Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

Maria Apostolaki

ETH Zürich

IEEE Security & Privacy

23 May 2017

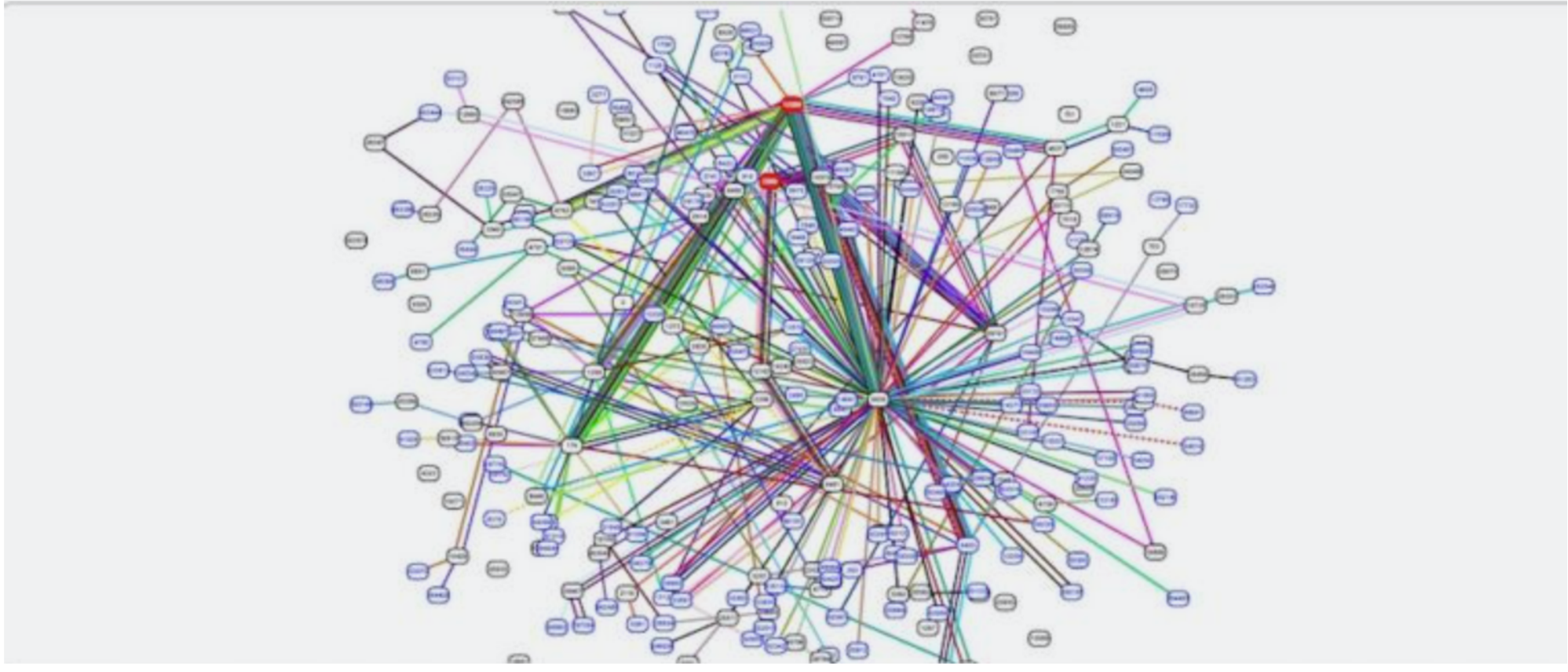
Joint work with Aviv Zohar and Laurent Vanbever

Routing attacks quite often make the news

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

THREAT LEVEL

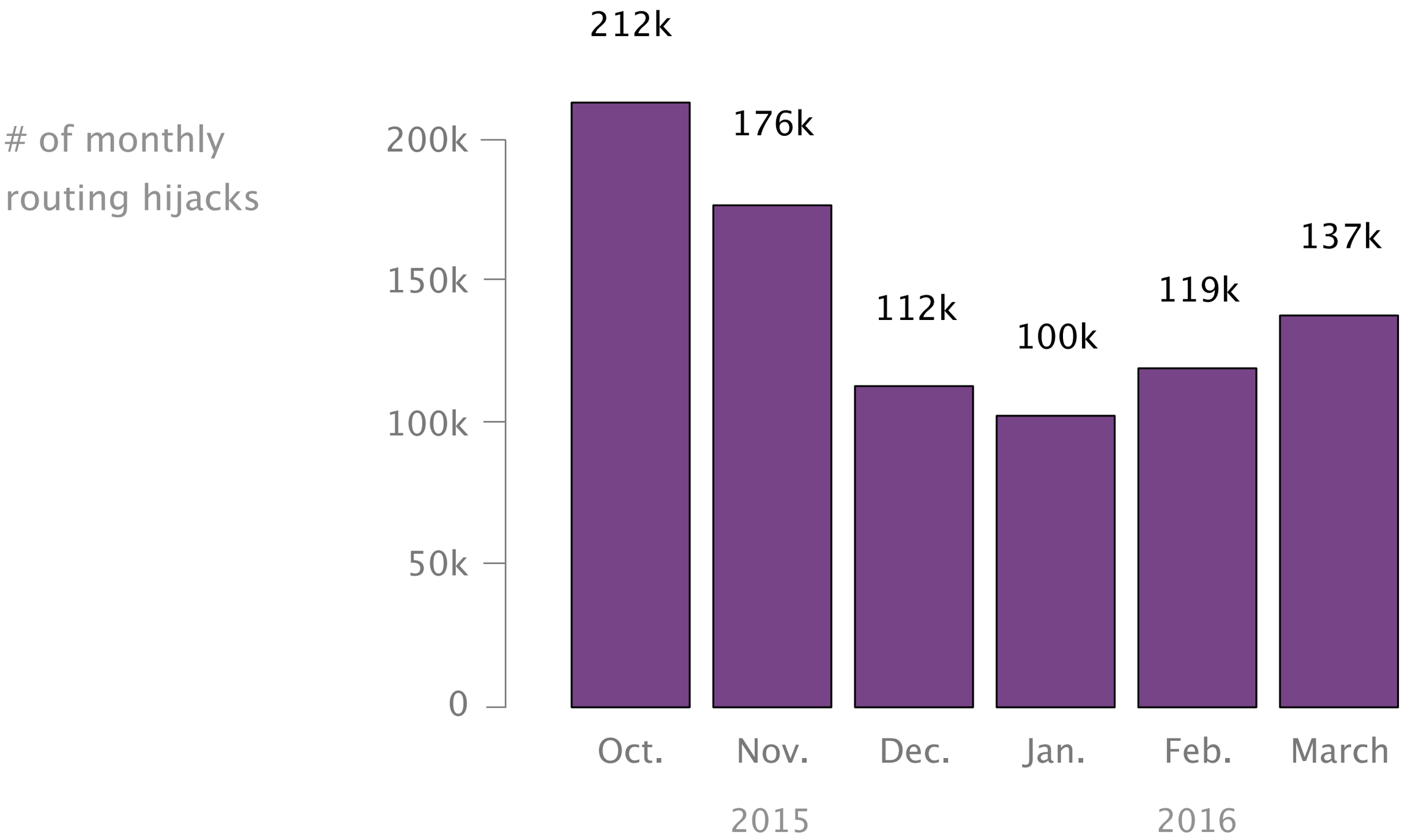
Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

BY ANDY GREENBERG 08.07.14 | 1:00 PM | PERMALINK

source: wired.com

That is only the tip of the iceberg of routing manipulations

# 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

Can routing attacks impact Bitcoin?

Bitcoin is highly decentralized

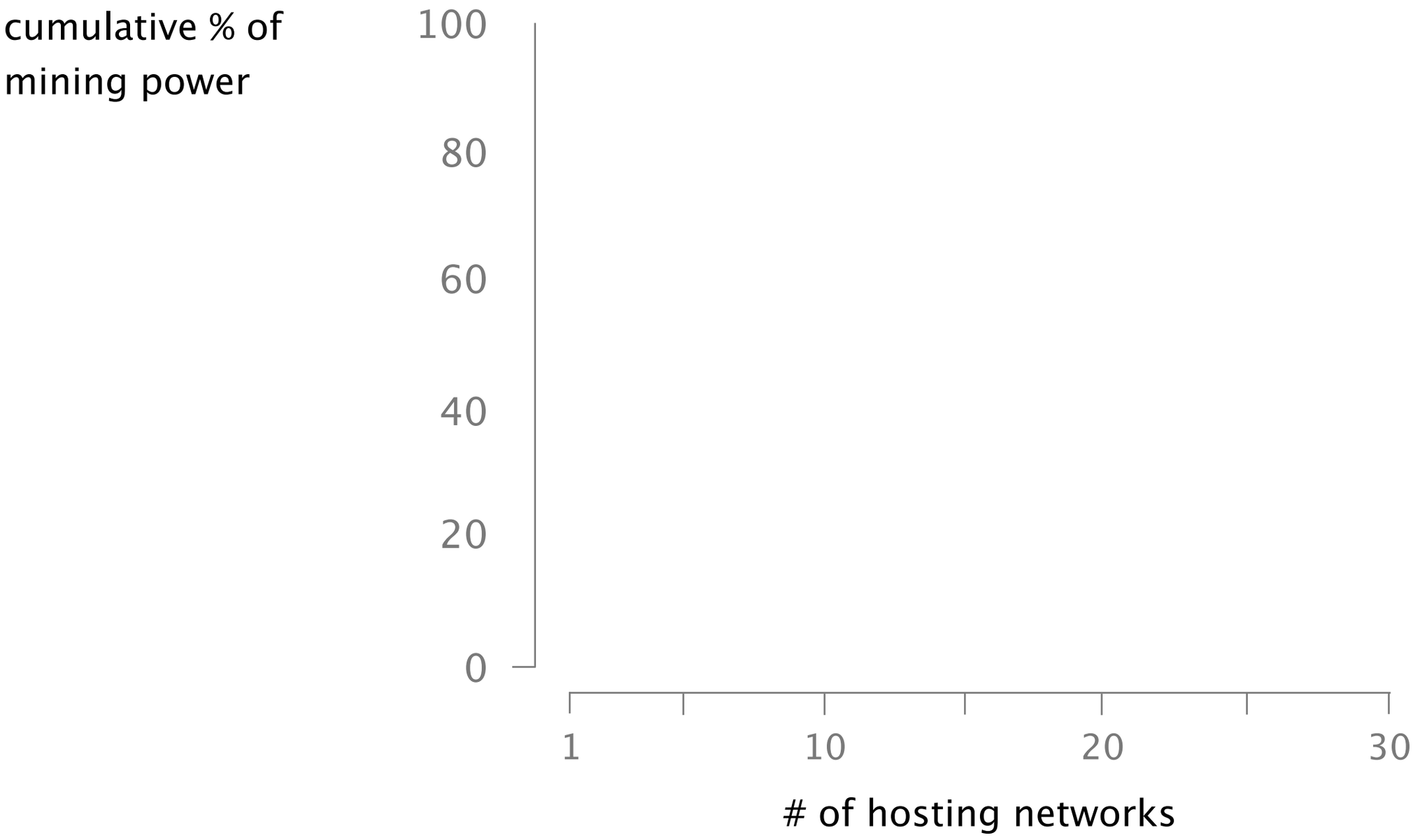
making it robust to routing attacks, in theory…

Bitcoin nodes …

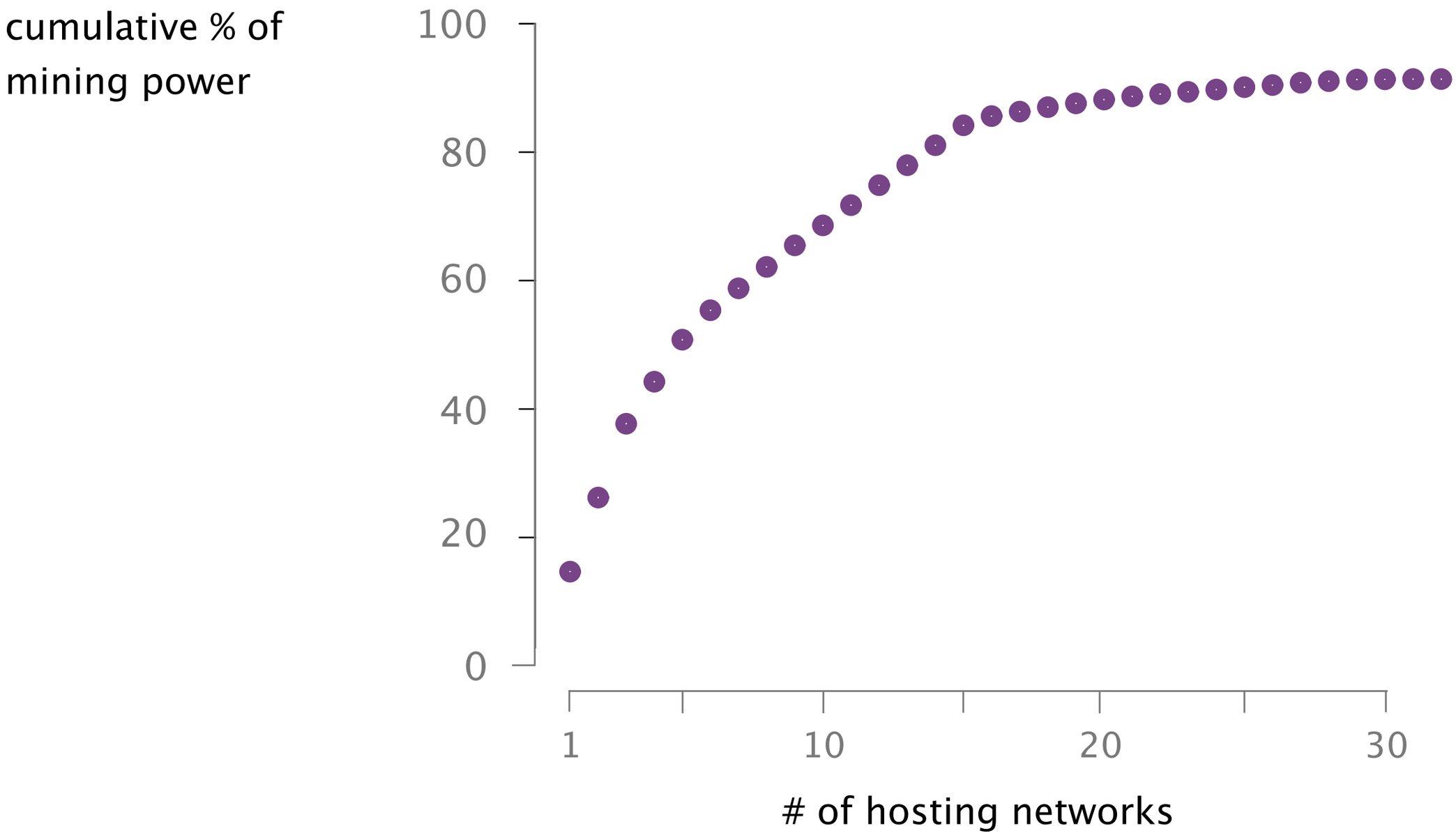
- are scattered all around the globe
- establish random connections
- use multihoming and extra relay networks

In practice, Bitcoin is highly centralized,

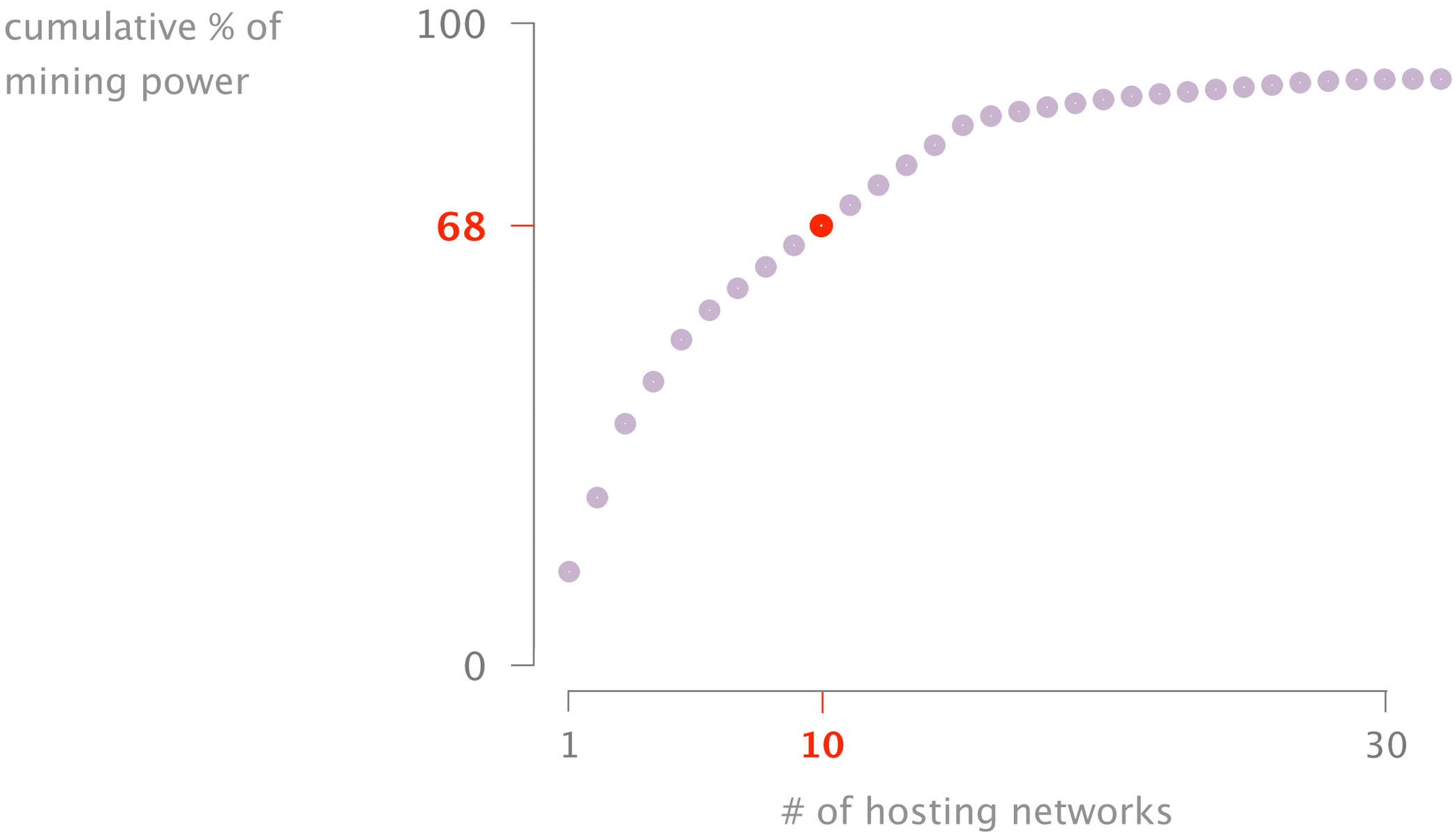
both from a routing and mining viewpoint

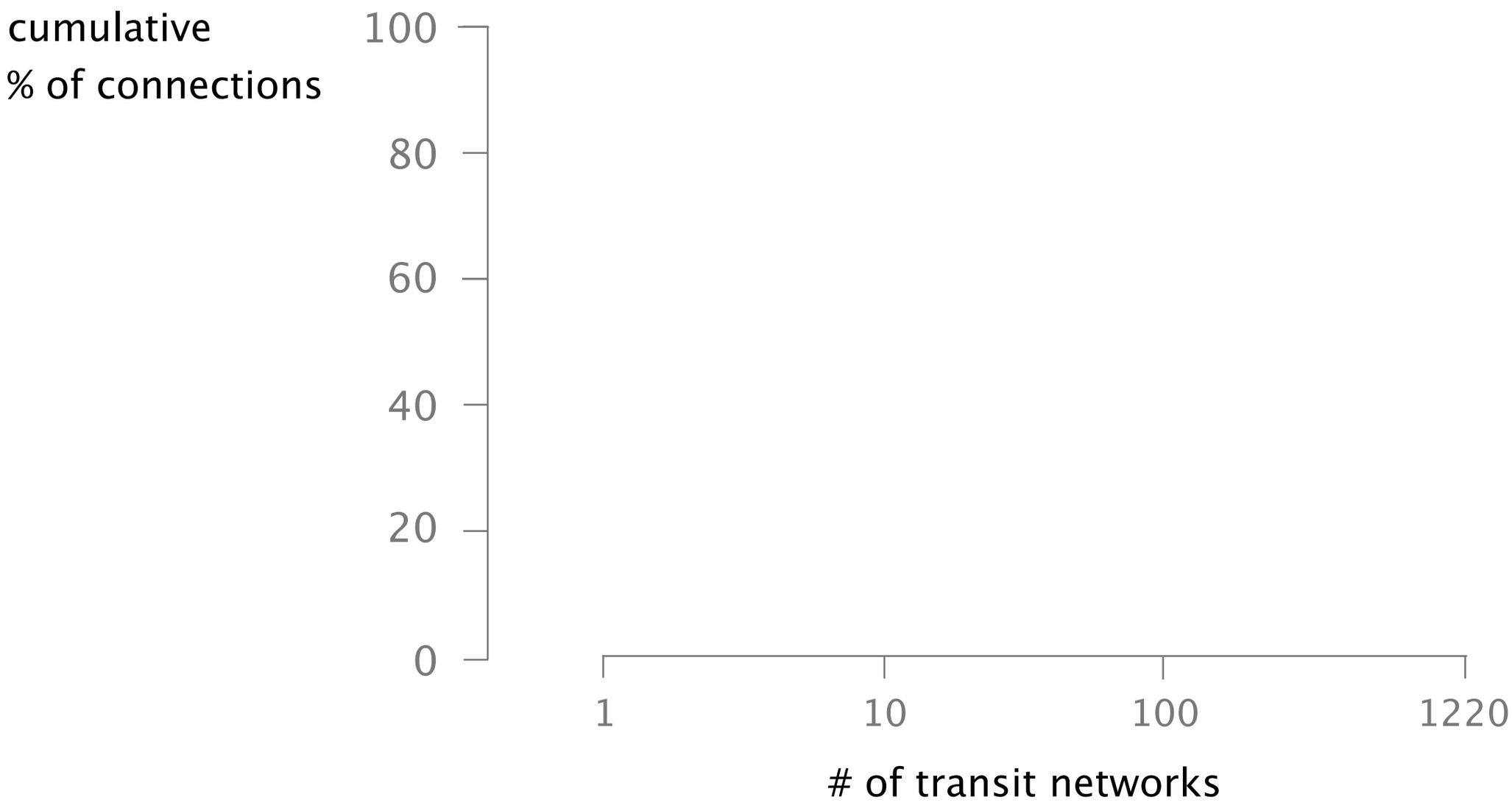

cumulative % of mining power
100
80
60
40
20
0
1
10
20
30
# of hosting networks

Mining power is centralized to few hosting networks

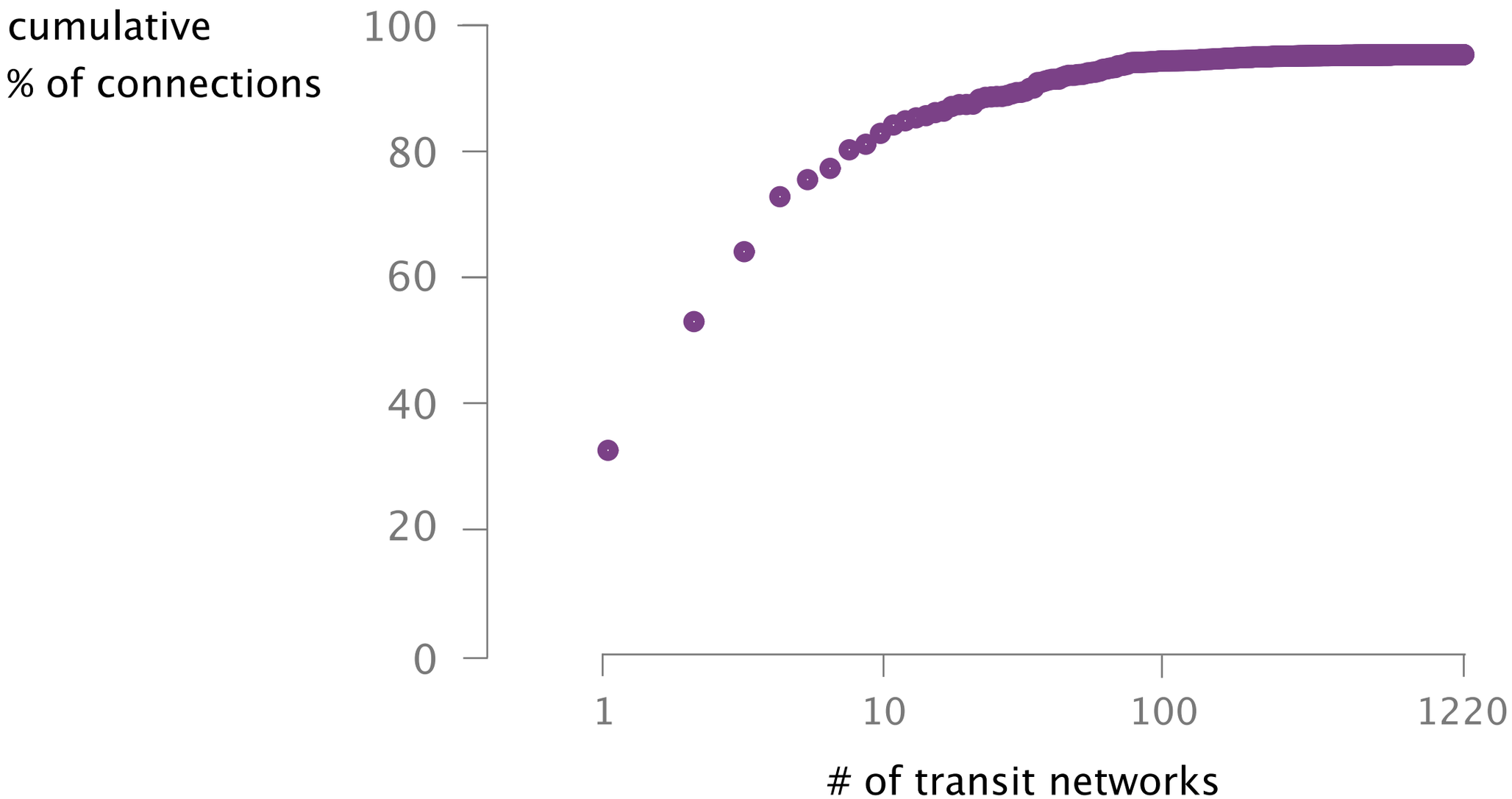


68% of the mining power is hosted in 10 networks only

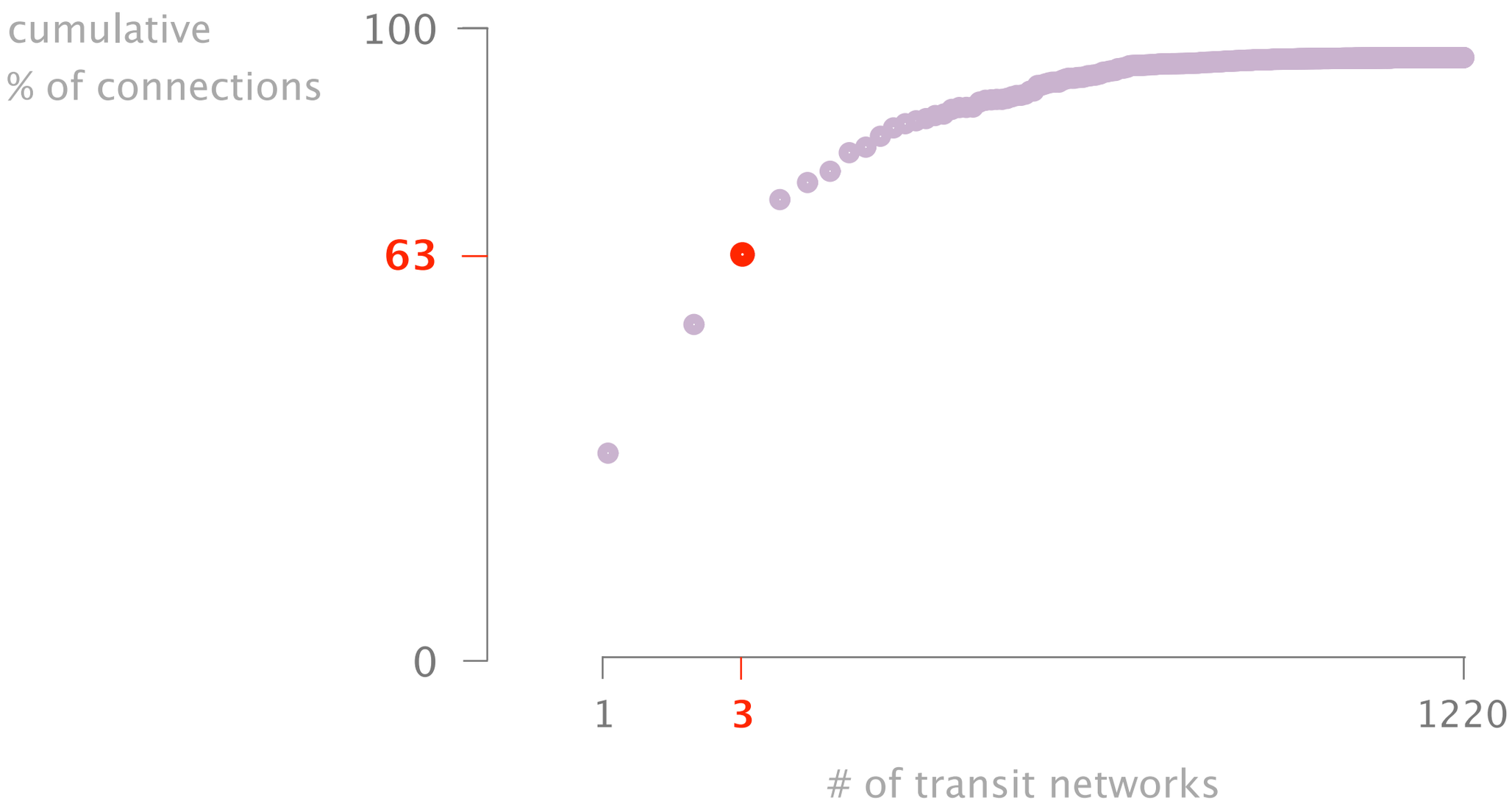



cumulative
% of connections
100
80
60
40
20
0
1
10
100
1220
# of transit networks

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 these characteristics 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	Attack 2
Partitioning	Delay
visible	invisible
network-wide attack	targeted attack (set of nodes)

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

Attack 1

Partitioning

visible

network-wide attack

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

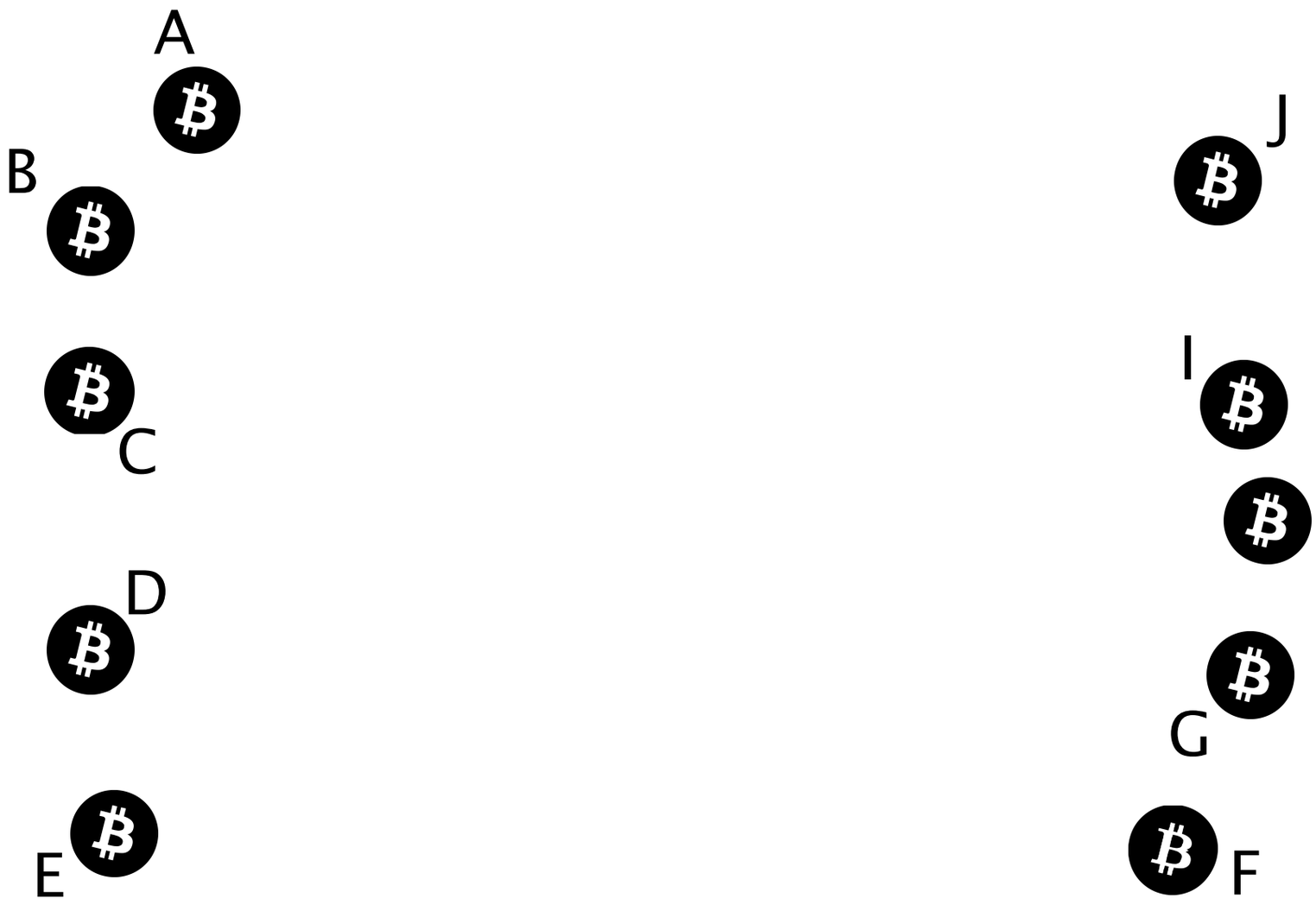
4 **Countermeasures**

short-term & long-term

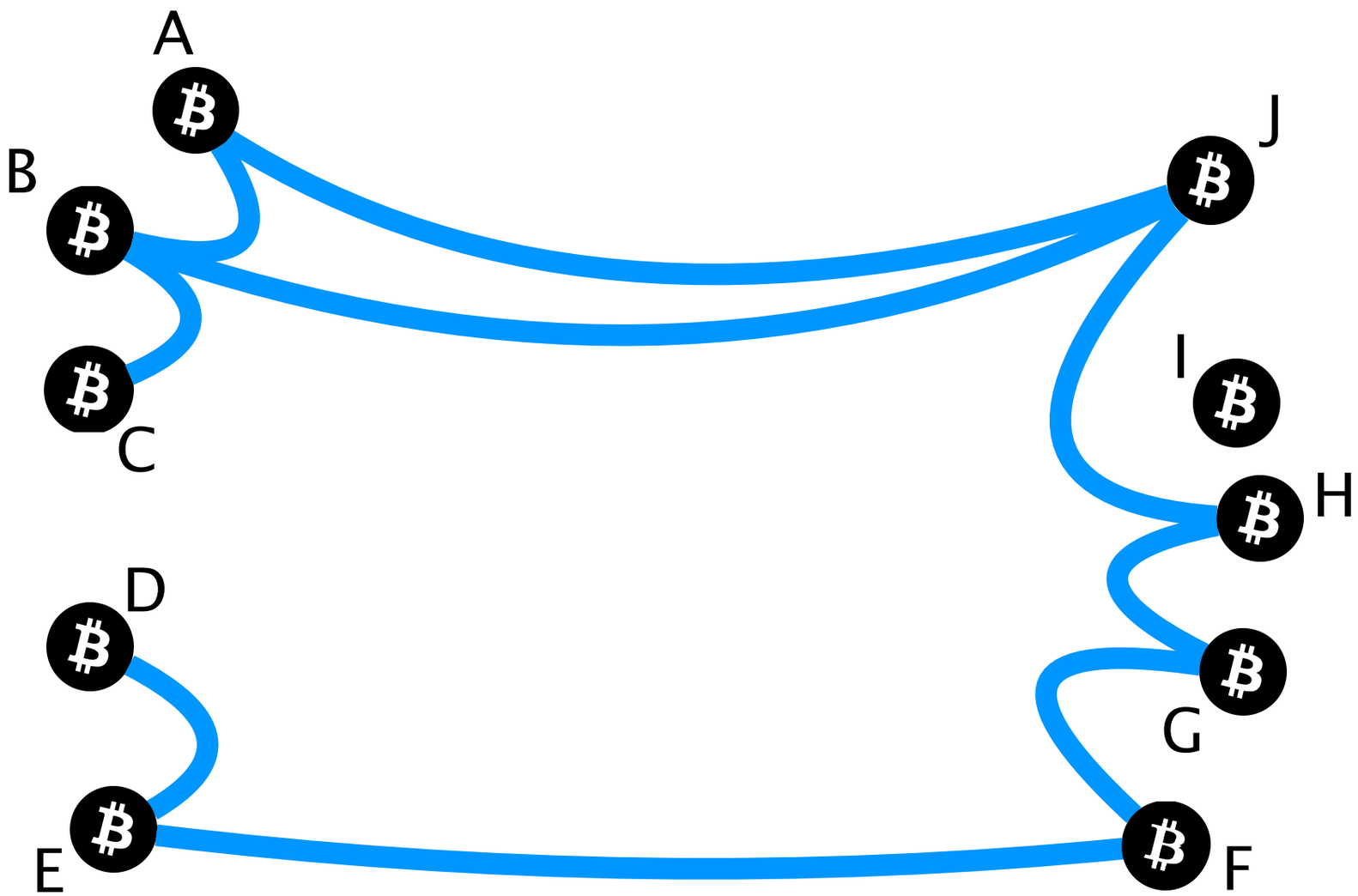
Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

Bitcoin is a distributed network of nodes



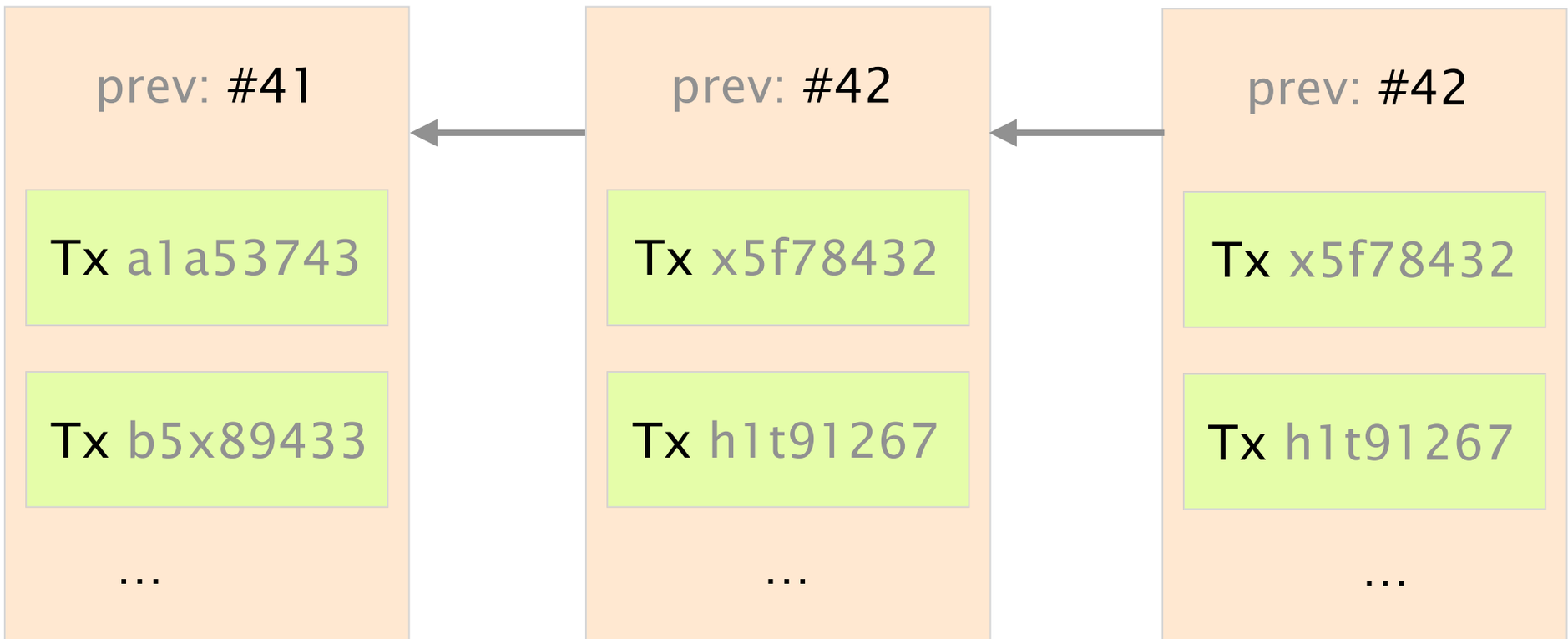
Bitcoin nodes establish random connections between each other



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

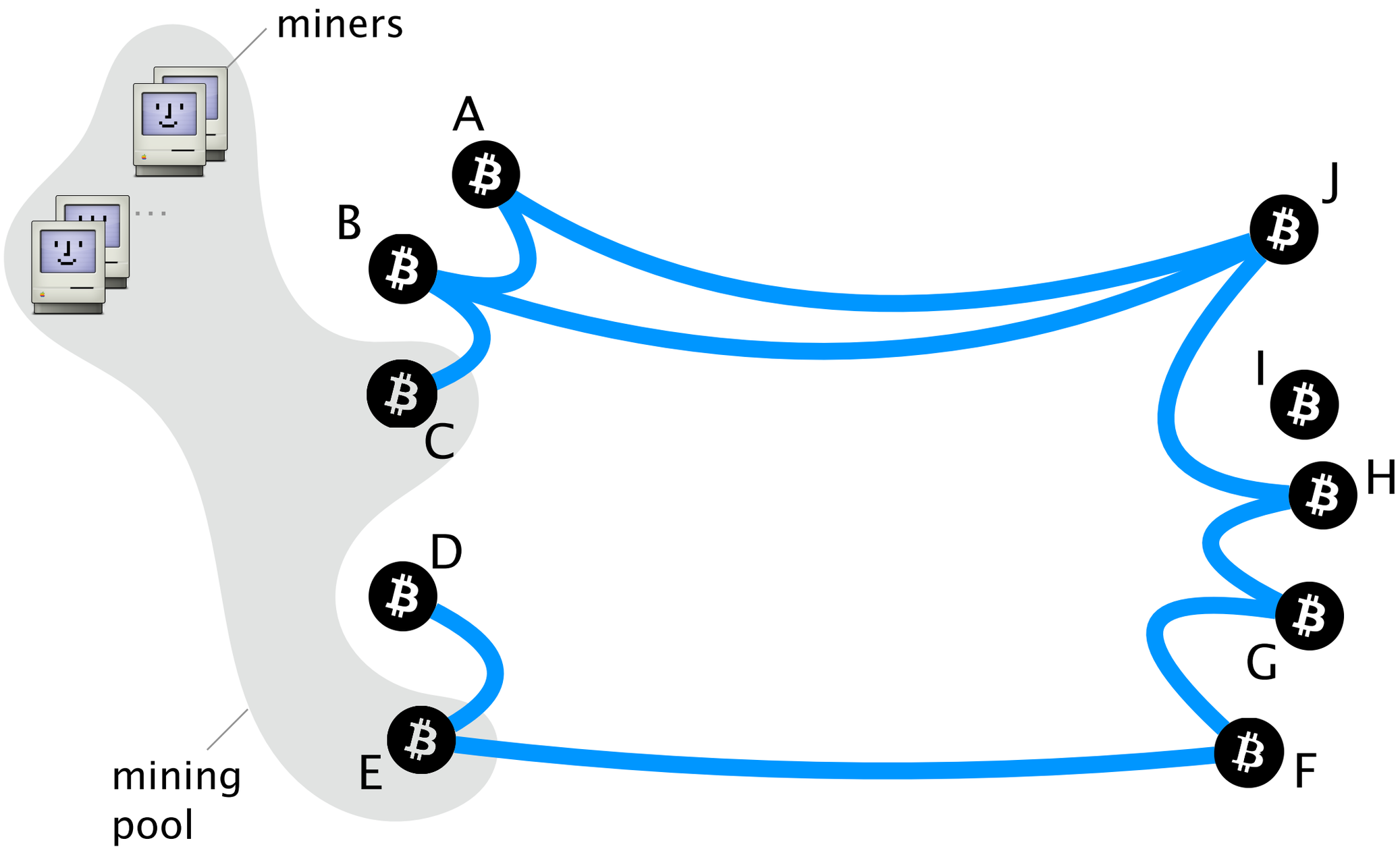
Tx a1a53743	Tx x5f78432	Tx x5f78432
Tx b5x89433	Tx h1t91267	Tx h1t91267
…	…	…

The Blockchain is a chain of Blocks

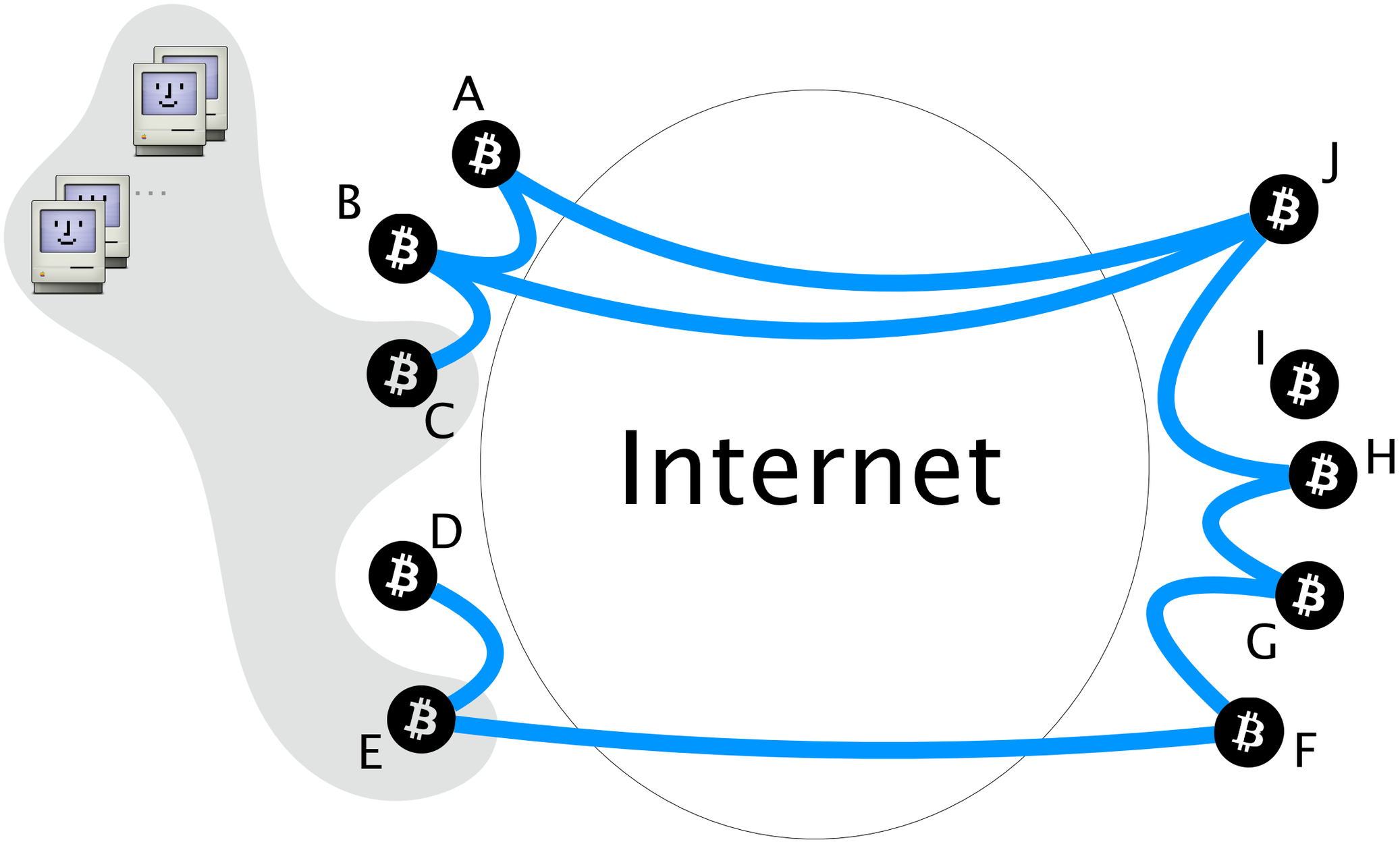


The Blockchain is extended by miners

Miners are grouped in mining pools



Bitcoin connections are routed over the Internet

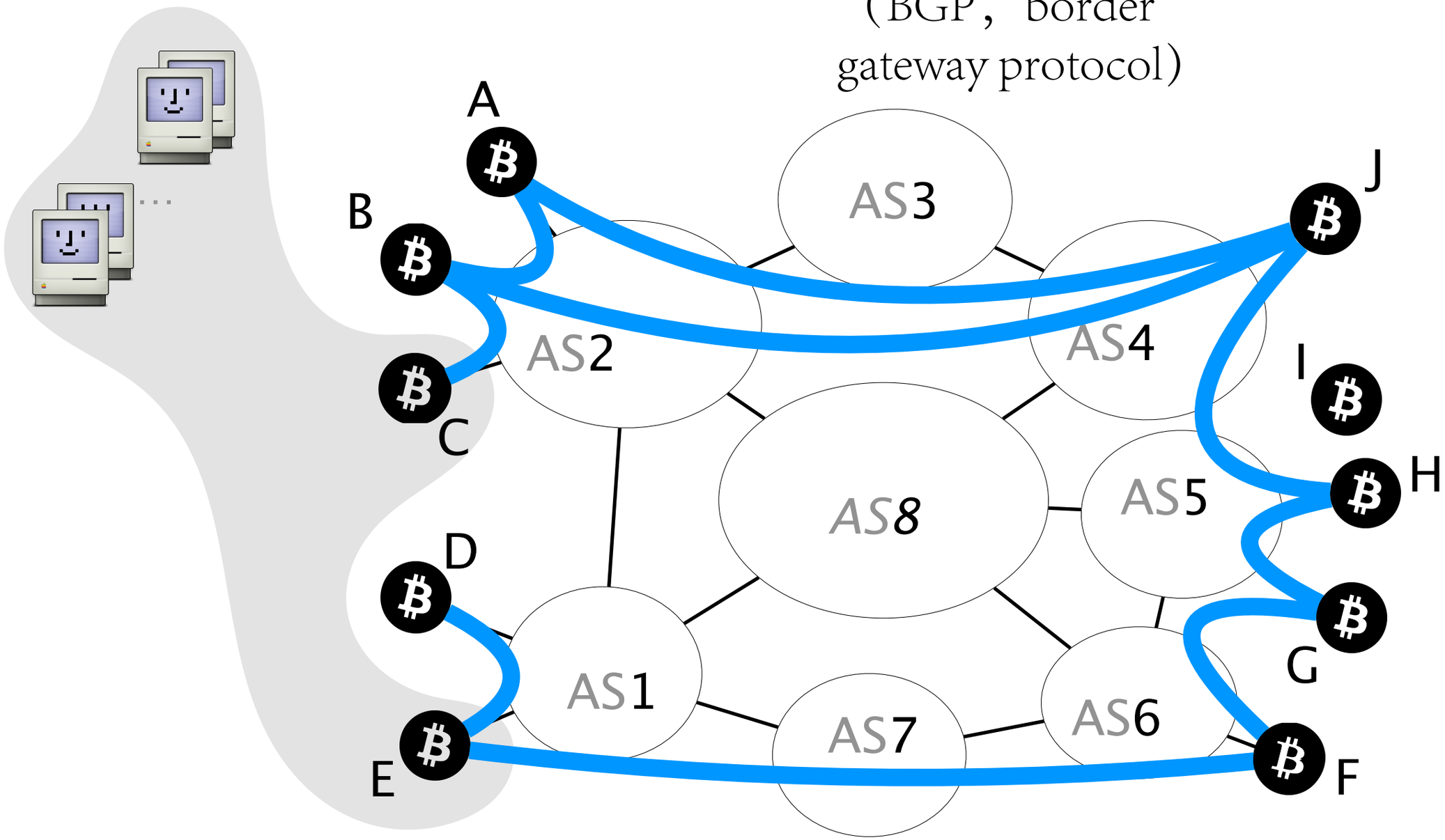


自治系统

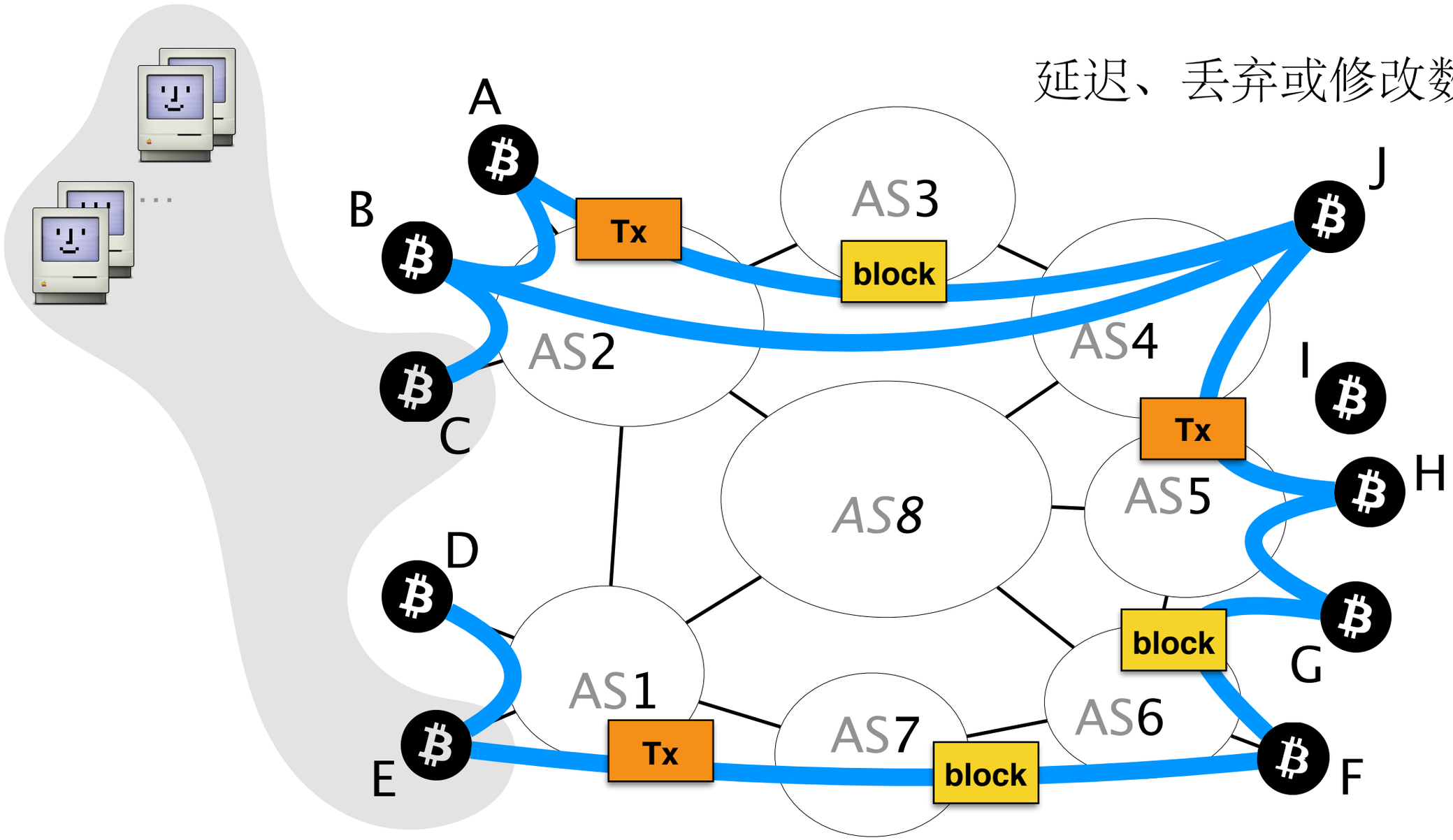
The Internet is composed of Autonomous Systems (ASes).

BGP computes the forwarding path across them

边界网关协议
（BGP，border
gateway protocol）



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

这两个部分之间无法进行信息交互

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

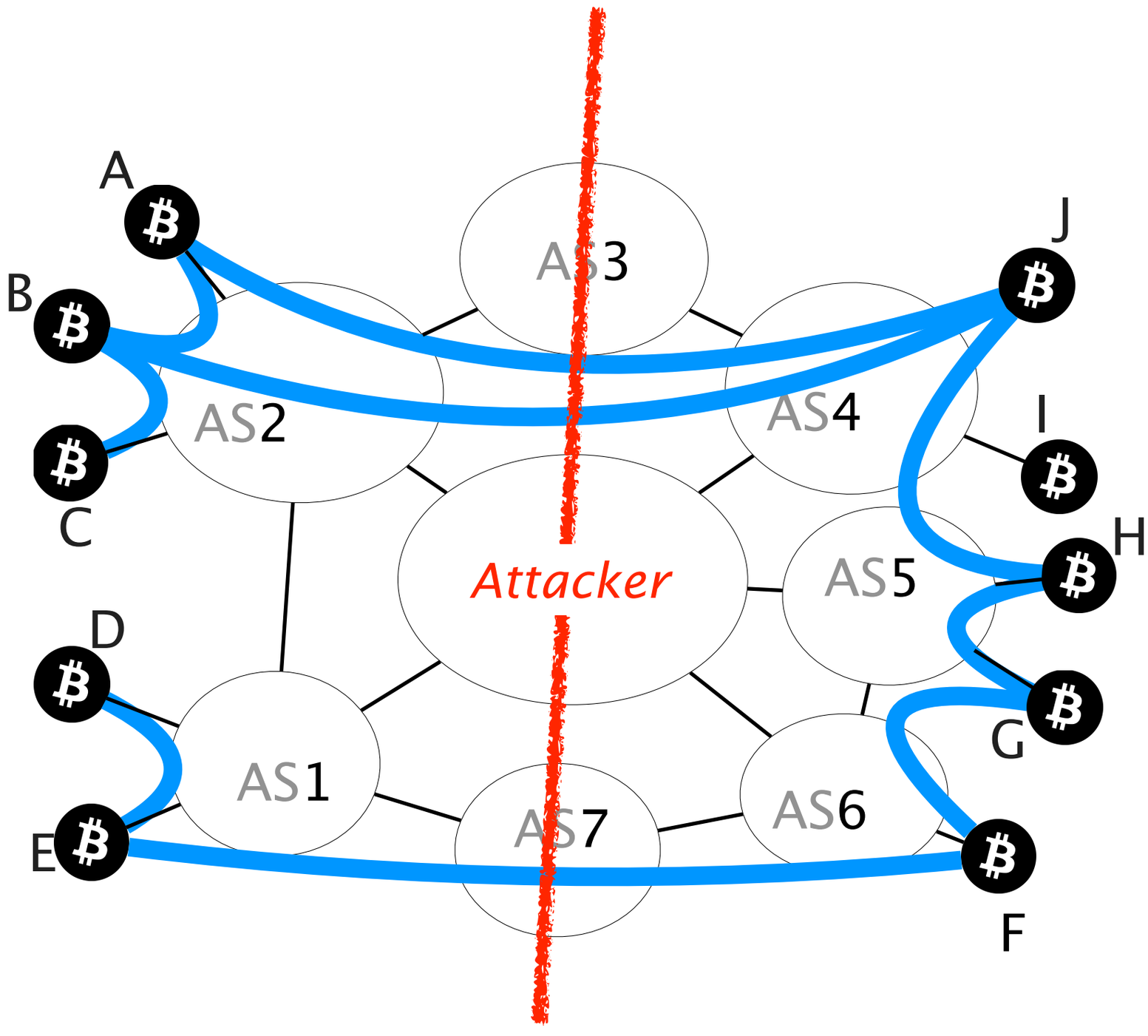
Revenue Loss

Double spending

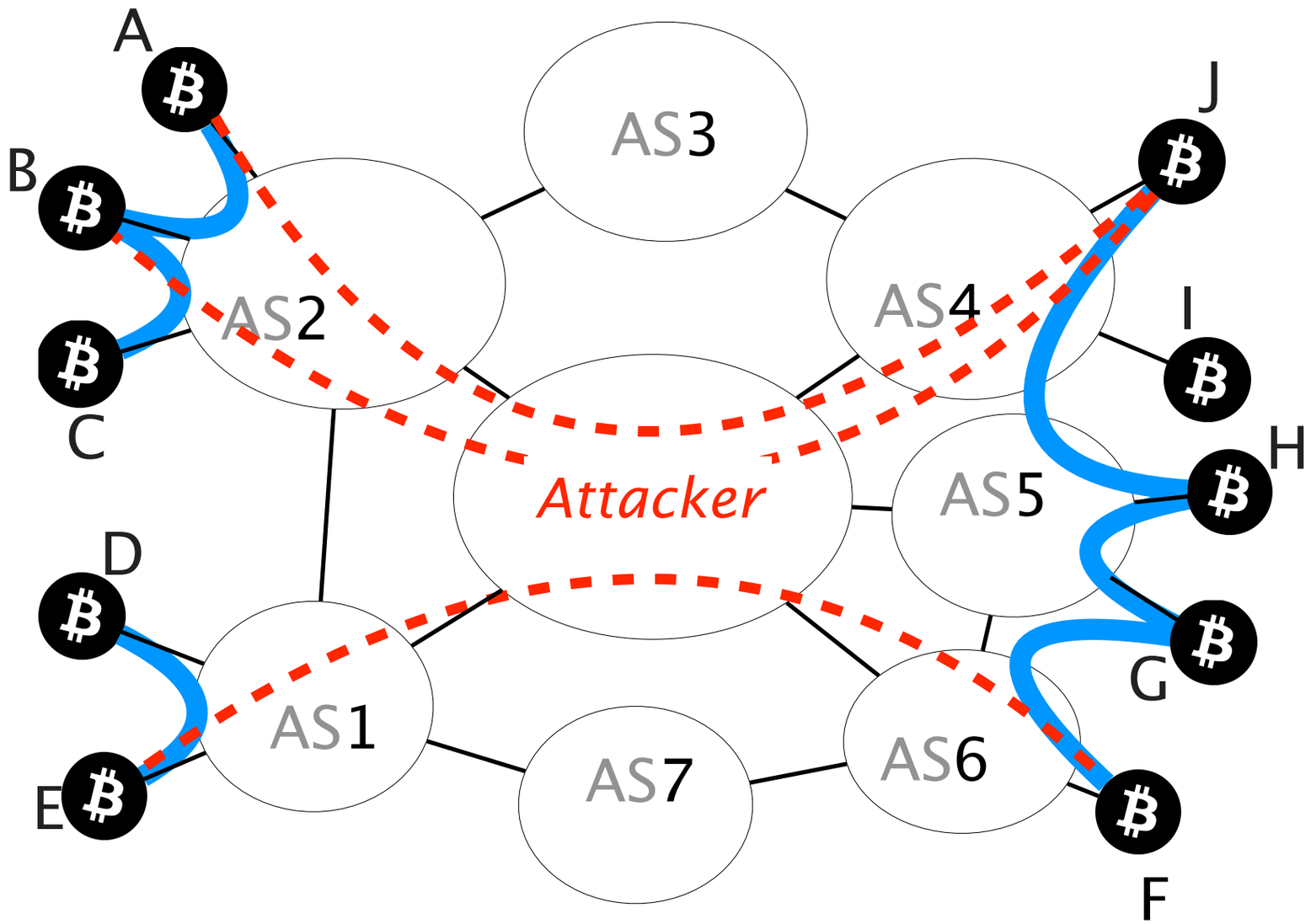
Transactions in components with less mining power can be reverted

How does the attack work?

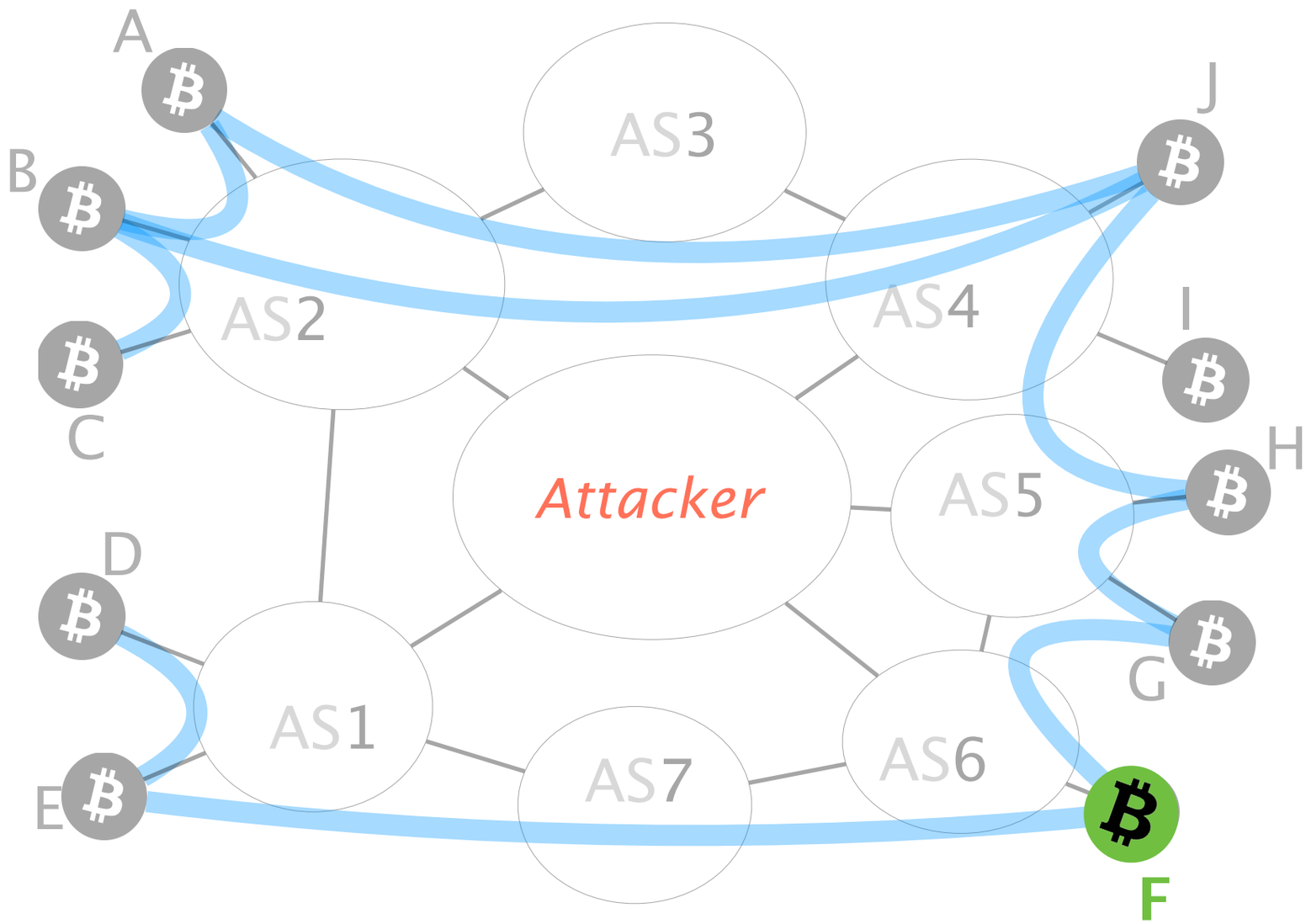
Let’s say an attacker wants to partition the network into the left and right side



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

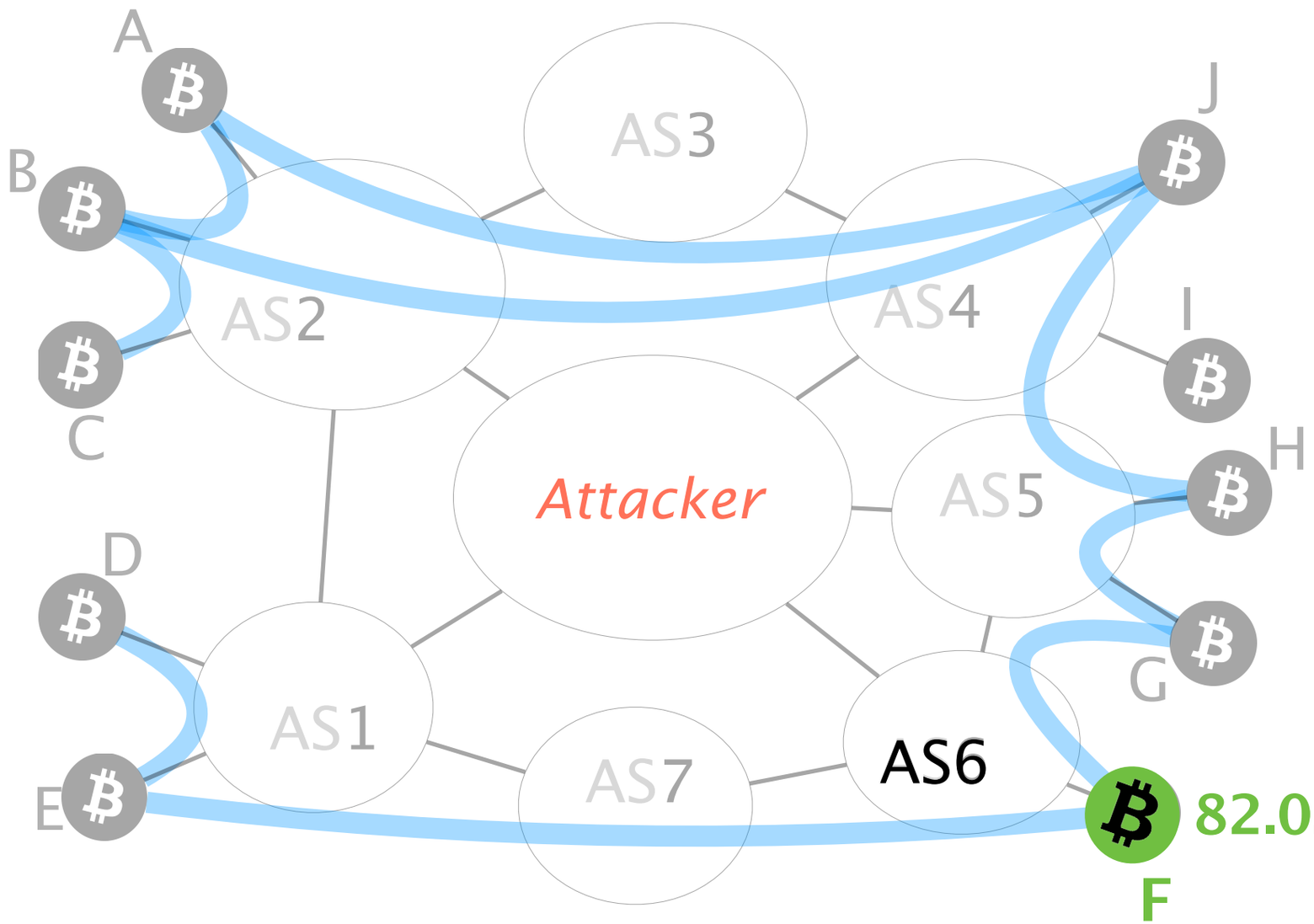


Let us focus on node F



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

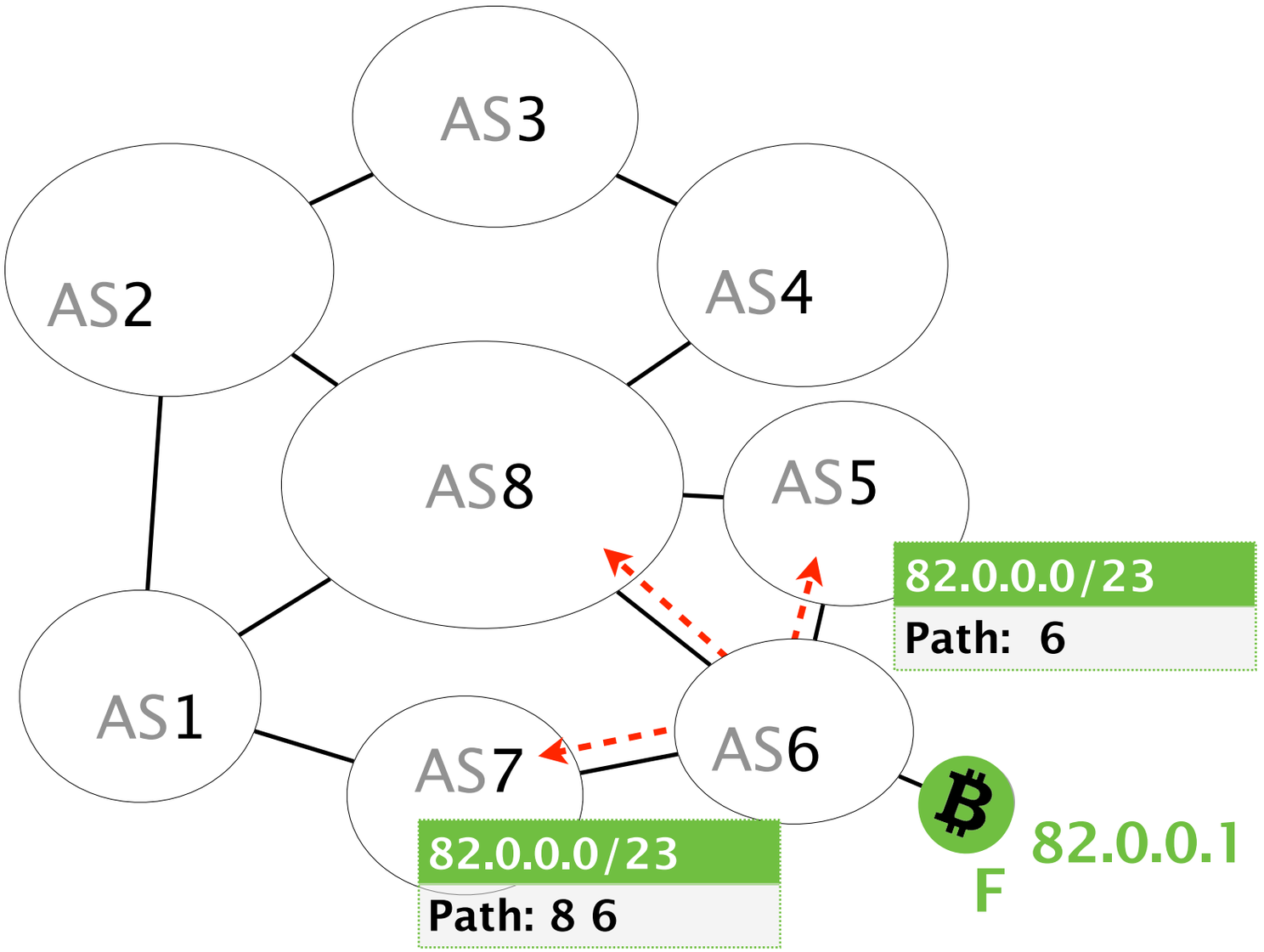
攻击者需要通过BGP劫持 吸引所有目的地是F的通信



F有一个属于它提供商AS6的IP地址。AS6需要告诉Internet一个地址前缀，包含AS6拥有的IP地址。

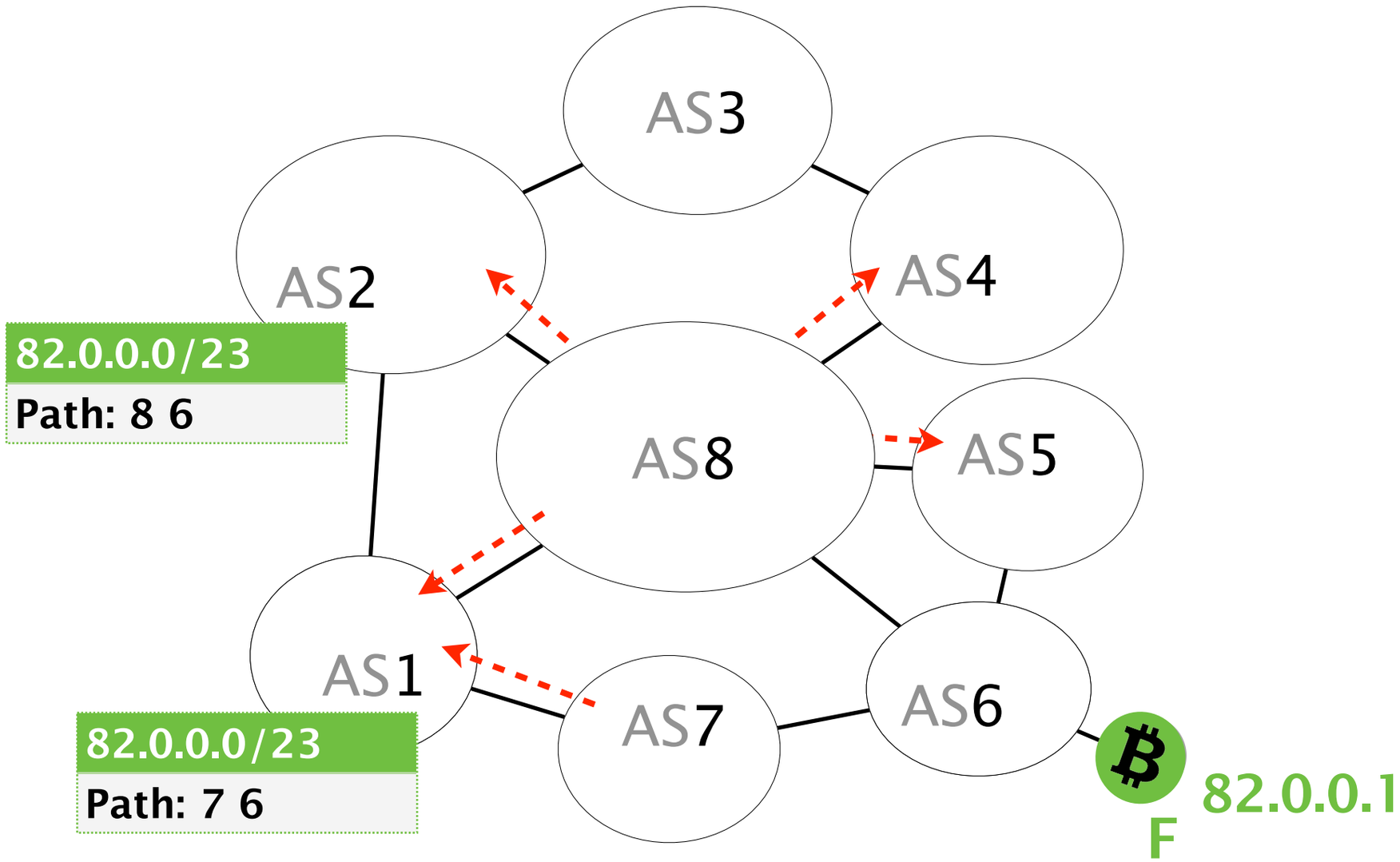
AS6 will create a BGP advertisement

AS6会创建一个BGP广播。



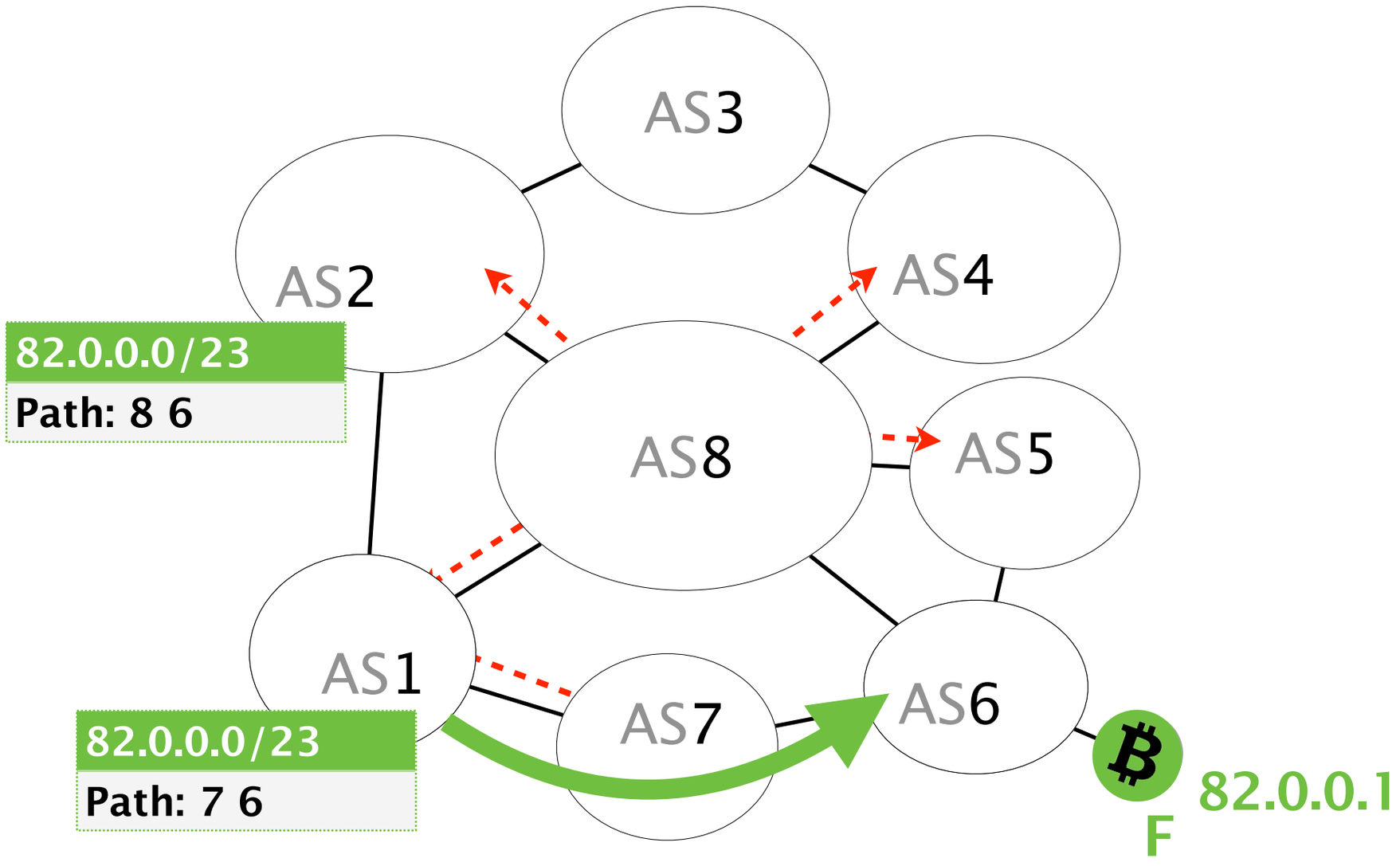
AS6's advertisement is propagated AS-by-AS until all ASes in the Internet learn about it

AS6传递广播由一个AS广播到另一个AS去。
直到所有AS都学习到前往目标前缀的路径。



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

AS6传递广播由一个AS广播到另一个AS去。
直到所有AS都学习到前往目标前缀的路径。



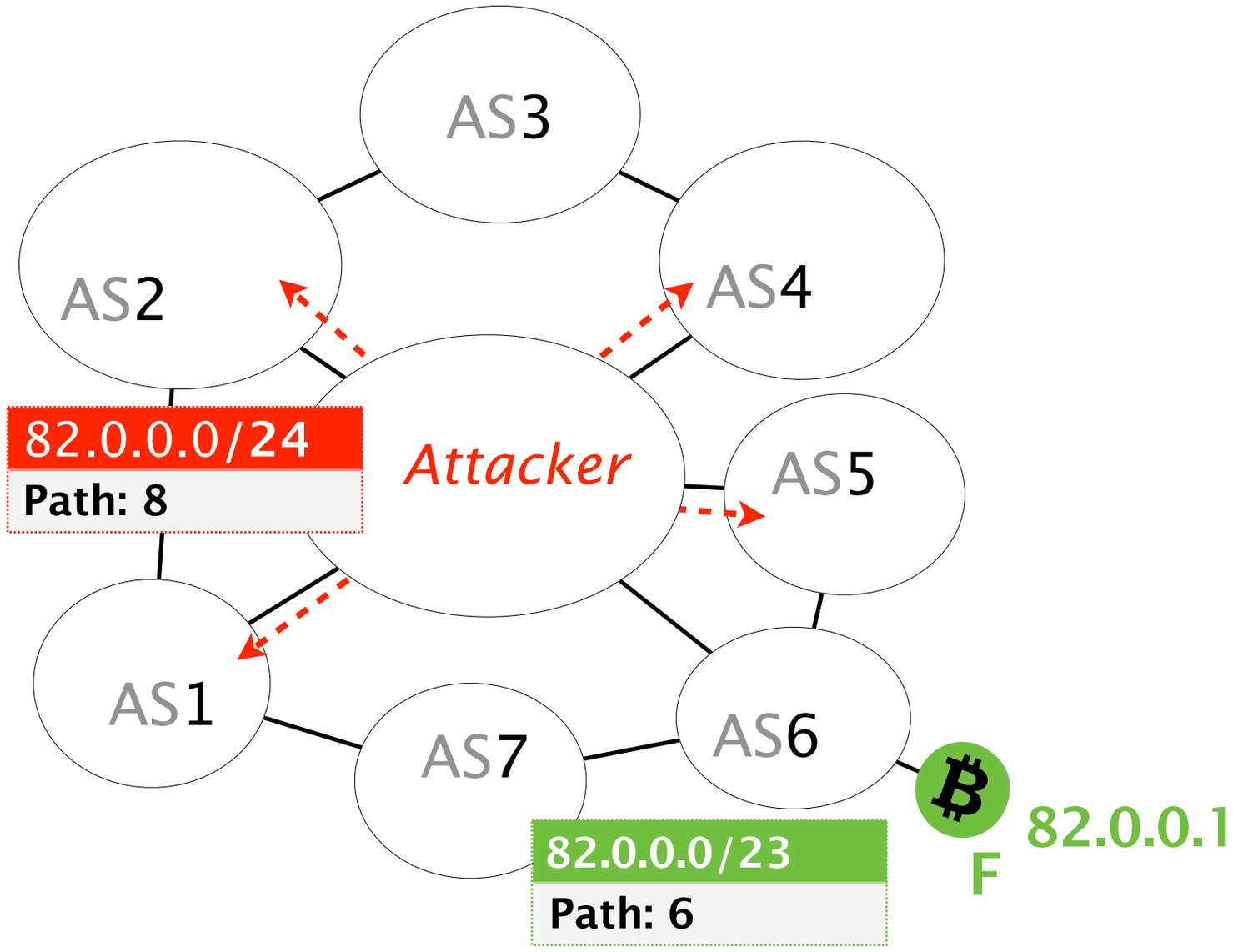
比如AS1会知道通过AS7前往AS6。

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

由于BGP不检查广播的有效性。因此任何AS都可以广播任意前缀。

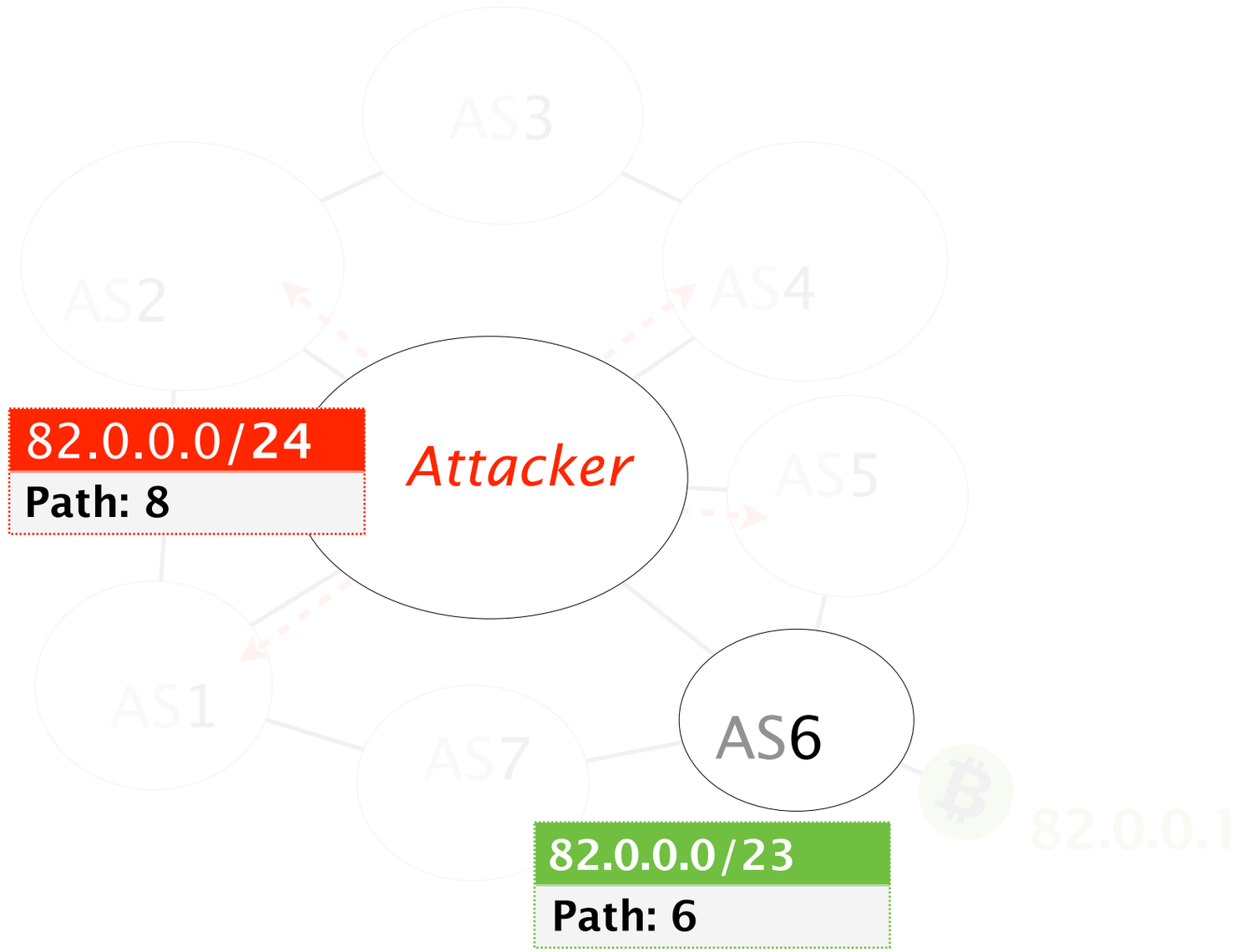
Consider that the attacker advertises a more-specific prefix covering F's IP address

我们假设攻击者广播了包含绿色节点IP的前缀。



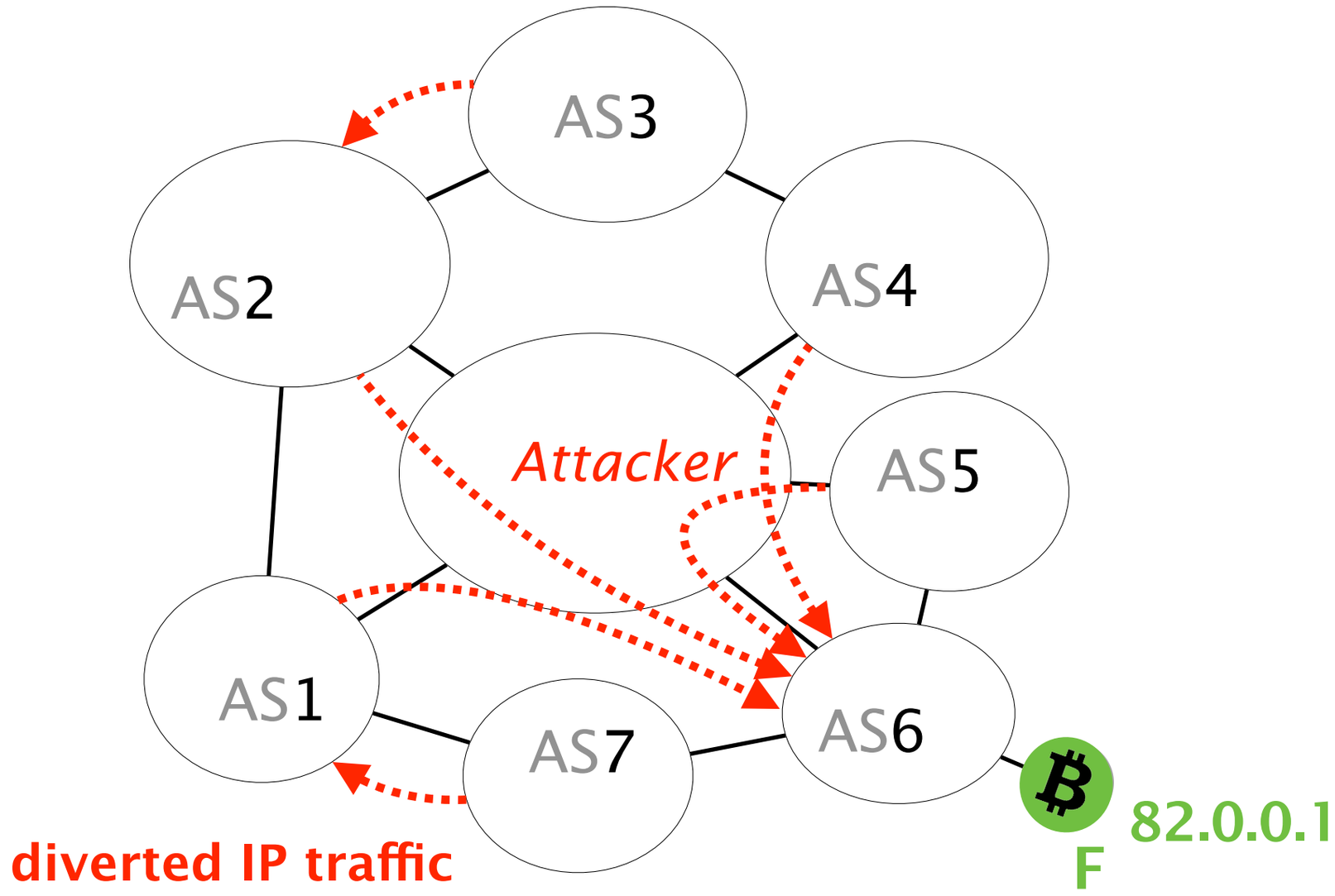
As IP routers prefer more-specific prefixes, the attacker route will be preferred

由于攻击者的广播更具体，网络部分的长度有24位。
Internet上的路由偏向于最长的前缀匹配，因此实际上会使用恶意的广播



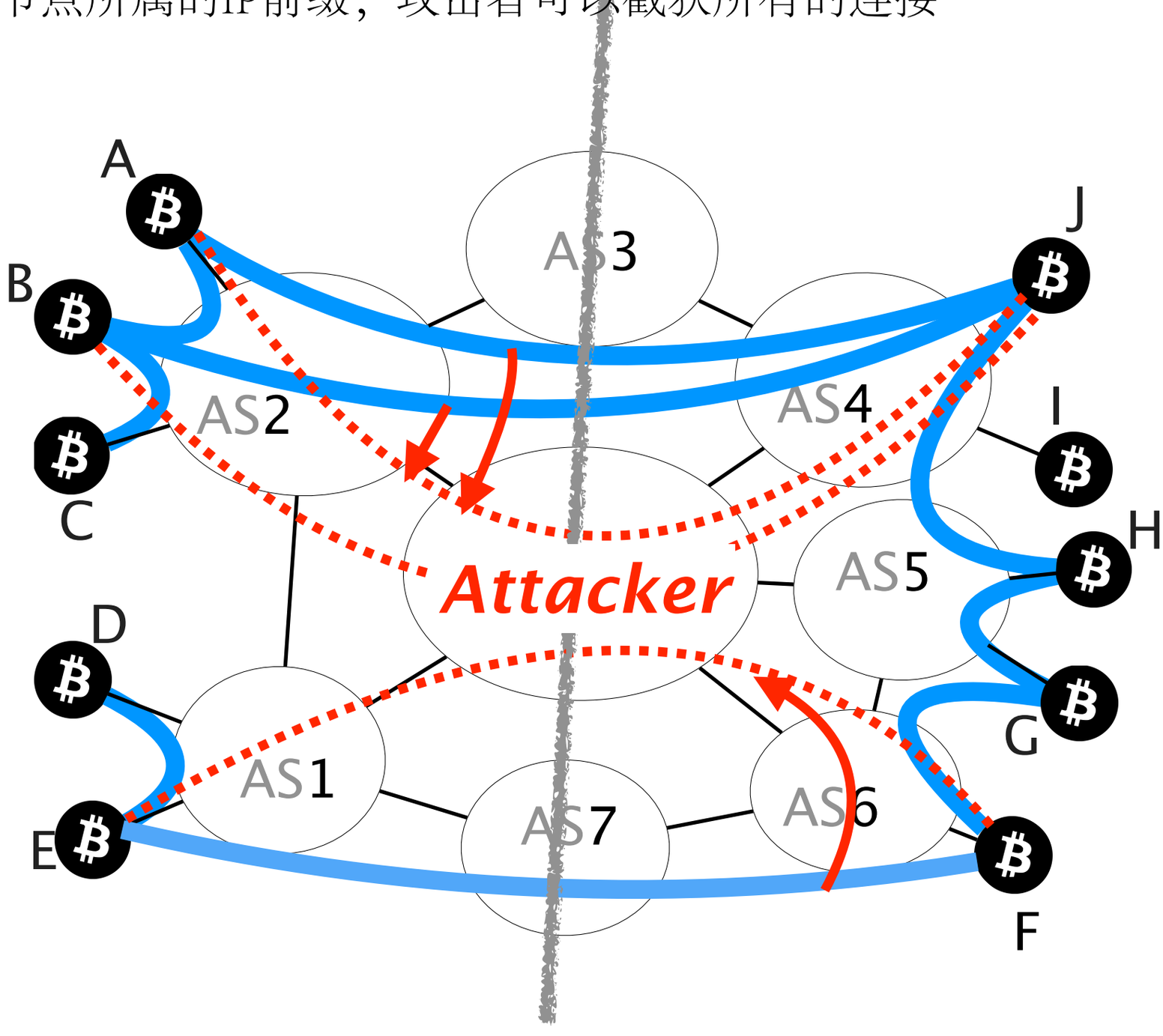
Traffic to node F is hijacked

因此所有去往绿色节点的通信都会被攻击者转发



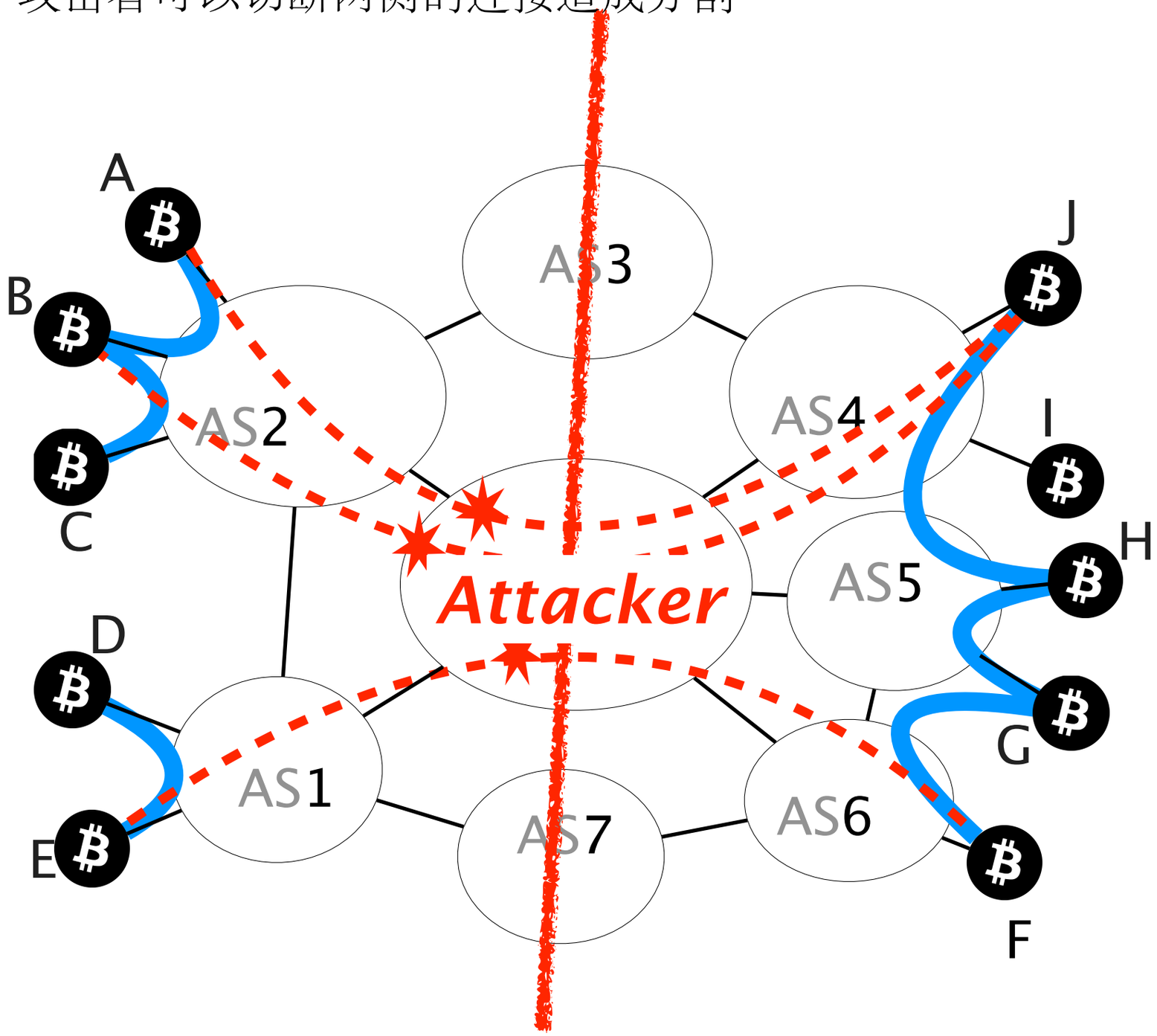
By hijacking the IP prefixes pertaining to the right nodes, the attacker can intercept all their connections

通过劫持右侧节点所属的IP前缀，攻击者可以截获所有的连接



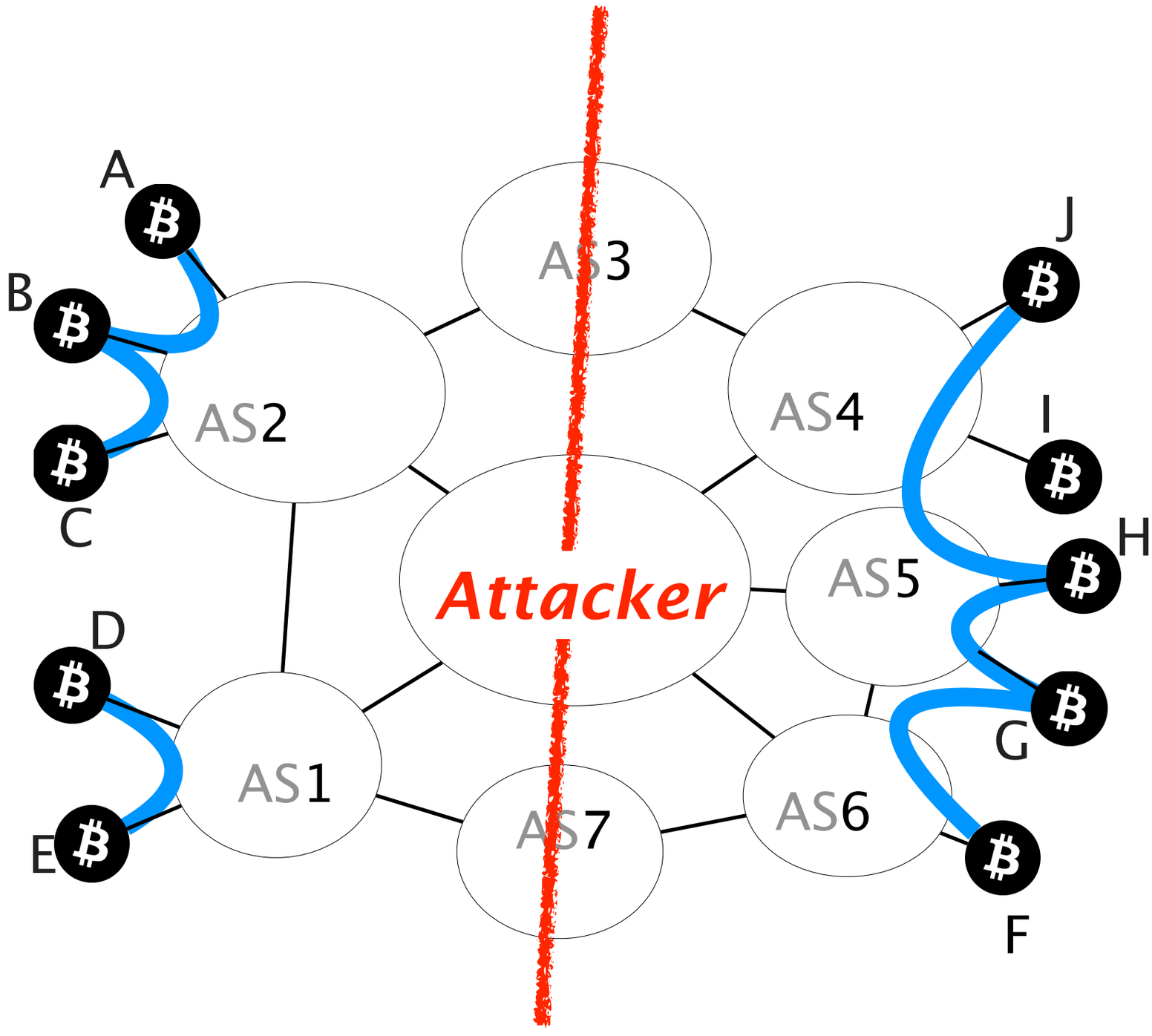
Once on-path, the attacker can drop all connections crossing the partition

一旦劫持成功，攻击者可以切断两侧的连接造成分割



The partition is created

一旦劫持成功，攻击者可以切断两侧的连接造成分割



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

当然实际上分割不是那么简单的。有的连接是无法拦截的。

Bitcoin connections established…

- within a mining pool
- within an AS
- between mining pools with private agreements

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

即便如此，攻击者也可以探测并定位这些连接
，剔除不可能分割的节点后再进行分割。

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

文章中给出了一个算法。
给定希望从网络中分割出去的节点集合，存在攻击者可以分割的唯一最大节点子集。

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

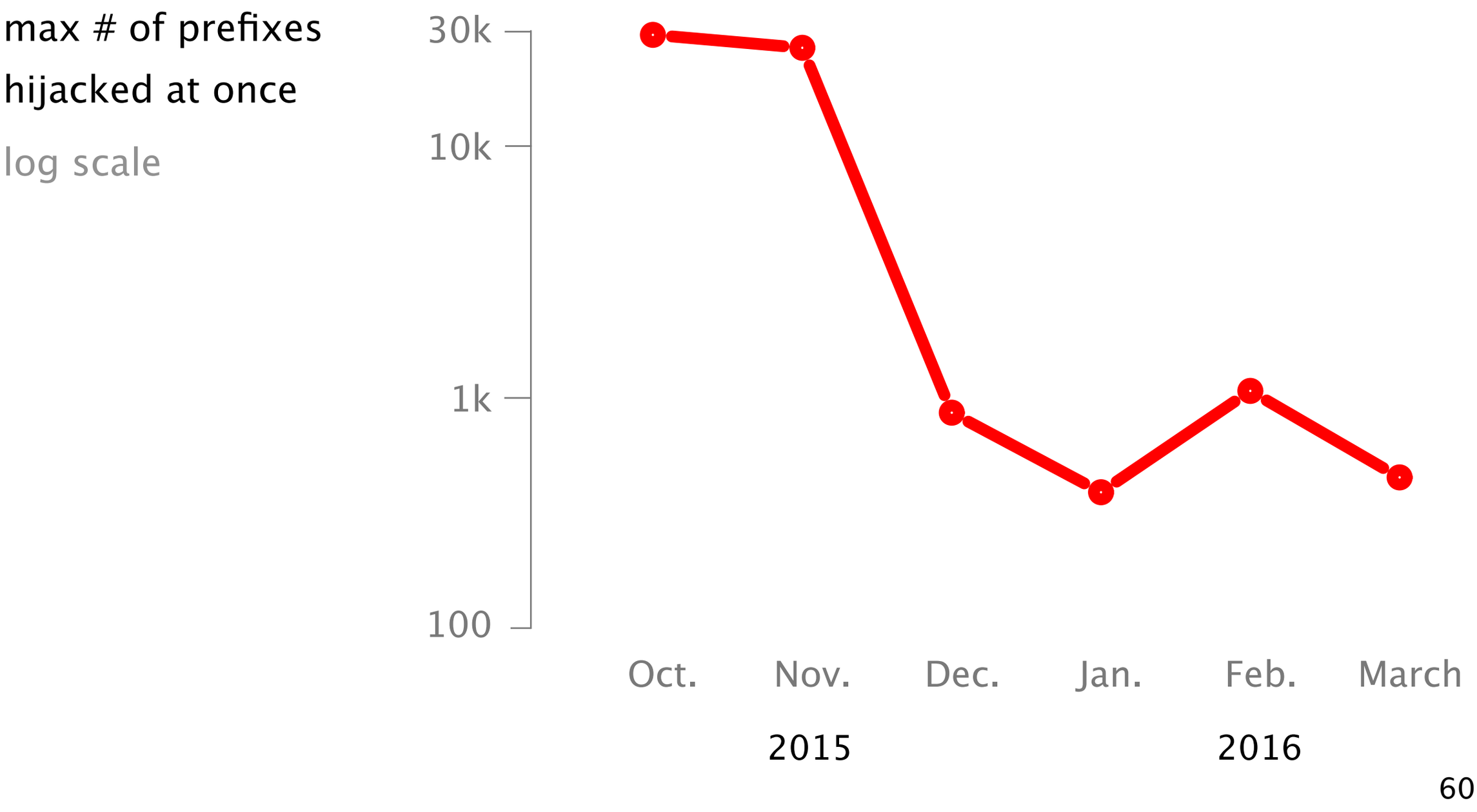
文章发现通过劫持少于100个前缀就可以将Bitcoin的算力一分为二。

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

negligible with respect to routinely observed hijacks

和已经观察到的每天发生的劫持相比，100个前缀是很少的。

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



We also evaluated the partition in terms of time efficiency

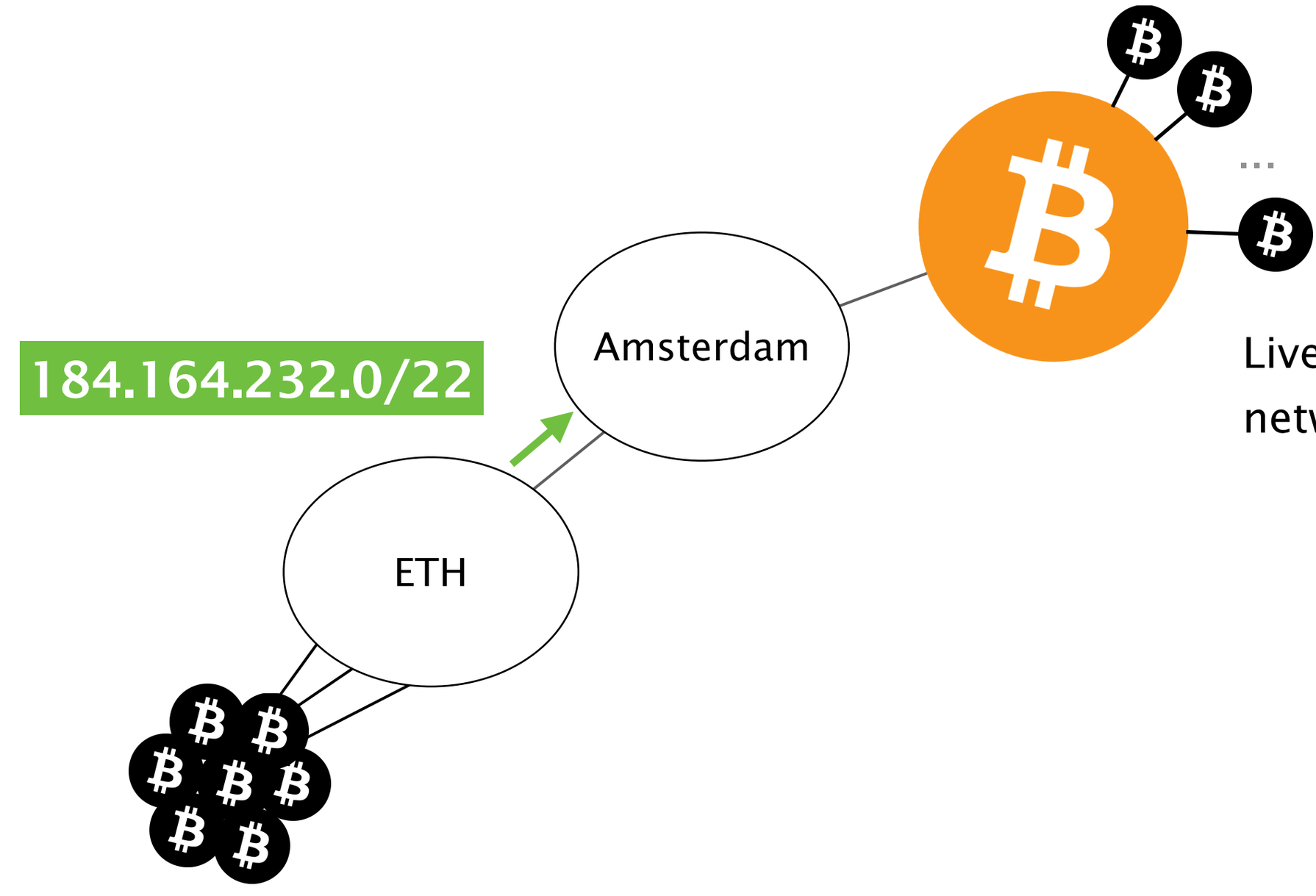
Practicality

Time efficiency

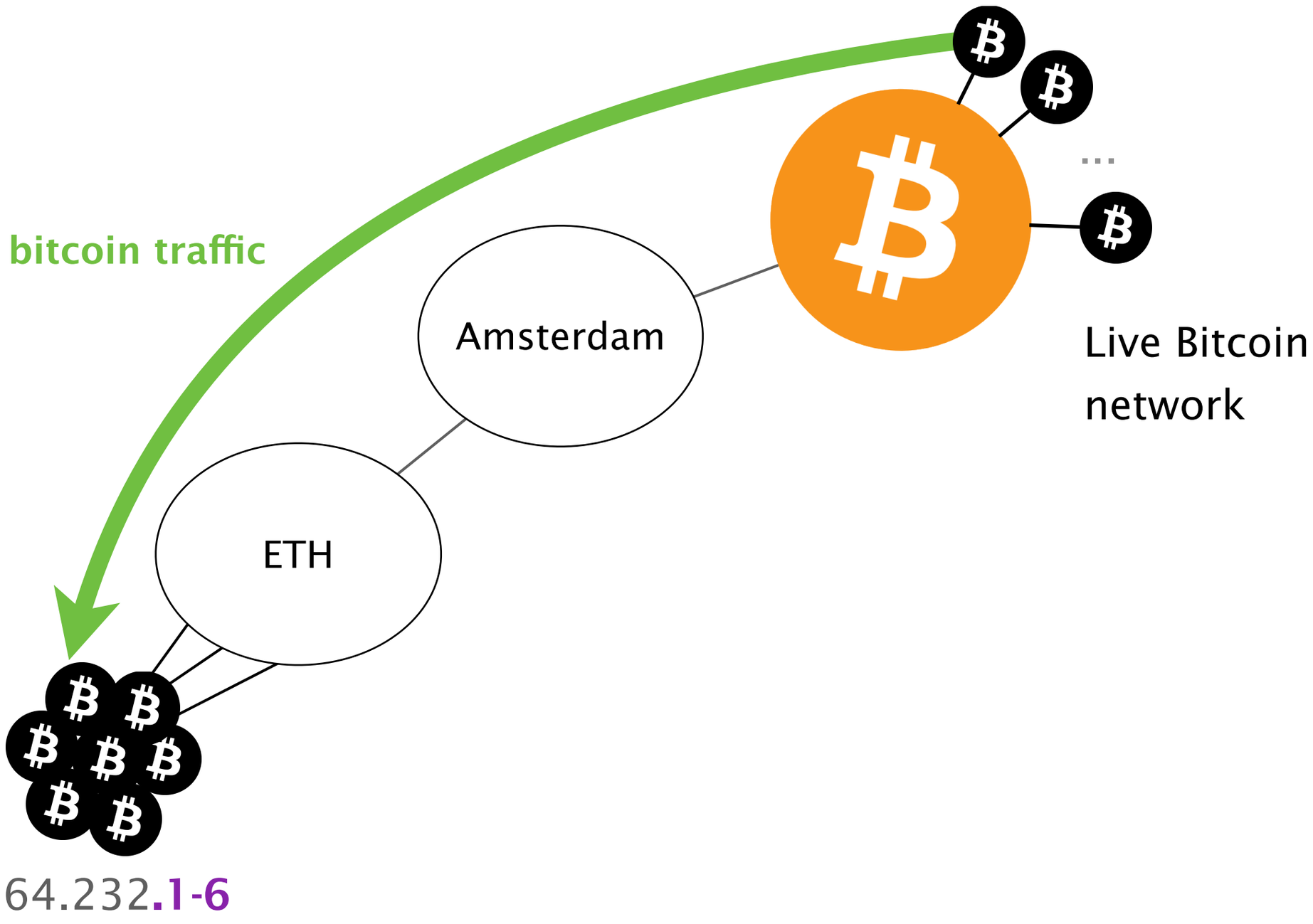
How long does it take?

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

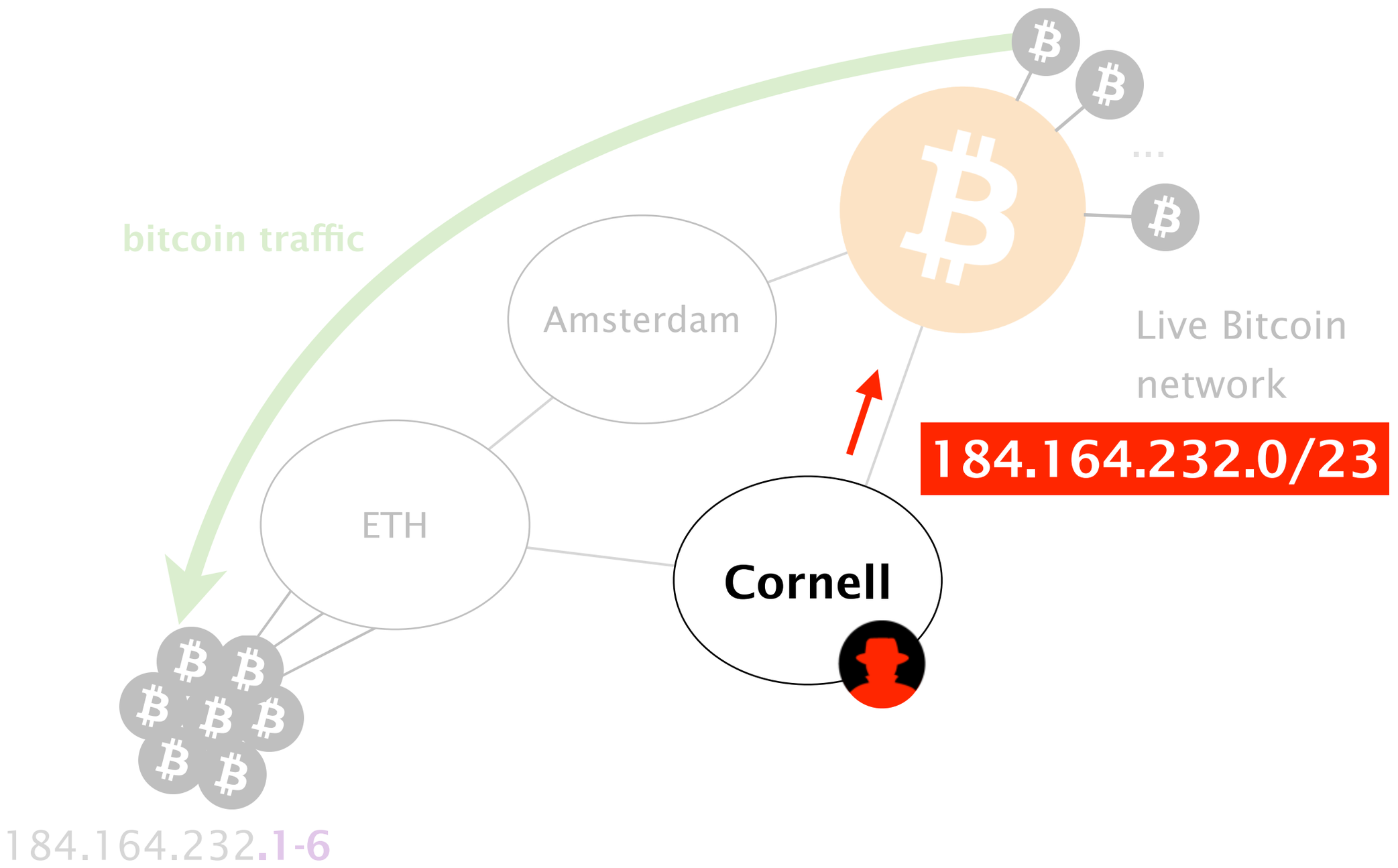
We hosted a few Bitcoin nodes at ETH and advertised a covering prefix via Amsterdam



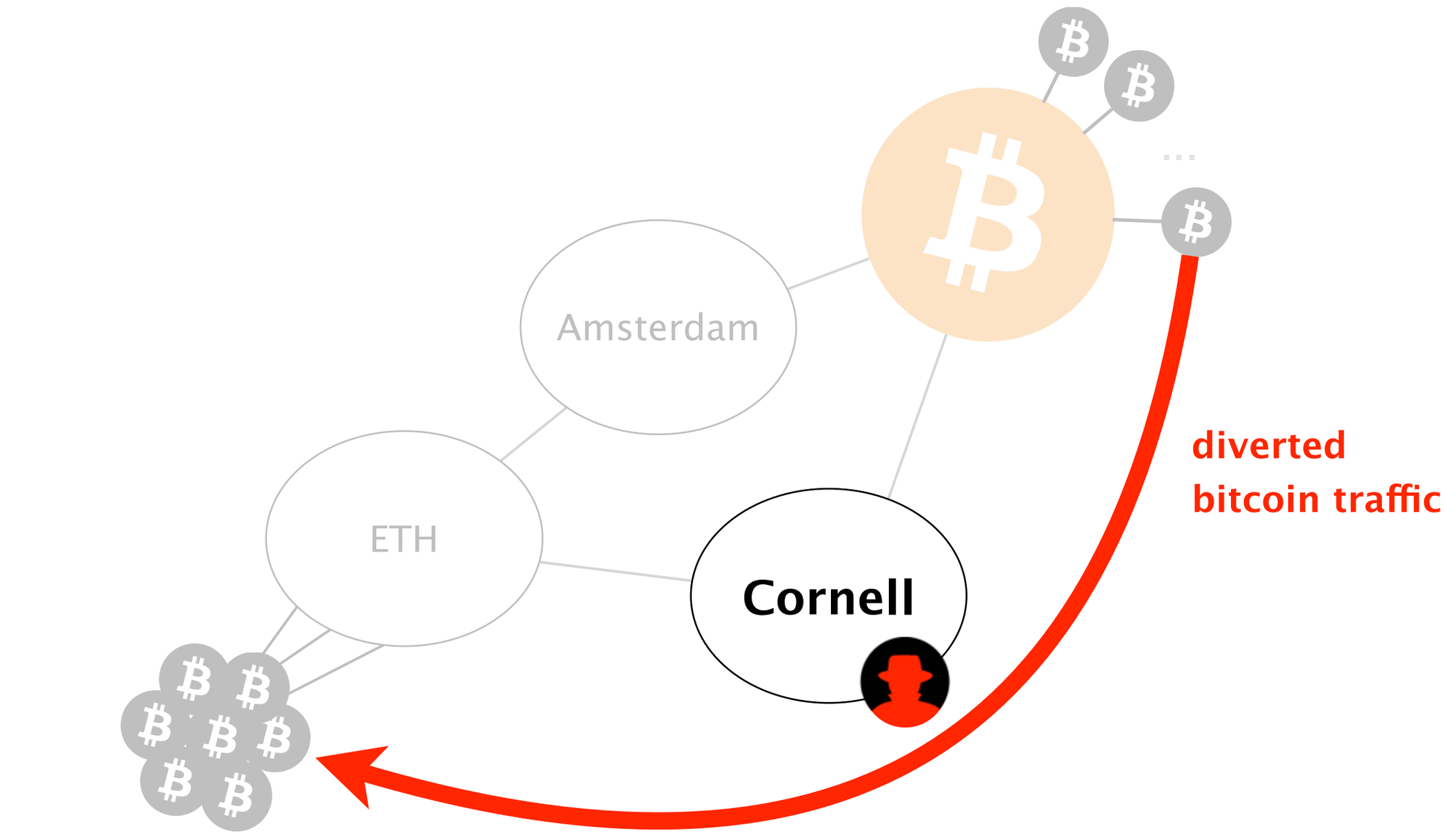
Initially, all the traffic to our nodes transits via Amsterdam

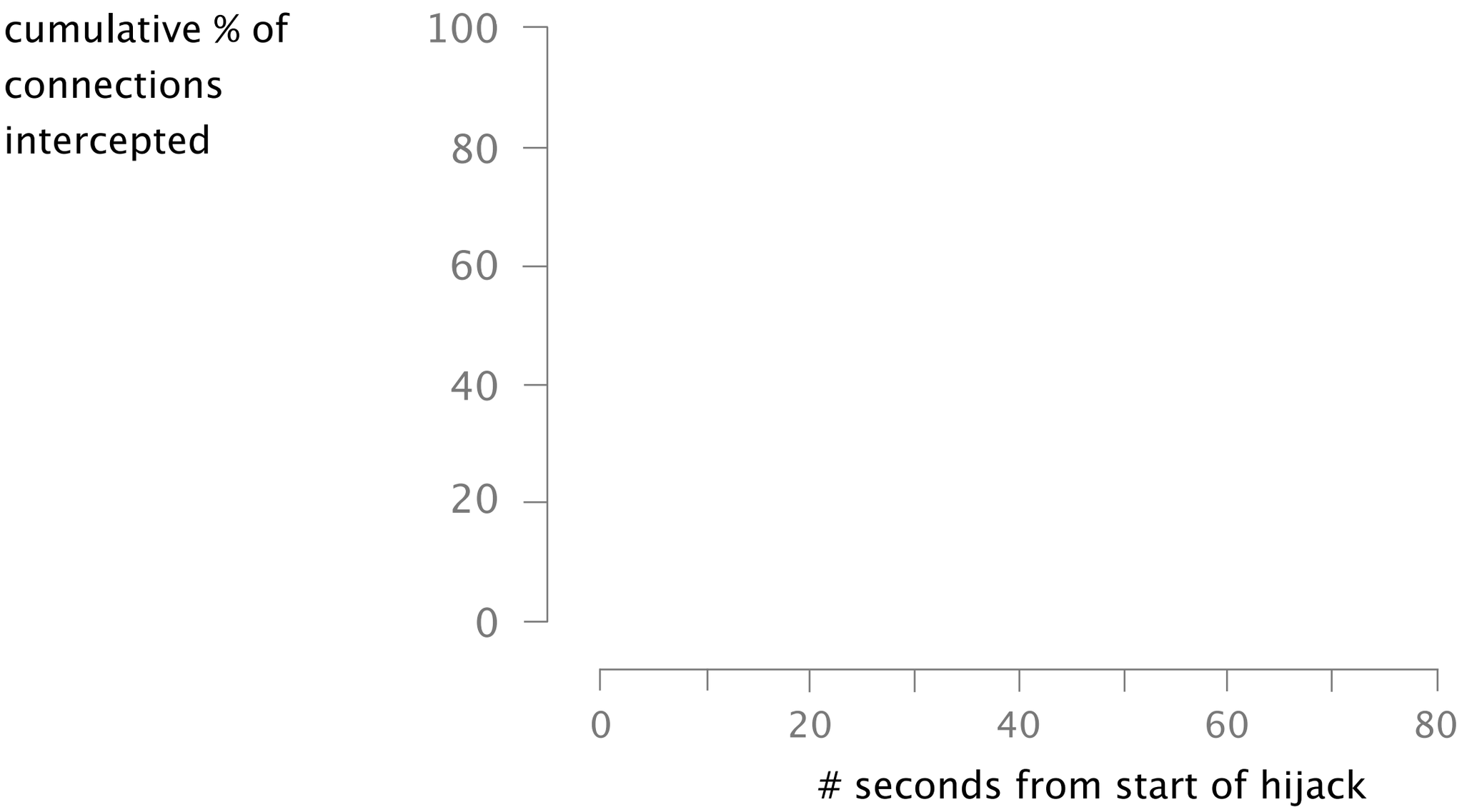


We hijacked our nodes

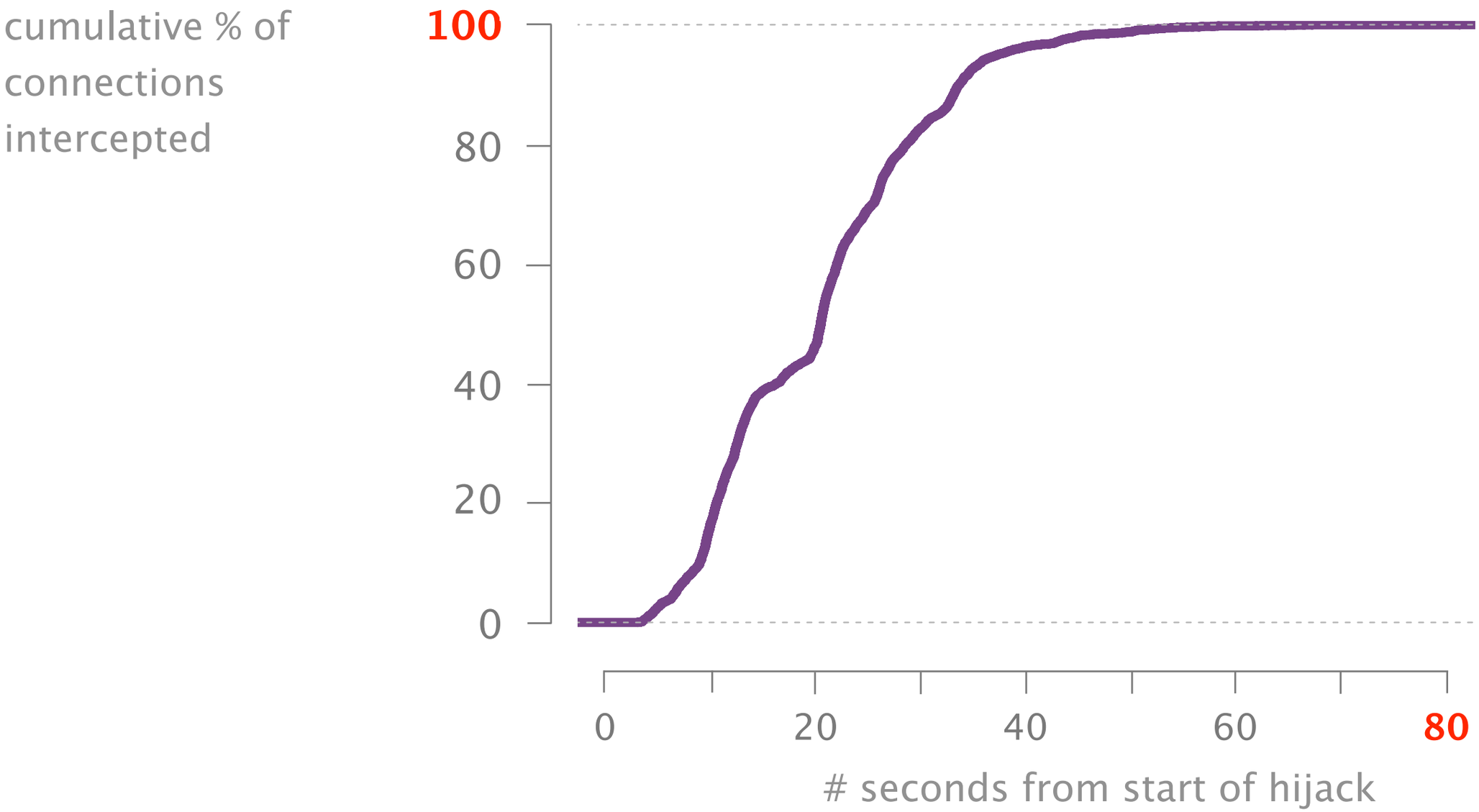


We measured the time required for a rogue AS to divert all the traffic to our nodes




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

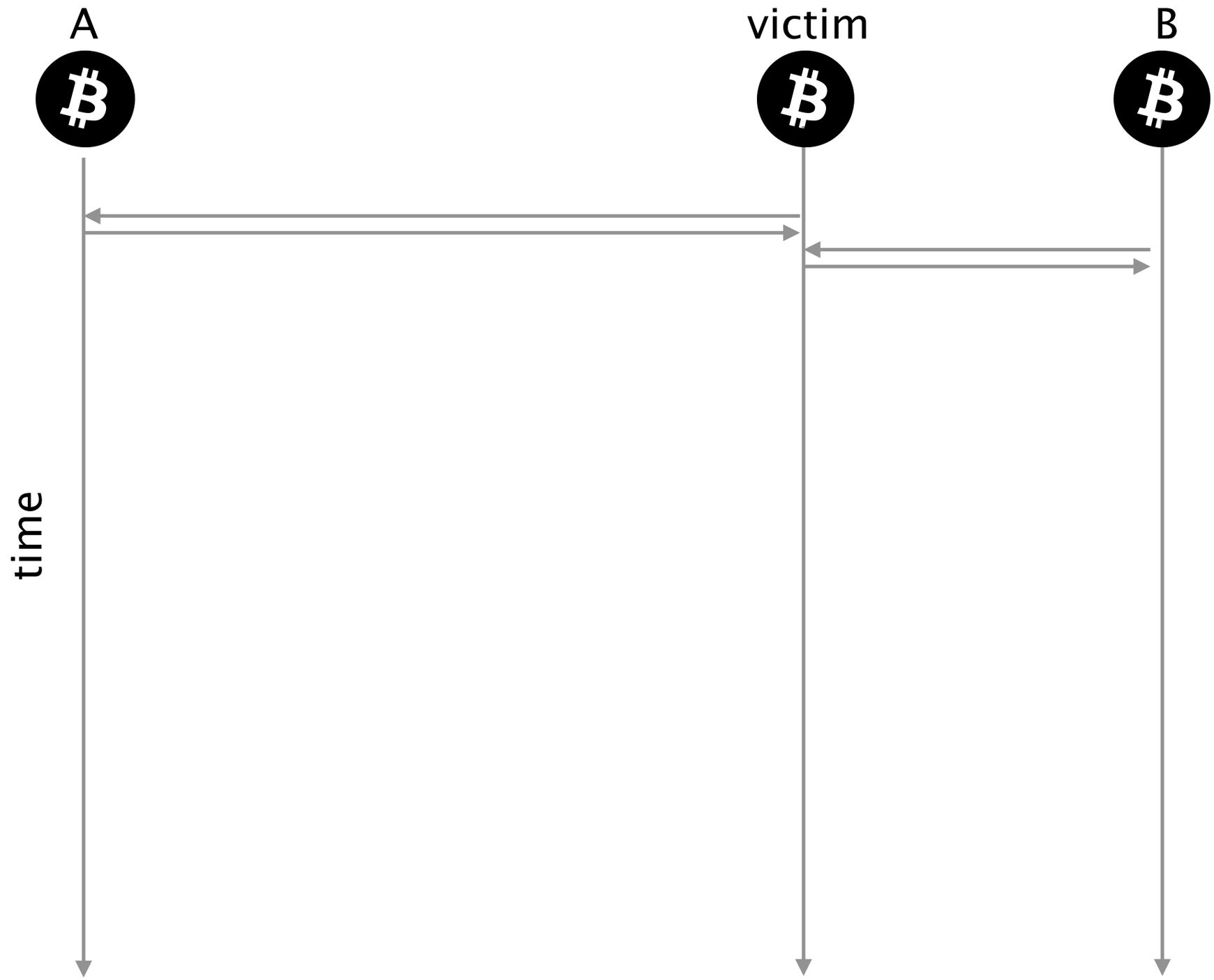
Mining pool

Regular node

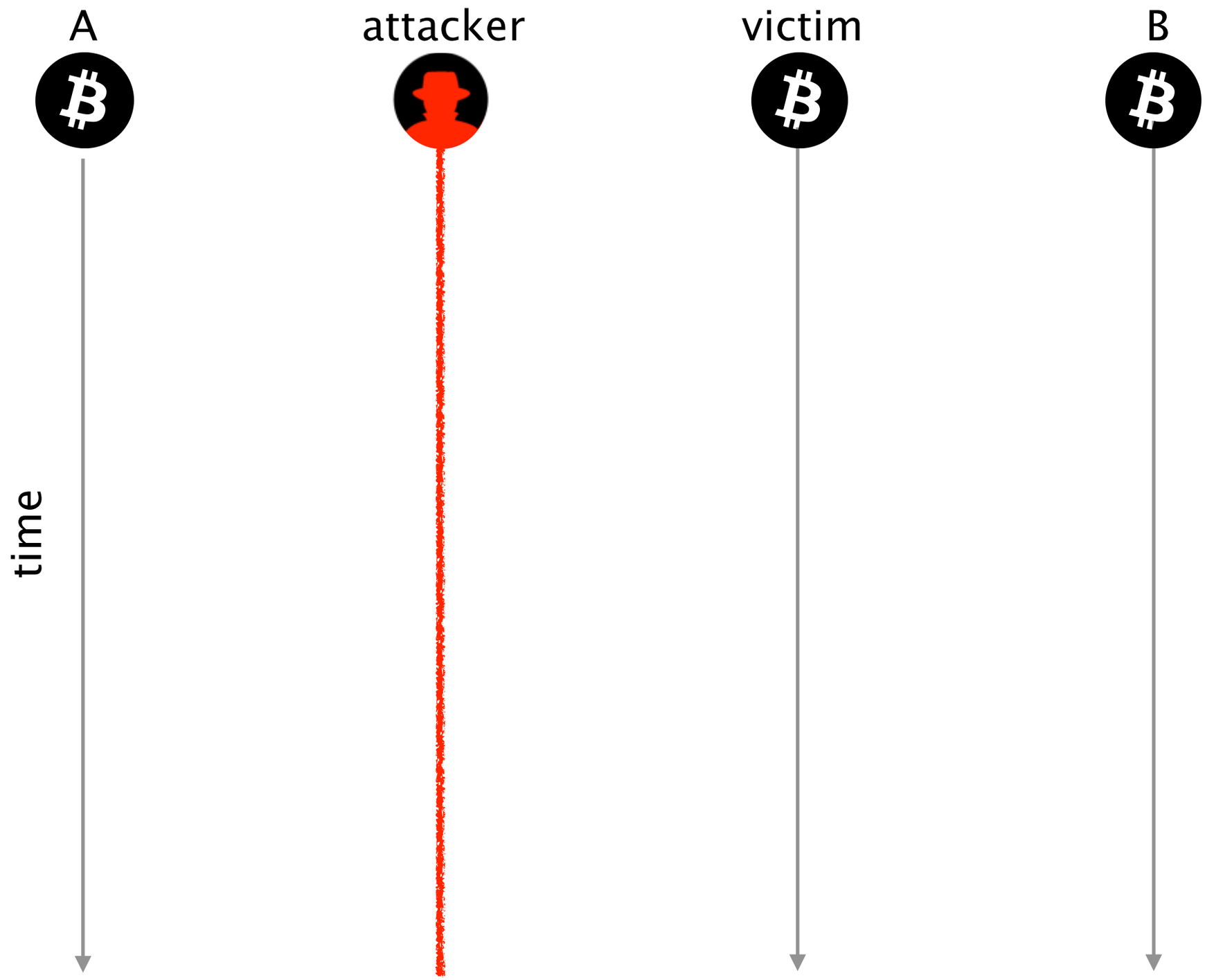
unable to collaborate to the peer-to-peer network

How does a delay attack work?

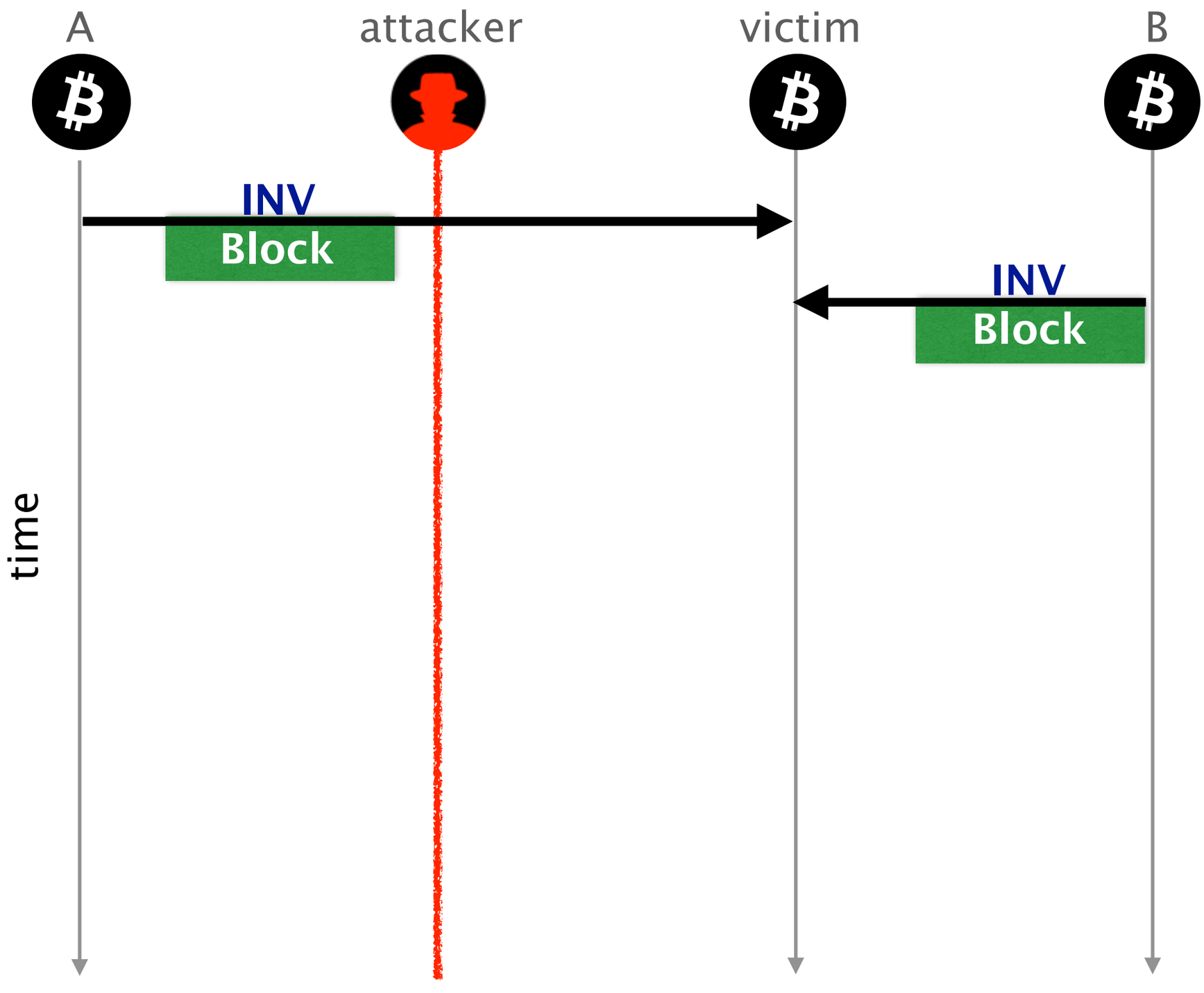
Consider these three Bitcoin nodes



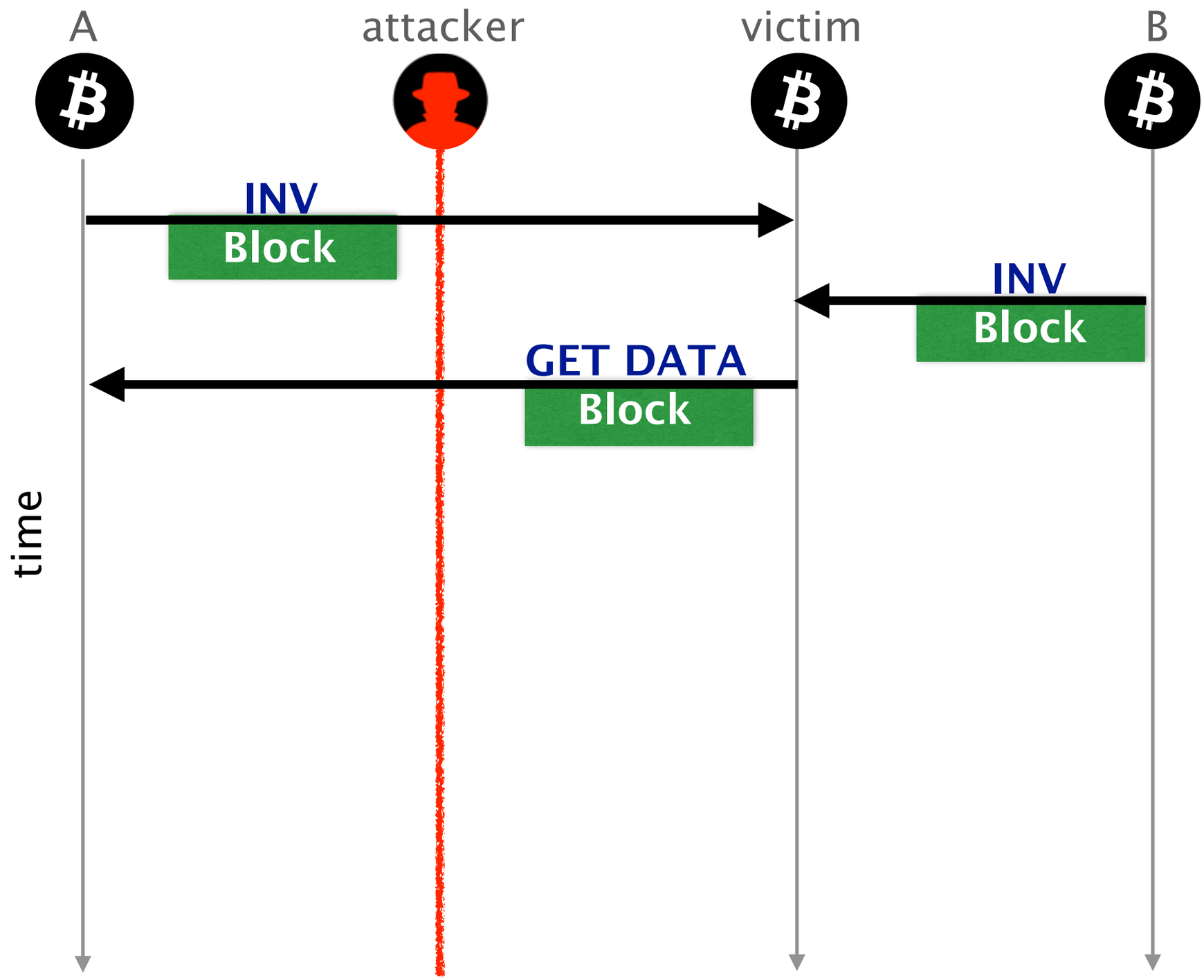
An attacker wishes to delay the block propagation towards the victim



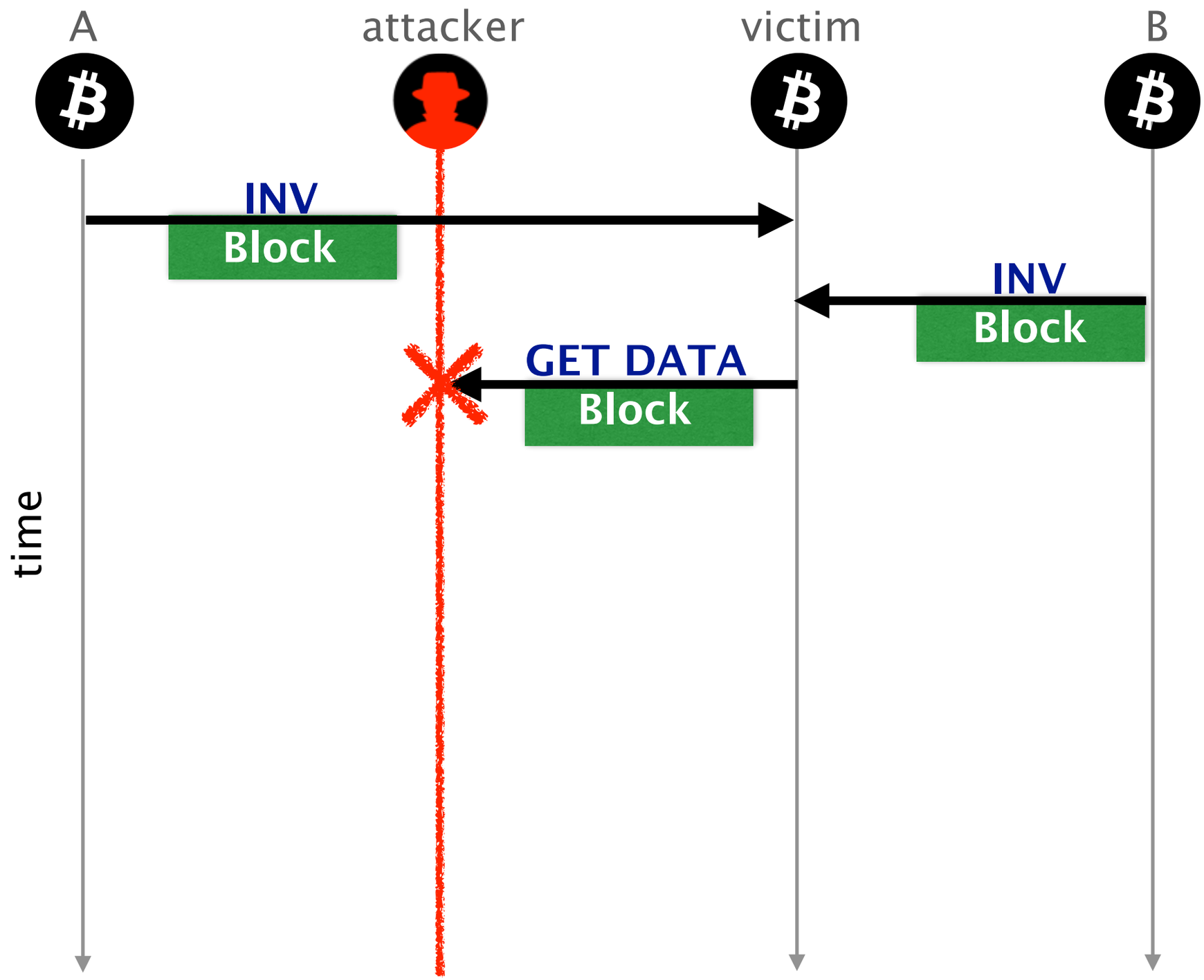
The victim receives two advertisement for the **block**



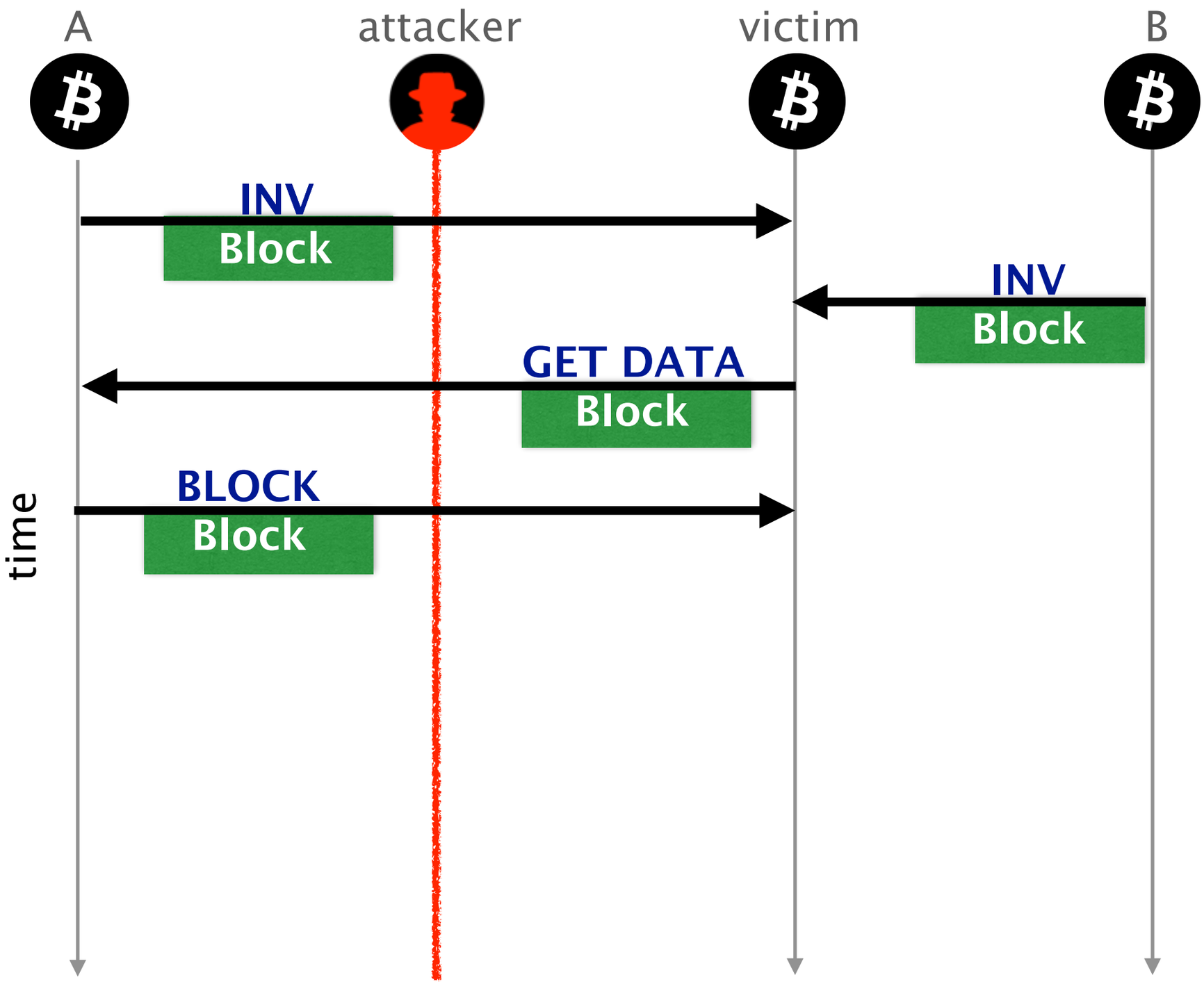
The victim requests the **block** to one of its peer, say A



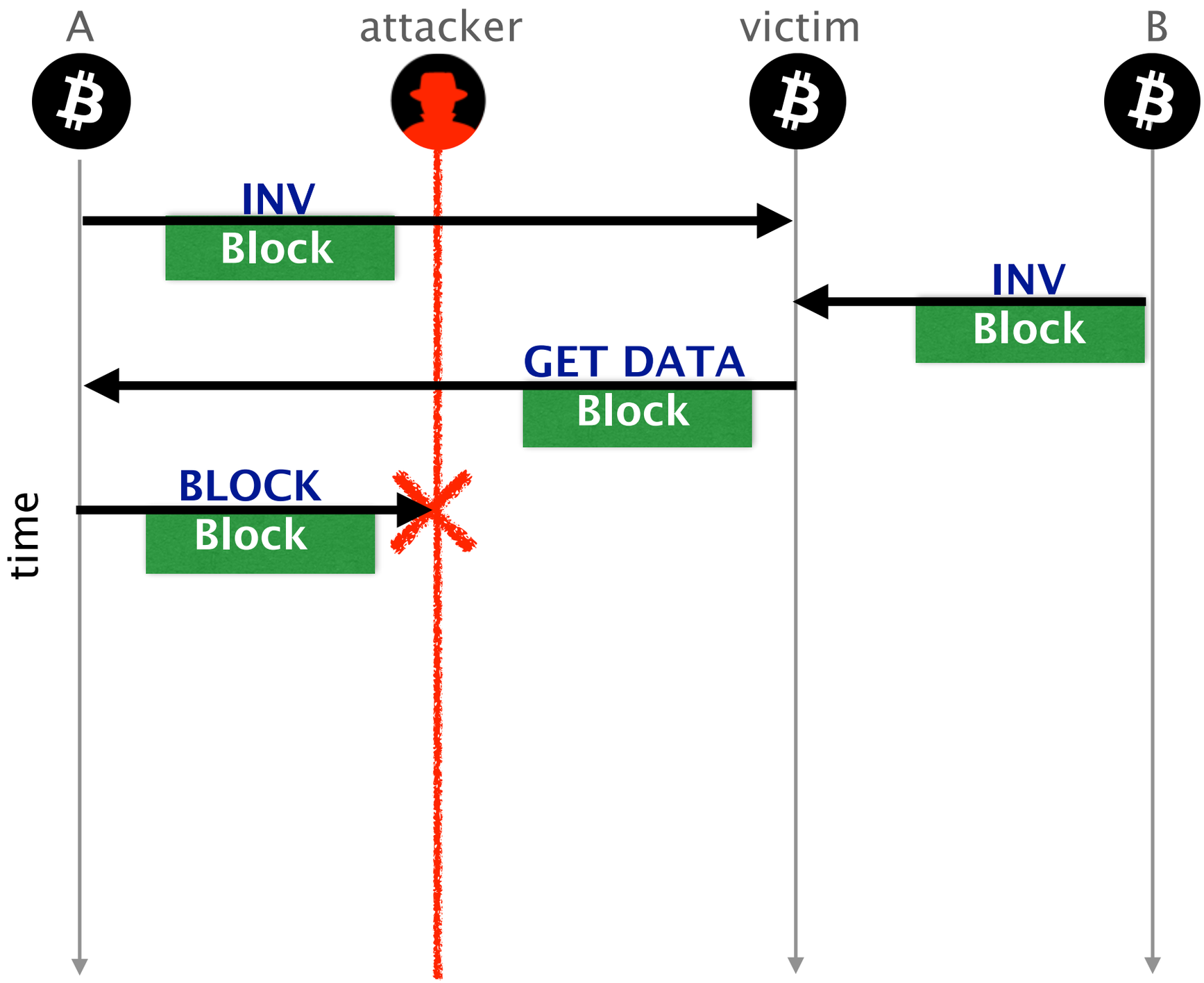
As a MITM, the attacker could drop the **GETDATA** message



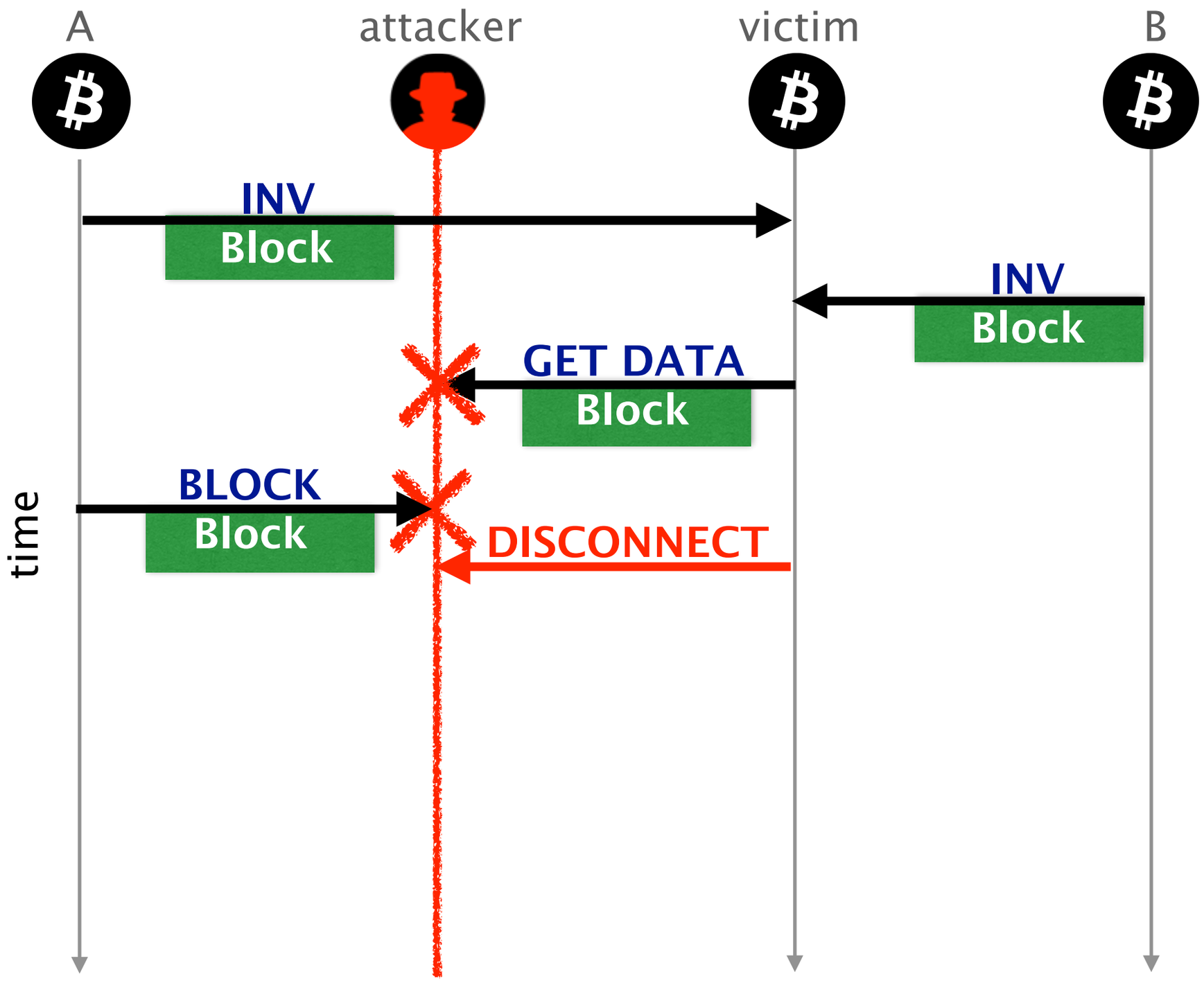
Similarly, the attacker could drop the delivery of the **block** message



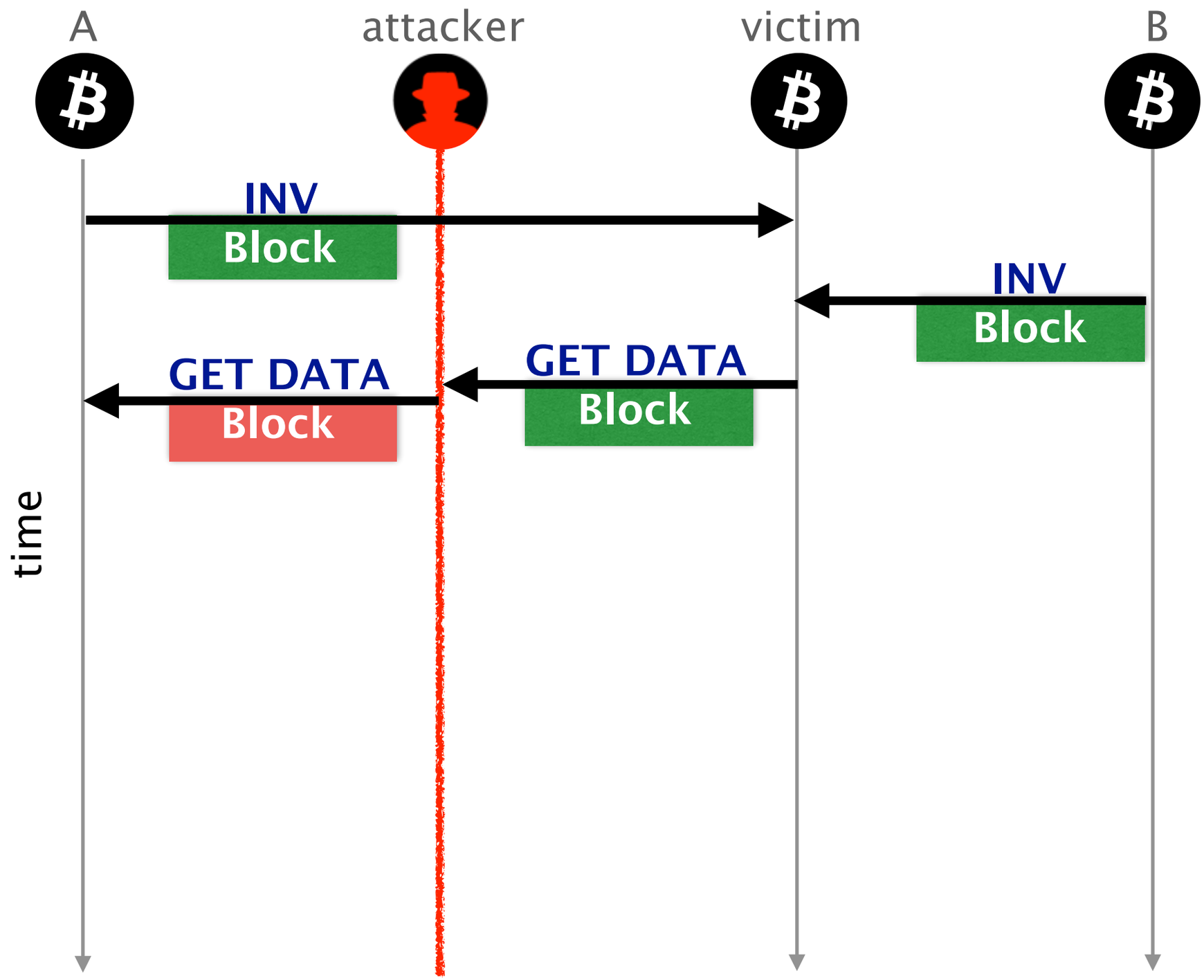
Similarly, the attacker could drop the delivery of the **block** message



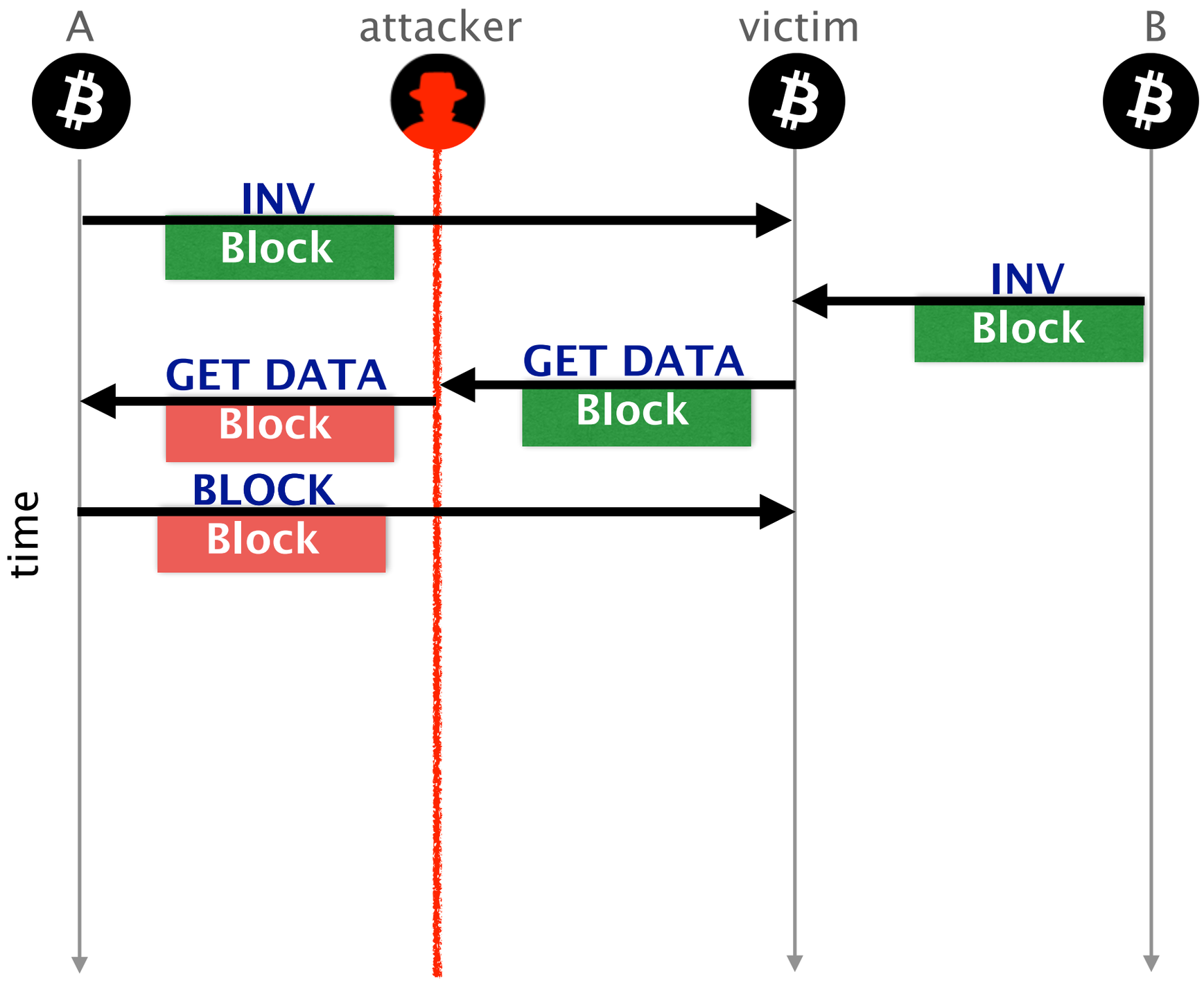
Yet, both cases will lead to the victim killing the connection (by the TCP stack on the victim)



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

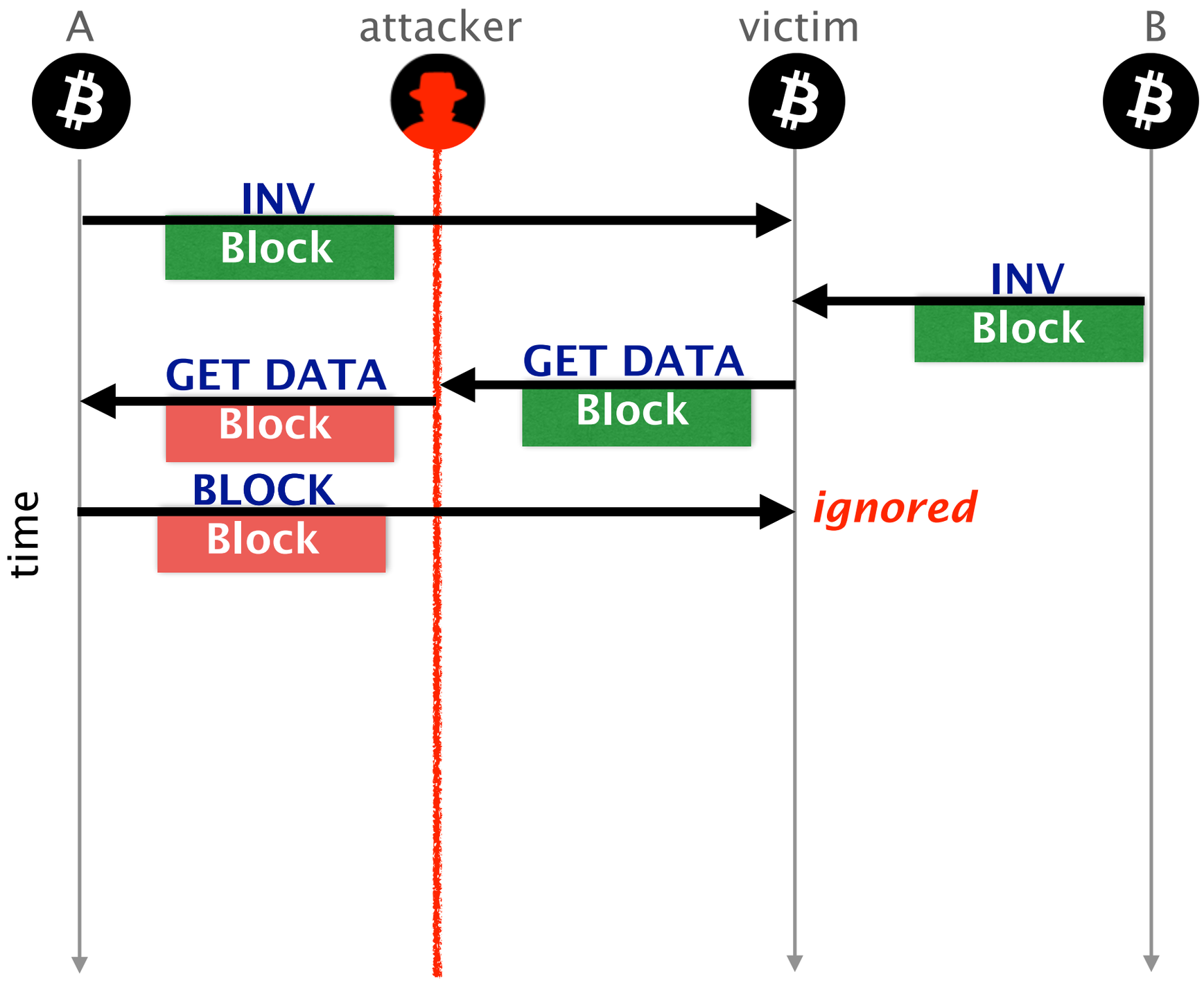


By modifying the ID of the requested block,
the attacker triggers the delivery of an older **block**

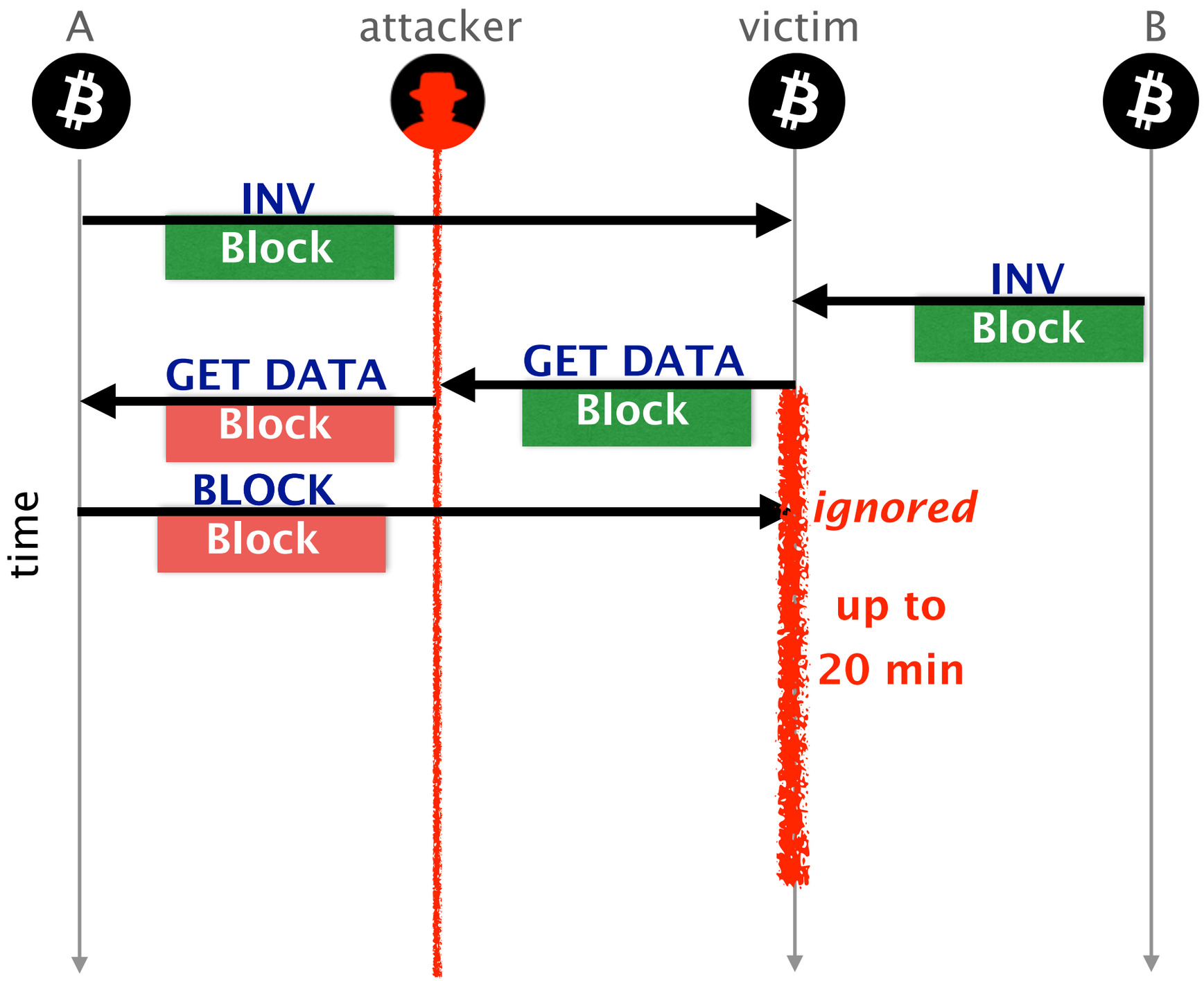


The delivery of an older block triggers

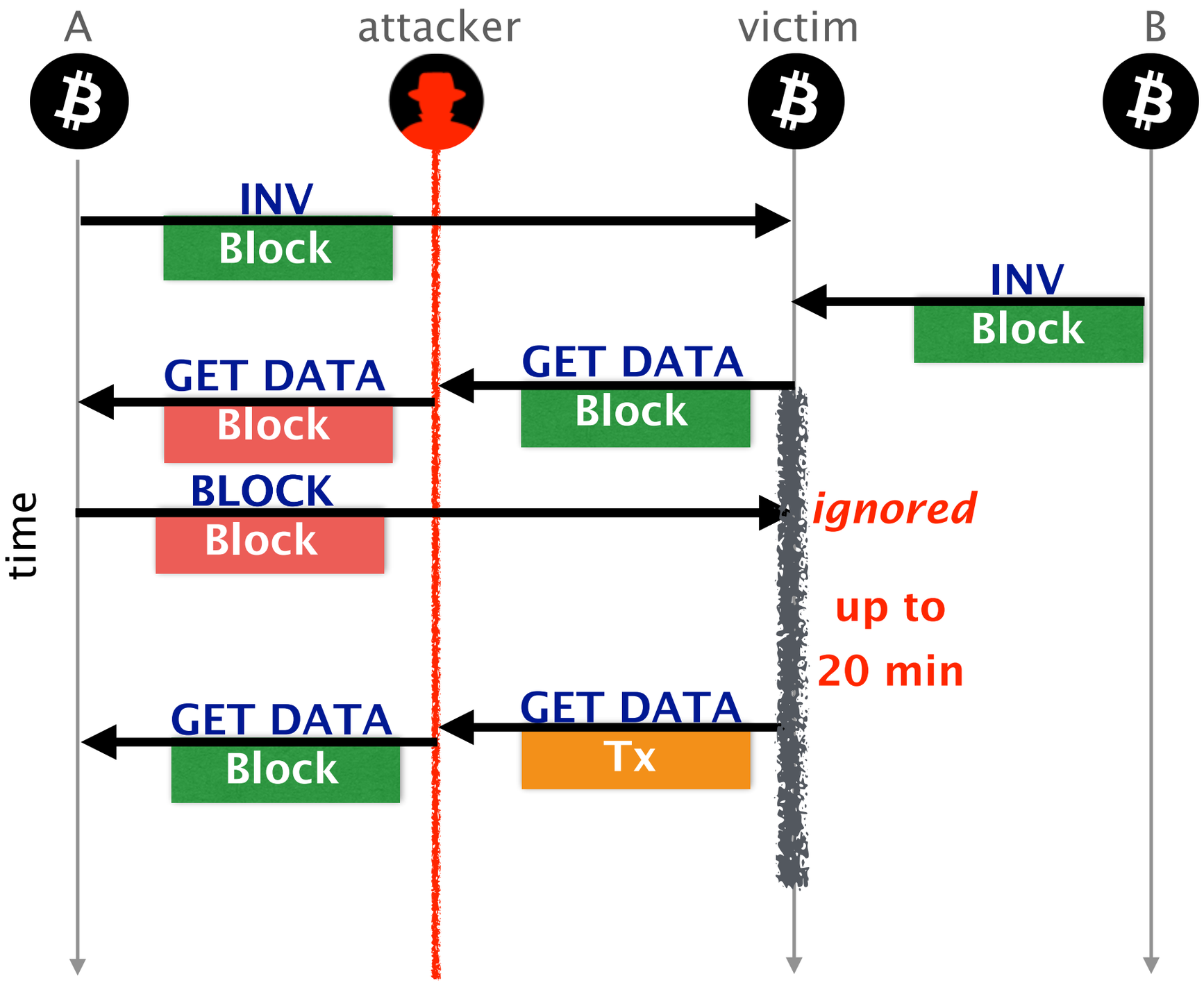
no error message at the victim



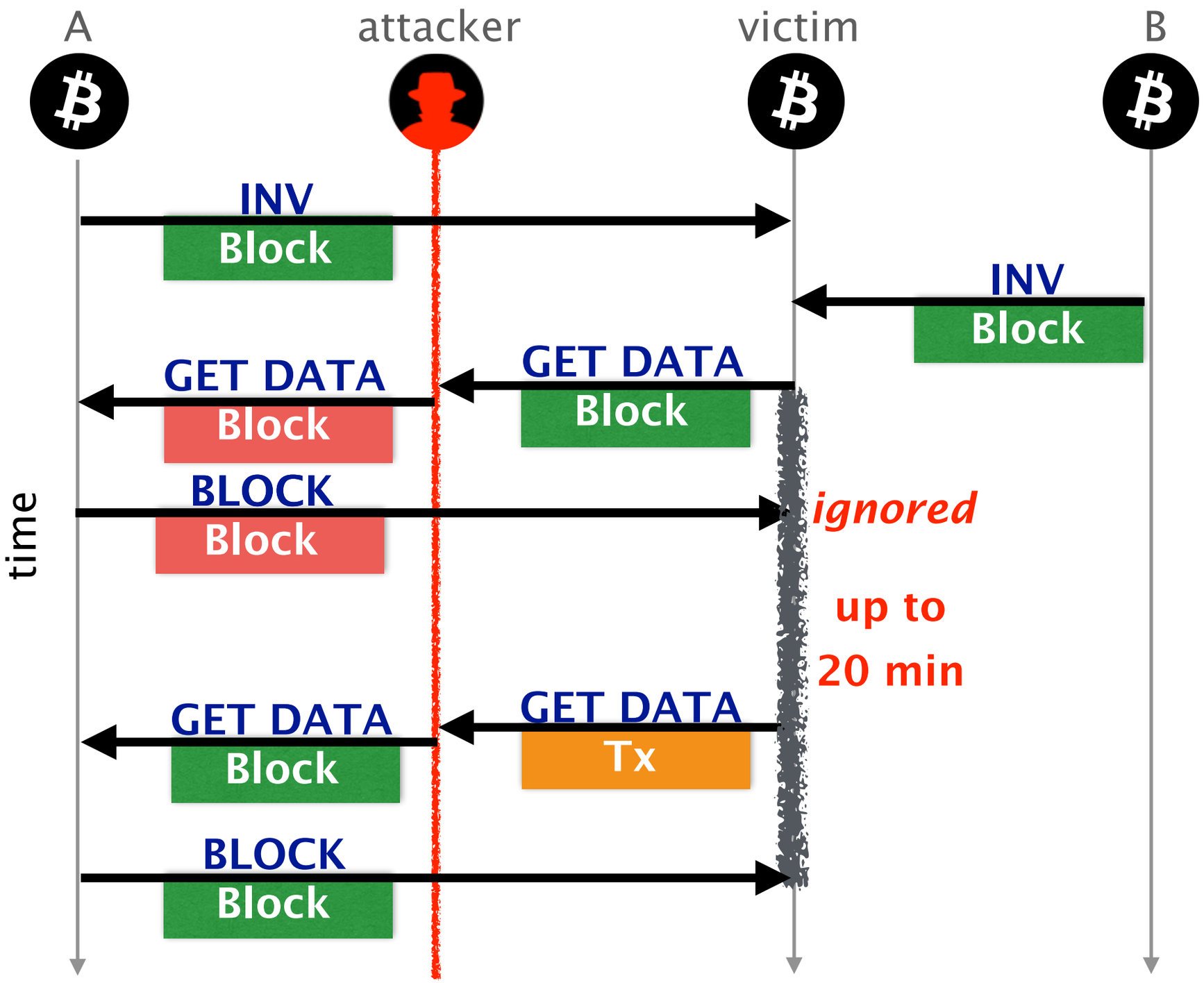
From there on, the victim will wait for 20 minutes for the actual block to be delivered



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

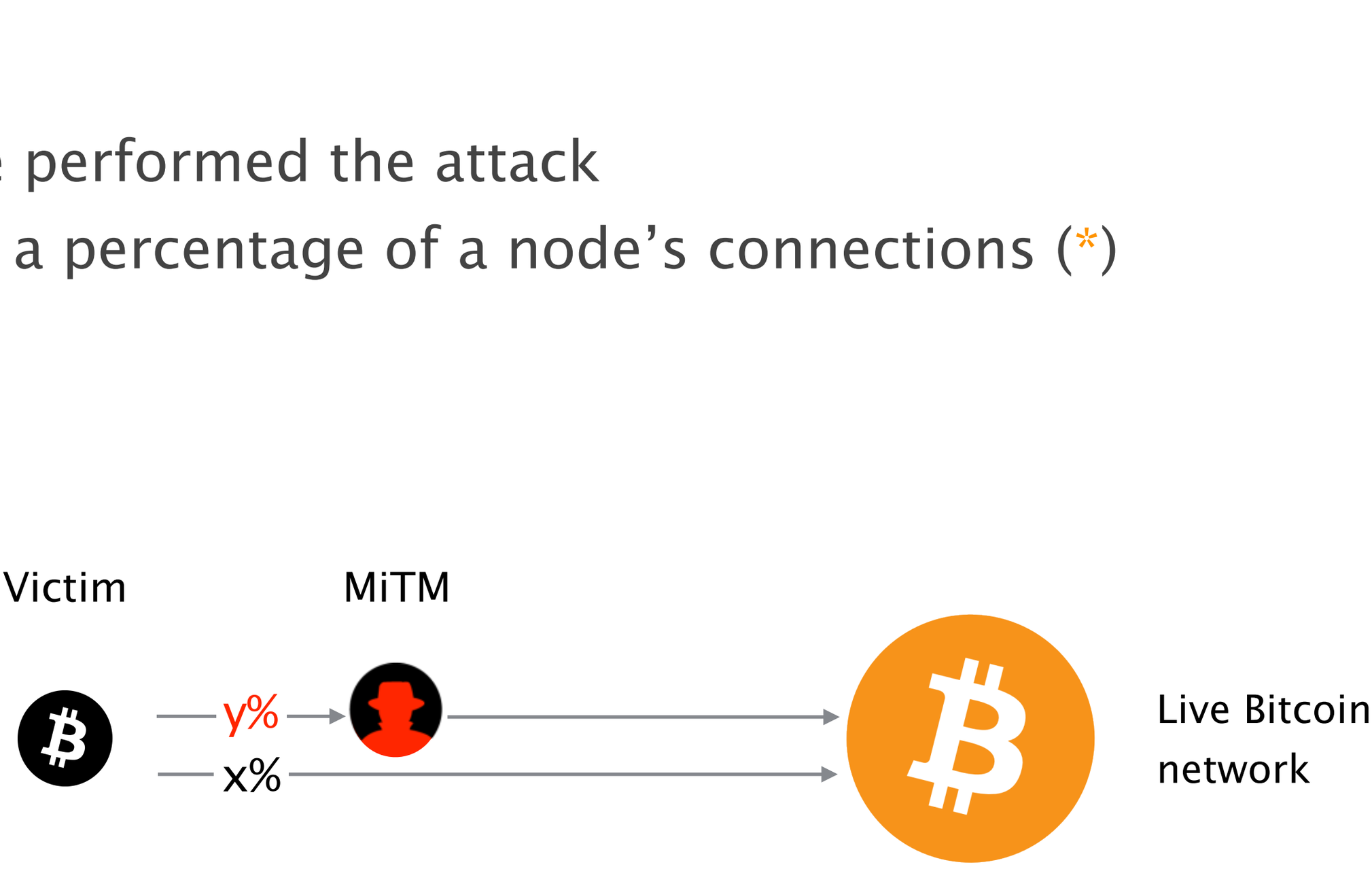
Effectiveness

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

实验结果表明，受害者在连接到网络的大部分时间都无法及时接收到最新块。

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

即便攻击者仅仅截获了一部分的节点连接

% intercepted connections	50%

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

The vast majority of the Bitcoin network is at risk

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

Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

Both sort-term and long-term countermeasures exist

Short-term countermeasures are simple shifts in the Bitcoin clients

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

Maria Apostolaki

ETH Zürich

IEEE Security & Privacy

23 May 2017

Visit our website: **https://btc-hijack.ethz.ch**

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

Visit our website: **https://btc-hijack.ethz.ch**