Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

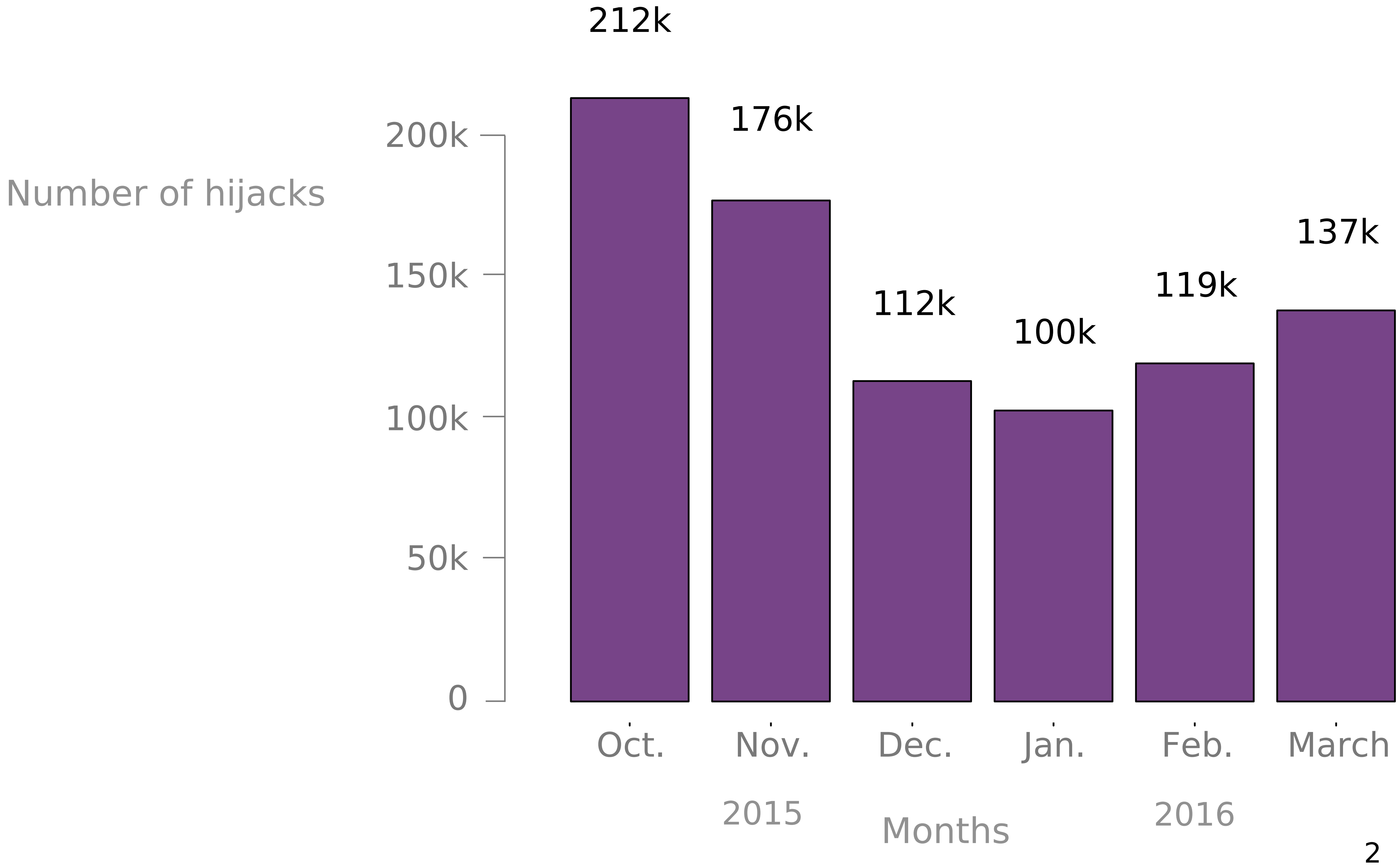
UNIVERSITÄT BERN

Hichem Belhocine

Bern Universität

19 March 2019

Lecturer: Prof. Dr. Christian Cachin


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

Can routing attacks impact Bitcoin?

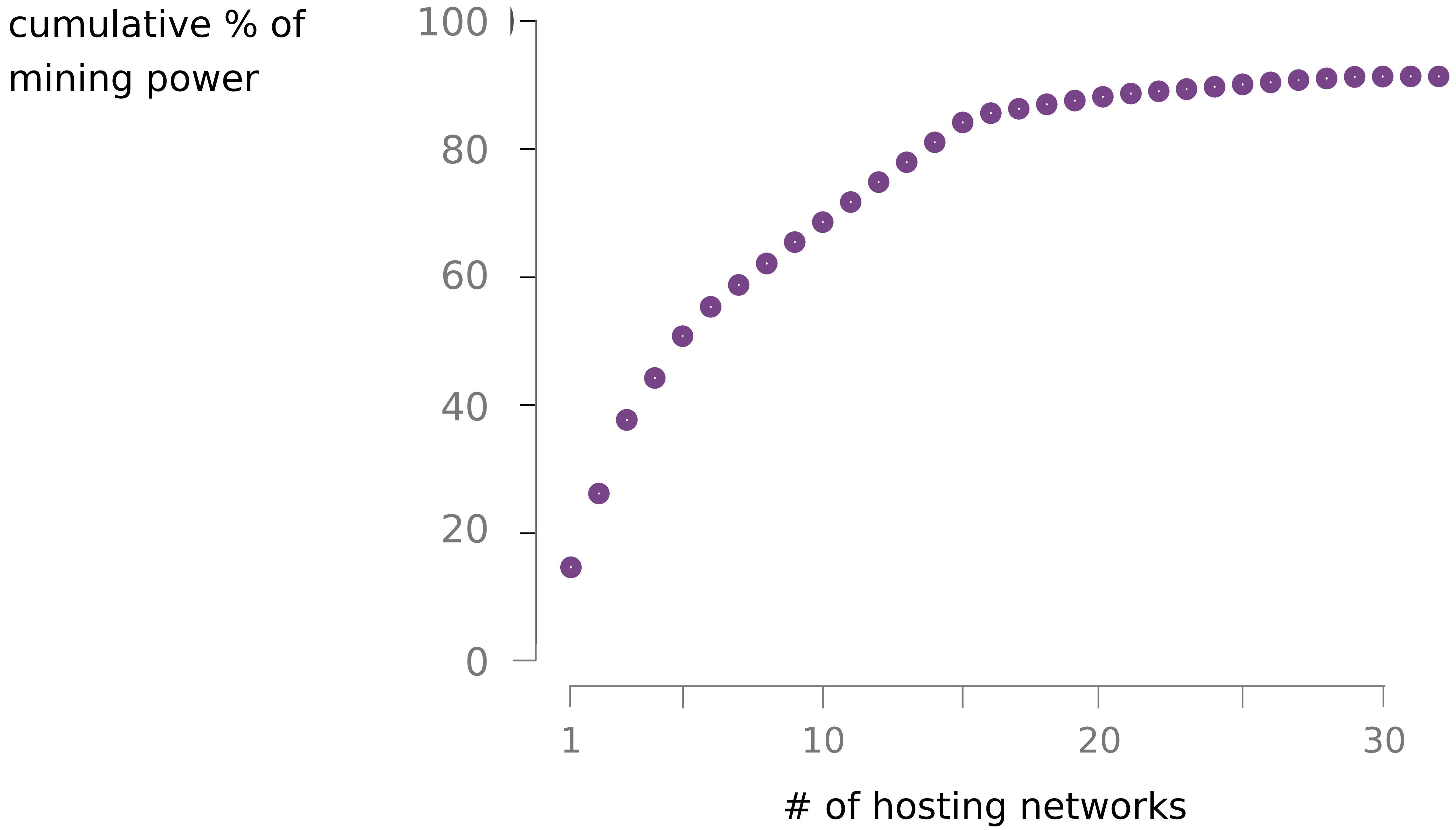
Bitcoin should be robust against routing attacks
Bitcoin is highly decentralized network of nodes

Bitcoin nodes …

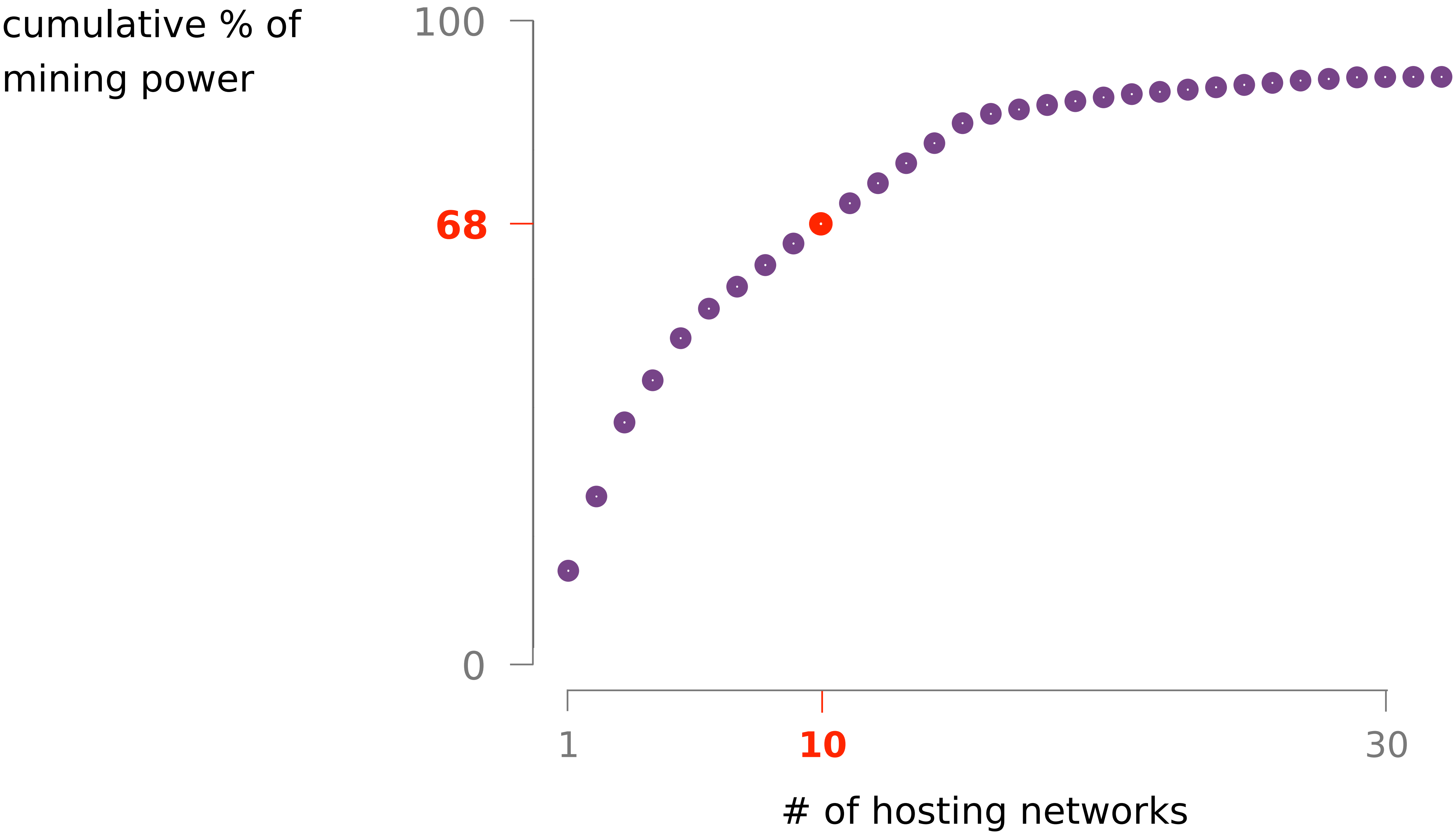
- are scattered all around the globe
- establish random connections
- use multihoming and additional overlay networks

Bitcoin is highly centralized from both routing and mining viewpoint

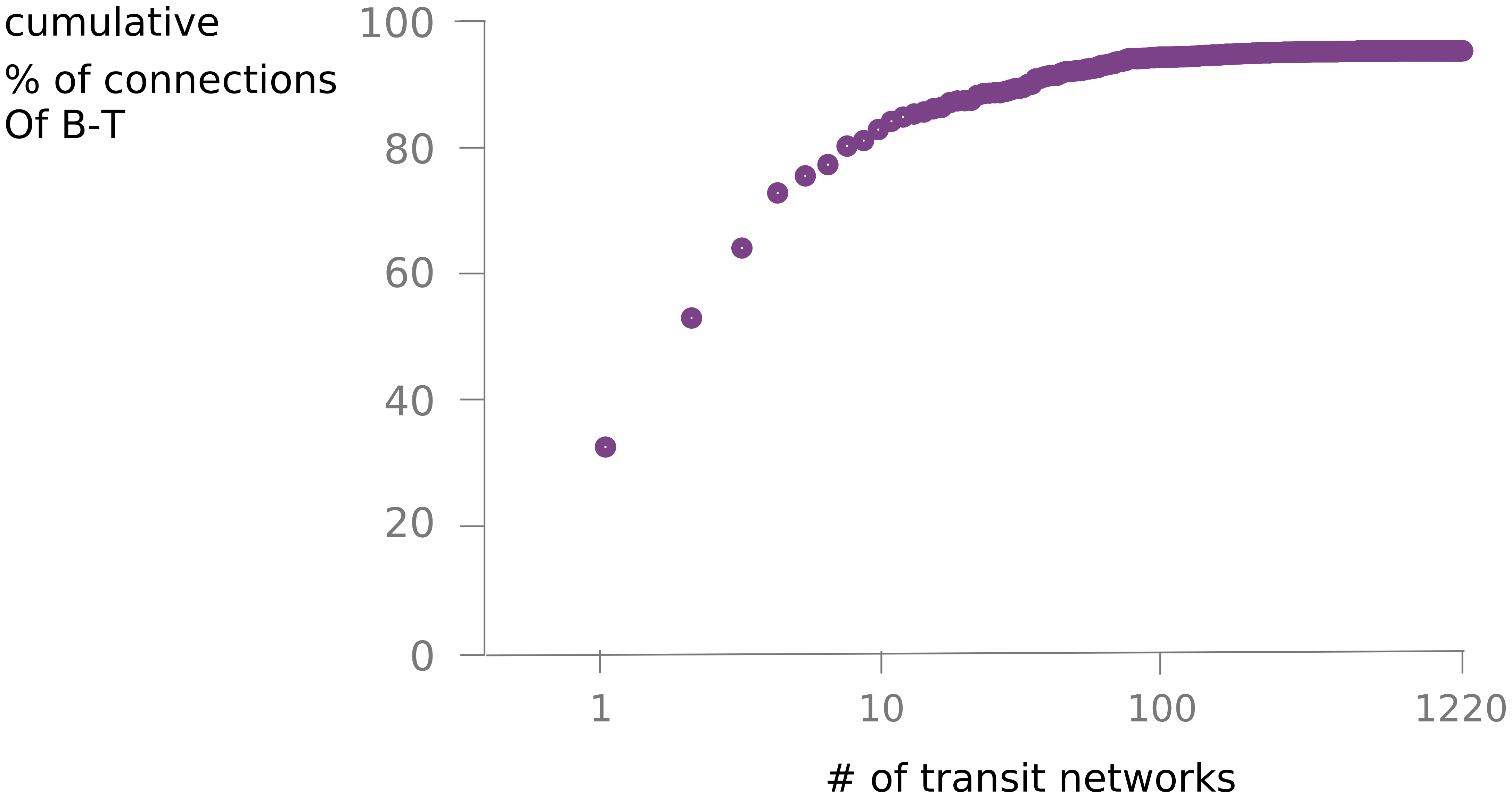
Mining power is centralized to few hosting networks



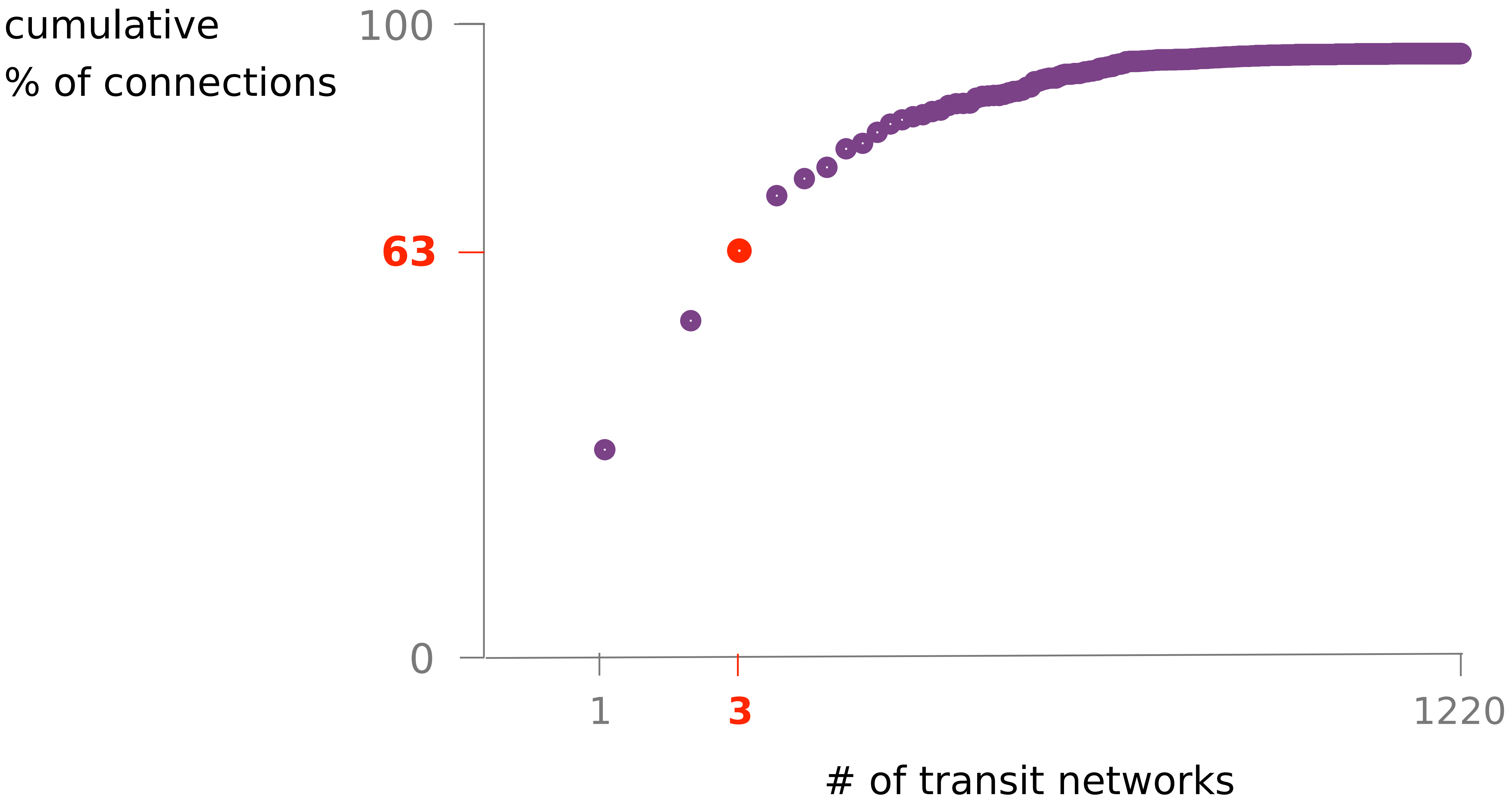
68% of the mining power is only hosted in 10 networks



Few transit networks can intercept a large fraction of the Bitcoin connections



63% of Bitcoin traffic is only intercepted by 3 networks



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

Partitioning

visible

network-wide attack

Attack 2

Delay

invisible

targeted attack (set of nodes)

Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

1 **Background**

BGP and Bitcoin

Partitioning attack

splitting the network

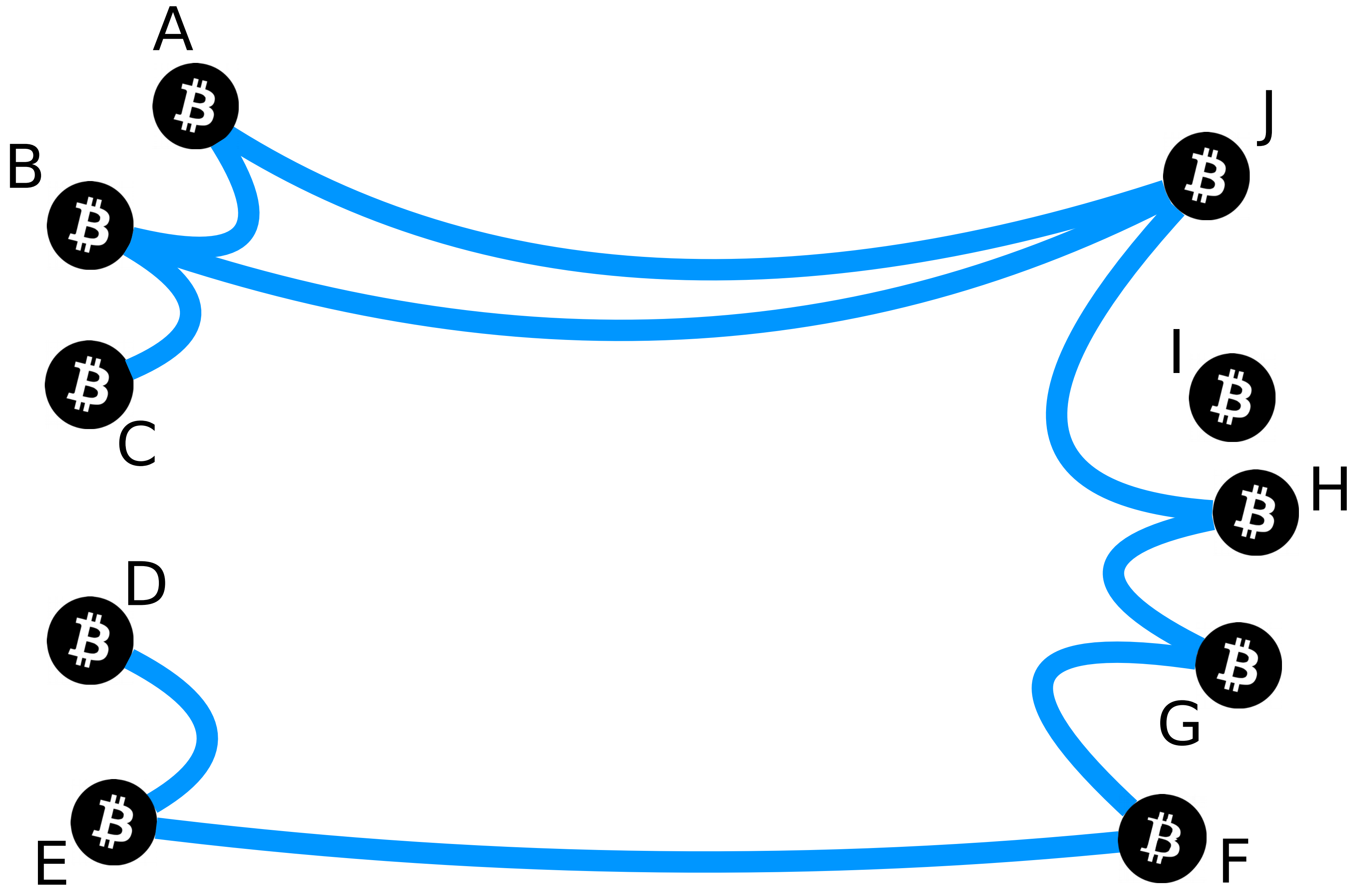
Delay attack

slowing the network down

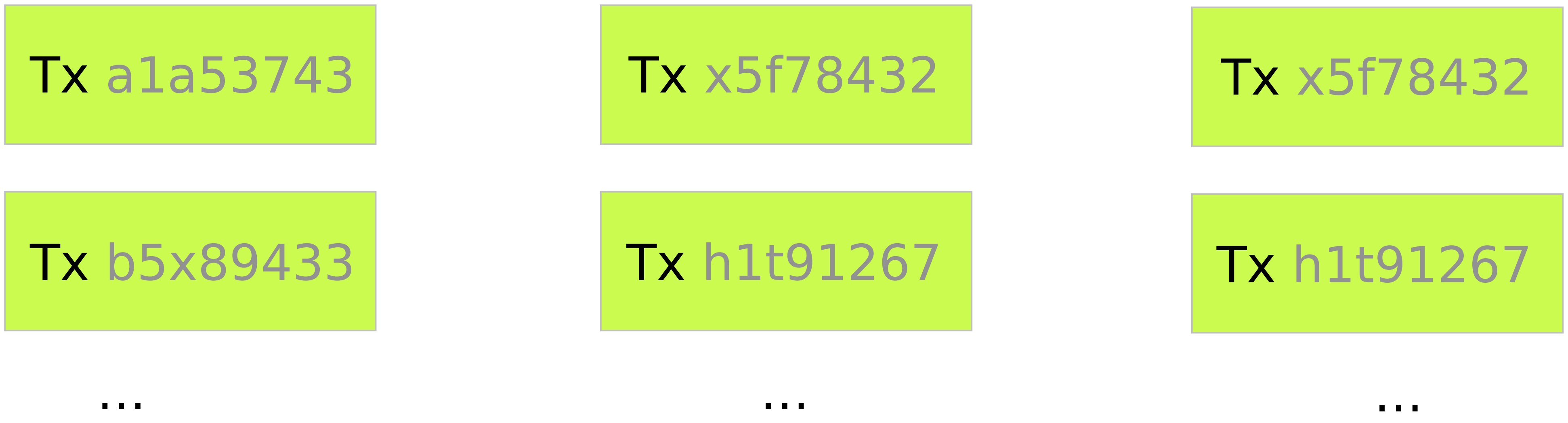
Countermeasures

short-term and long-term

Bitcoin is a distributed network of 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

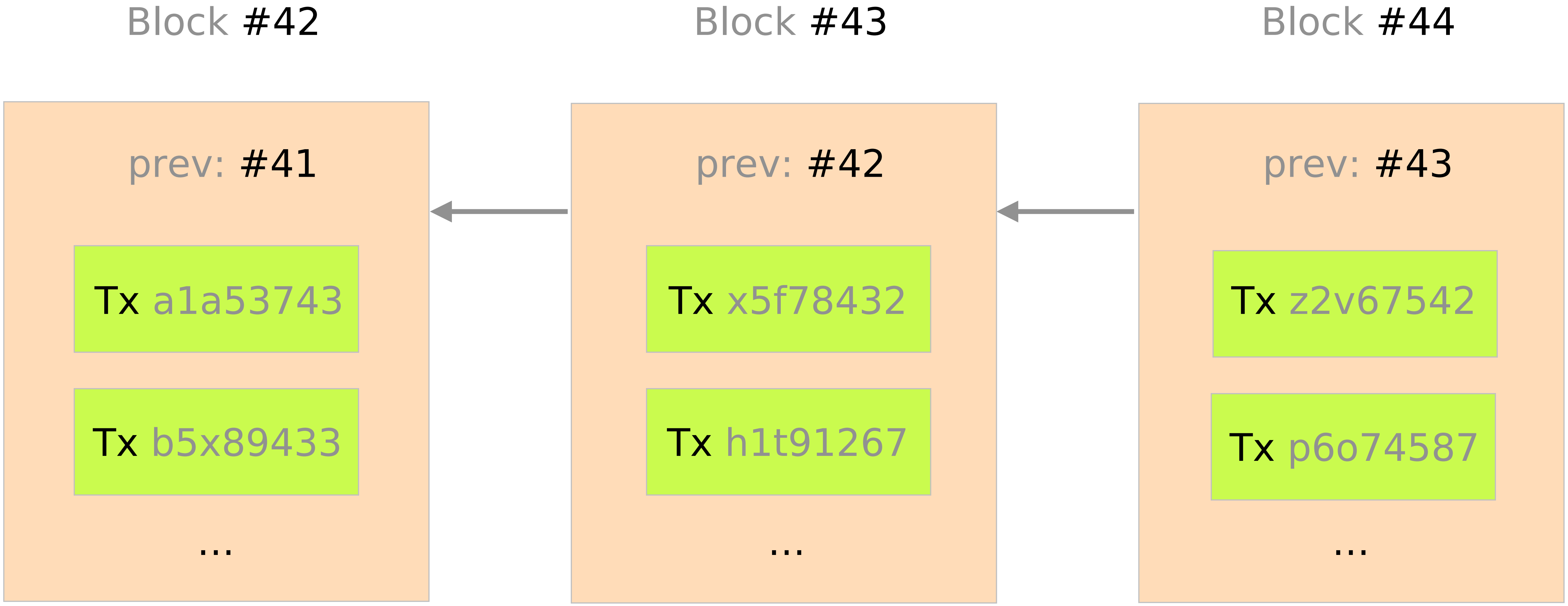
…

Tx x5f78432

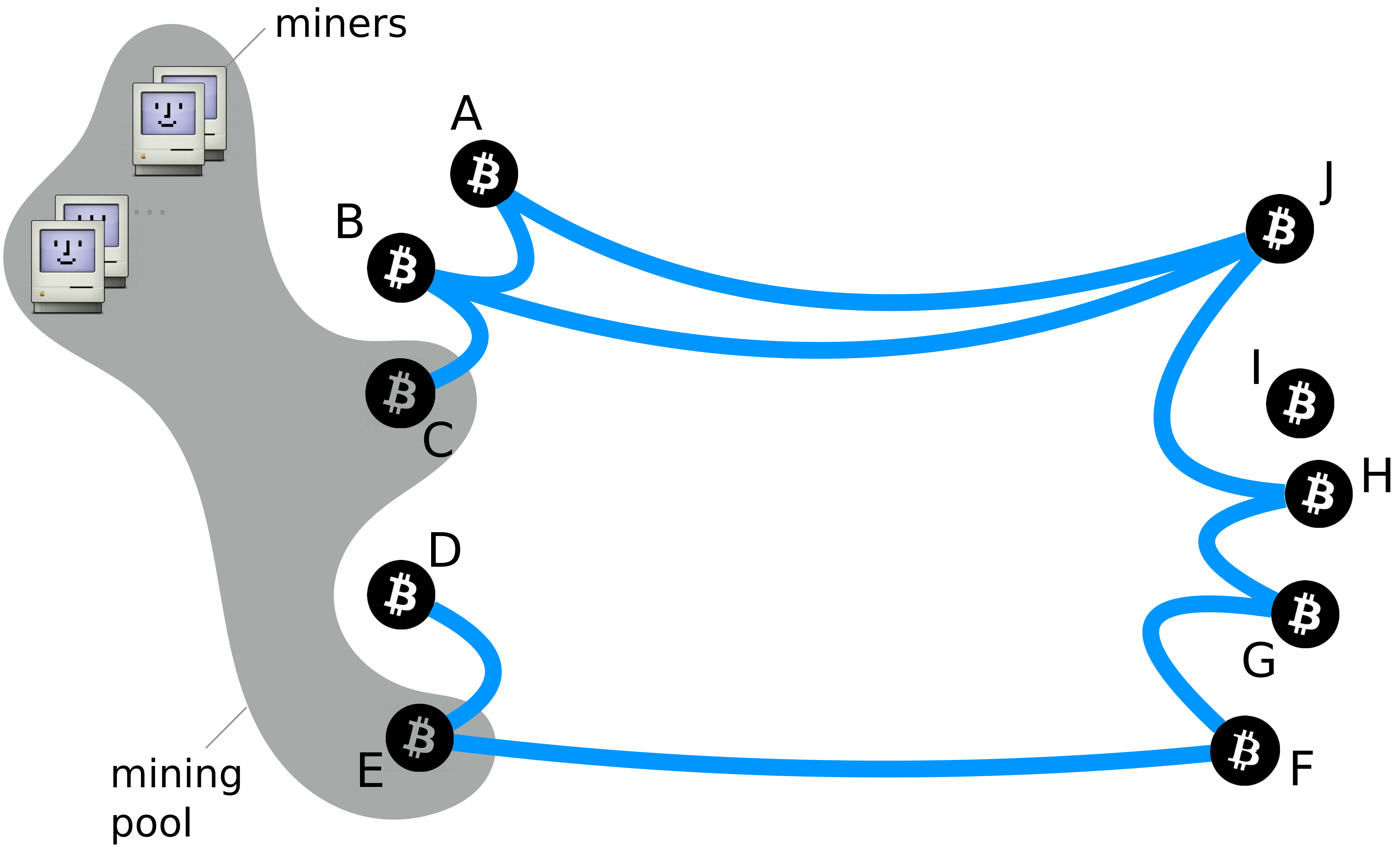
Tx h1t91267

…

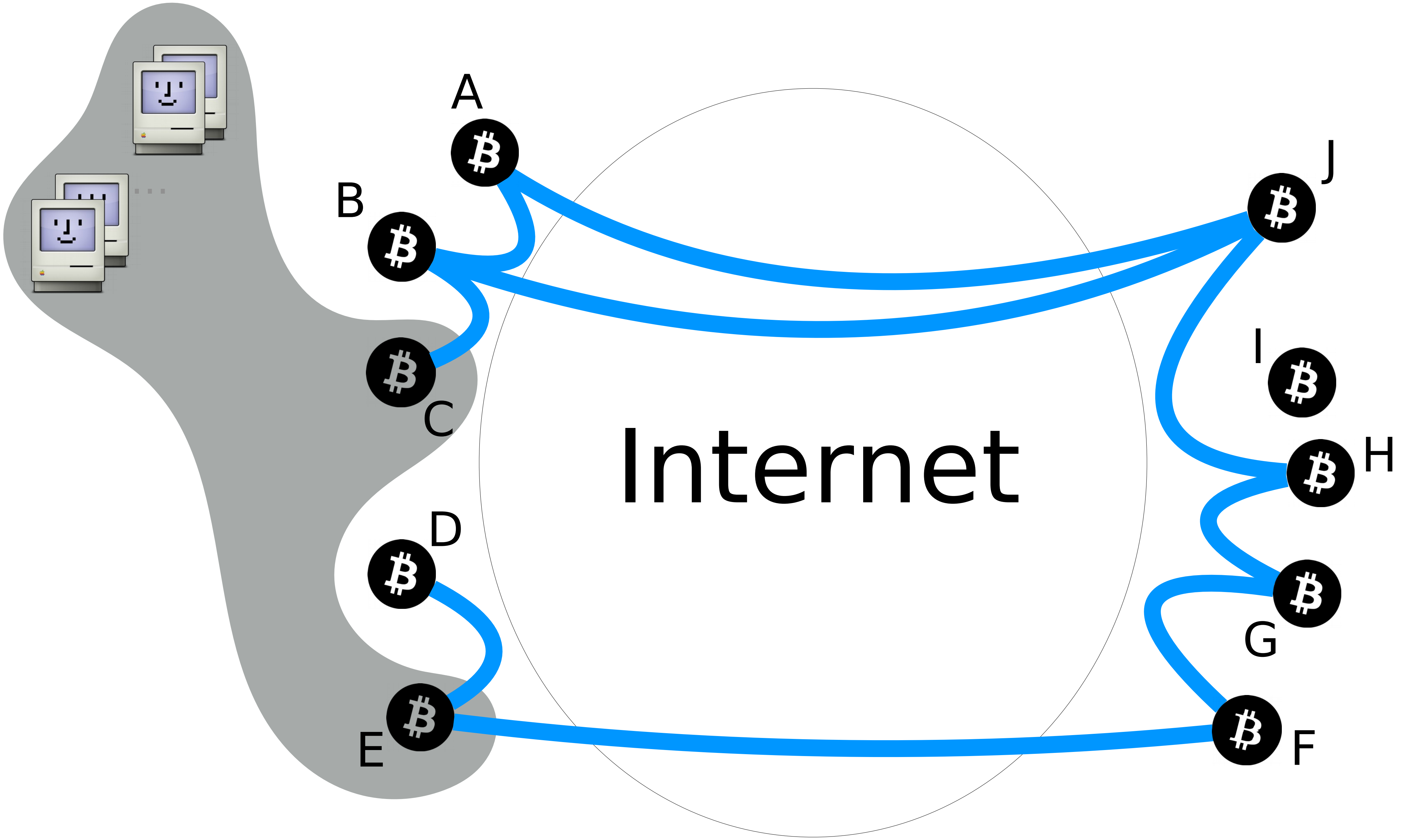
The Blockchain is a chain of Blocks
The Blockchain is extended by miners



Miners collaborate forming mining pools

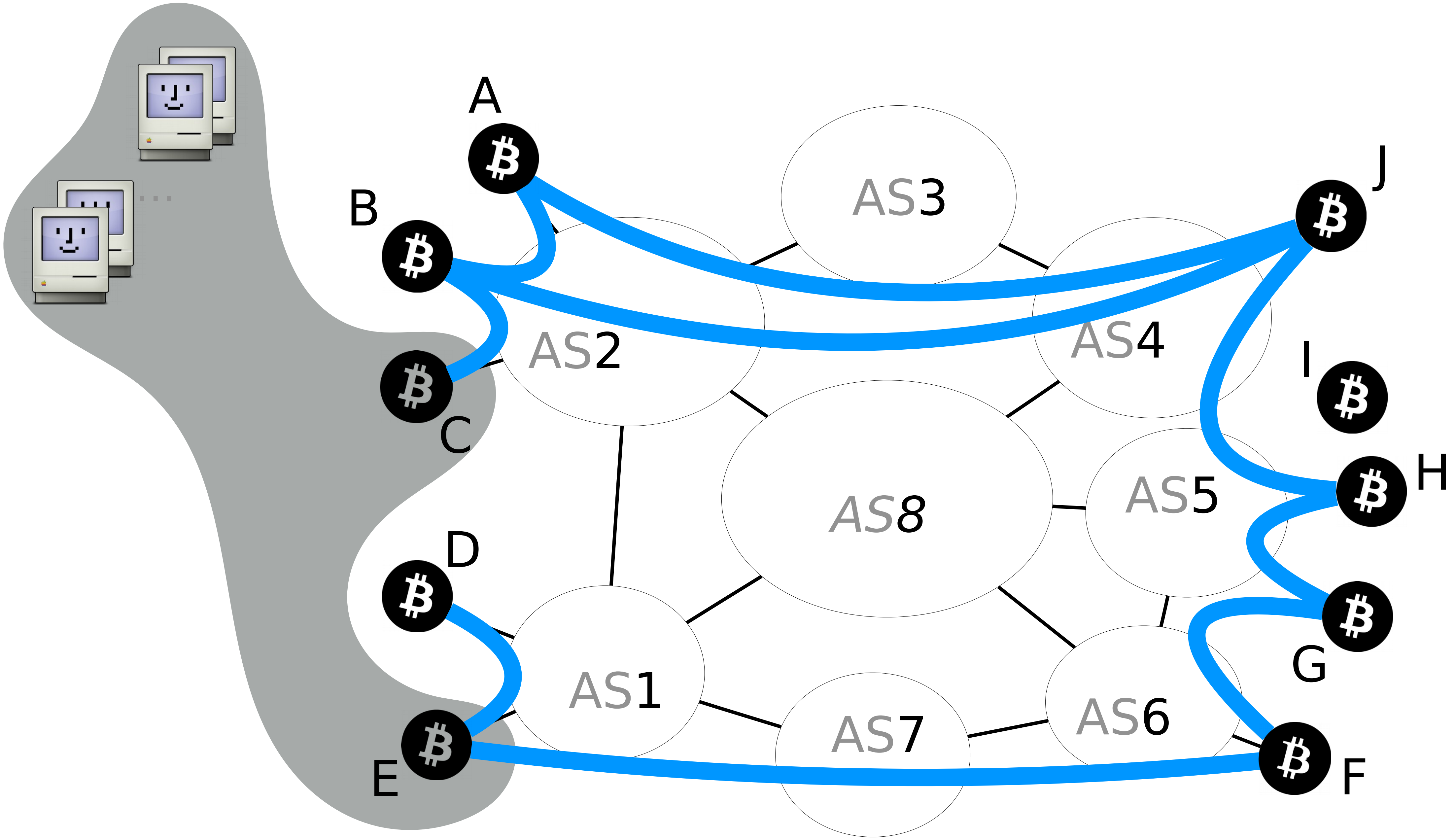


Bitcoin connections are routed over the Internet

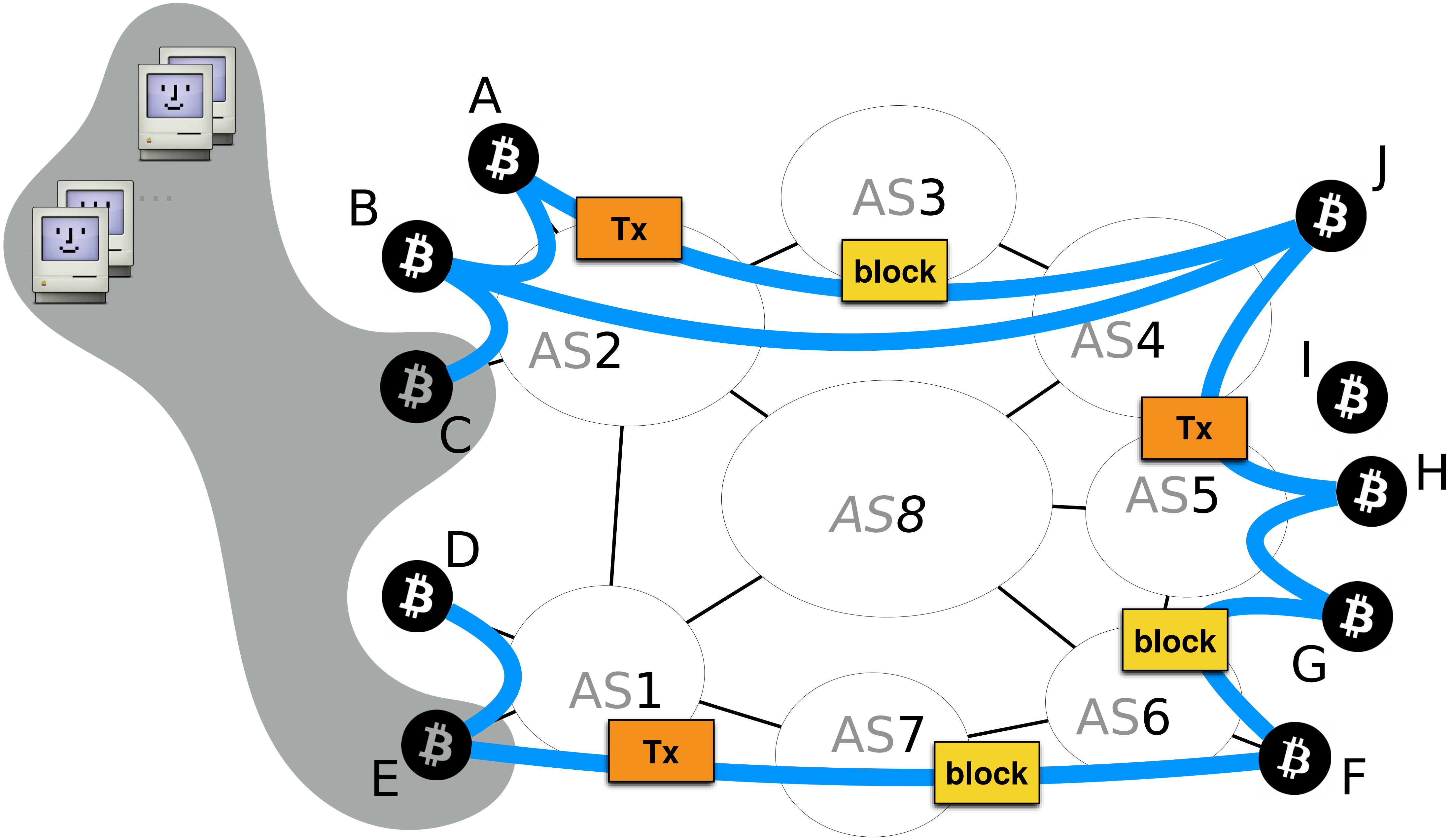


The Internet is composed of Autonomous Systems (ASes)

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 and Bitcoin

2 Partitioning attack

splitting the network

Delay attack

slowing the network down

Countermeasures

short-term and 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 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

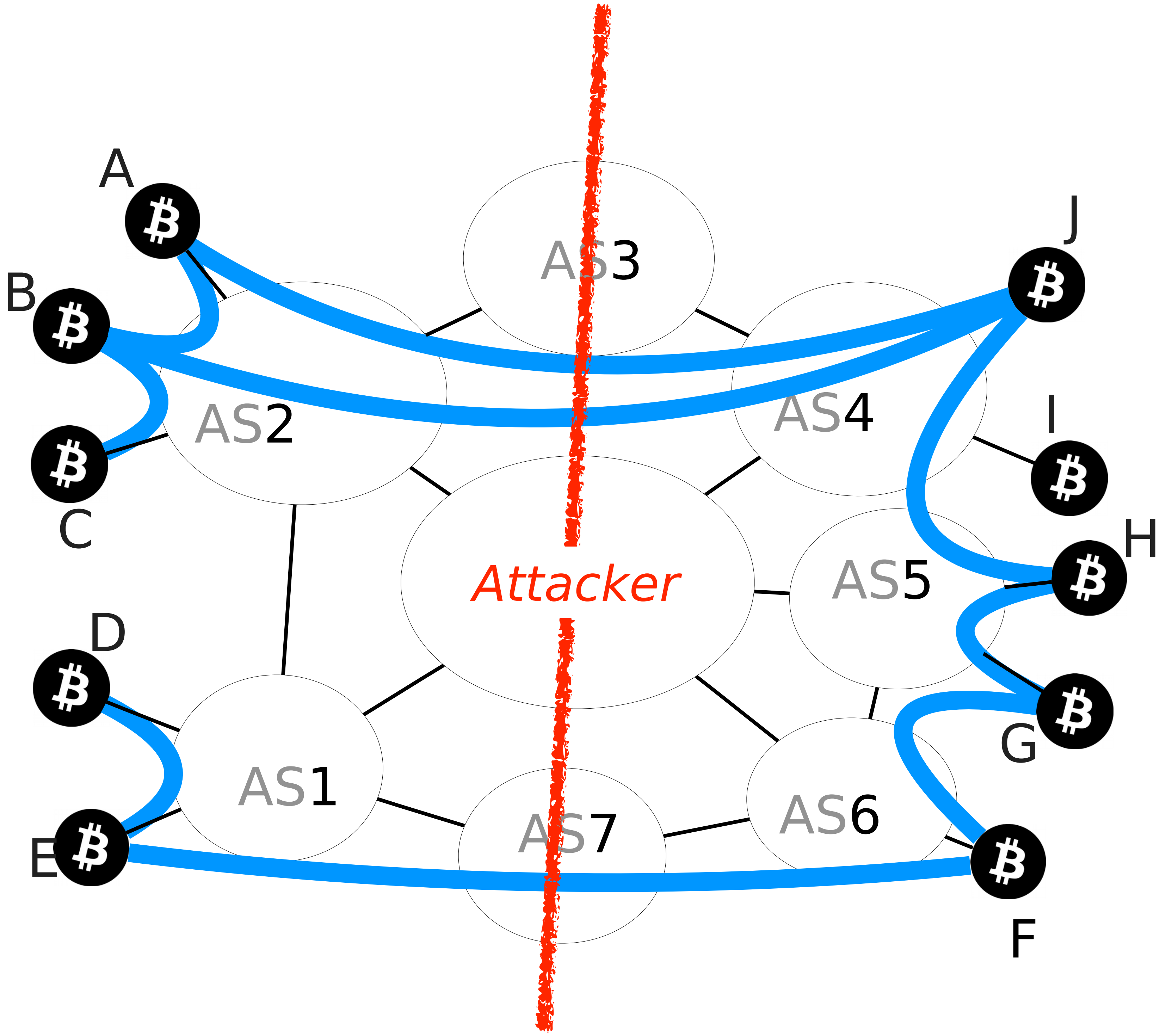
Revenue Loss

Double spending

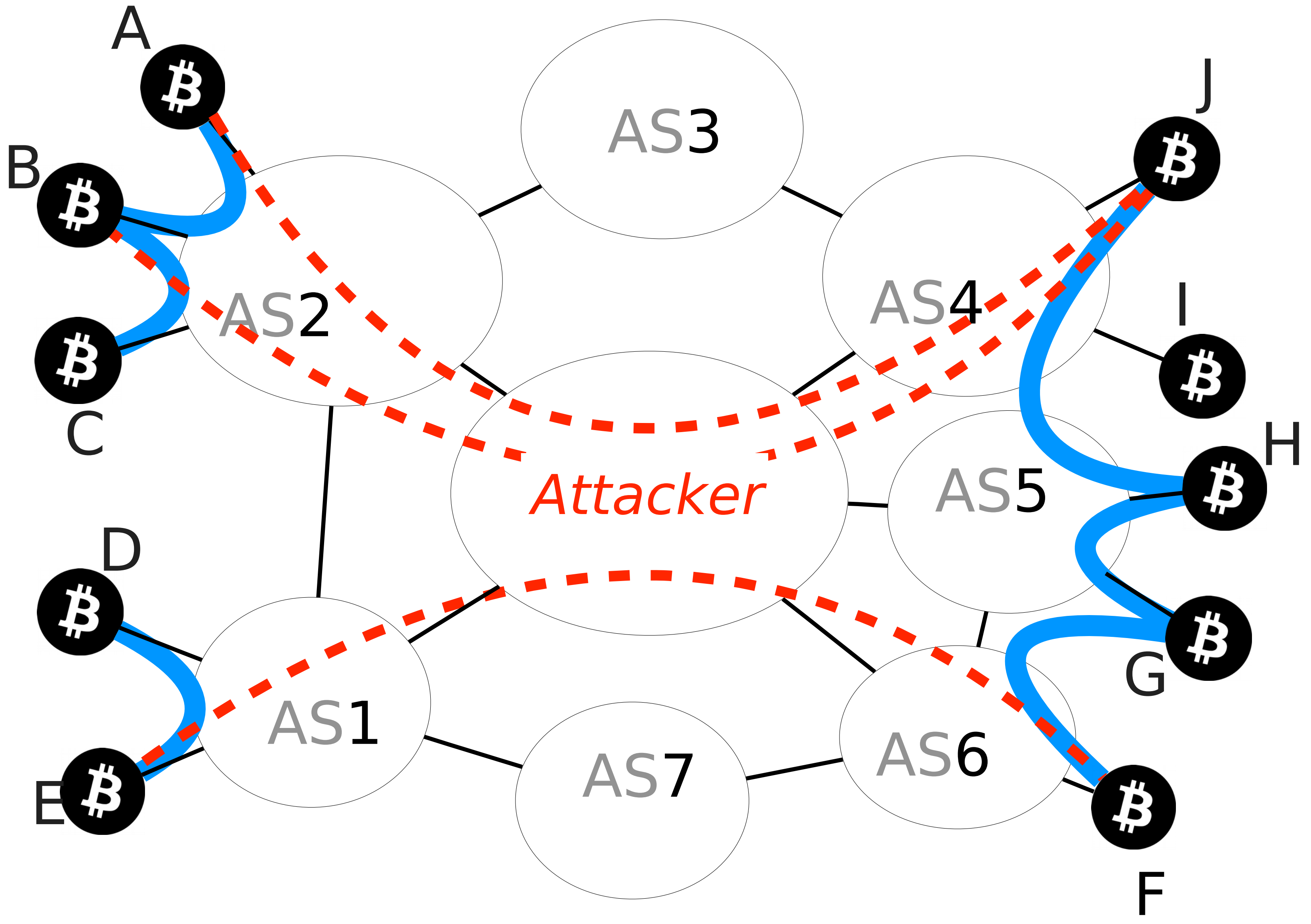
Transactions in components with less mining power can be reverted

How does the attack work?

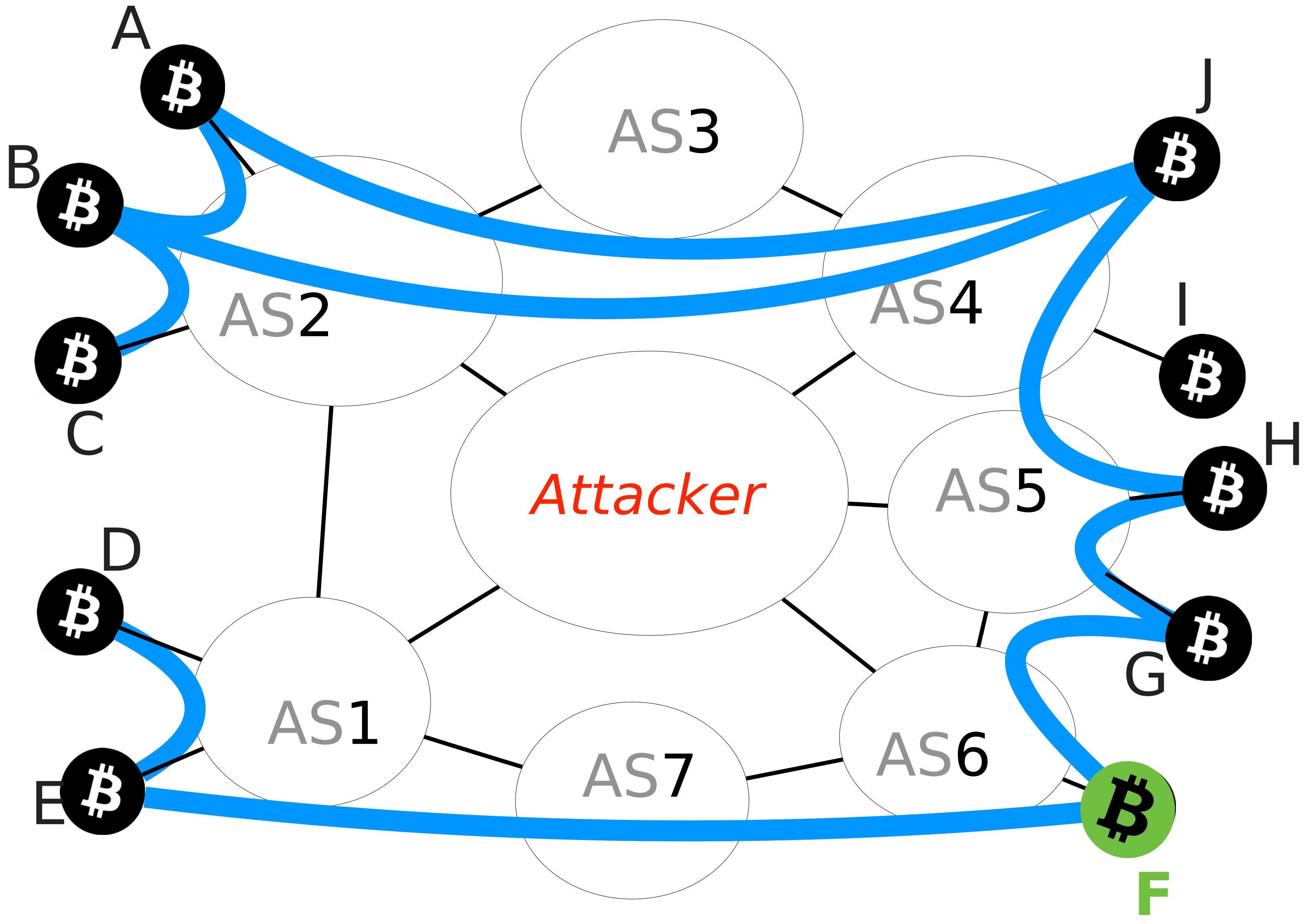
Let’s say an attacker wants to partition the network into the left and right side



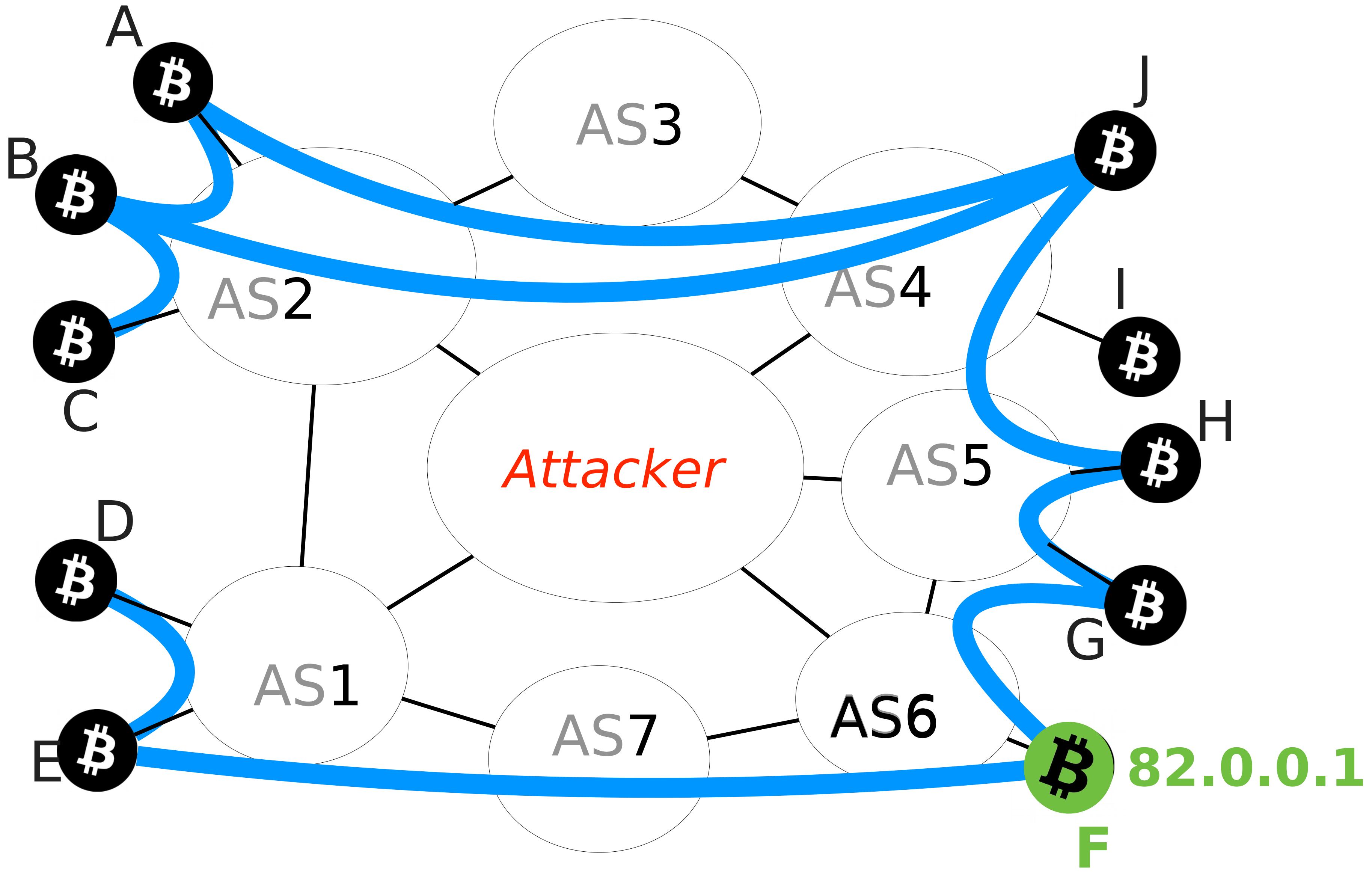
For doing so, the attacker will manipulate BGP routes to intercept any traffic to the nodes in the right



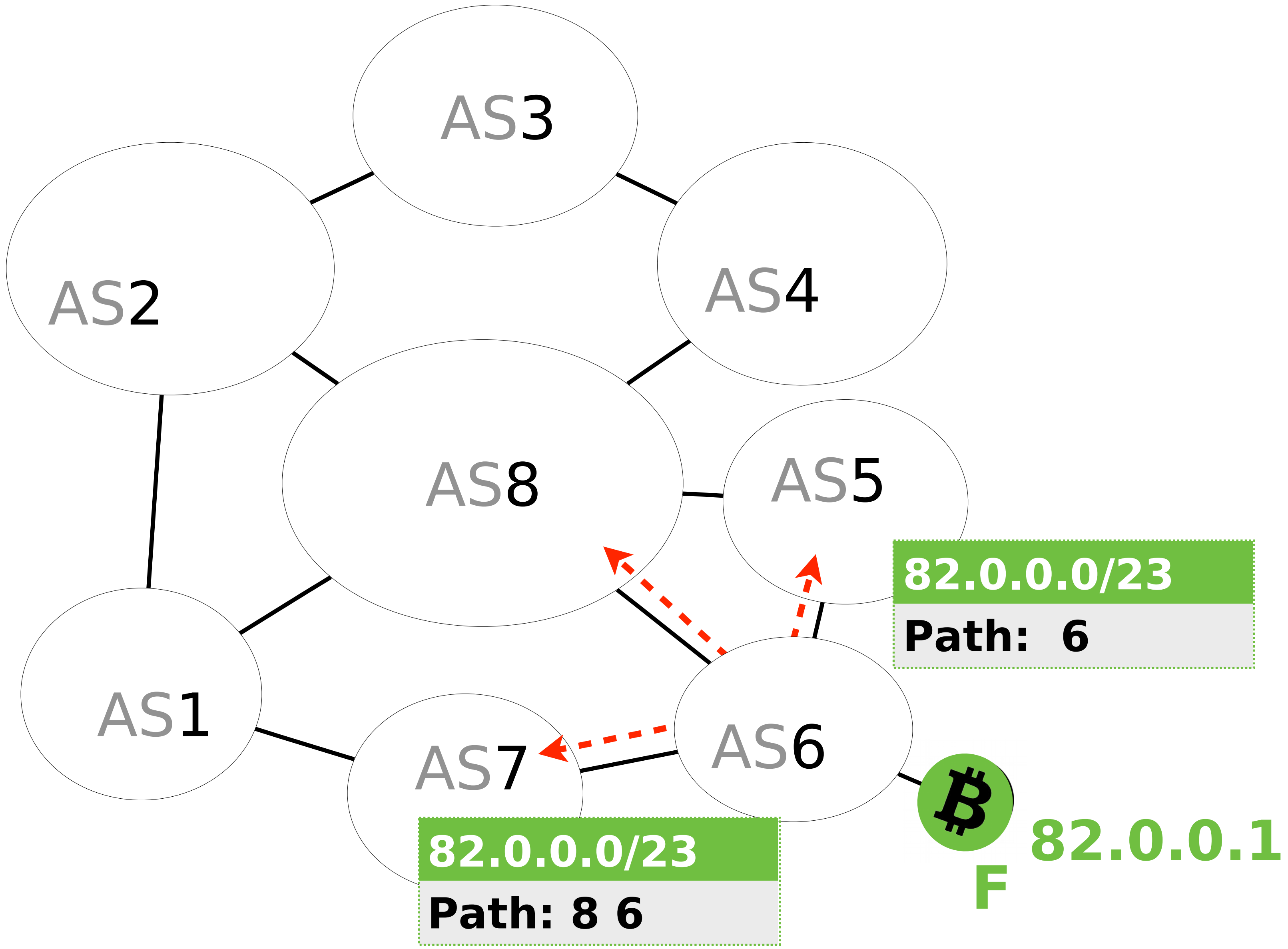
Let us focus on node F



Provider (AS6) is responsible for IP prefix



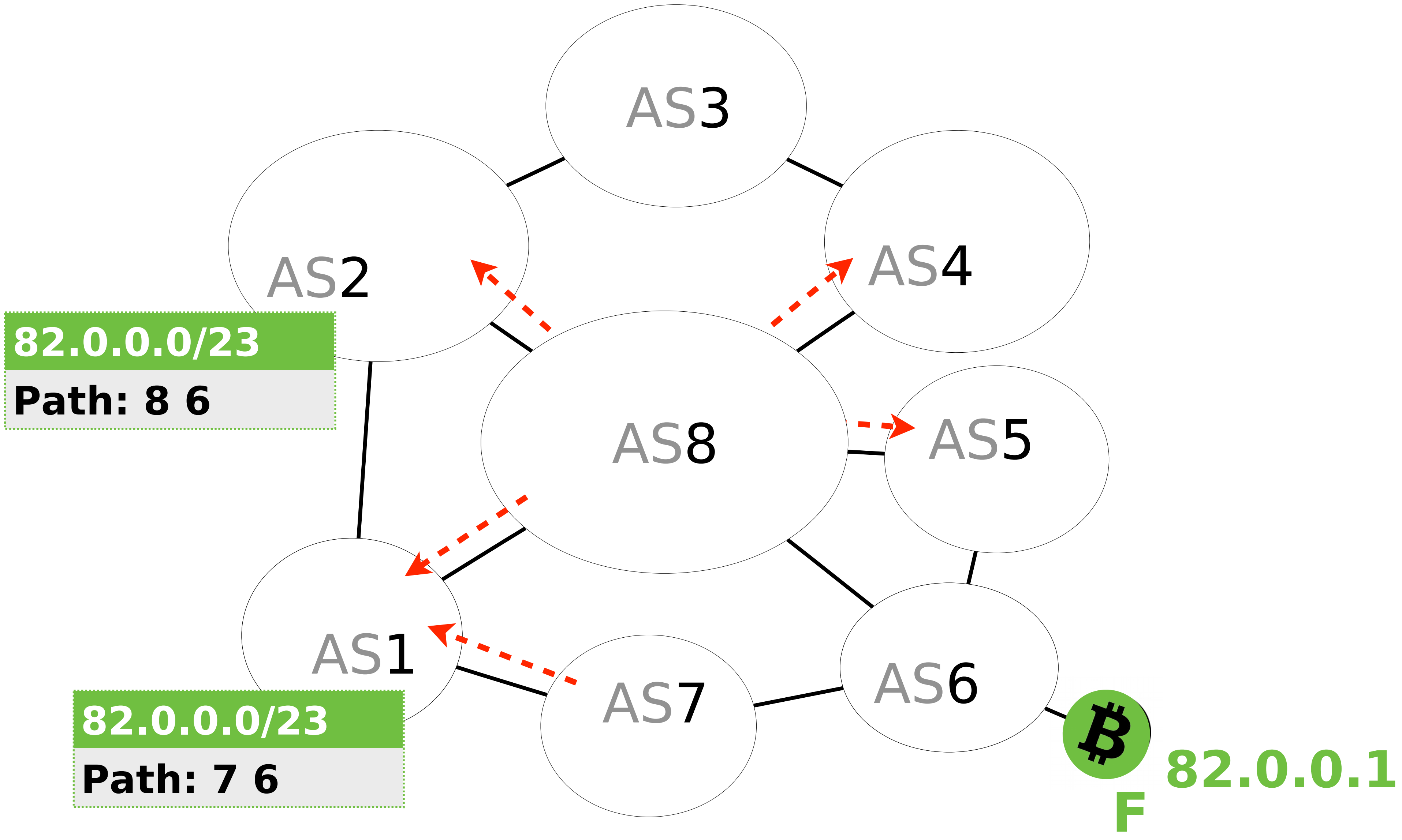
AS6 will create a BGP advertisement



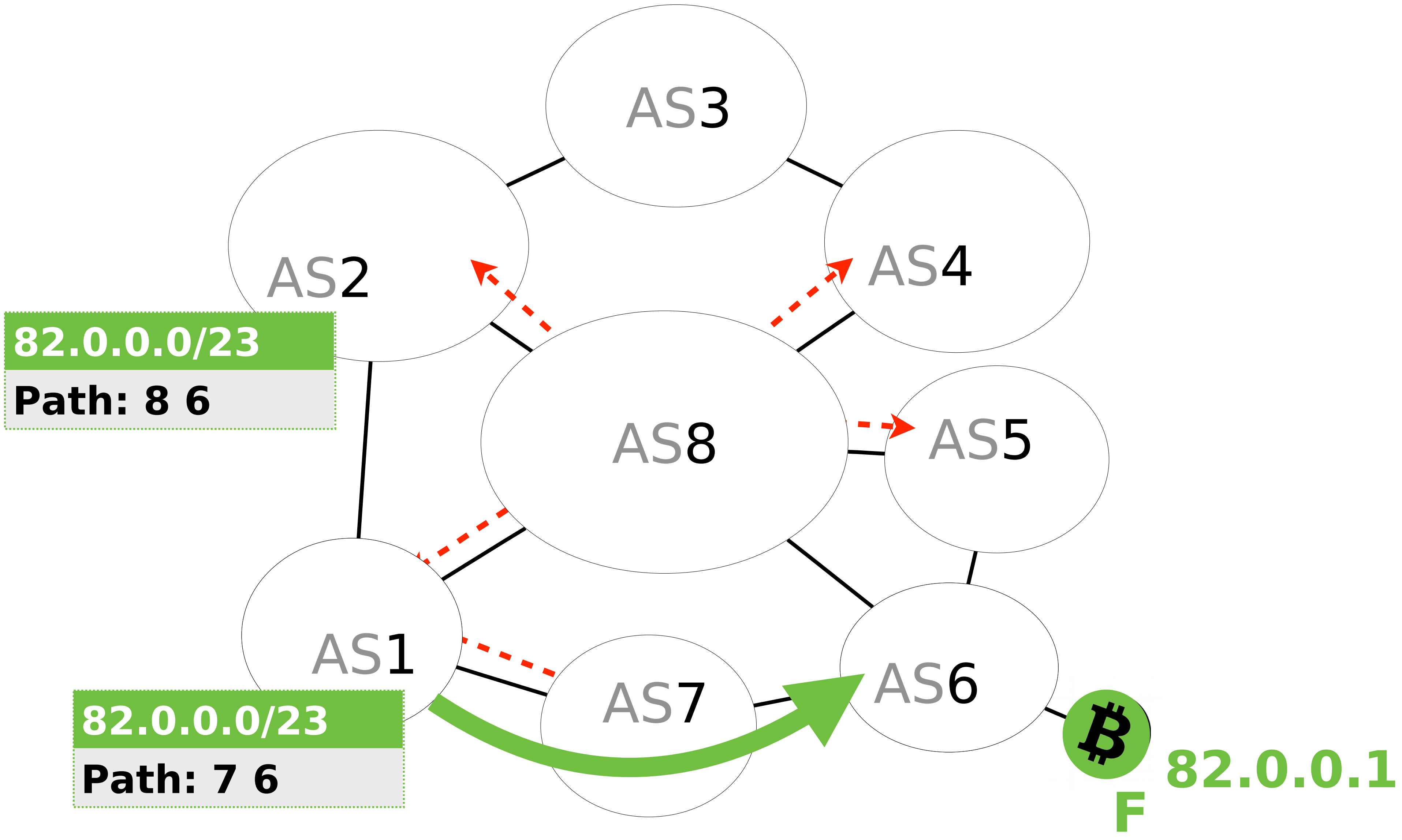
82.0.0.0/23
Path: 6

82.0.0.0/23
Path: 8 6

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



AS1 will learn the path via AS7 then AS6

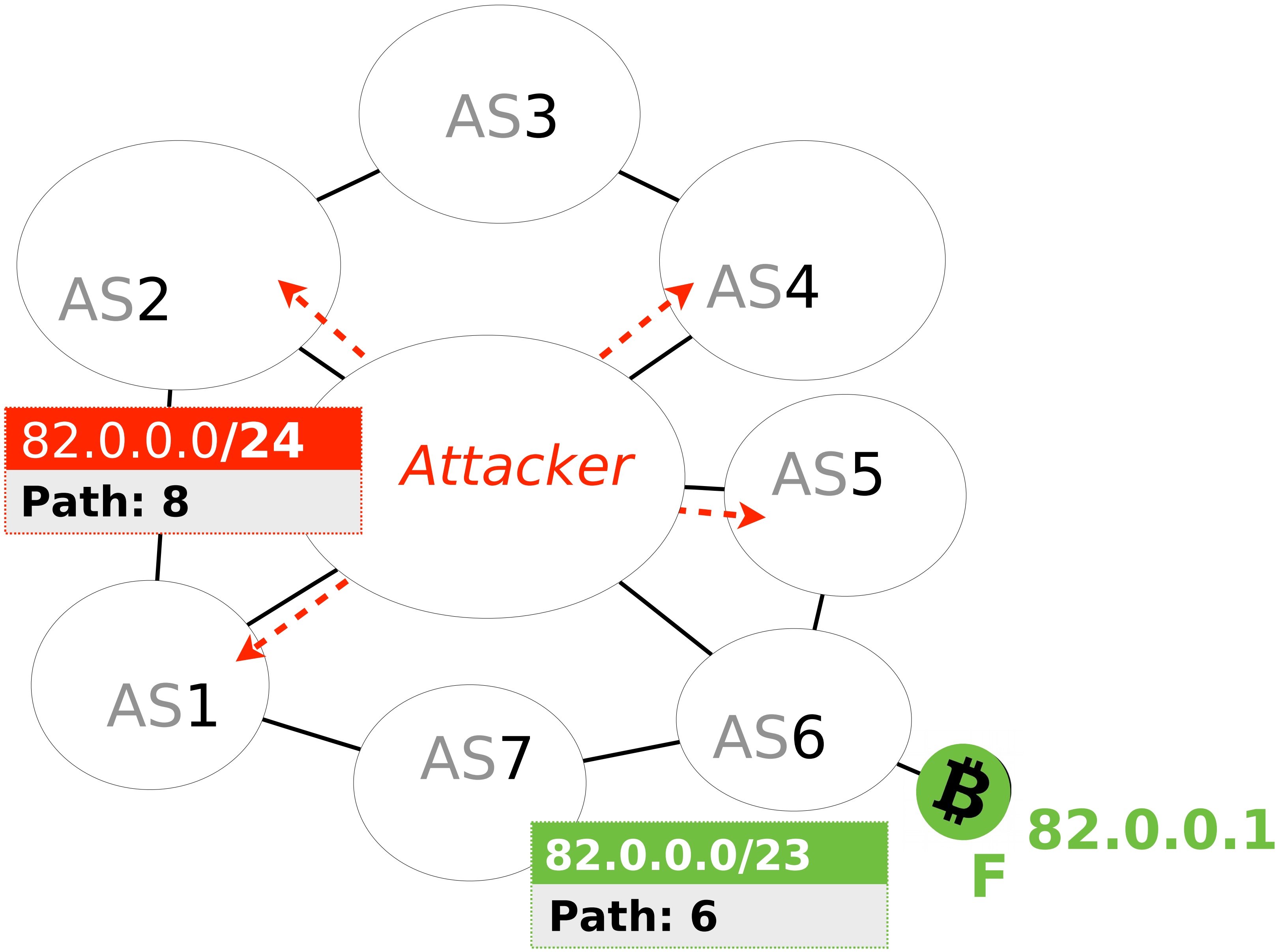


82.0.0.0/23
Path: 8 6

82.0.0.0/23
Path: 7 6

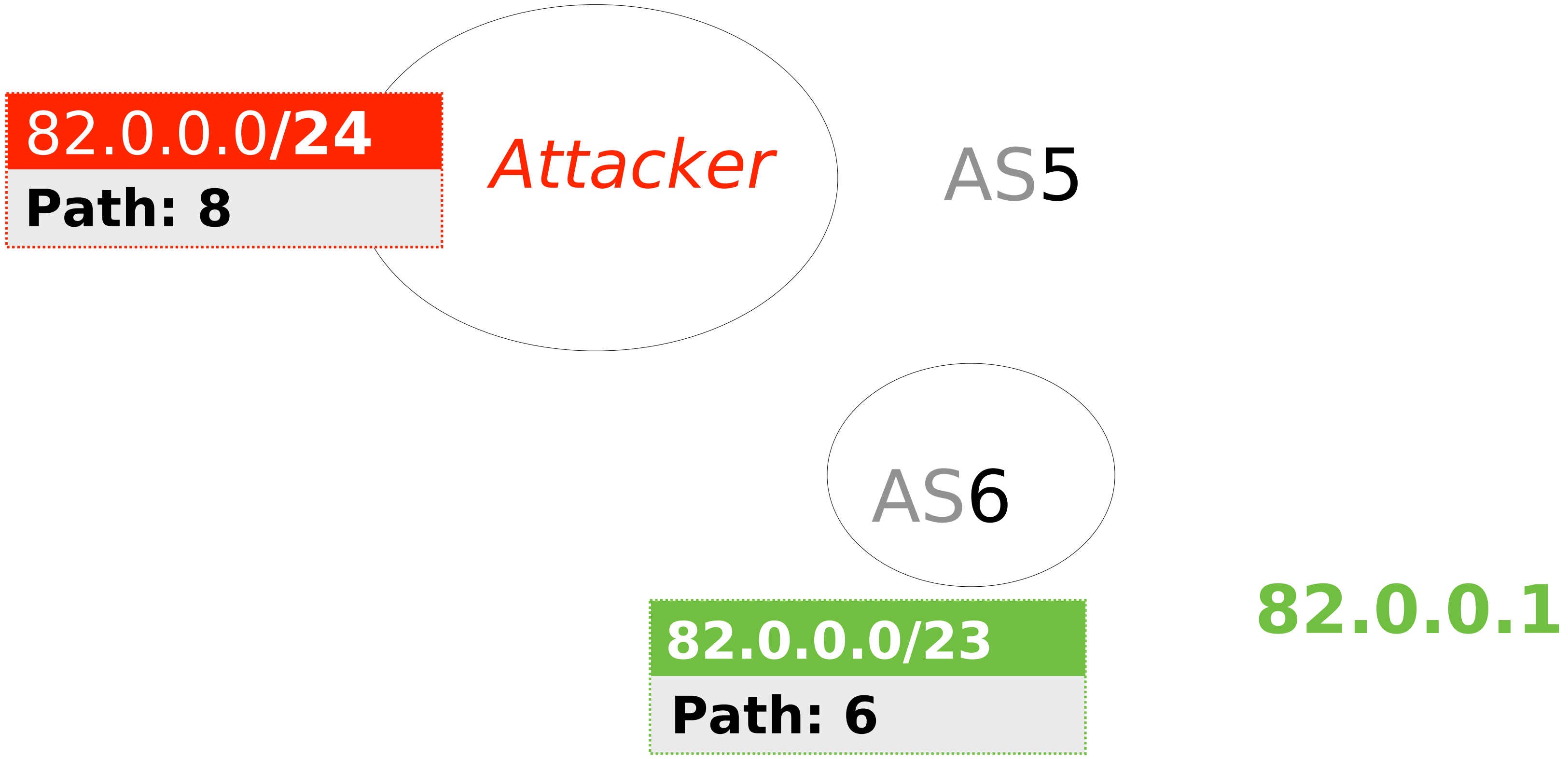
BGP does not check the validity of advertisements, meaning any AS can announce any prefix

Consider that the attacker advertises a prefix that cover the IP of F

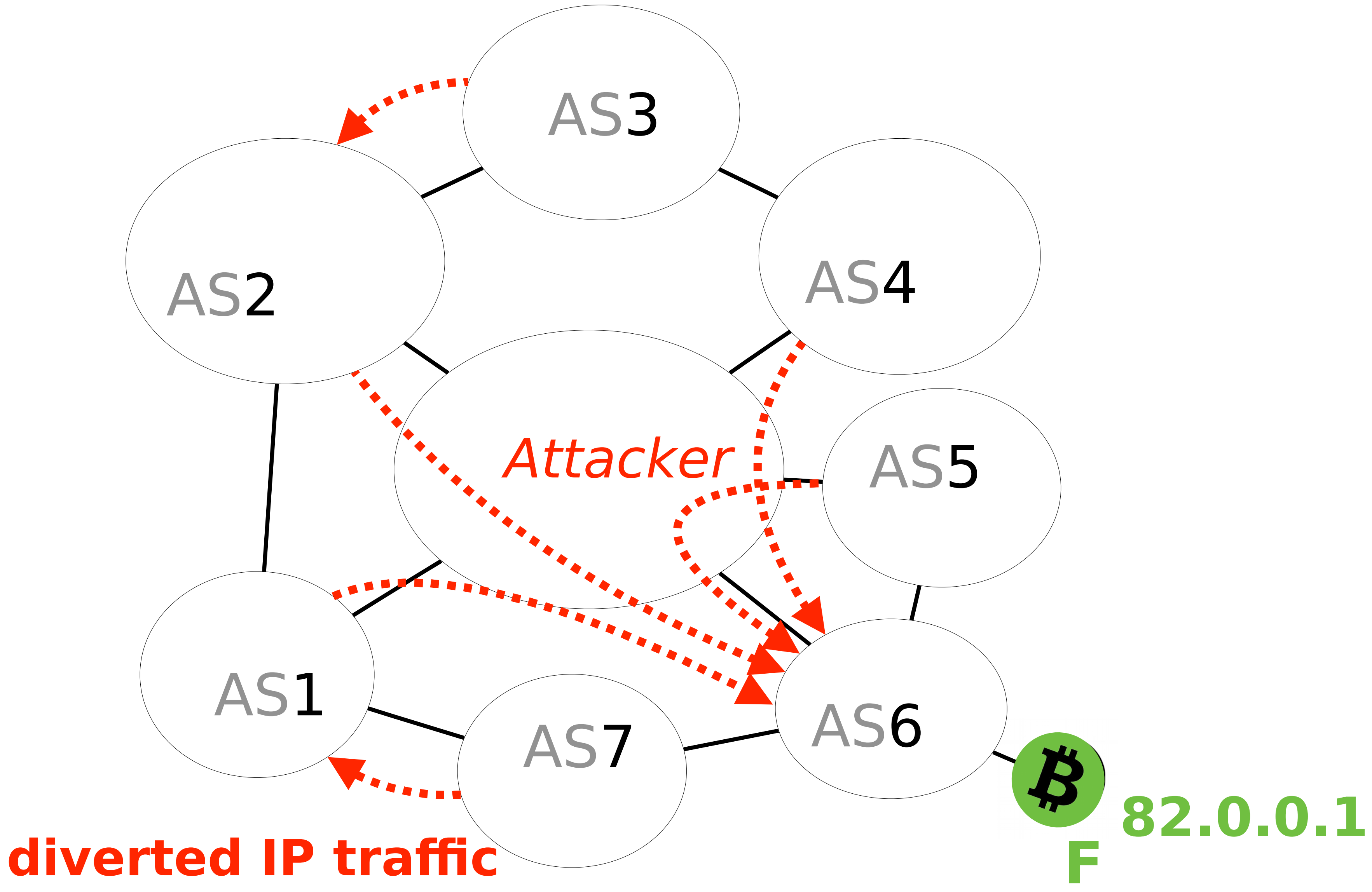


The advertisement of the attacker is more-specific

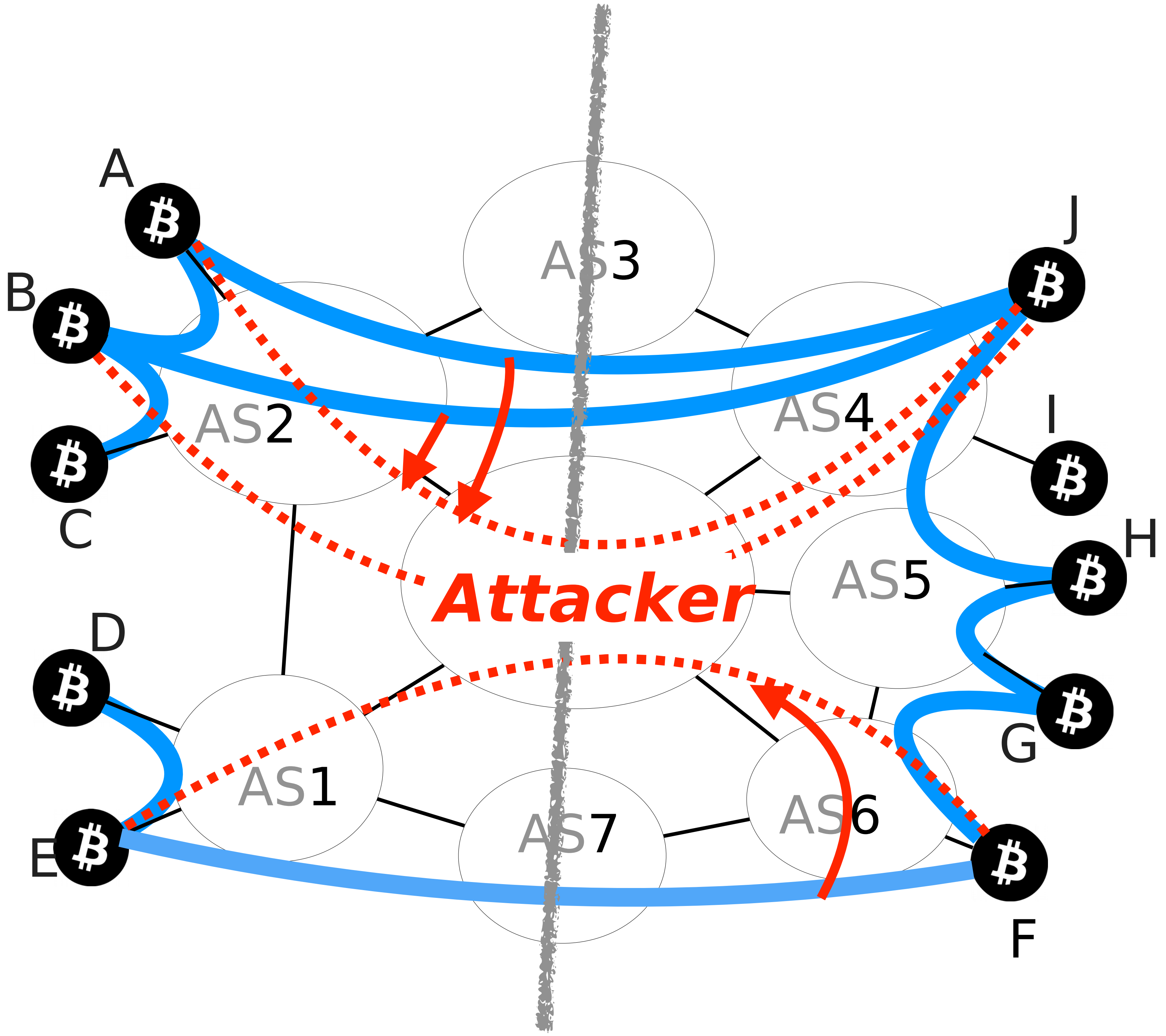
As IP routers prefer more-specific prefixes, the attacker route will be preferred



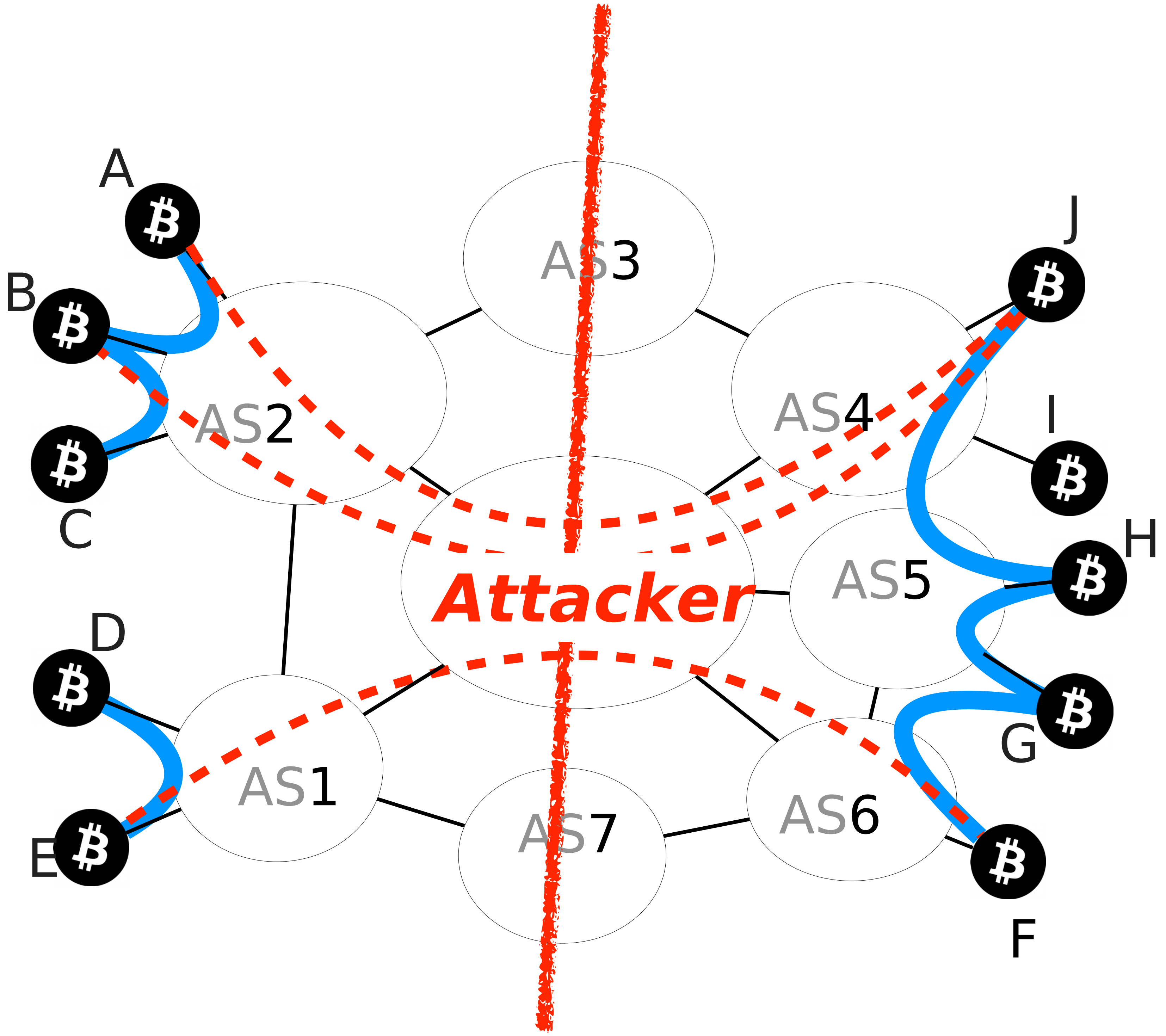
Traffic to node F is hijacked



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



The attacker can drop all connections crossing the partition



Not all partition are feasible in practice:

some connections cannot be intercepted

Bitcoin connections:

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

The partition attack is evaluated in terms of practicality and time efficiency

Practicality

Time efficiency

Can it actually happen?

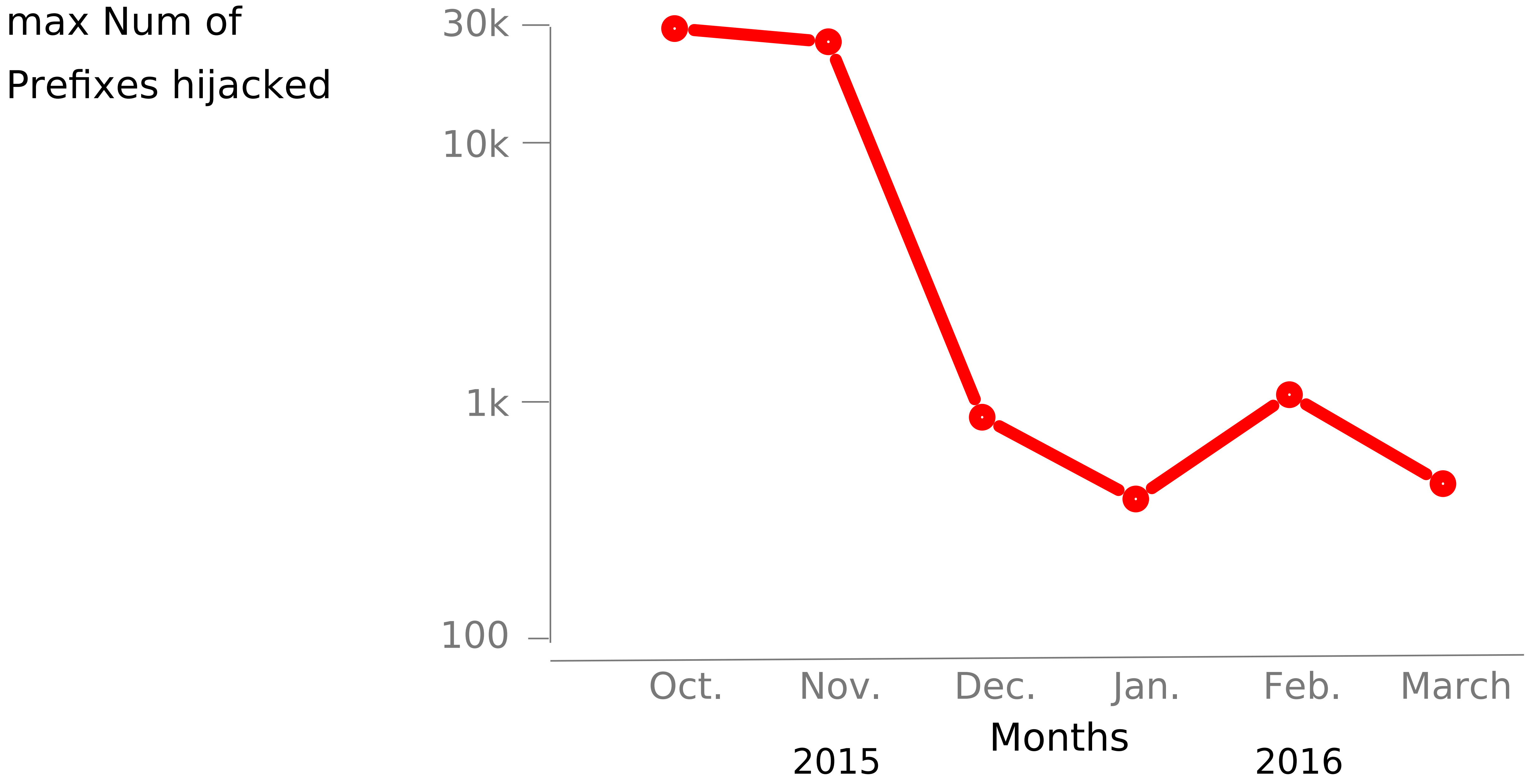
Infer the Bitcoin topology

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 compared to the hijacks
That happening in the internet every day

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



The partition attack is also evaluated in terms of time efficiency

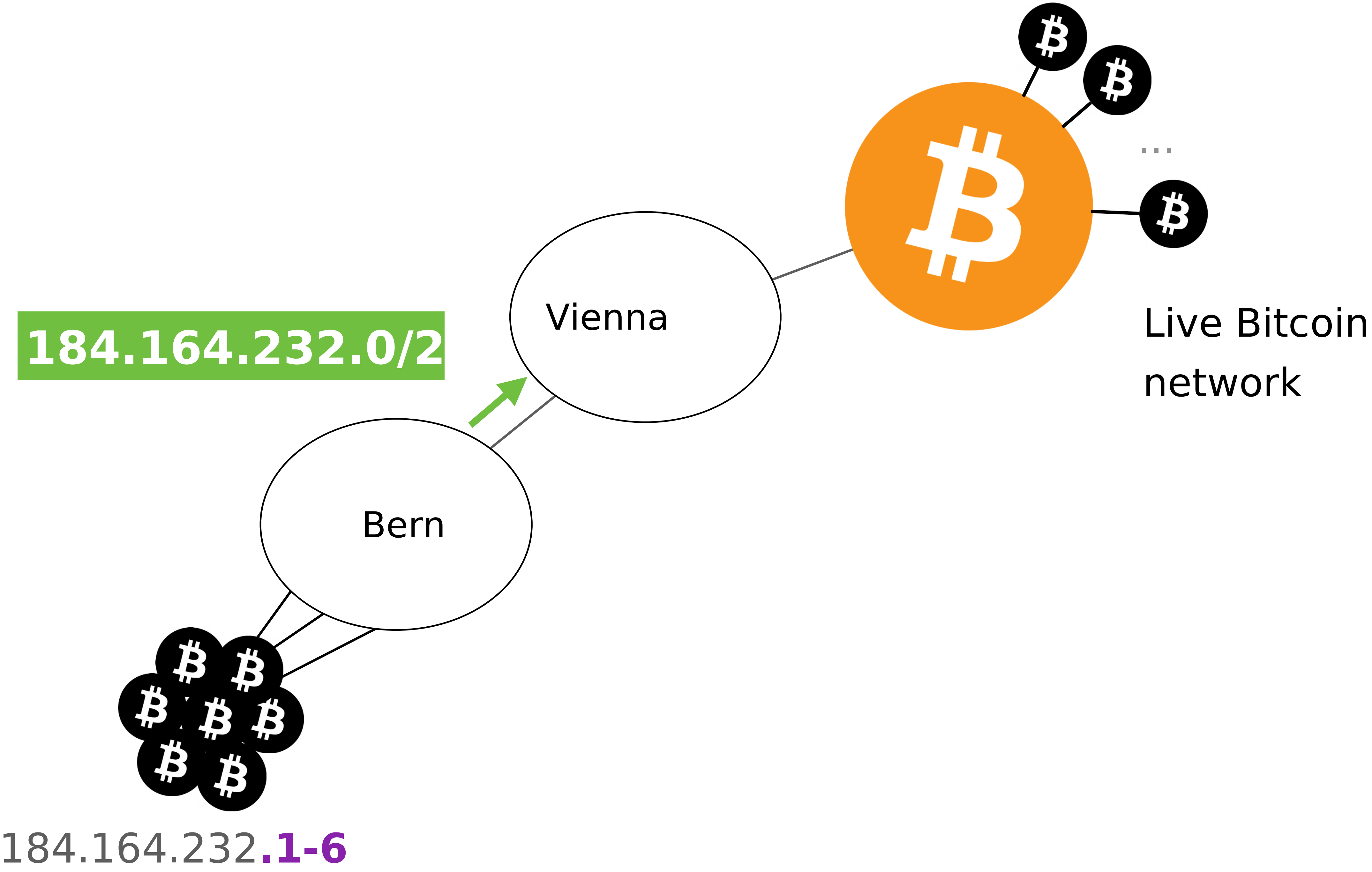
Practicality

Time efficiency

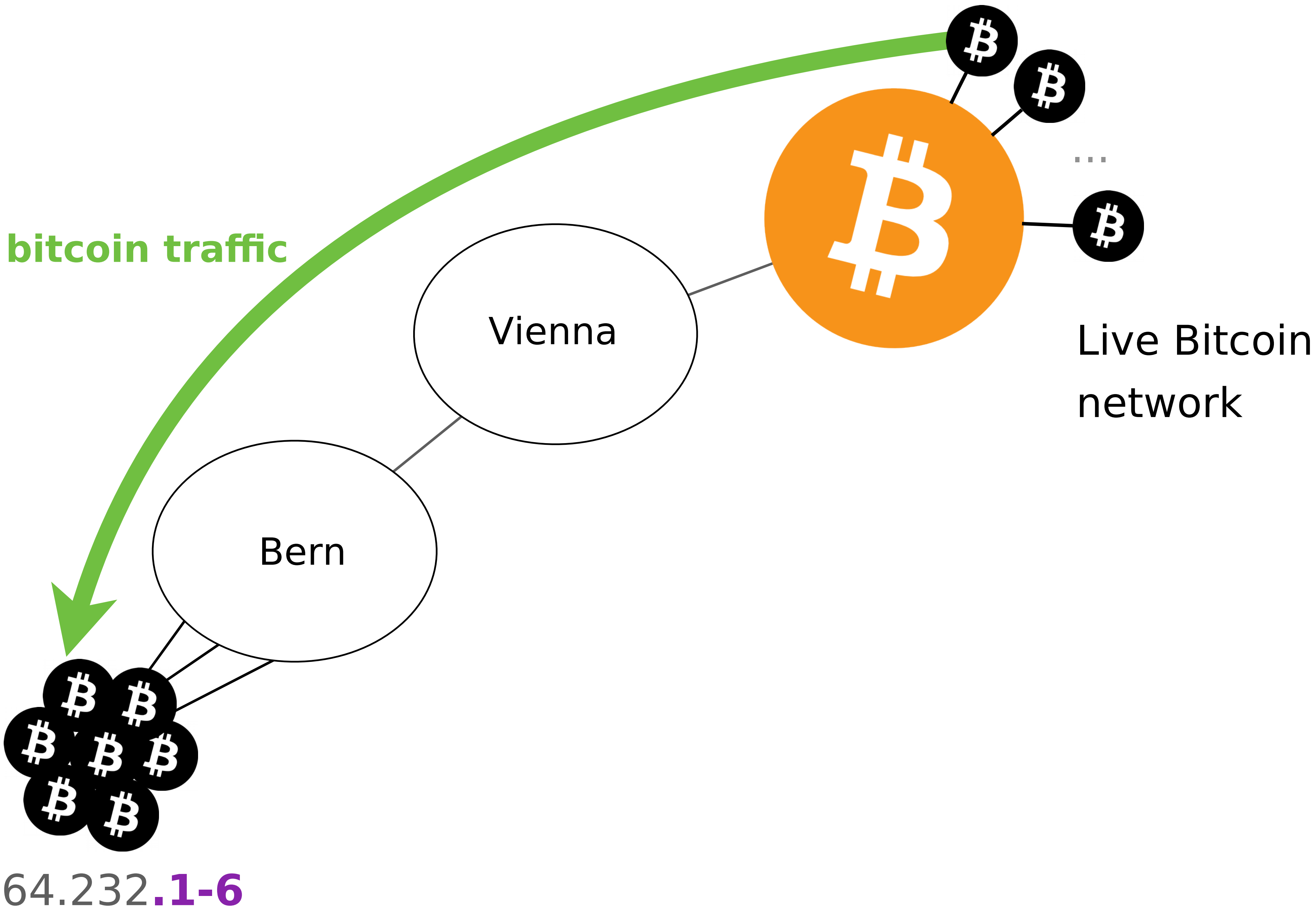
How long does it take?

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

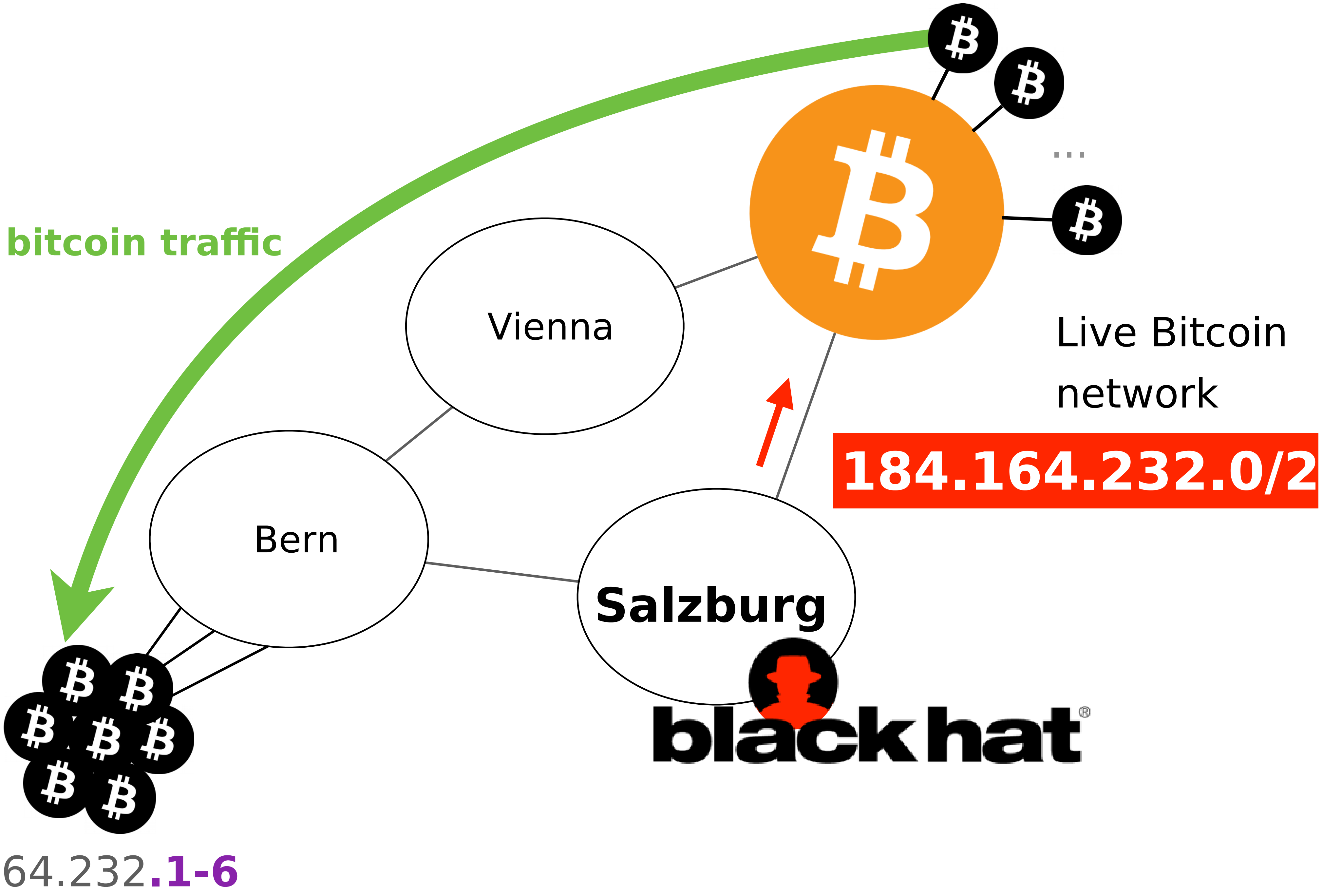
We hoste a few Bitcoin nodes at Bern and advertise a covering prefix via Vienna



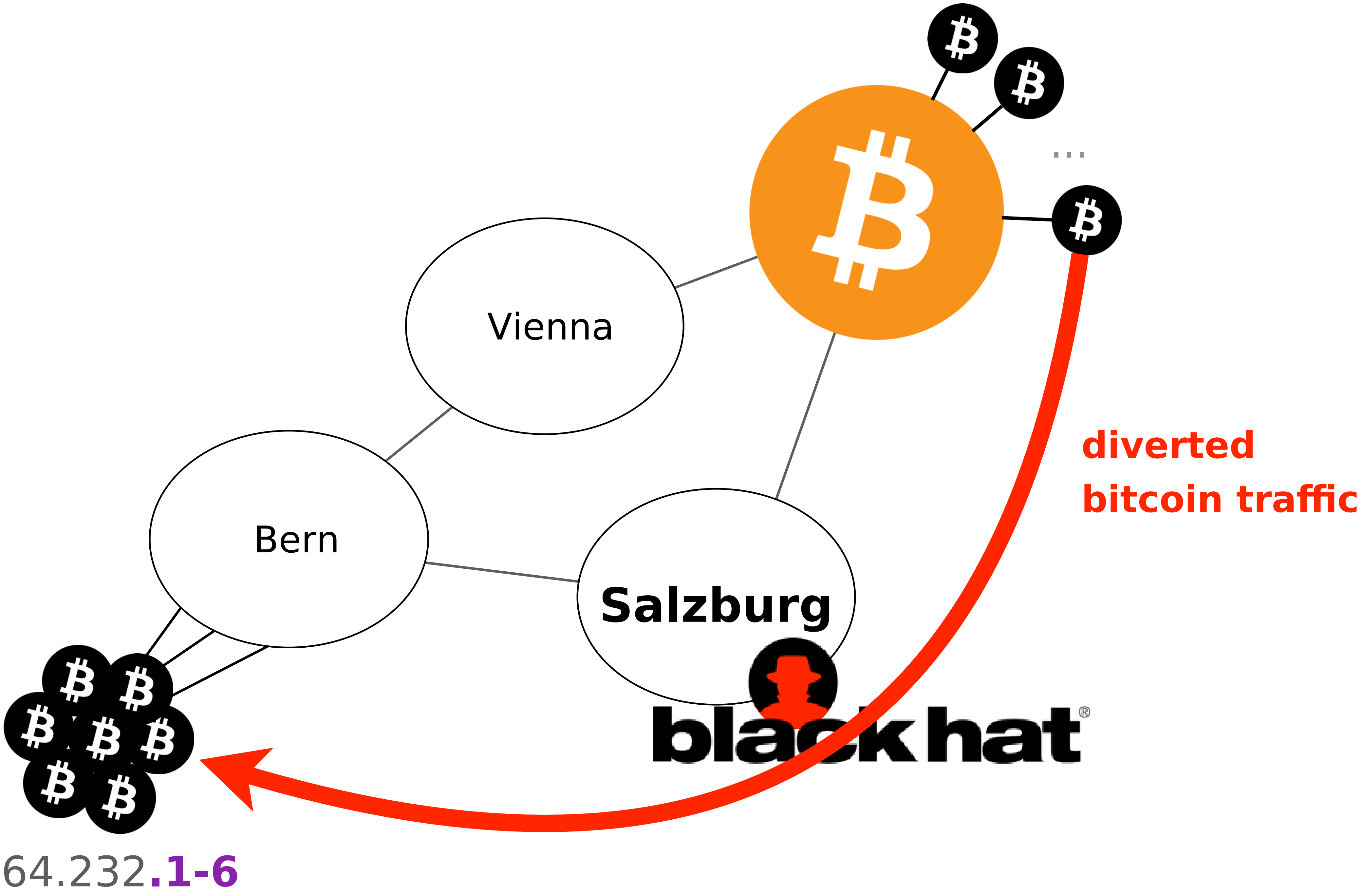
All the traffic to our nodes are routed via Vienna



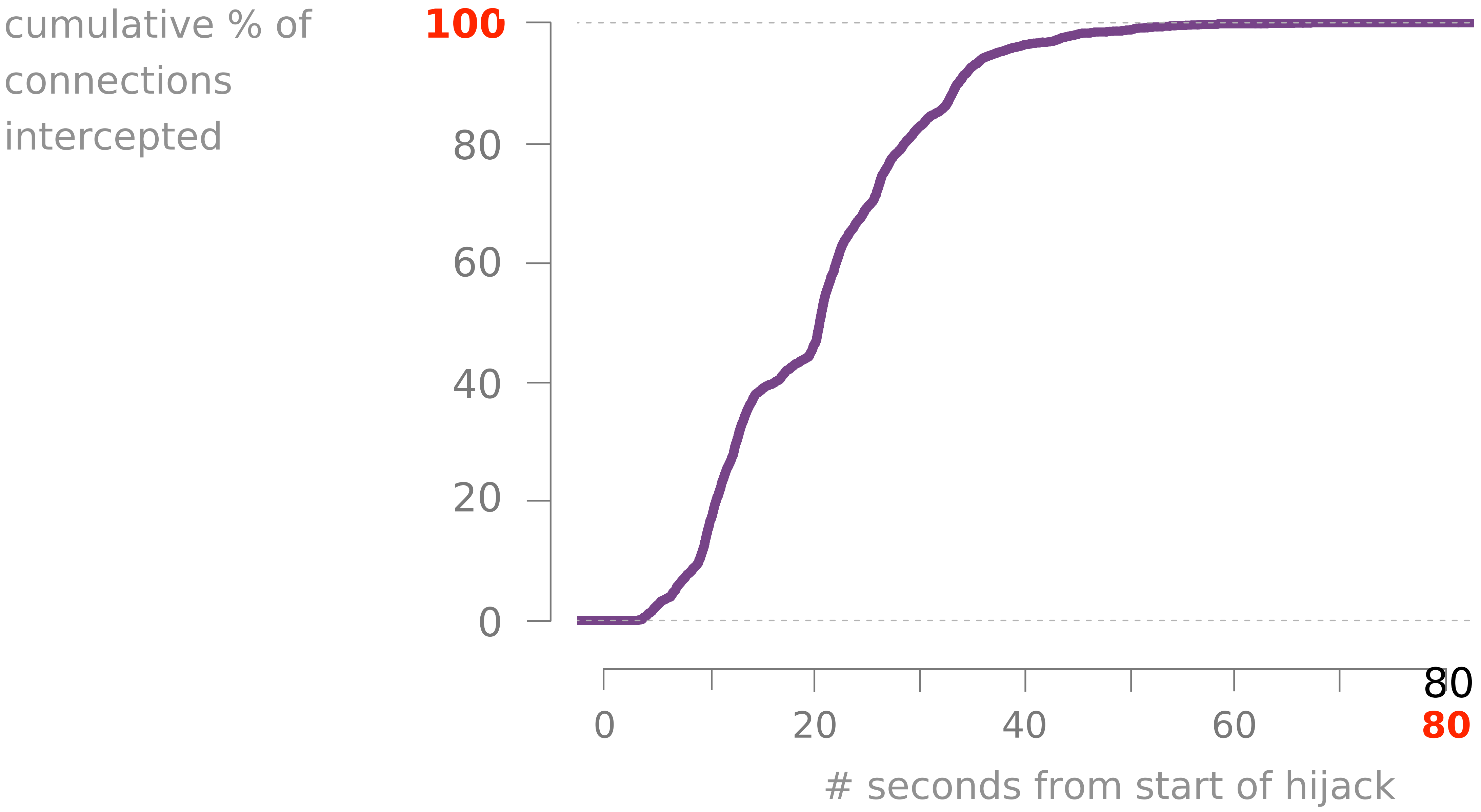
We hijacke our nodes by another BGP peer that Located in Salzburg



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



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



Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

1 Background

BGP and Bitcoin

2 Partitioning attack

splitting the network

3 Delay attack

slowing the network down

4 Countermeasures

short-term and 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 double-spending attacks

Mining pool

Regular node

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

Merchant

Mining pool

waste their mining power by mining on an obsolete chain

Regular node

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

Merchant

Mining pool

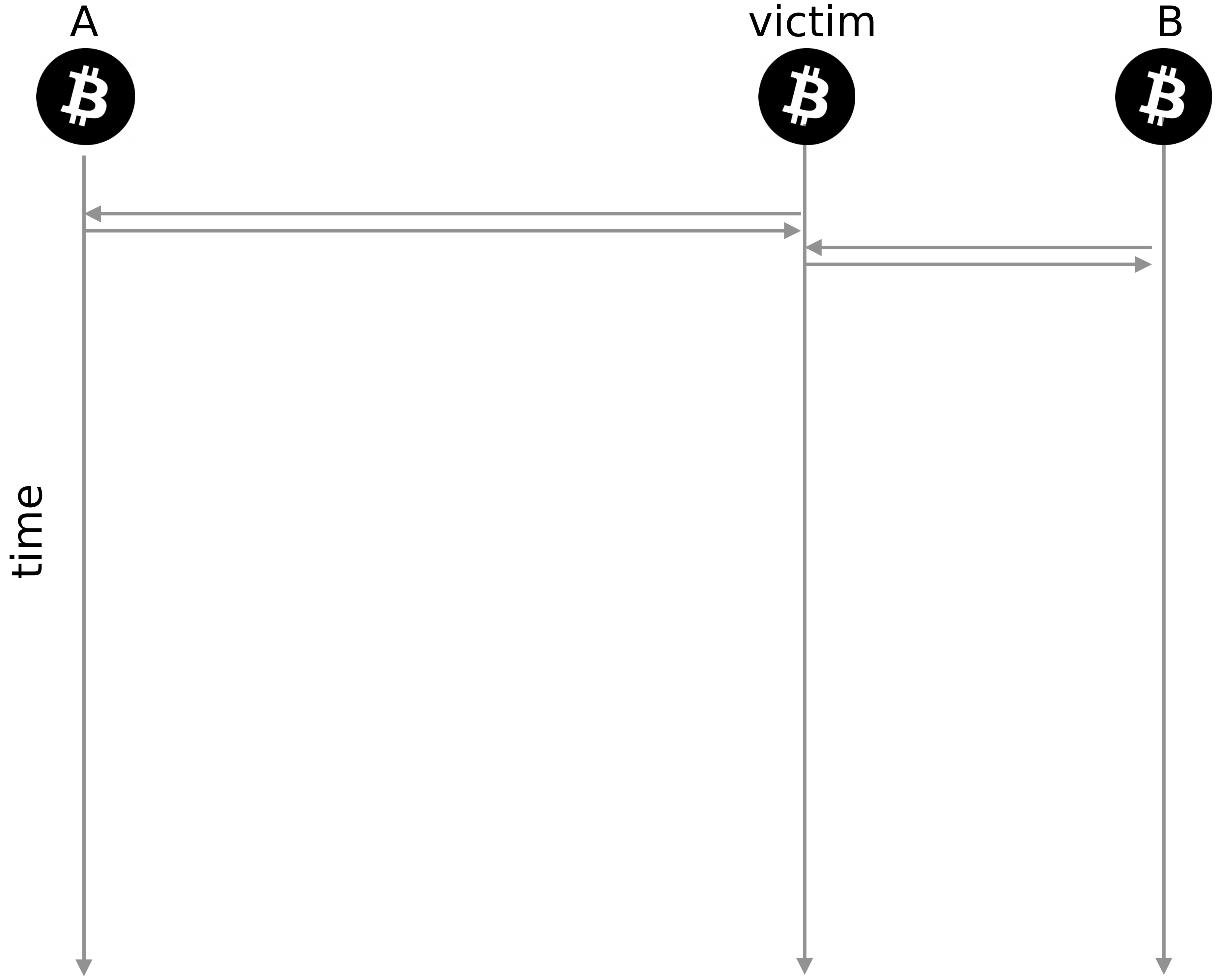
Regular node

unable to collaborate to the peer-to-peer network

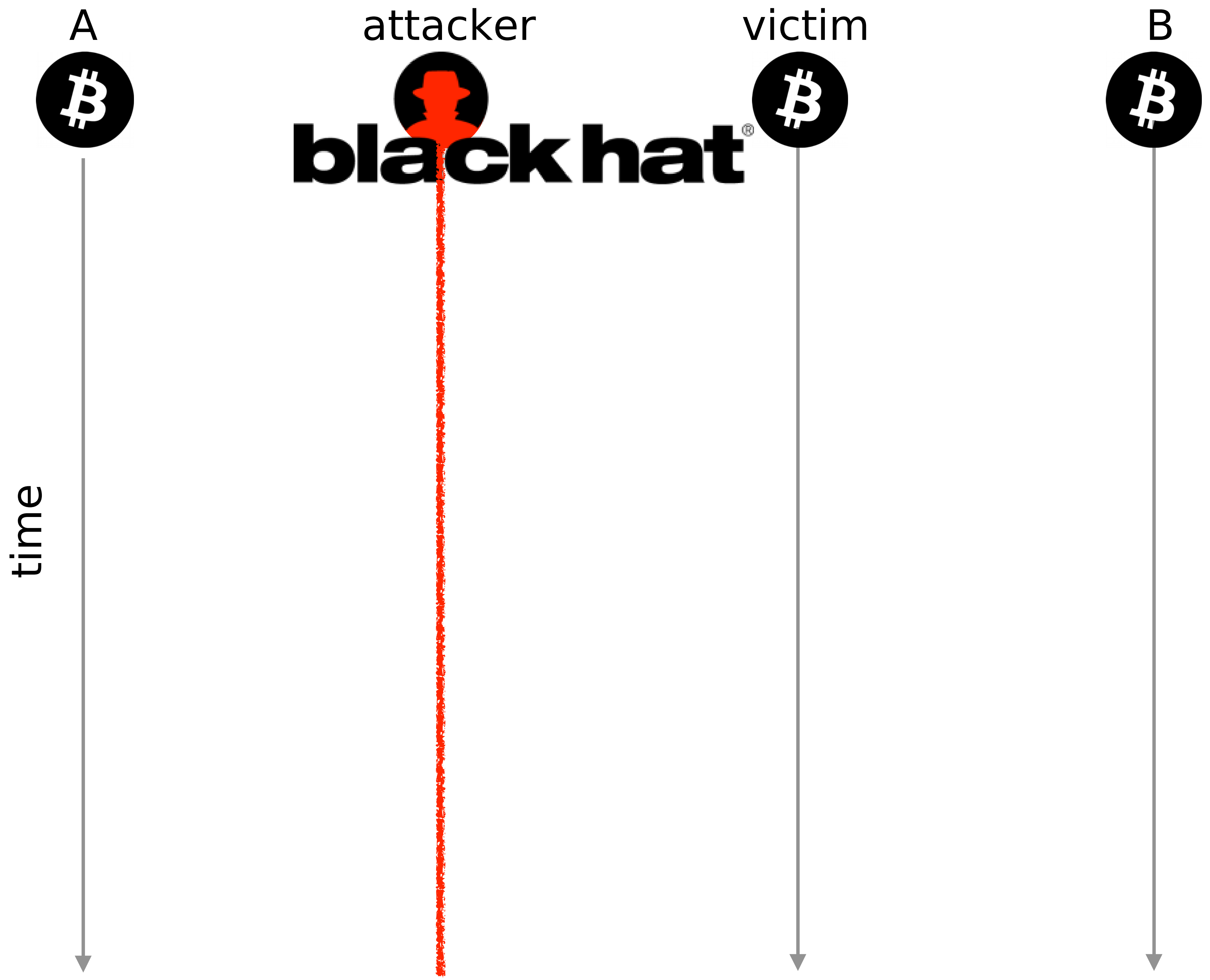
Merchant

How does a delay attack work?

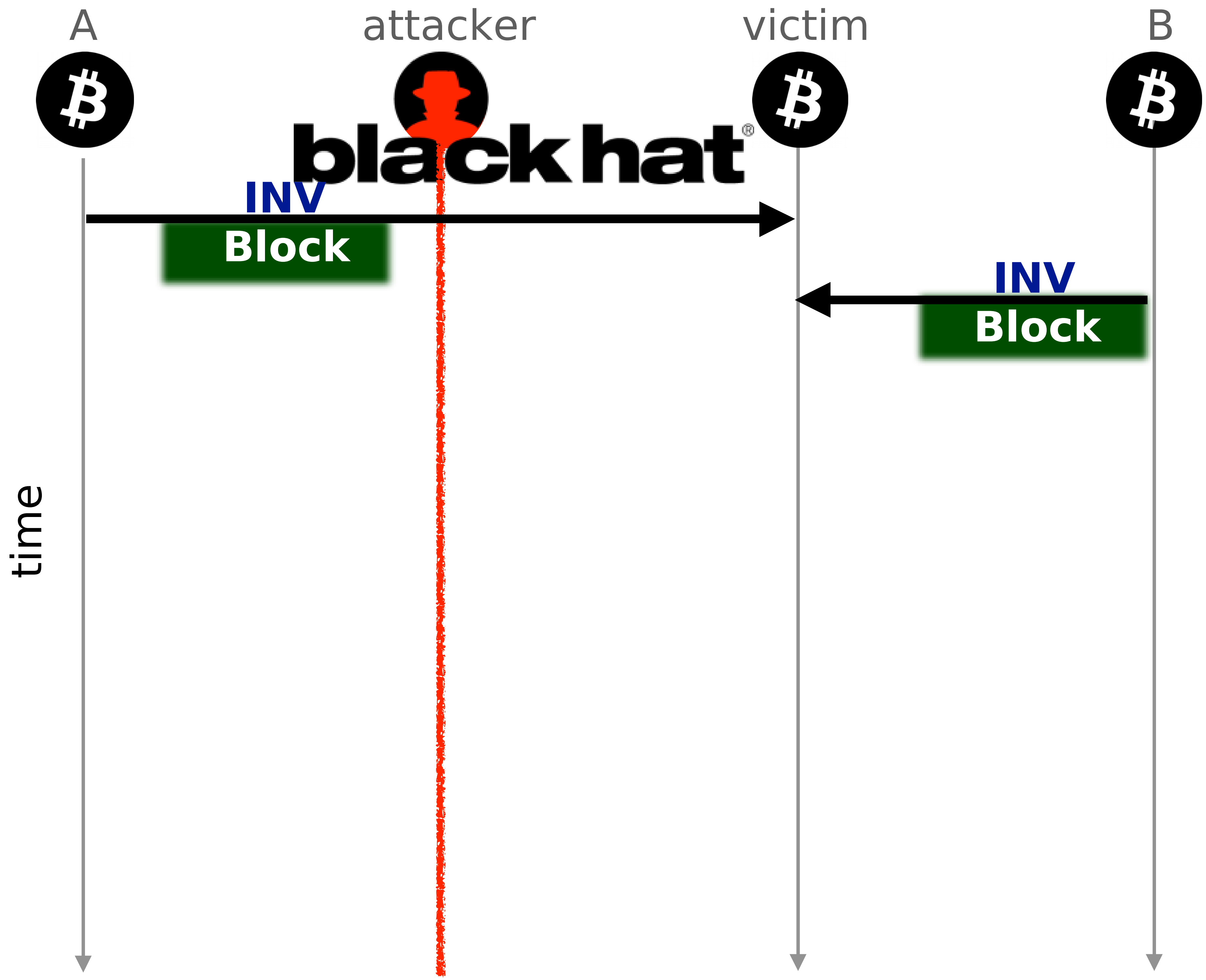
Consider these three Bitcoin nodes



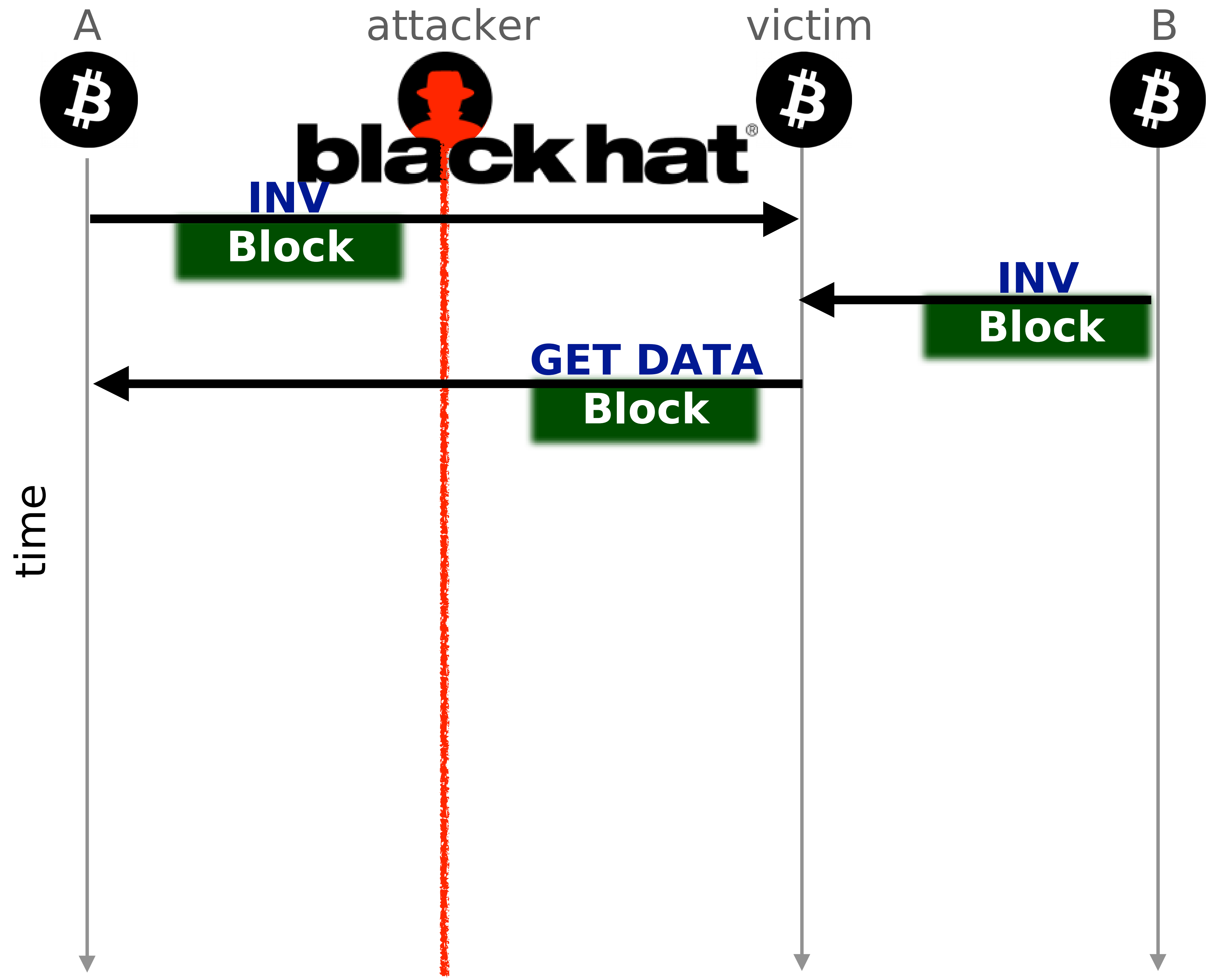
An attacker wishes to delay the block propagation Between node A and the victim



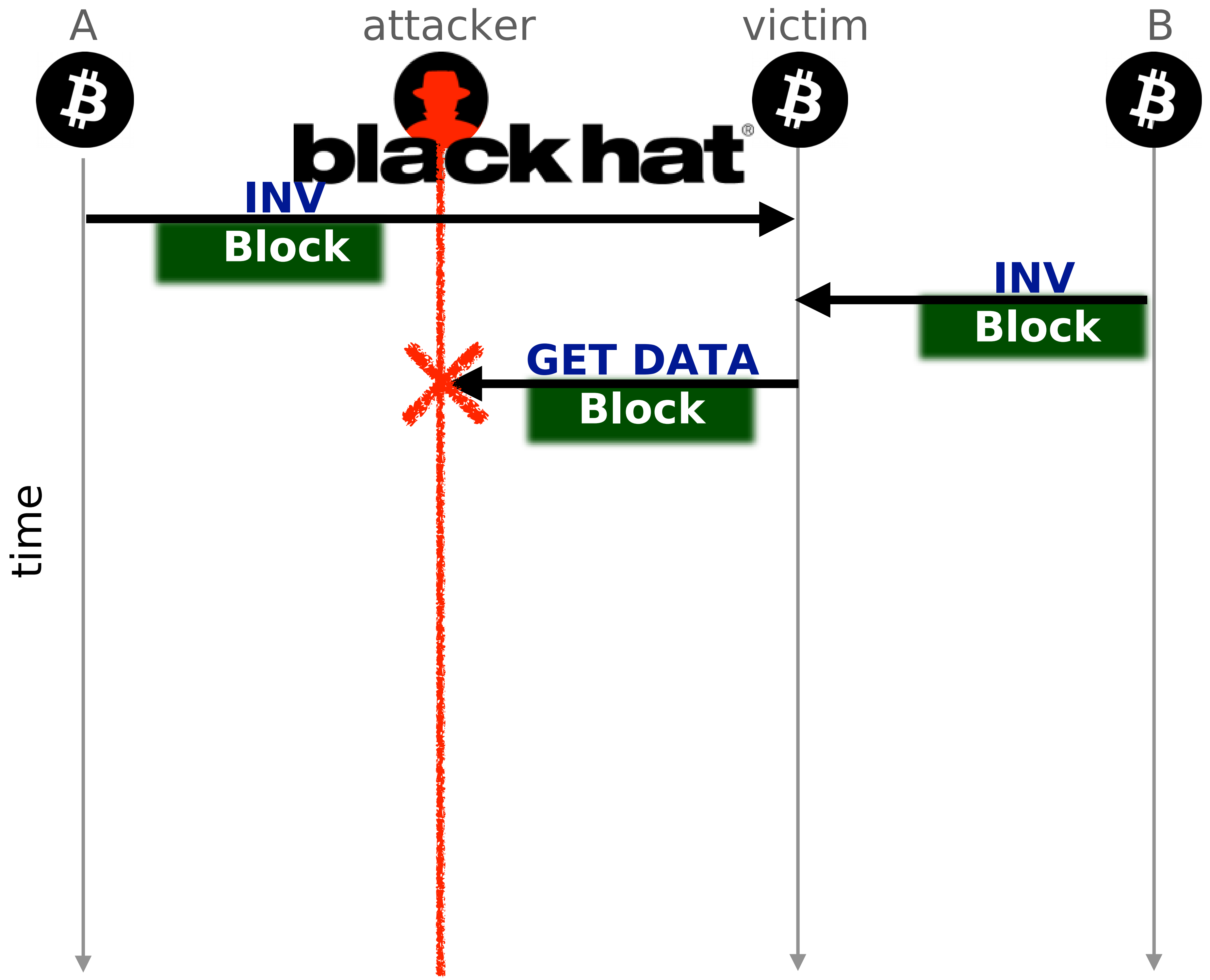
The victim receives two advertisement for the **block**



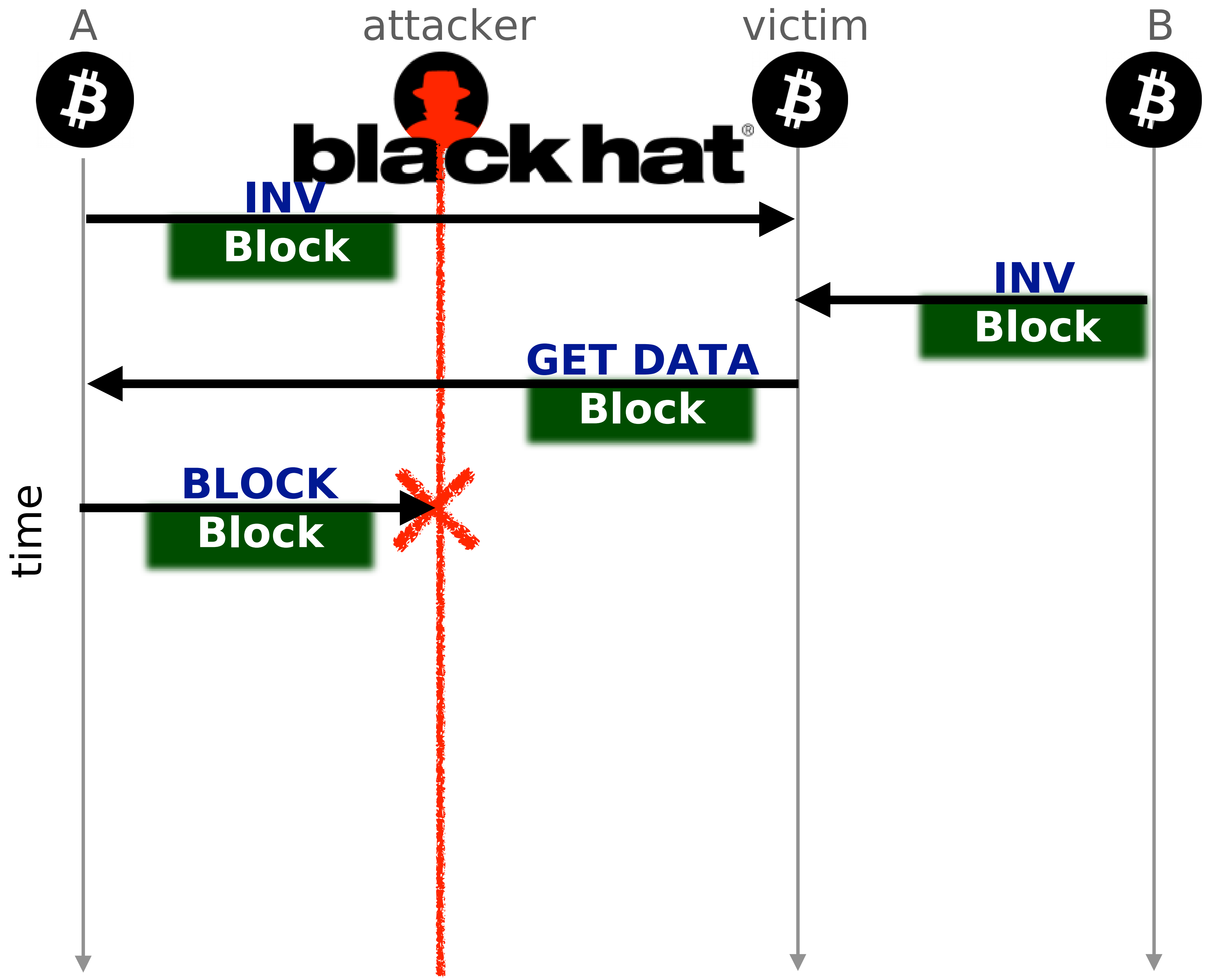
The victim requests the **block** to one of its peer, say A



The attacker could drop the **GETDATA** message

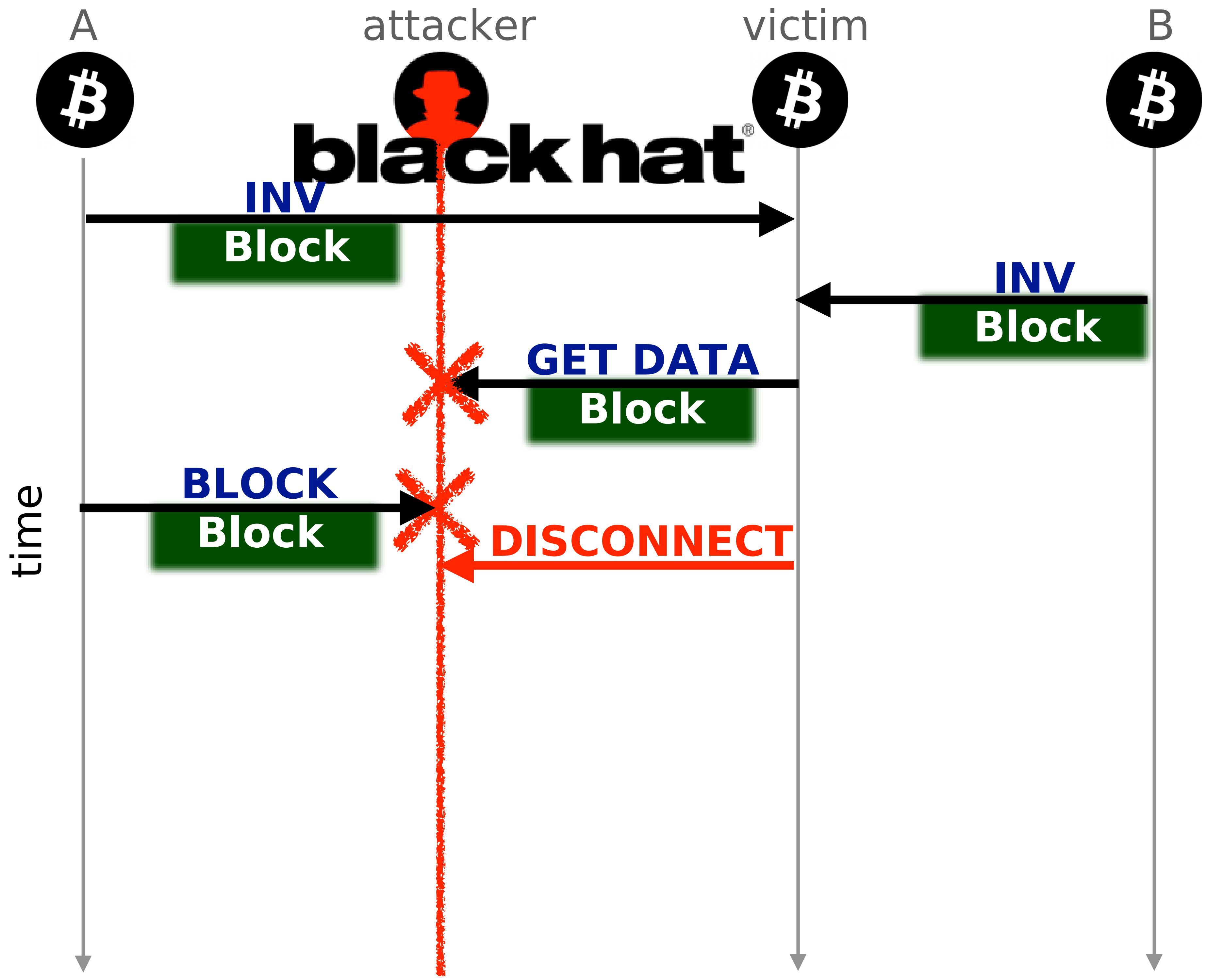


The attacker could drop the delivery of the **block** message itself

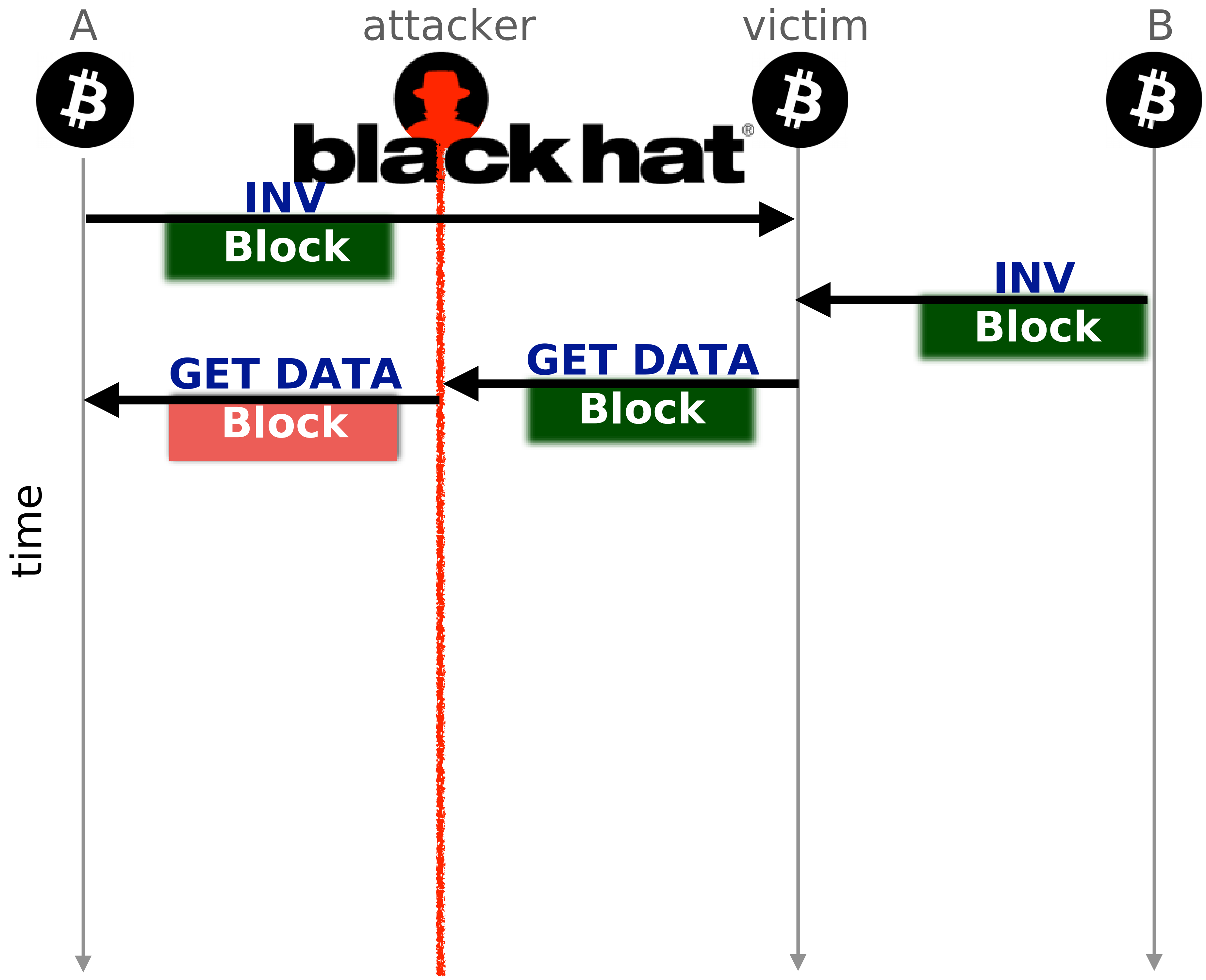


Both cases will lead the victim to kill the connection

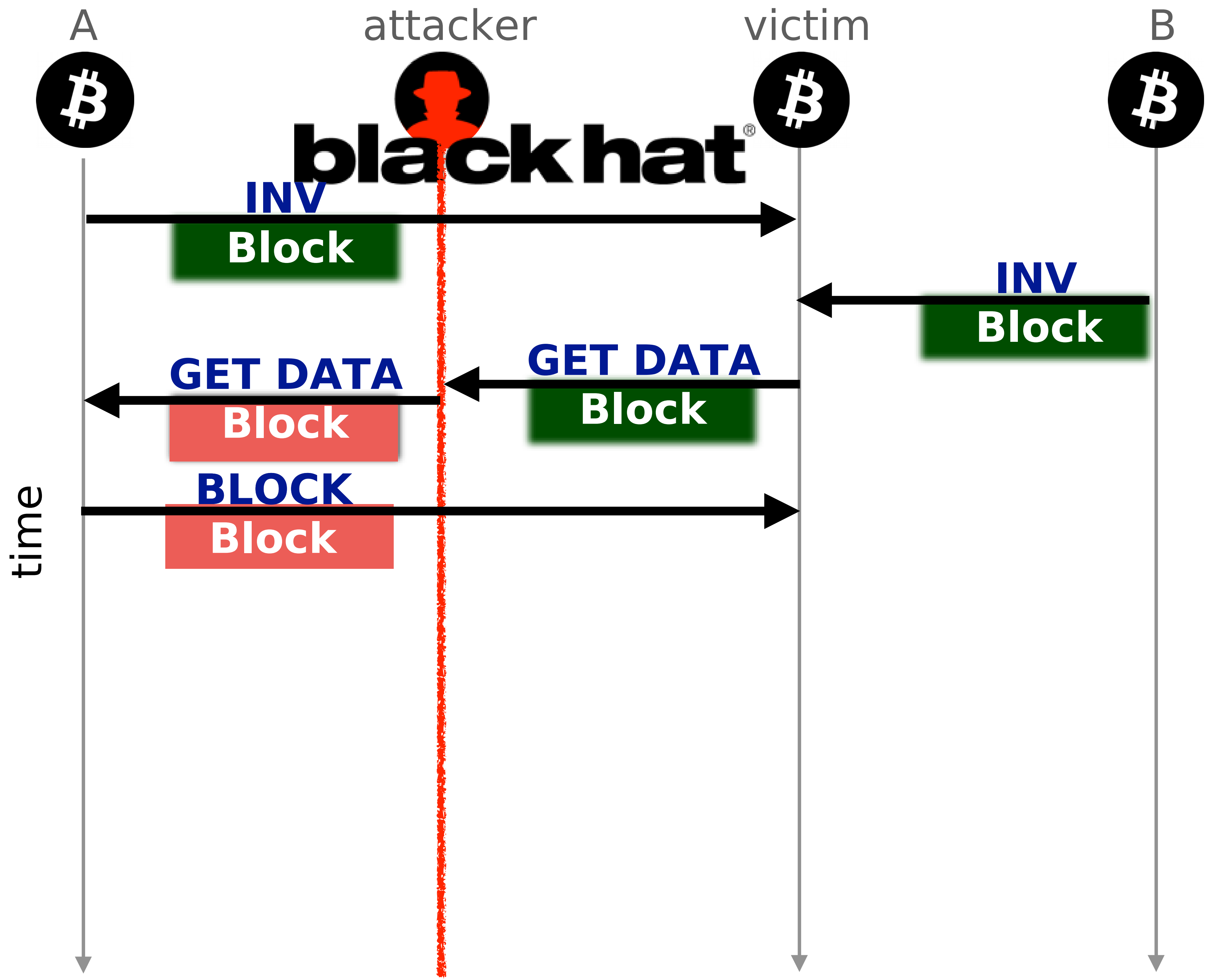
(Bitoin runs over TCP)



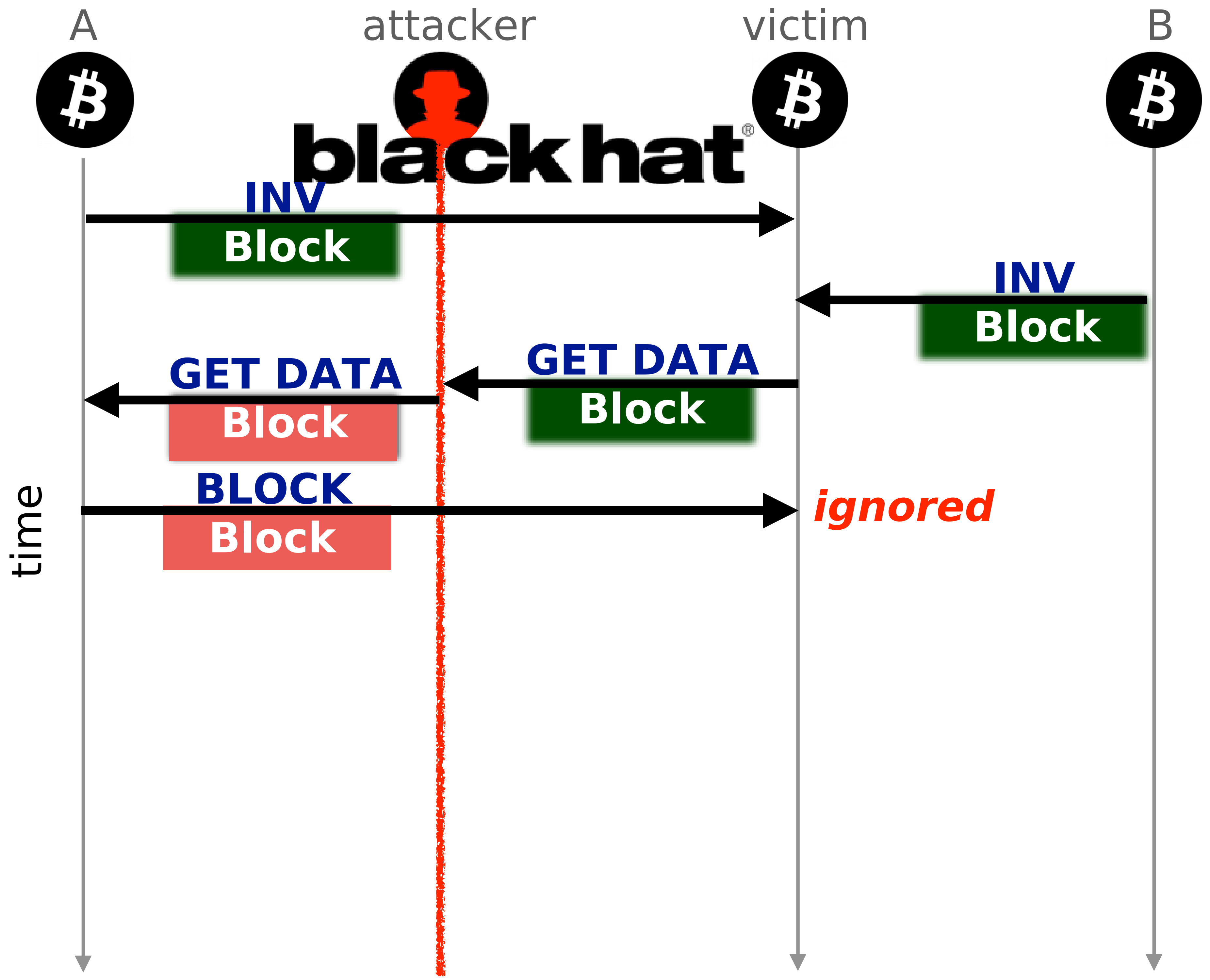
The attacker could intercept the **GETDATA** and modifies its content



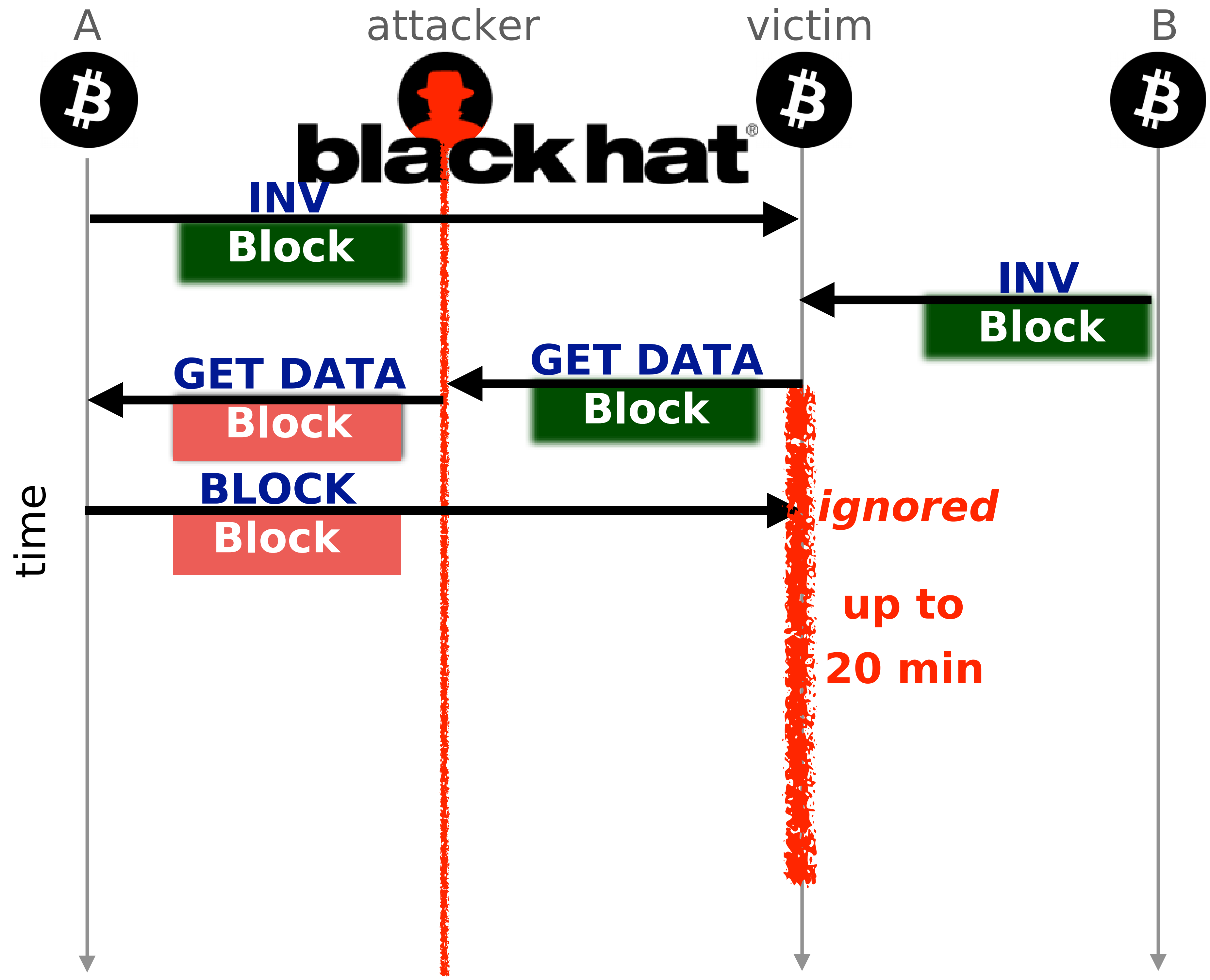
And by modifying the ID of the requested block, the attacker triggers the delivery of an older **block**



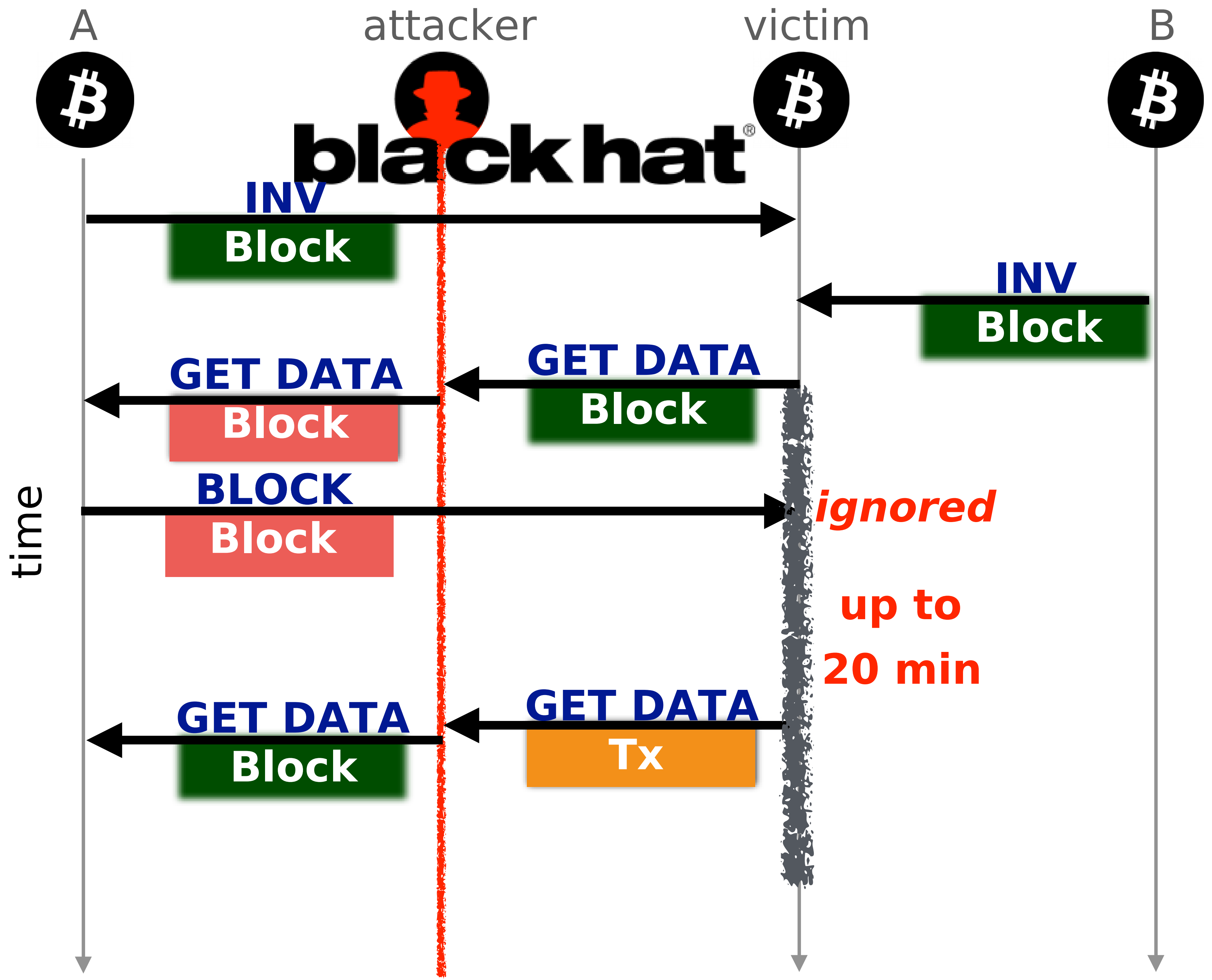
The delivery of the older block from node A triggers no error message at the victim



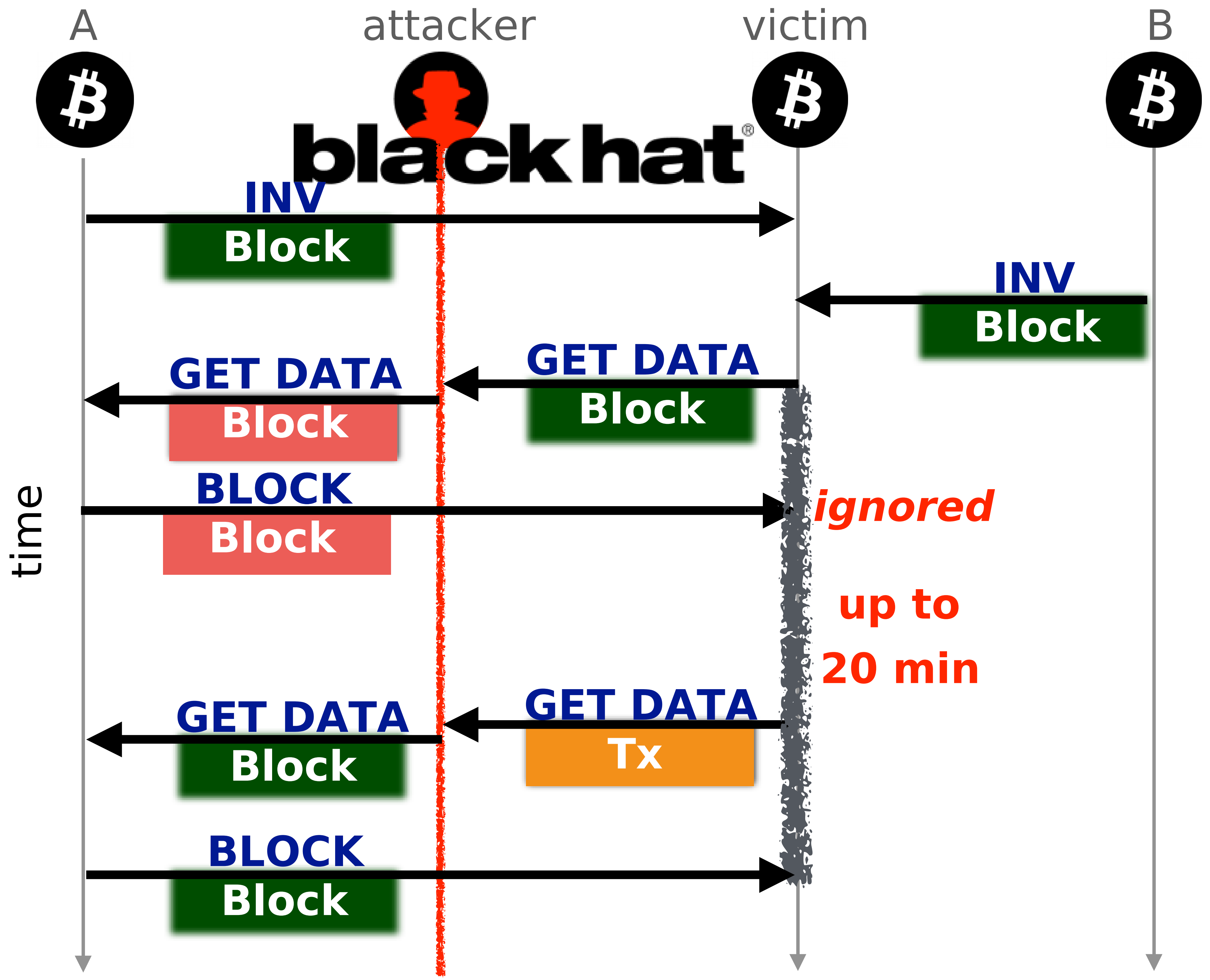
The victim will wait for 20 minutes for the actual block to be delivered



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



The block is delivered before the timeout and the attack goes undetected



The delay attack is evaluated in terms of effectiveness and practicality

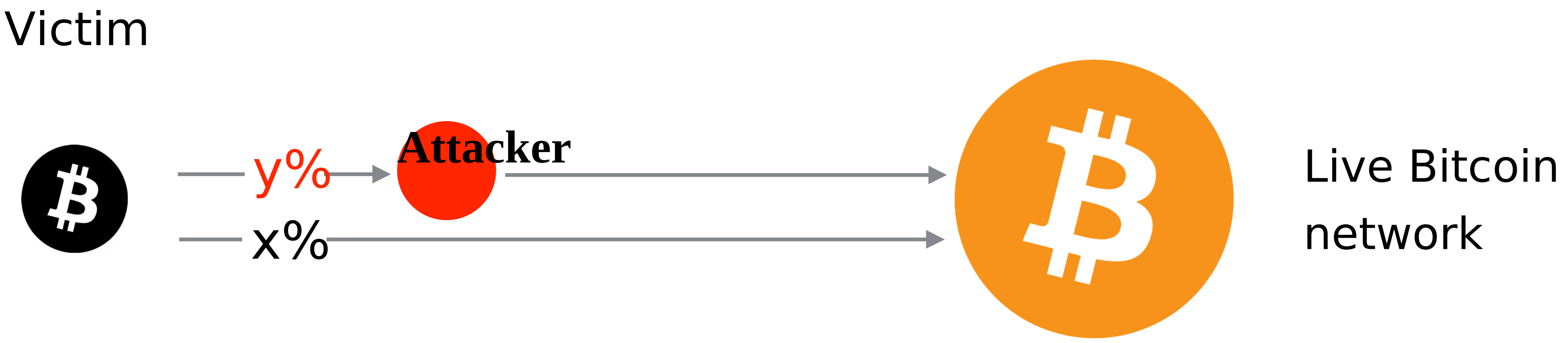
Effectiveness

How much time does the victim stay uniformed?

Practicality

Is it likely to happen?

Connect the victim with the Bitcoin network
Assume, the fraction of his connections are routed by the attacker



Doing so. The attacker can keep the victim uninformed for most of its uptime

Using this setup, we find that

If the attacker intercept 50% of the victim connections

The victim will stay uninformed 63% Of it’s uptime

The vast majority of the Bitcoin network is at risk

If the attacker intercept 50% of the victim connections

The victim will stay uninformed 63% Of it’s uptime

67% nodes vulnerable to attack by at least by one AS adversary

Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

1 **Background**

BGP and Bitcoin

2 **Partitioning attack**

splitting the network

3 **Delay attack**

slowing the network down

4 **Countermeasures**

short-term and long-term

Both sort-term and long-term countermeasures exist

Short-term countermeasures are simple shifts in the Bitcoin clients

Short-term

Bitcoin client could select it’s peer in Routing-aware manner

reduce risk of having one ISP seeing all connections

Bitcoin client could monitor the behavior with it’s peer

Detect abnormal changes that might be a sign of a partition

Long-term countermeasures provide more guarantees

Long-term

Use end-to-end encryption

prevent delay attacks (not partition attacks)

Deploy secure routing protocols

prevent partition attacks (not delay attacks)

Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

Bitcoin is vulnerable to routing attacks

The potential impact on the currency is worrying

Countermeasures exist