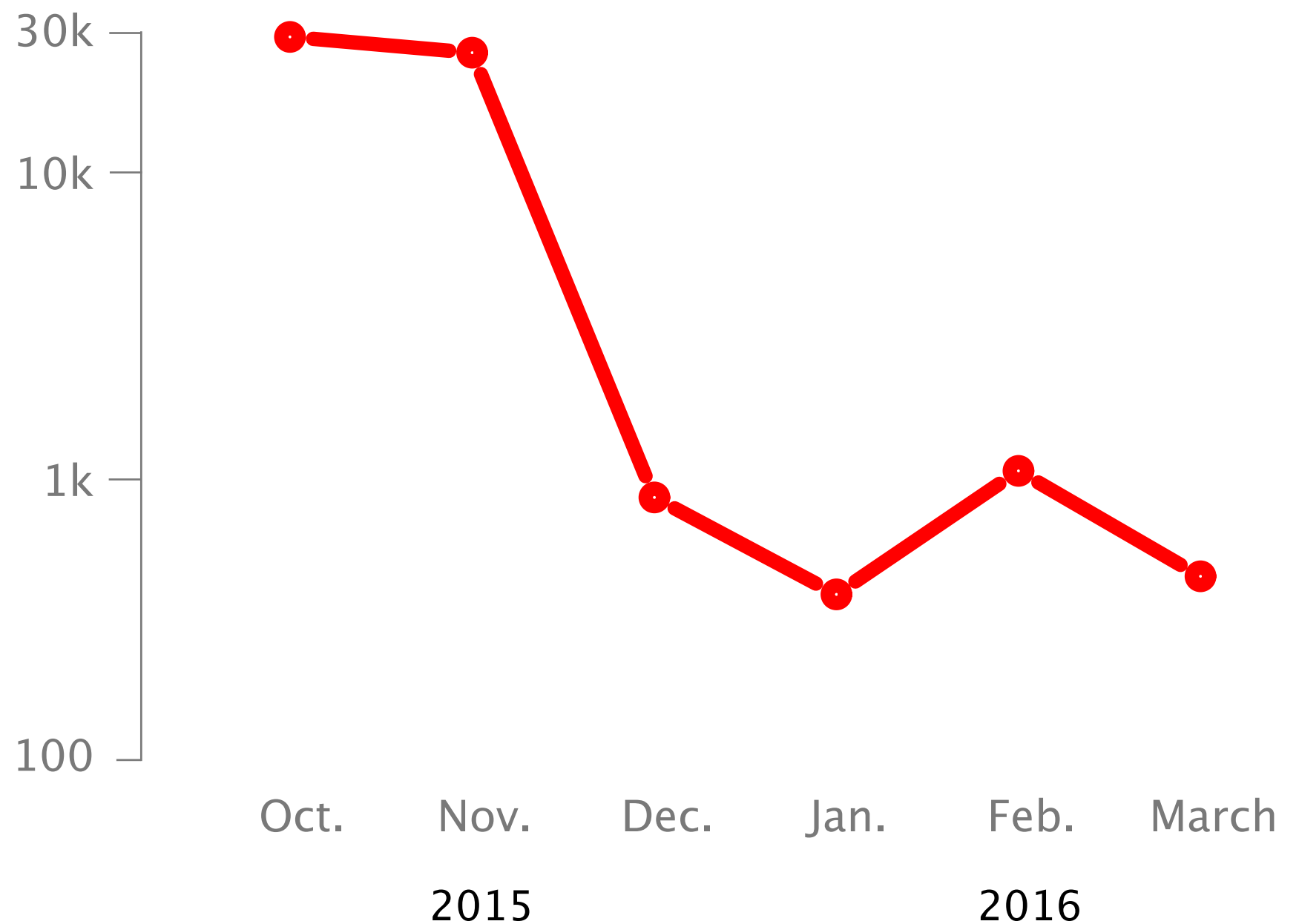
Splitting the mining power **even to half** can be done
by hijacking **less than 100** prefixes

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

max # of prefixes
hijacked at once
log scale



We also evaluated the partition in terms of
time efficiency



Practicality

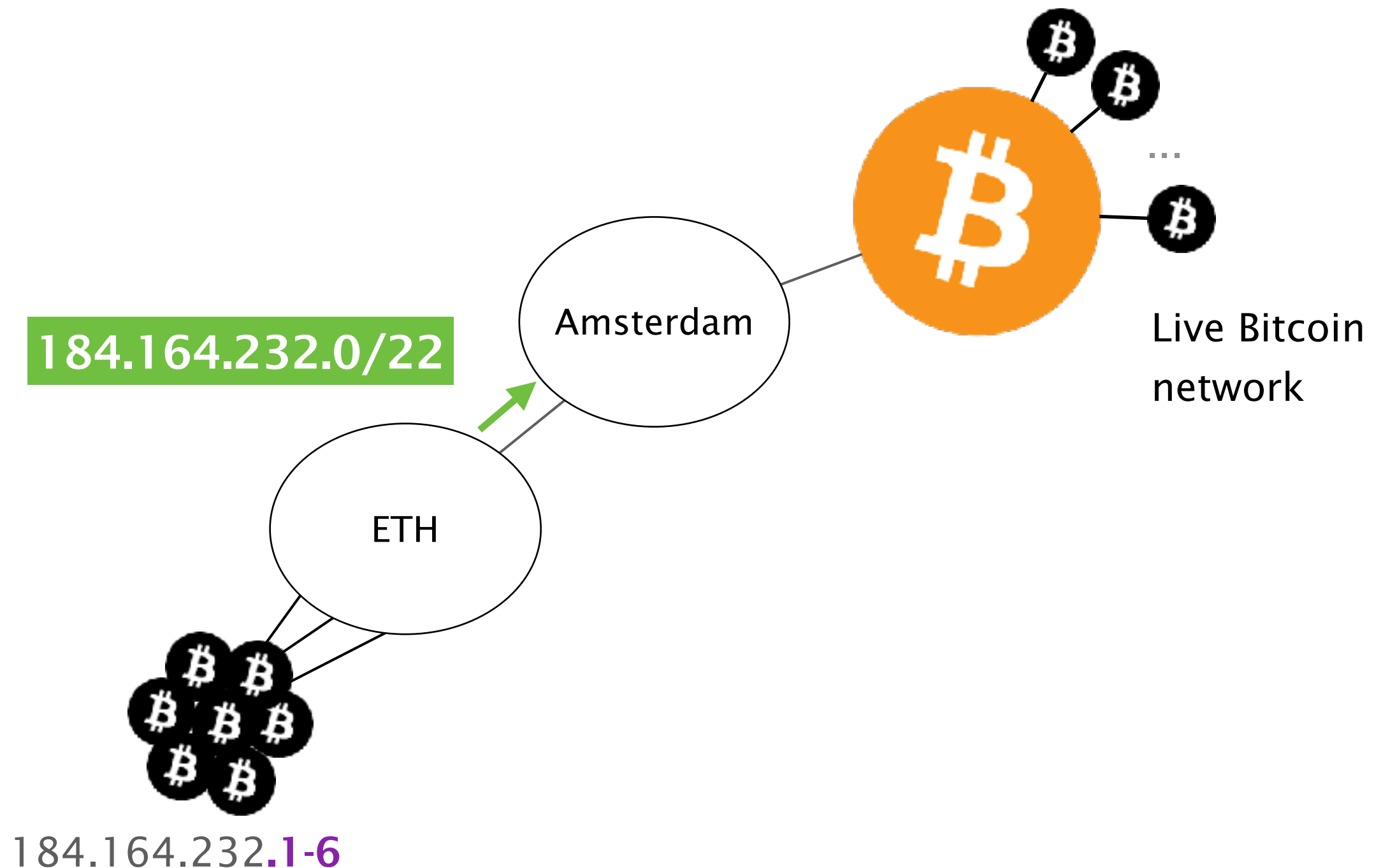


Time efficiency

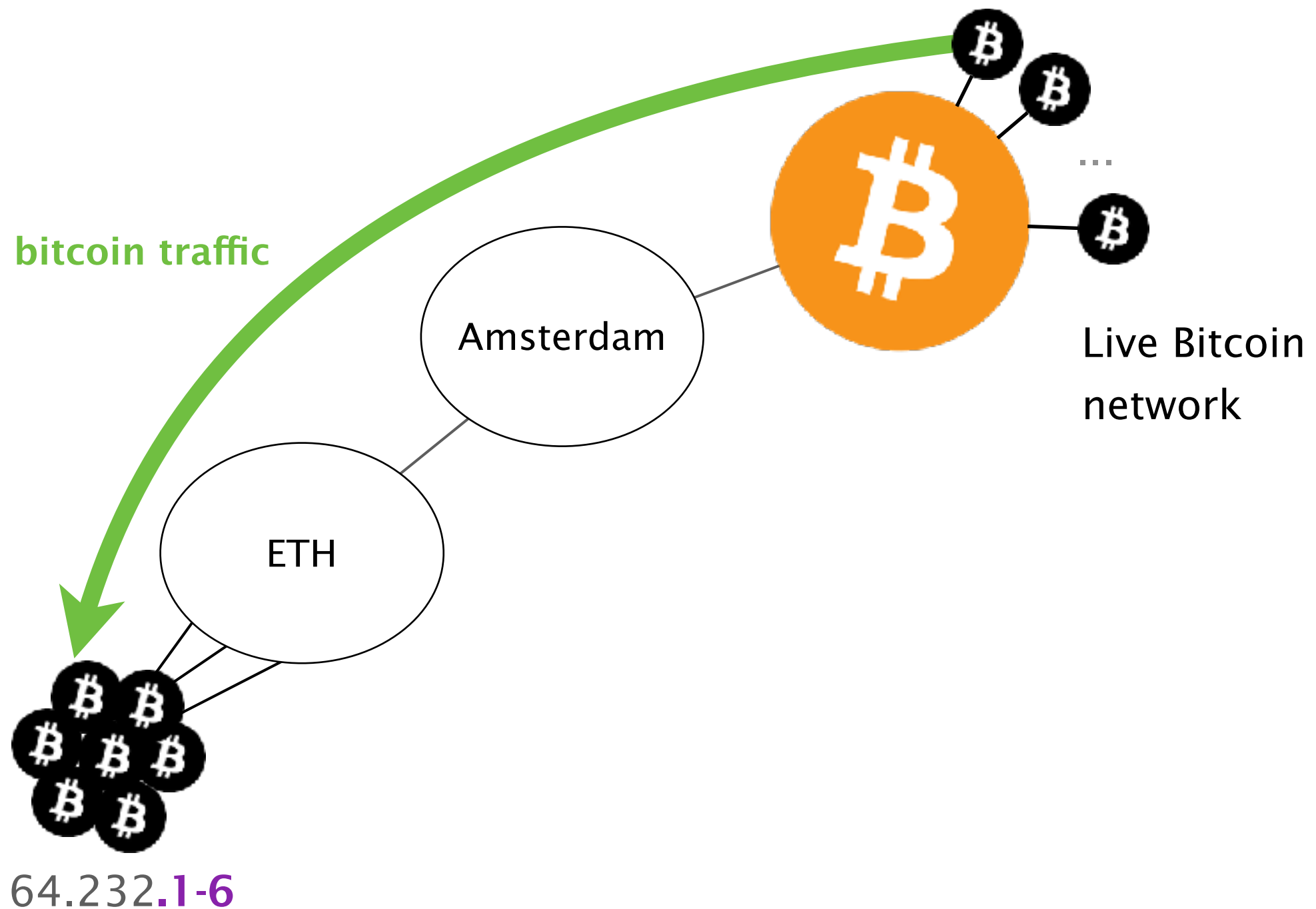
How long does it take?

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

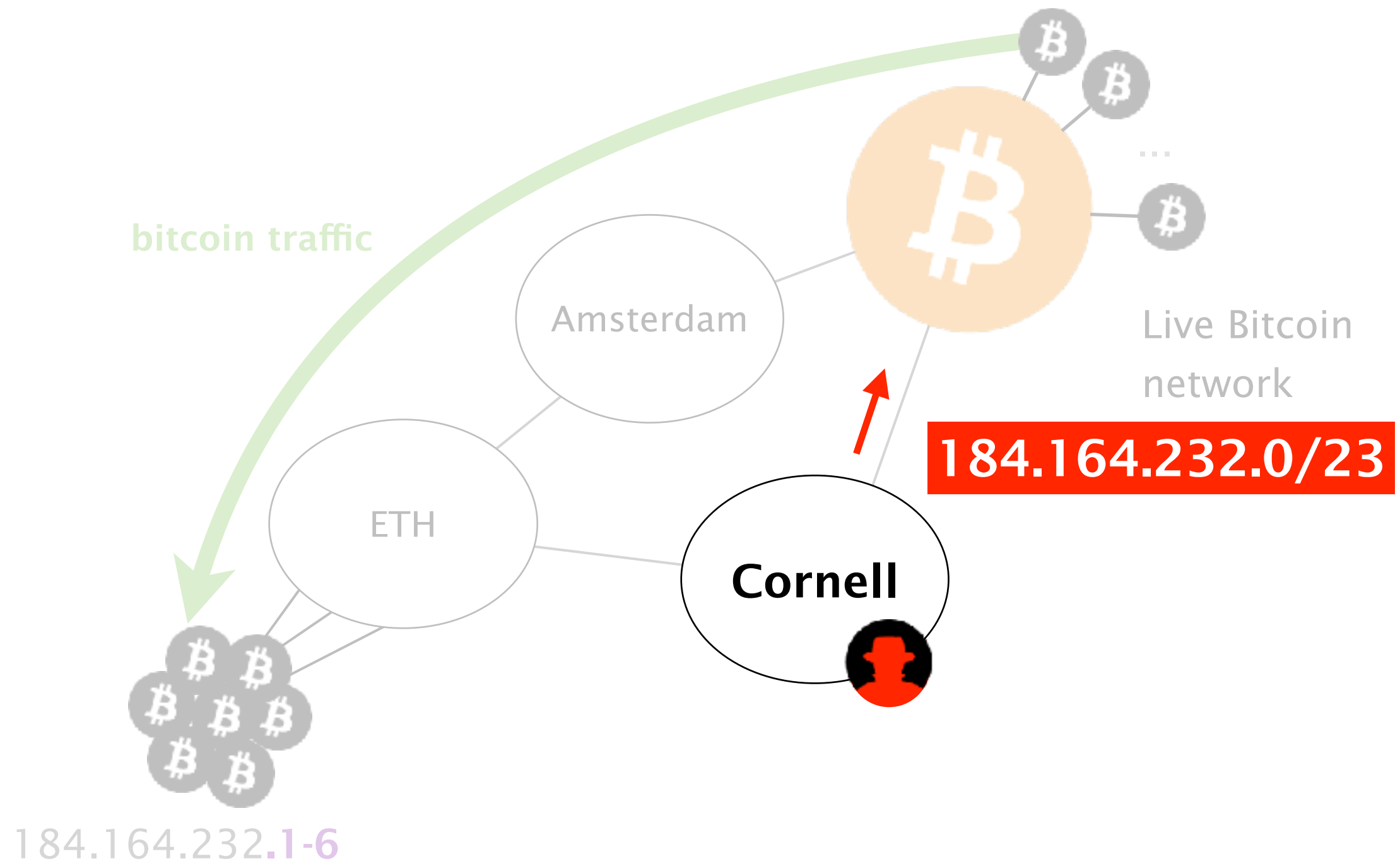
We hosted a few Bitcoin nodes at ETH and advertised a covering prefix via Amsterdam



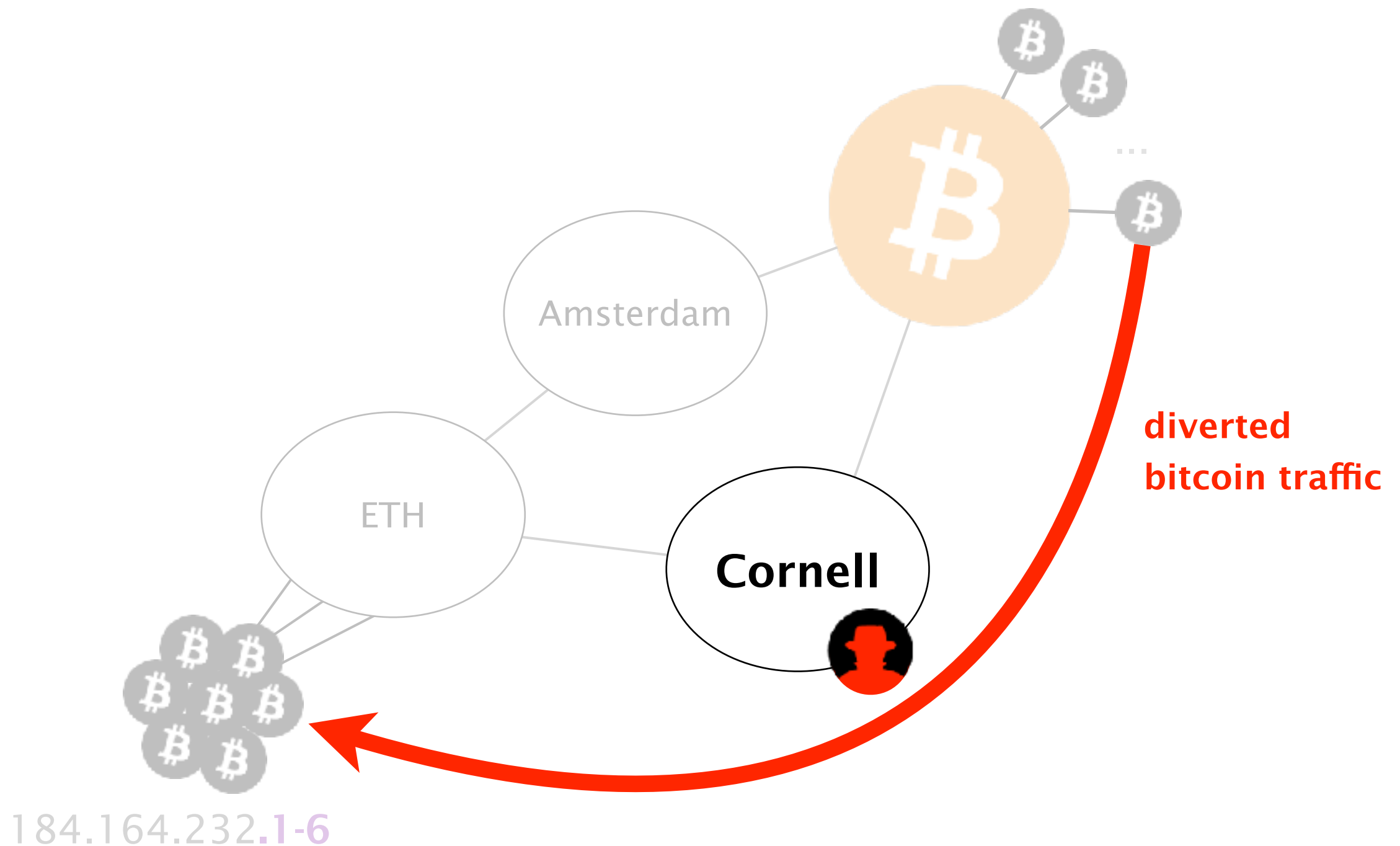
Initially, all the traffic to our nodes
transits via Amsterdam



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

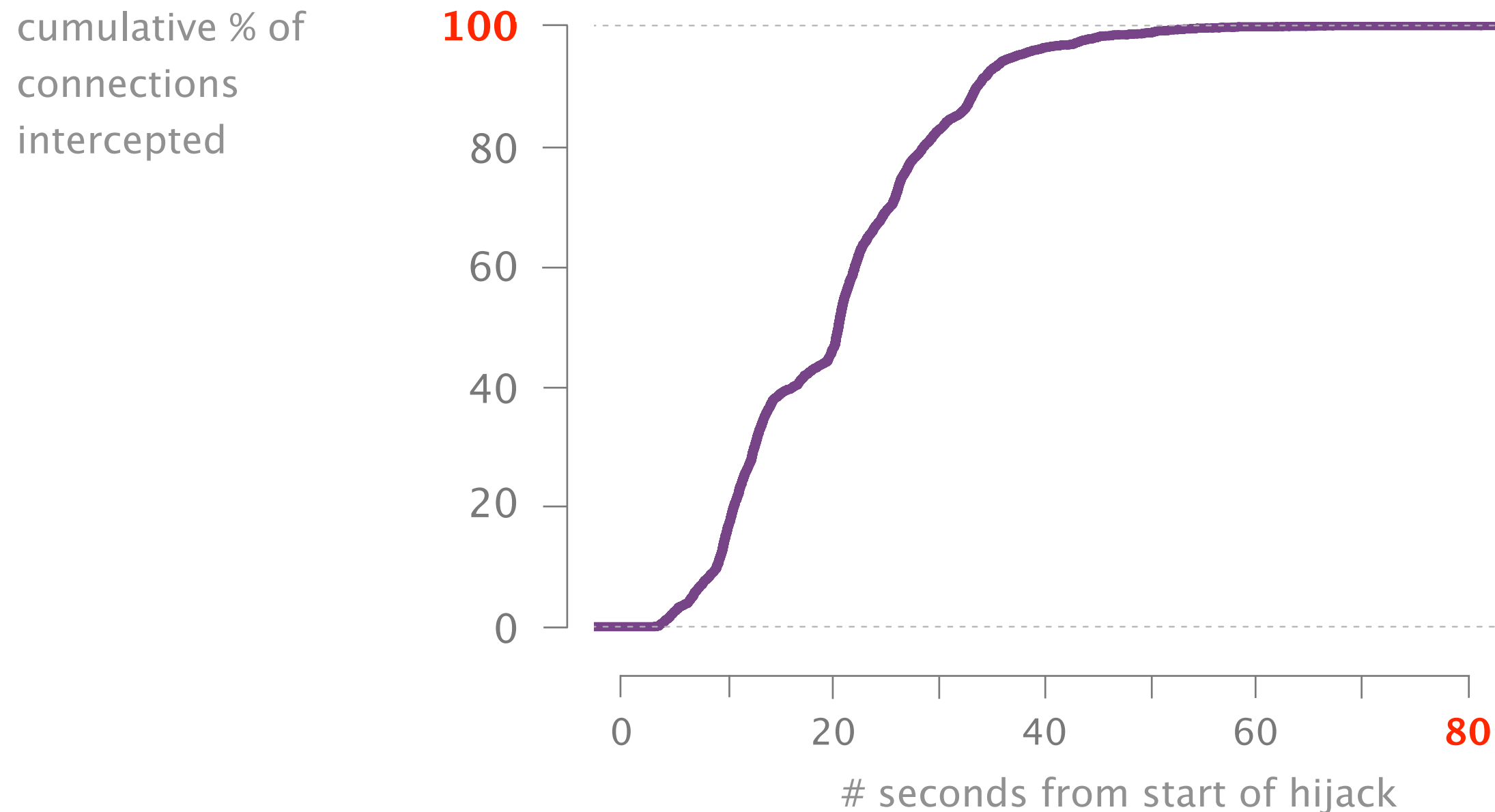
40

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



- 1 **Background**
BGP & Bitcoin
- 2 **Partitioning attack**
splitting the network
- 3 **Delay attack**
slowing the network down
- 4 **Countermeasures**
short-term & long-term

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



susceptible to be the victim
of double-spending attacks

Mining pool

Regular node

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

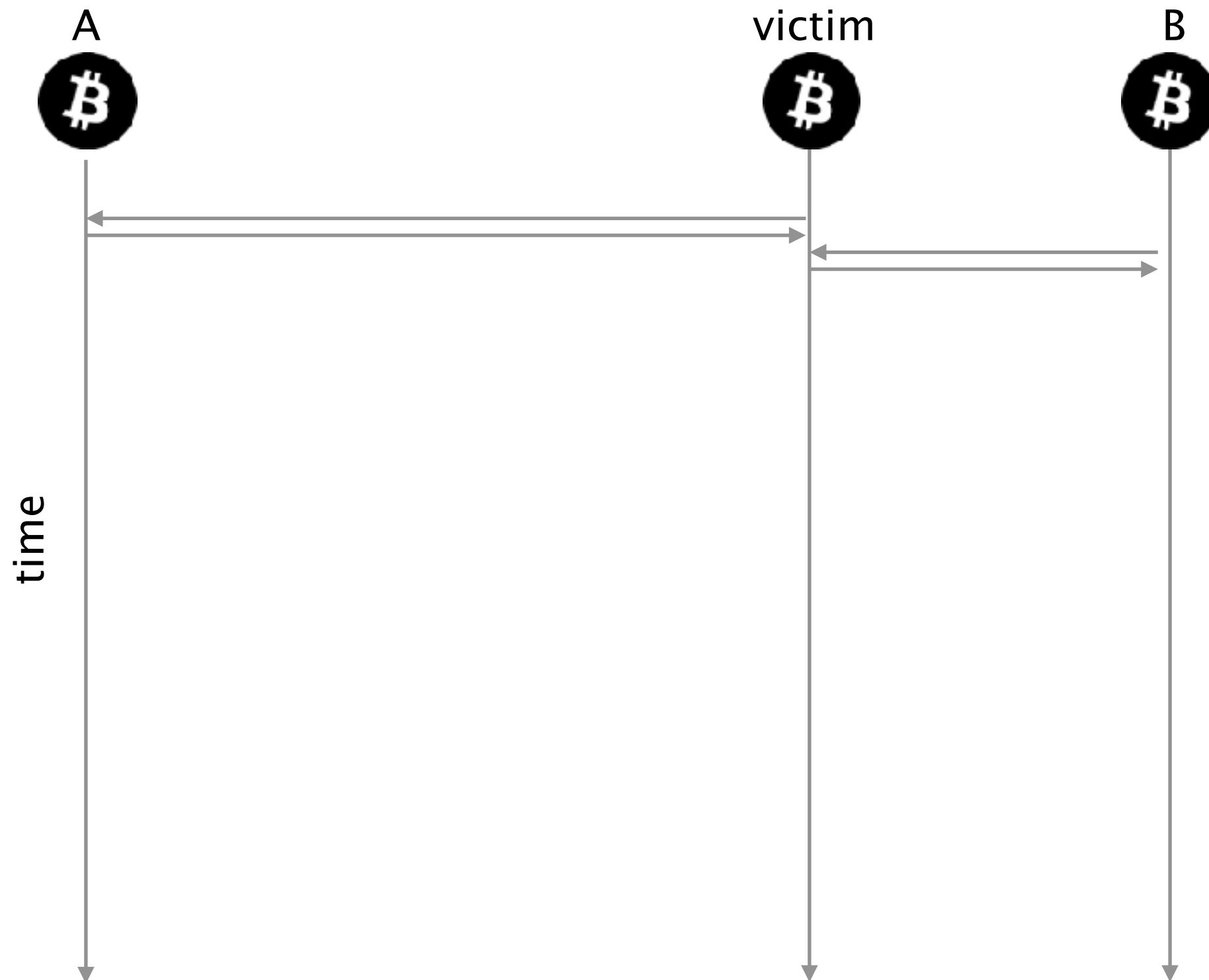
Regular node



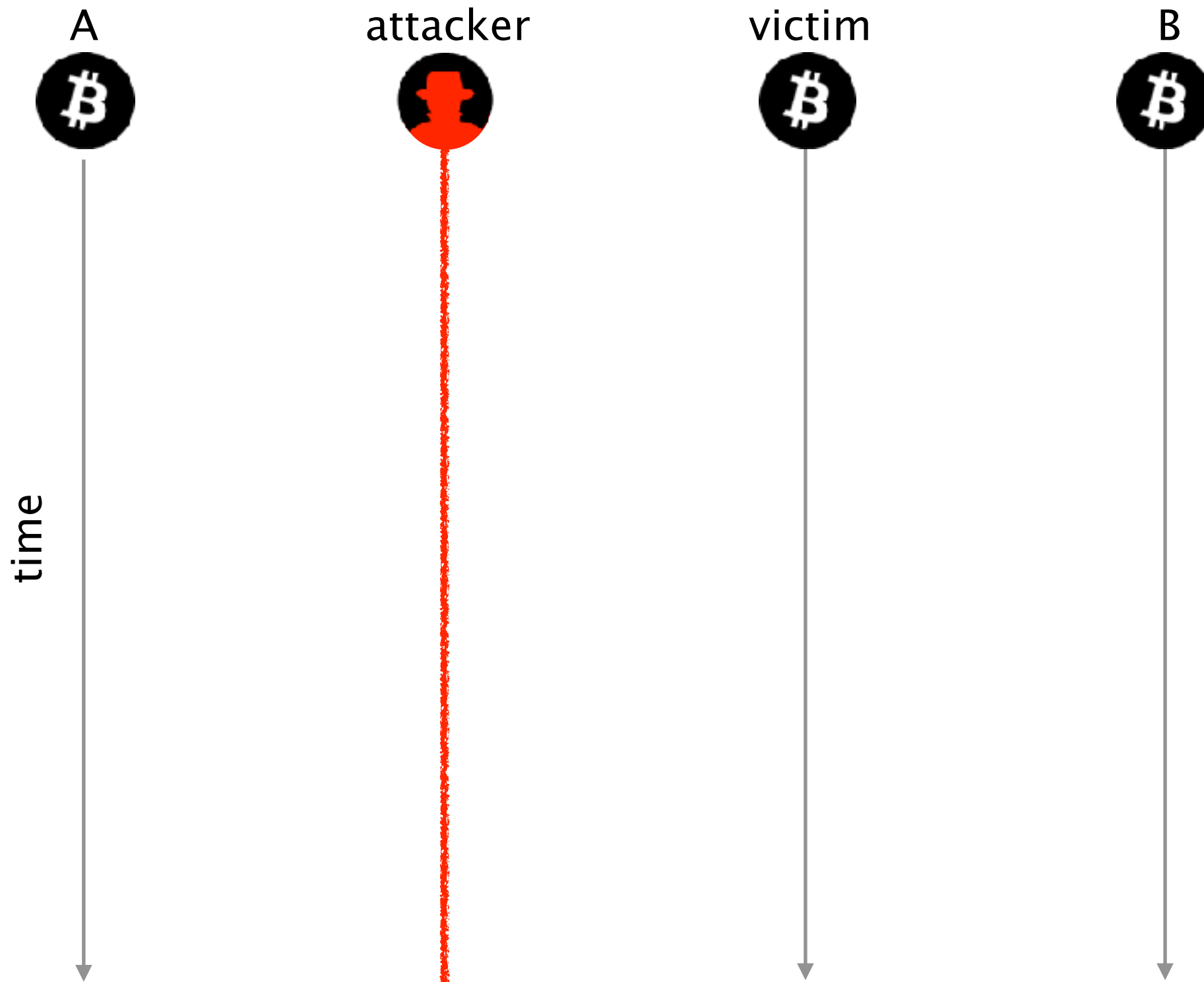
unable to collaborate to
the peer-to-peer network

How does a delay attack work?

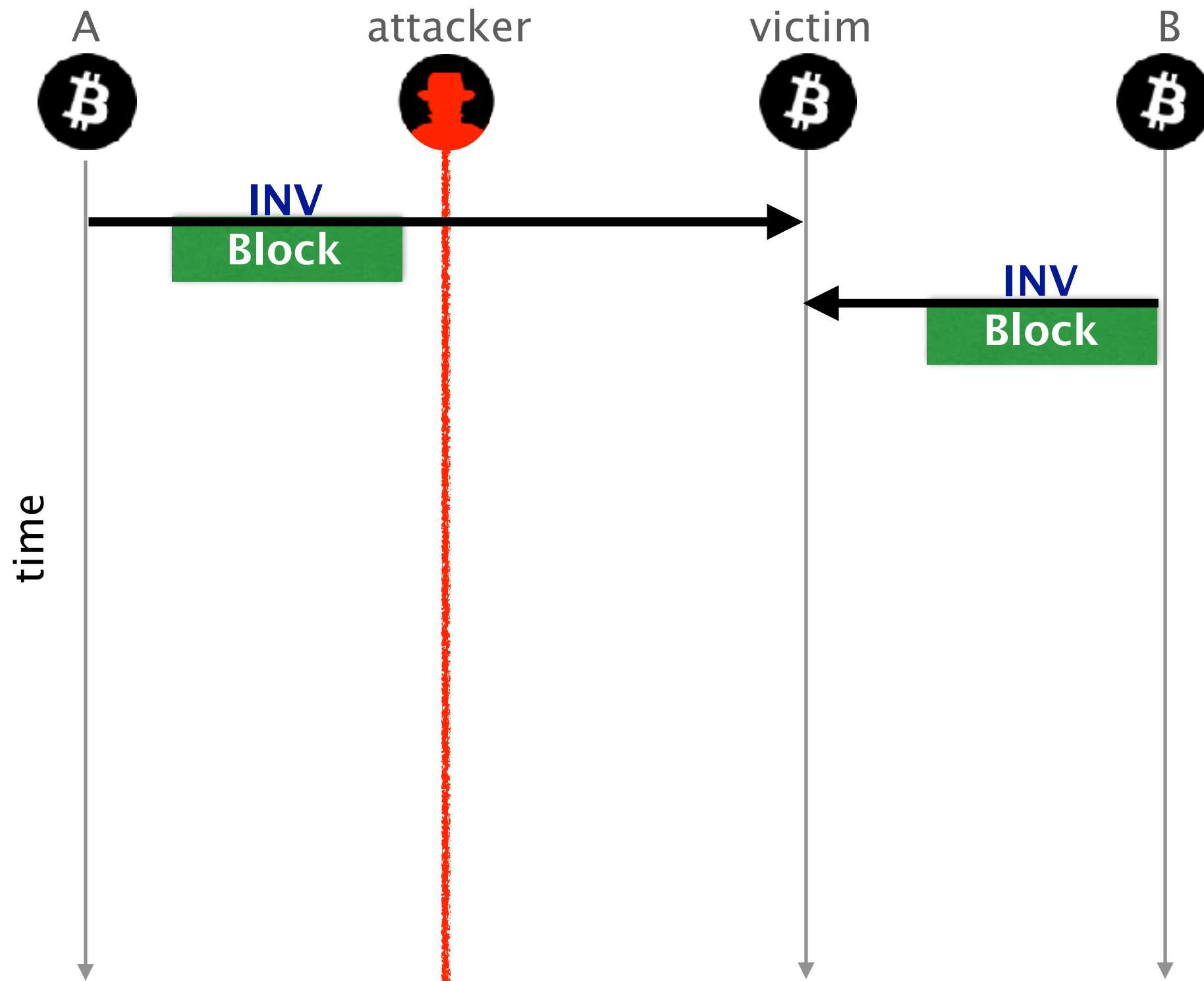
Consider these three Bitcoin nodes



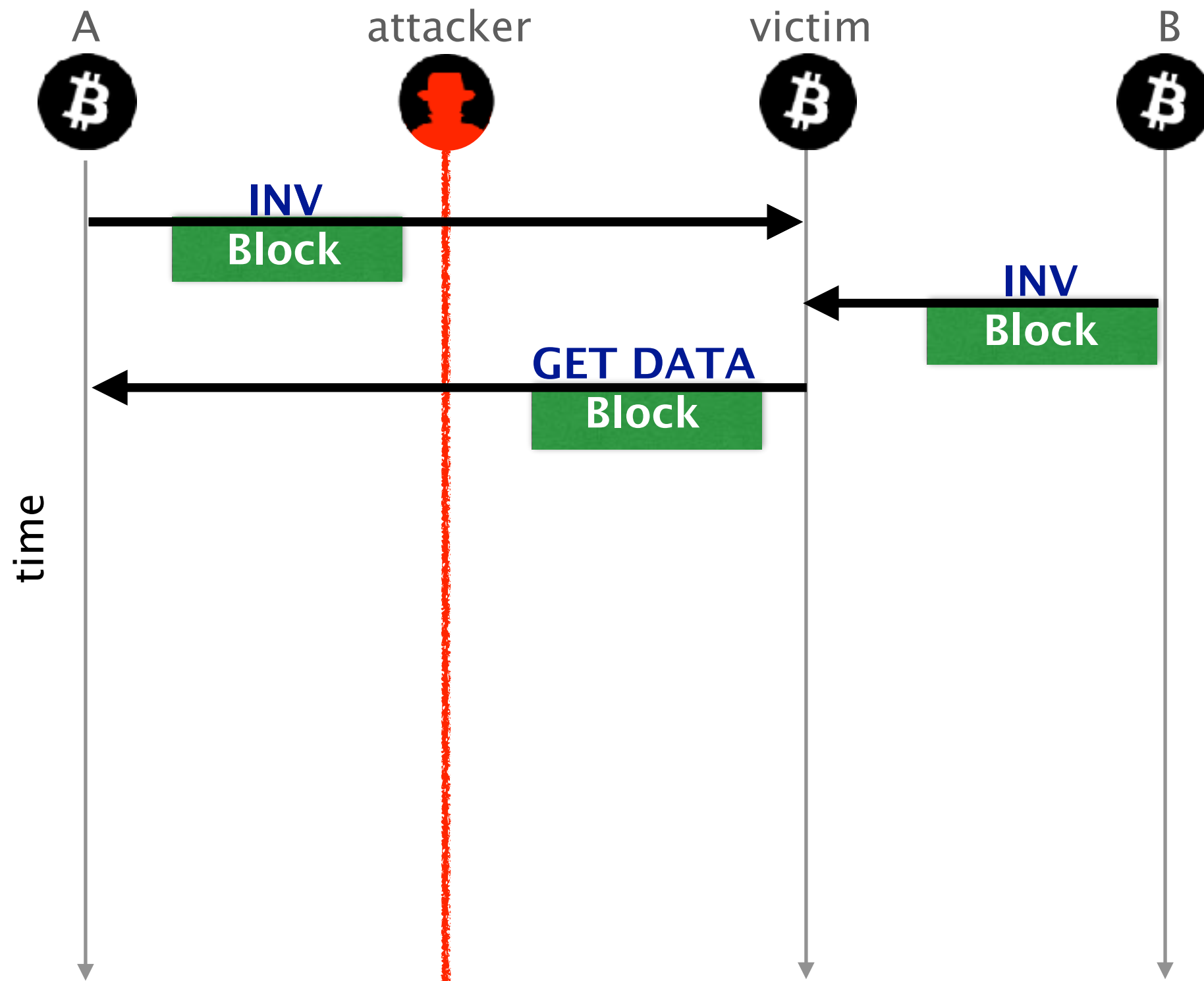
An attacker wishes to delay the block propagation towards the victim



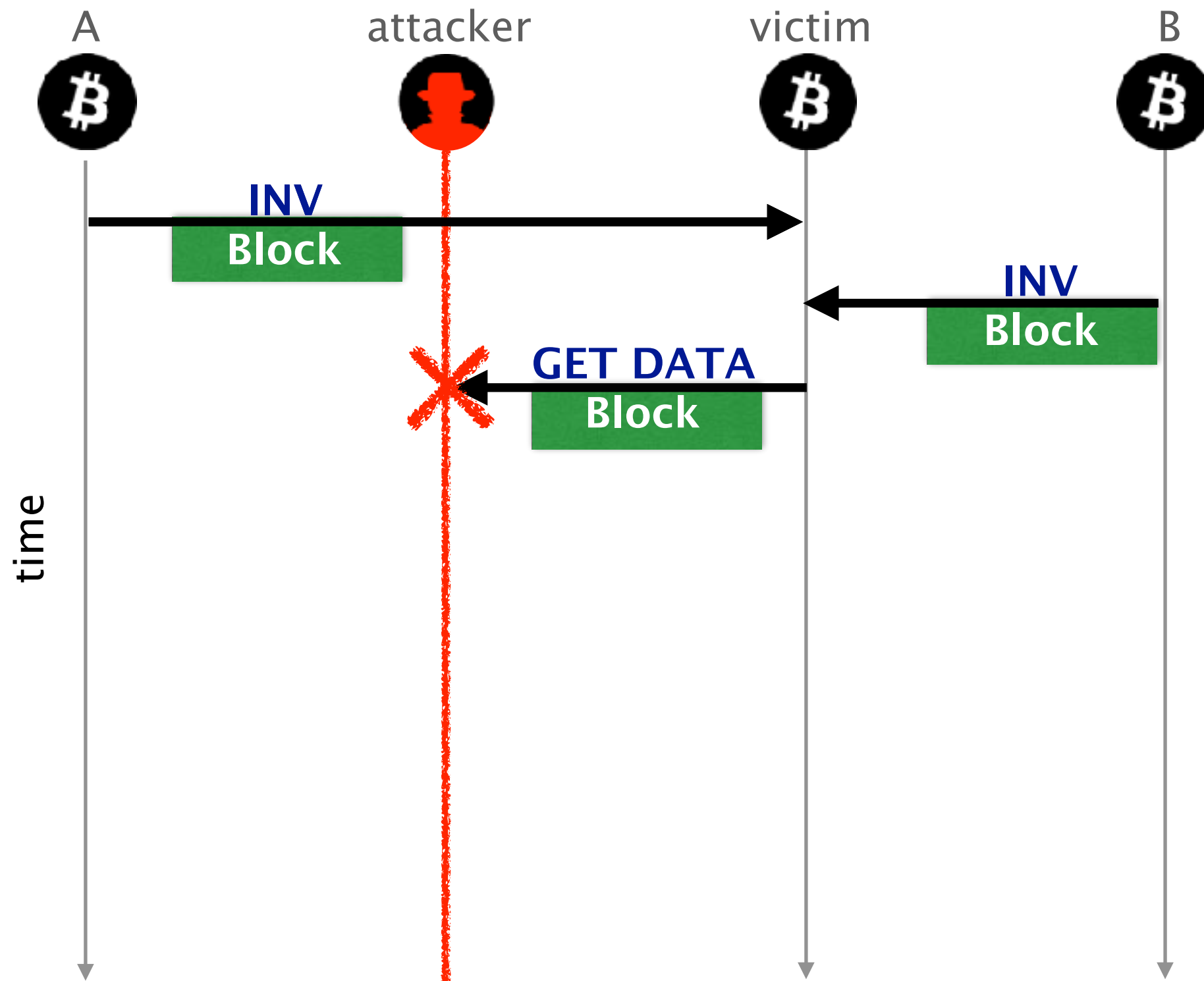
The victim receives two advertisement for the **block**



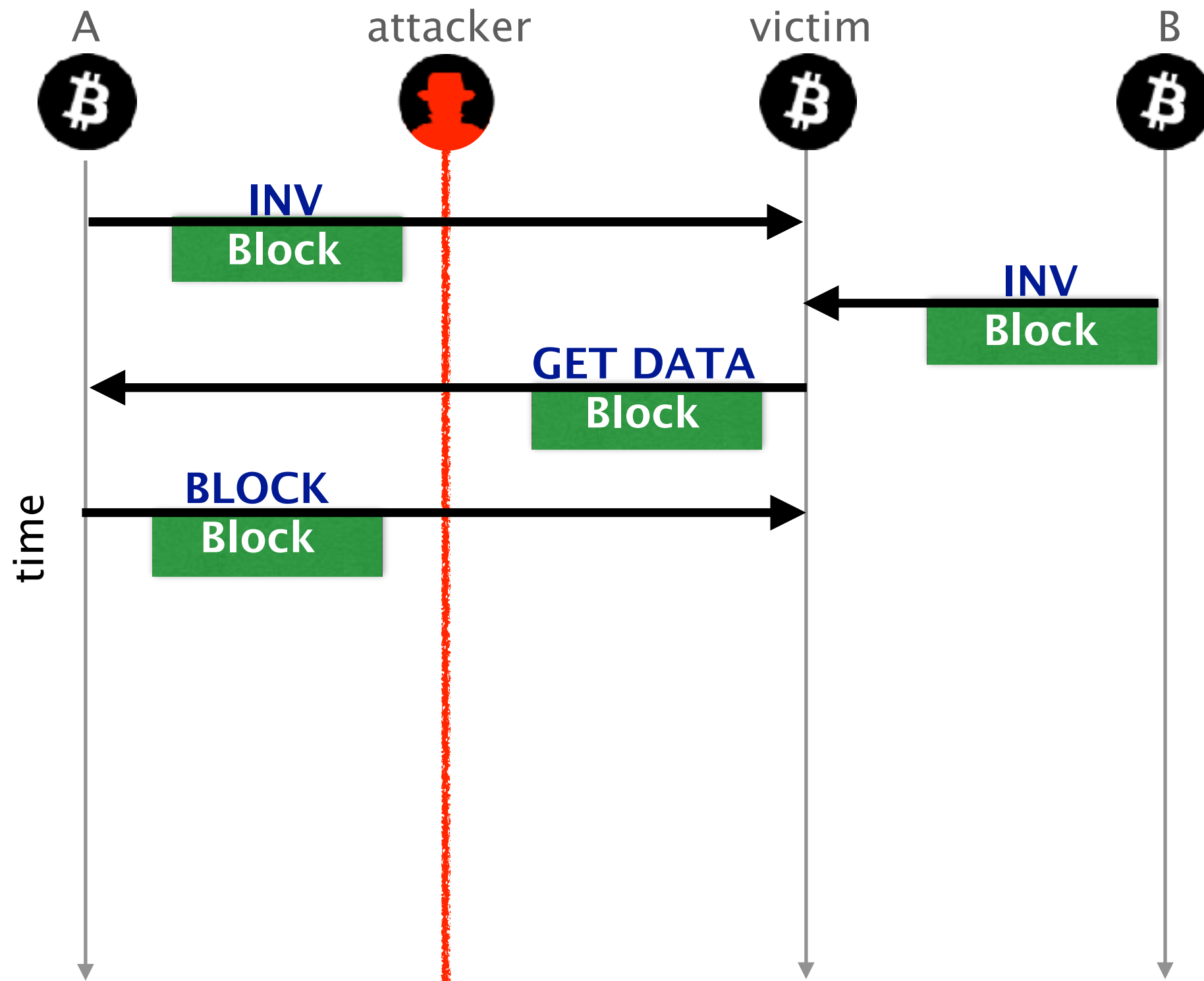
The victim requests the **block** to one of its peer, say A



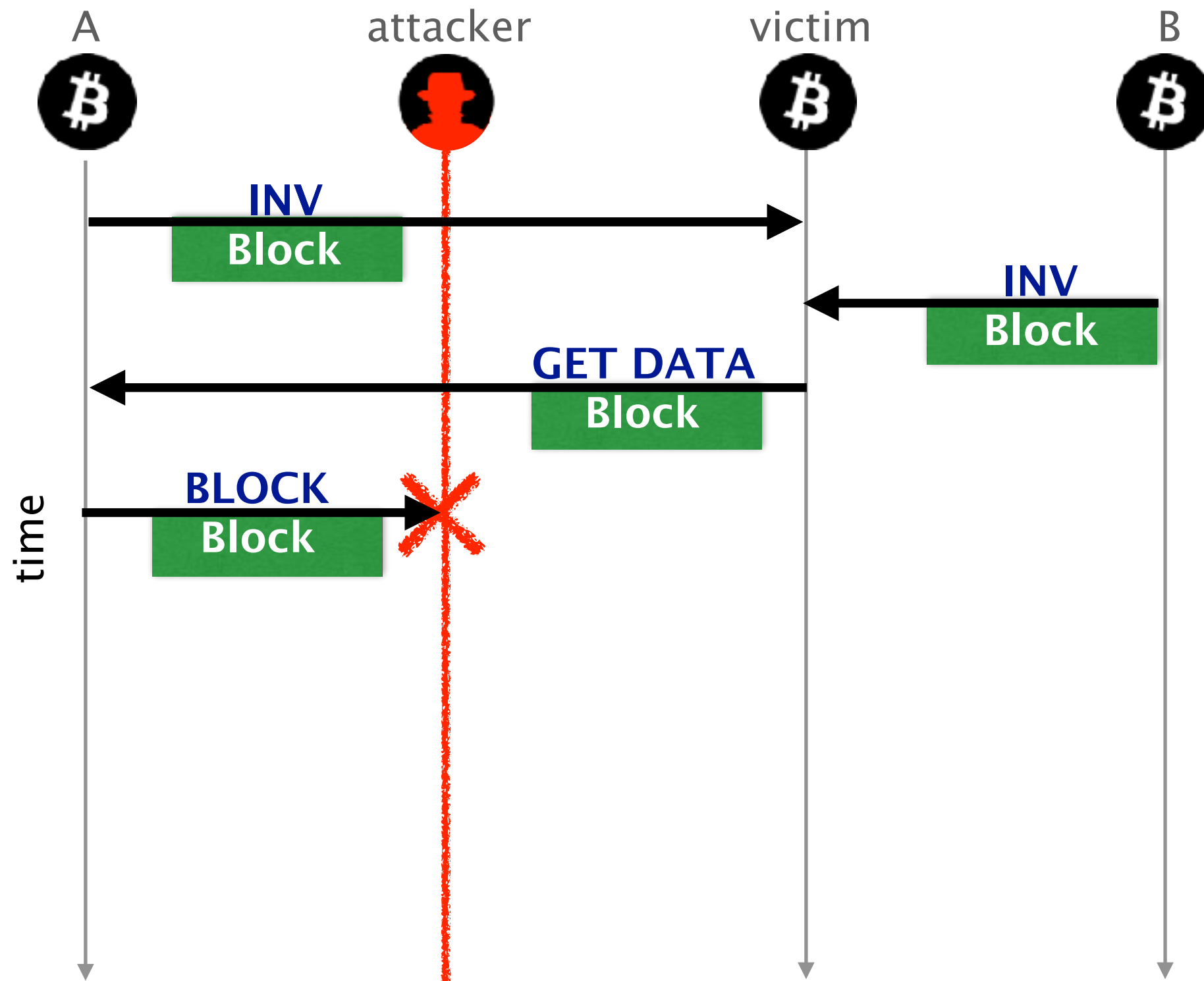
As a MITM, the attacker could drop the **GETDATA** message



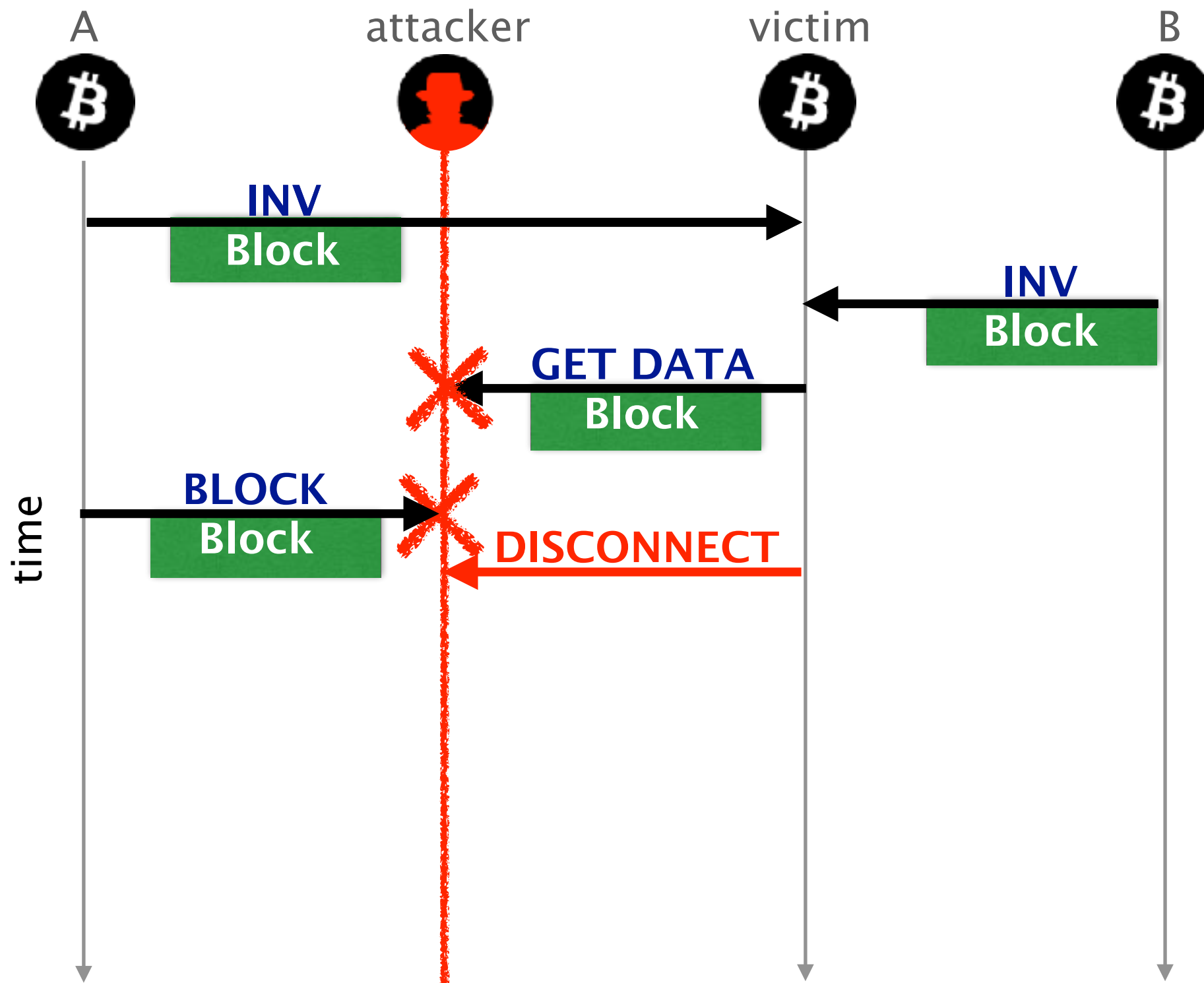
Similarly, the attacker could drop the delivery of the **block** message



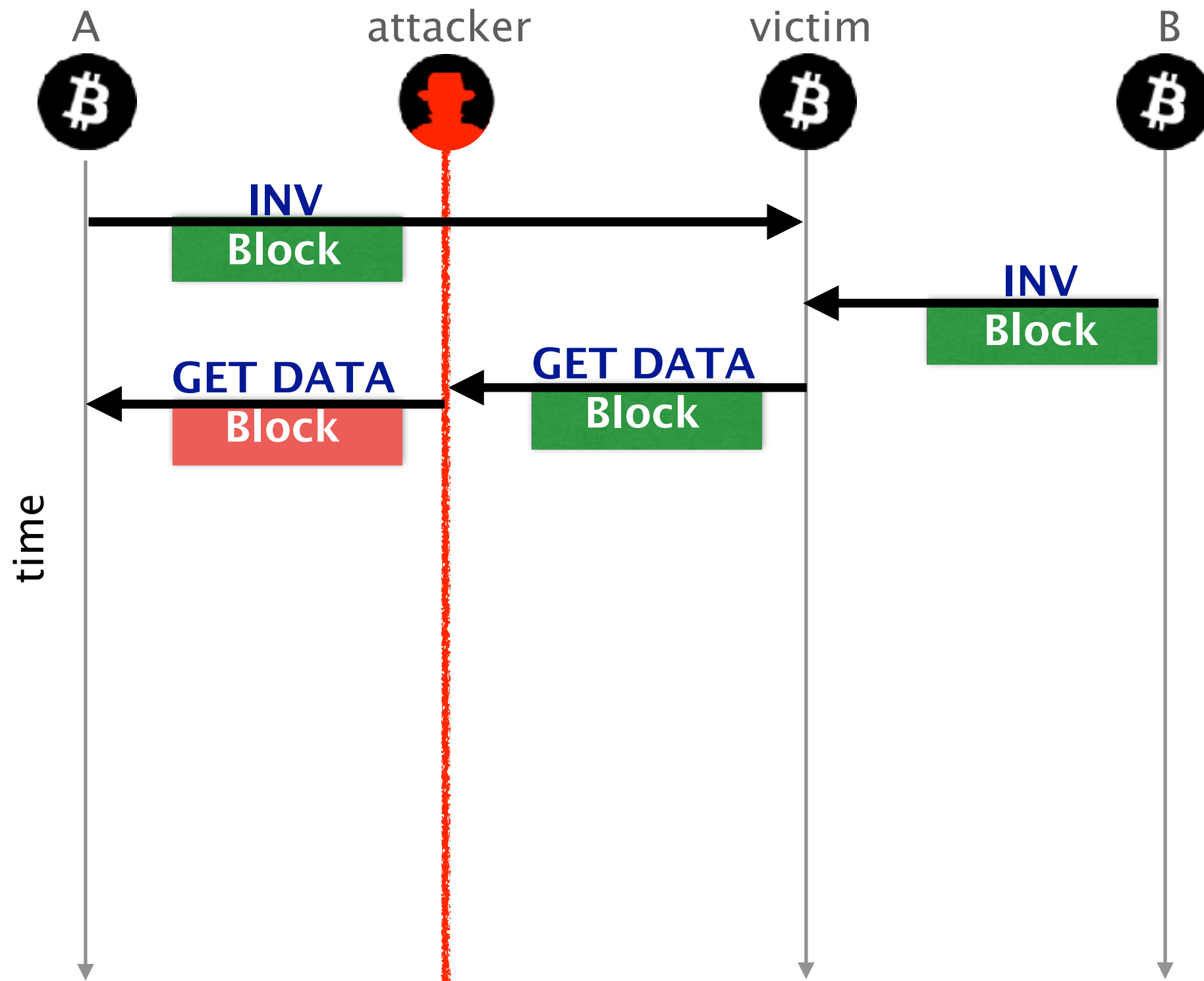
Similarly, the attacker could drop the delivery of the **block** message



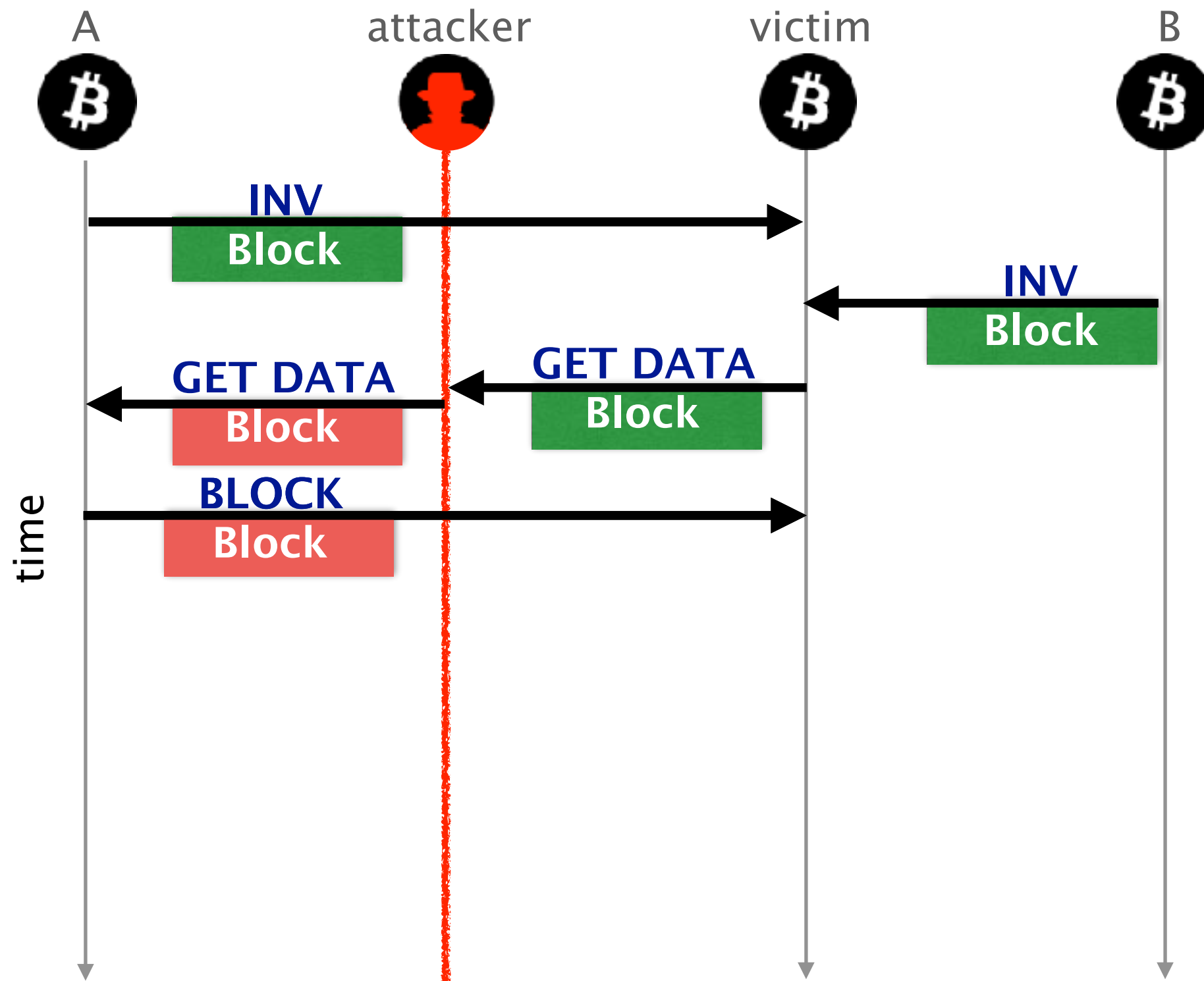
Yet, both cases will lead to the victim killing the connection (by the TCP stack on the victim)



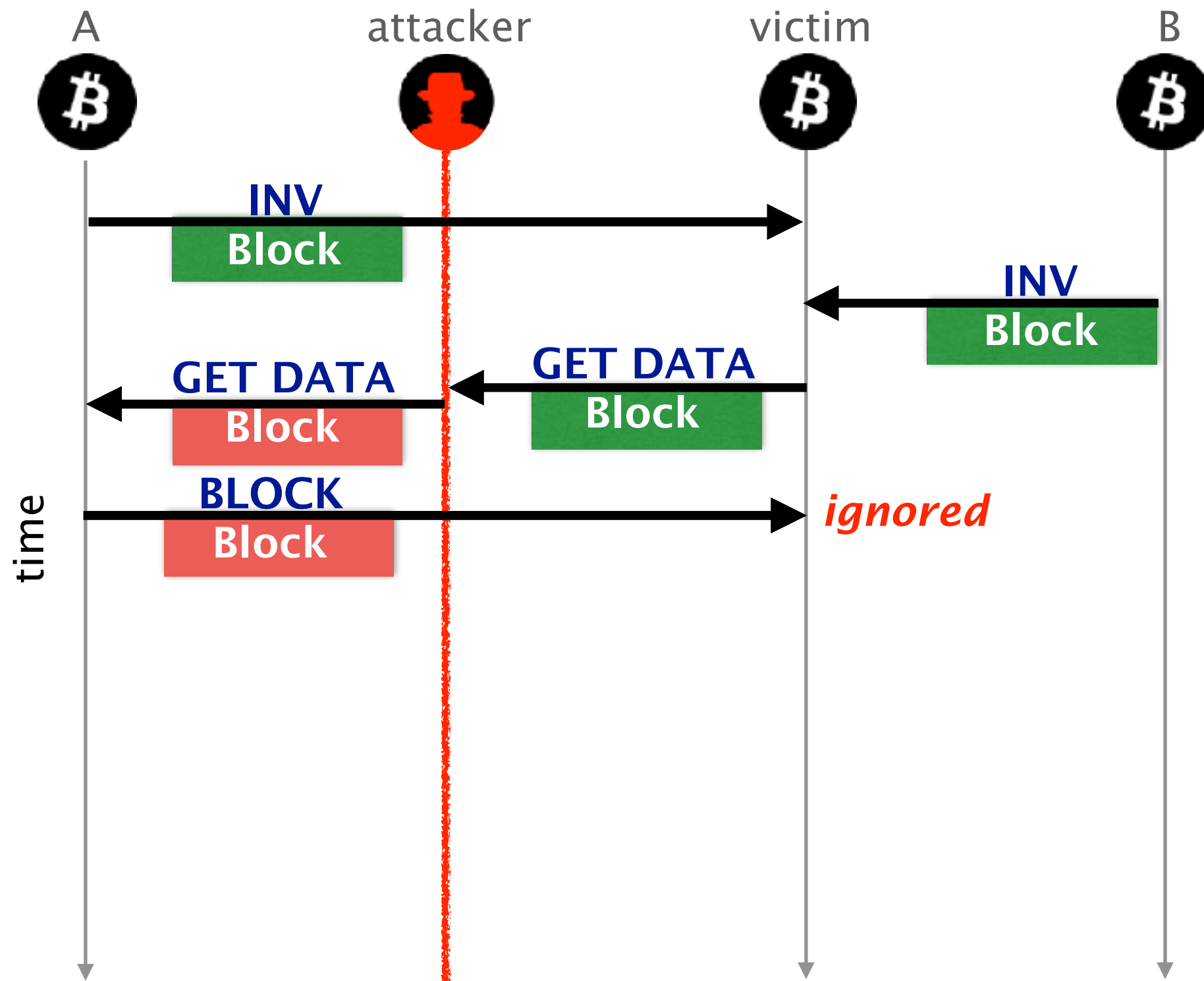
Instead, the attacker could intercept the **GETDATA** and **modifies its content**



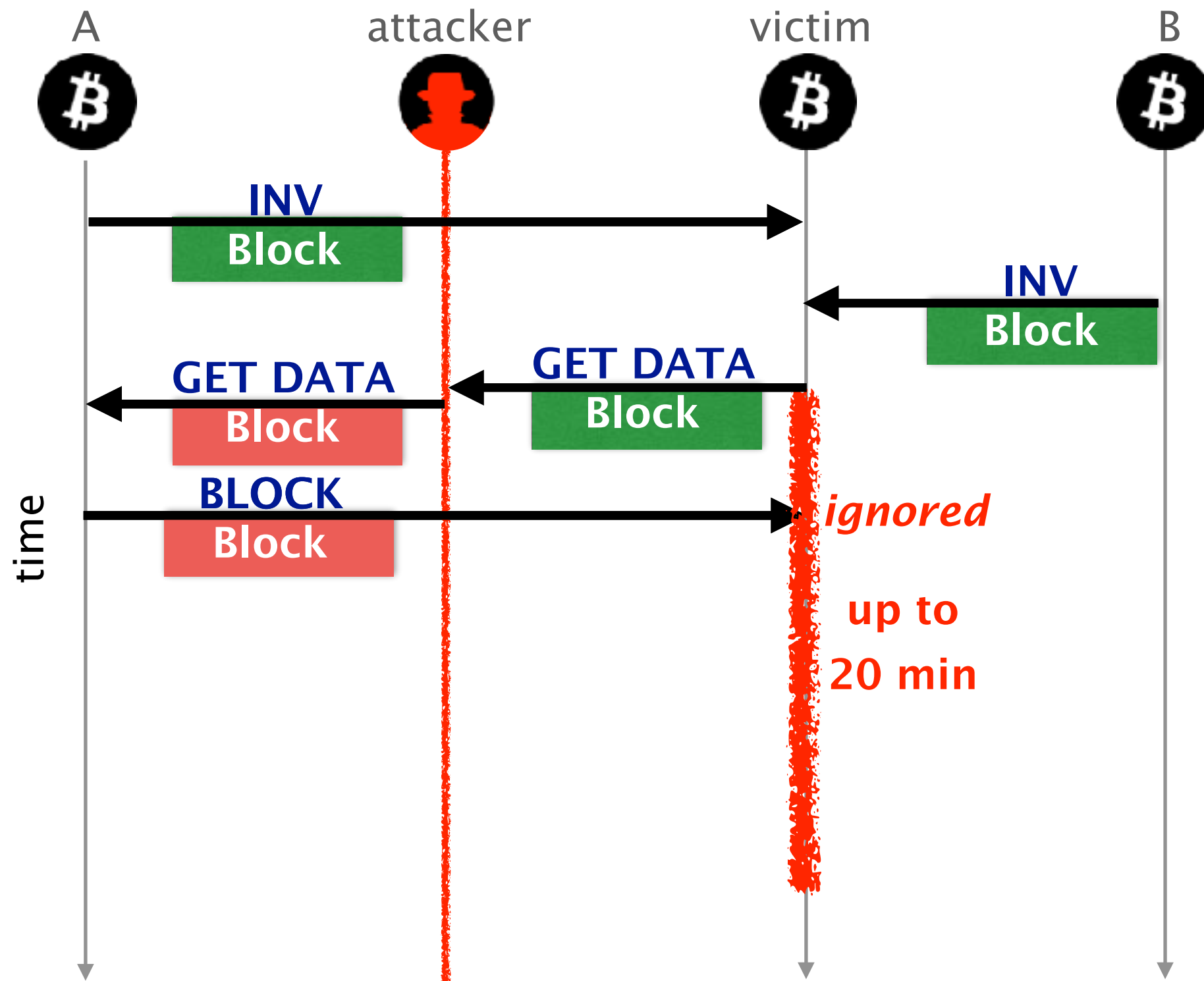
By modifying the ID of the requested block,
the attacker triggers the delivery of an older **block**



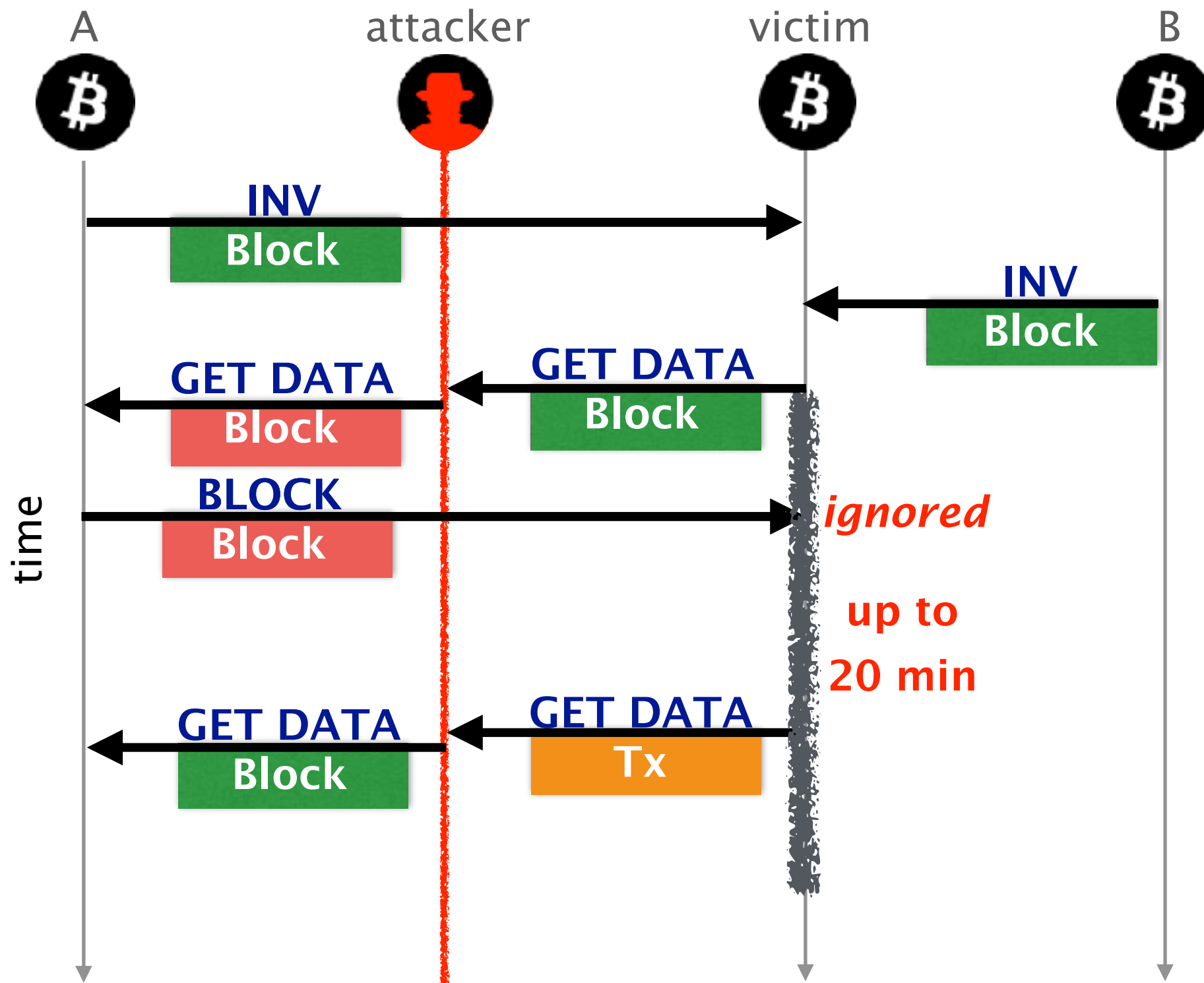
The delivery of an older block triggers
no error message at the victim



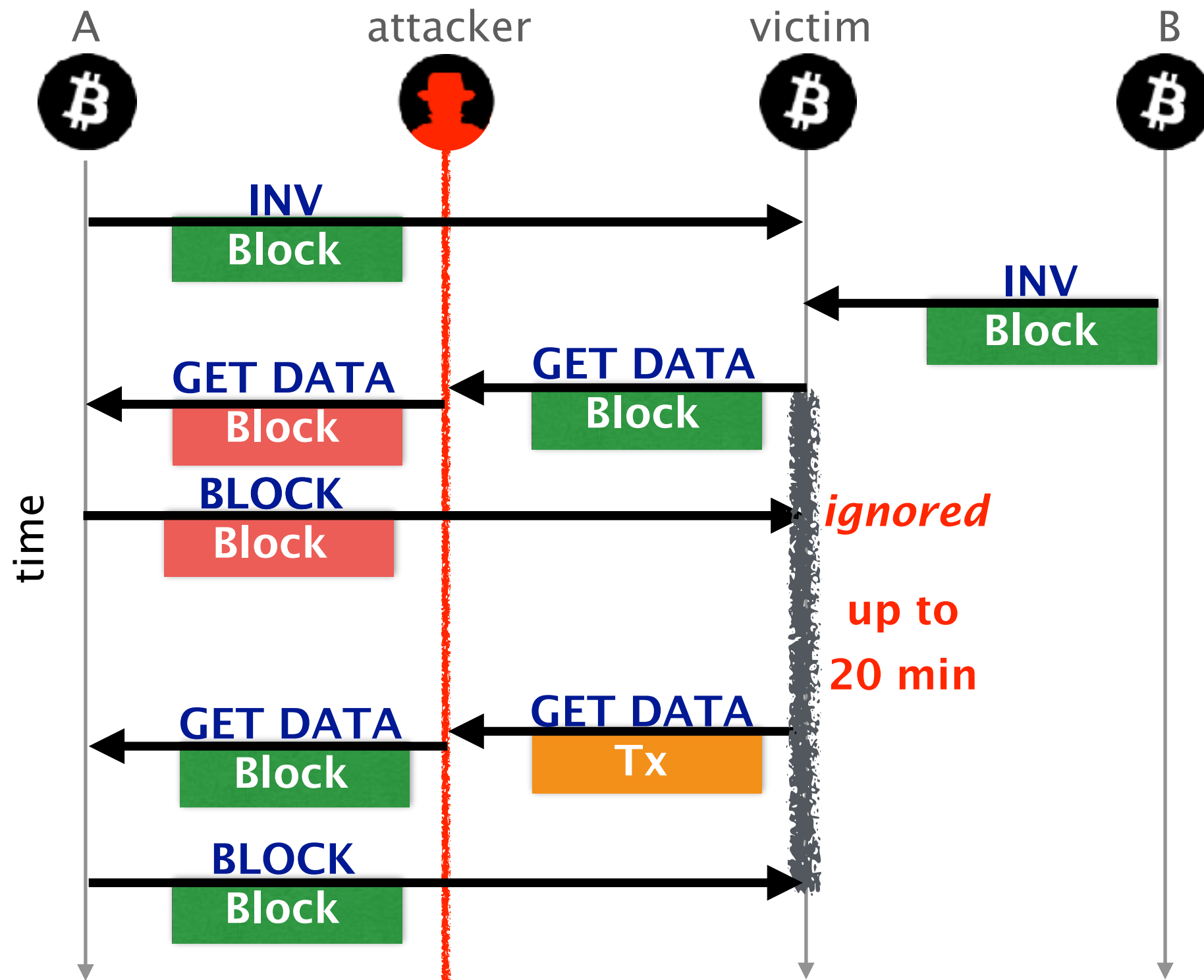
From there on, the victim will wait **for 20 minutes** for the actual block to be delivered



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

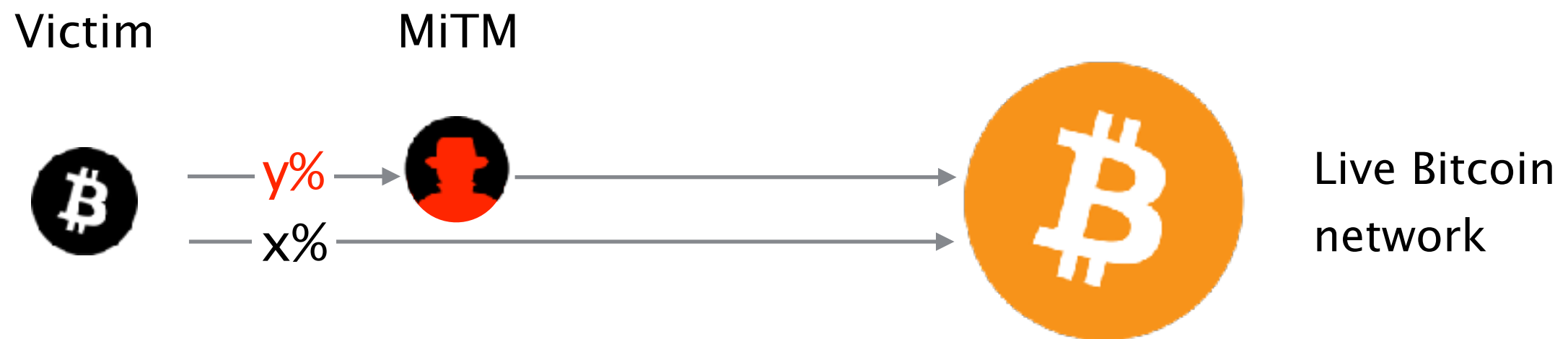
How much time does
the victim stay uniformed?



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



- 1 **Background**
BGP & Bitcoin
- 2 **Partitioning attack**
splitting the network
- 3 **Delay attack**
slowing the network down
- 4 **Countermeasures**
short-term & long-term

Both short-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]