Routing attacks on Cryptocurrency Mining Pools

Muoi Tran

Theo von Arx

Laurent Vanbever

IEEE S&P

May 22 2024

ETH zürich

United we stand,
divided we fall.

– Aesop

Apostolaki et al. [S&P 2017]

Tran et al. [S&P 2020]

Saad et al. [S&P 2023]

...

United cryptocurrencies stand,
divided cryptocurrencies fall.

This work

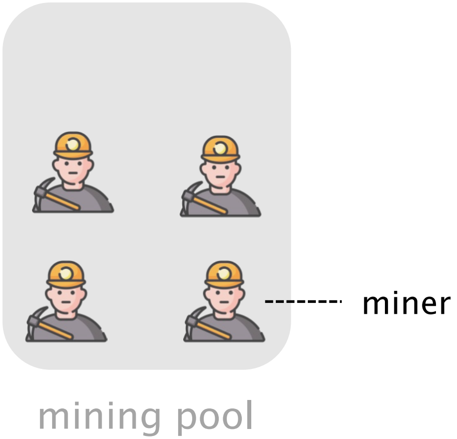
United cryptocurrencies also fall.

This work

Uncovering…

mining pools as a new attack target

A mining pool is a group of miners

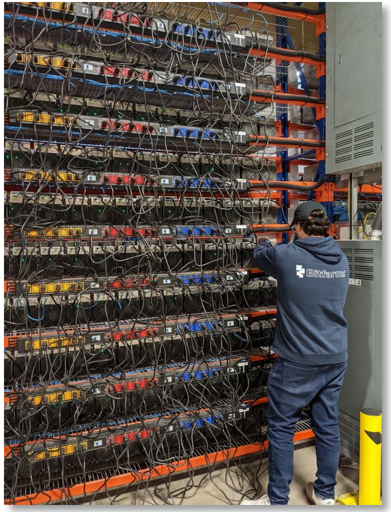


A mining pool is a group of miners

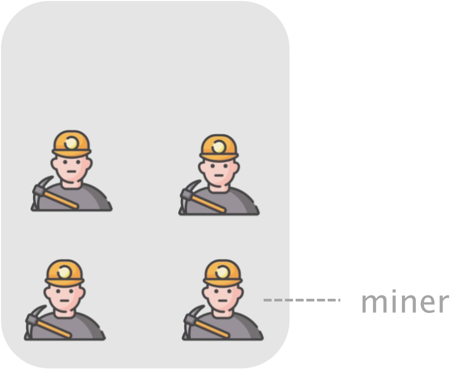
dedicated hardware

mining rig

ASIC miner



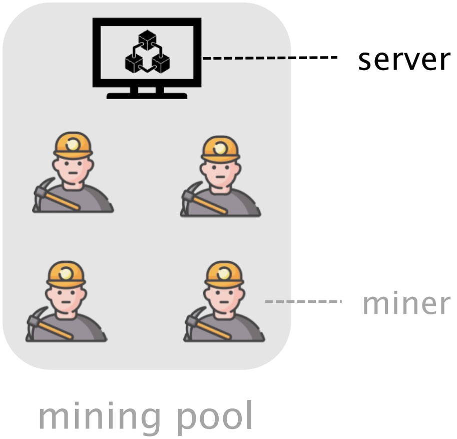
mining facility



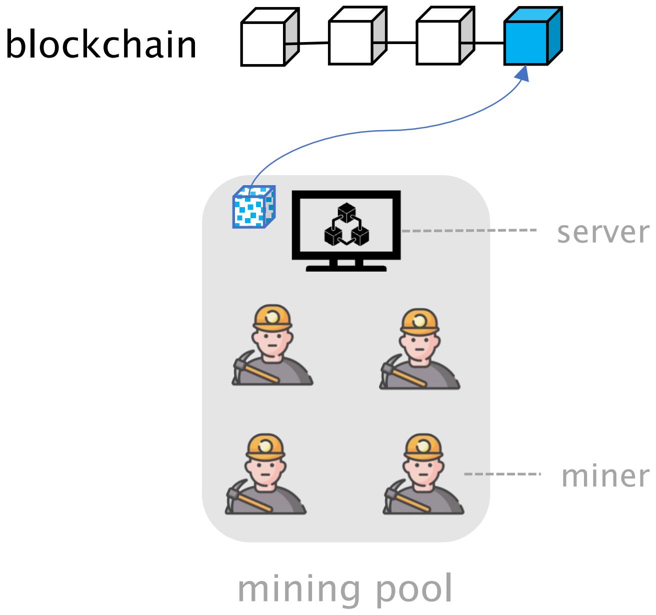
mining pool

A mining pool is a group of miners

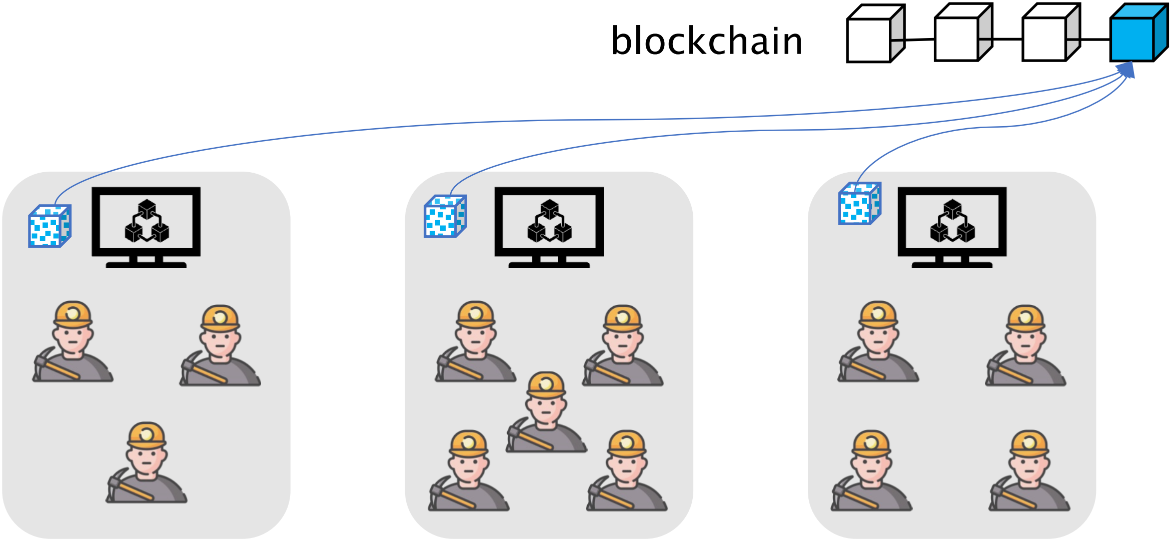
coordinated by a server



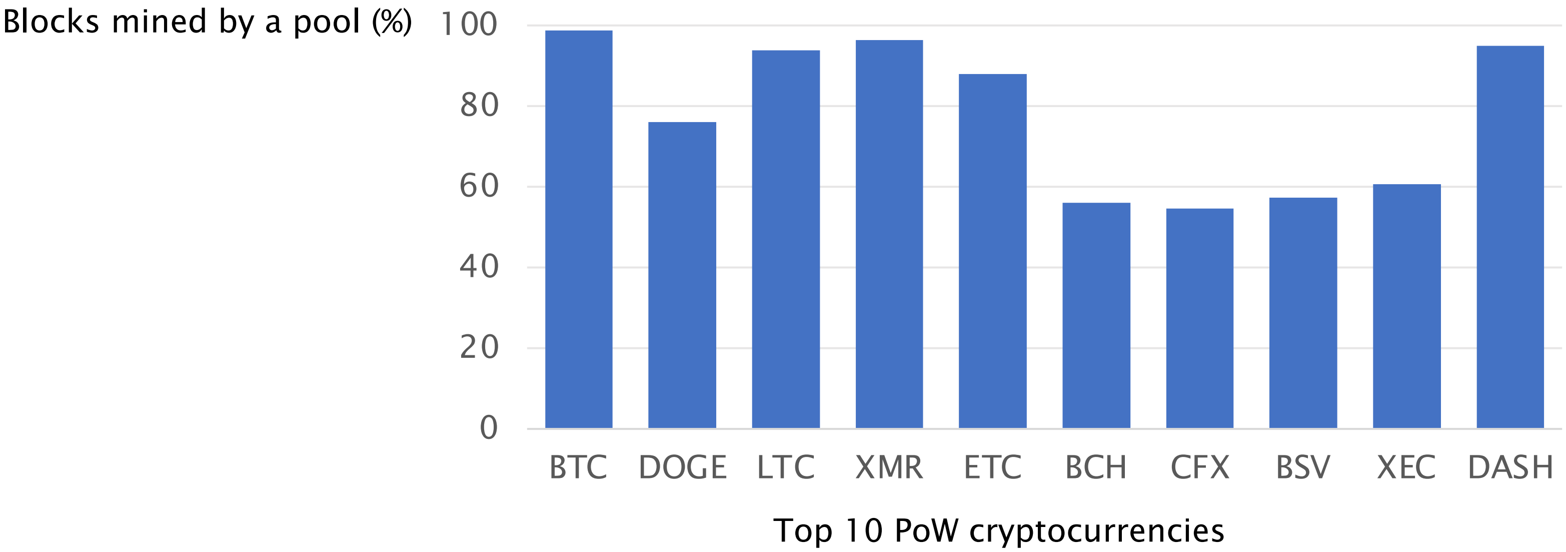
A mining pool is a group of miners coordinated by a server to find new blocks



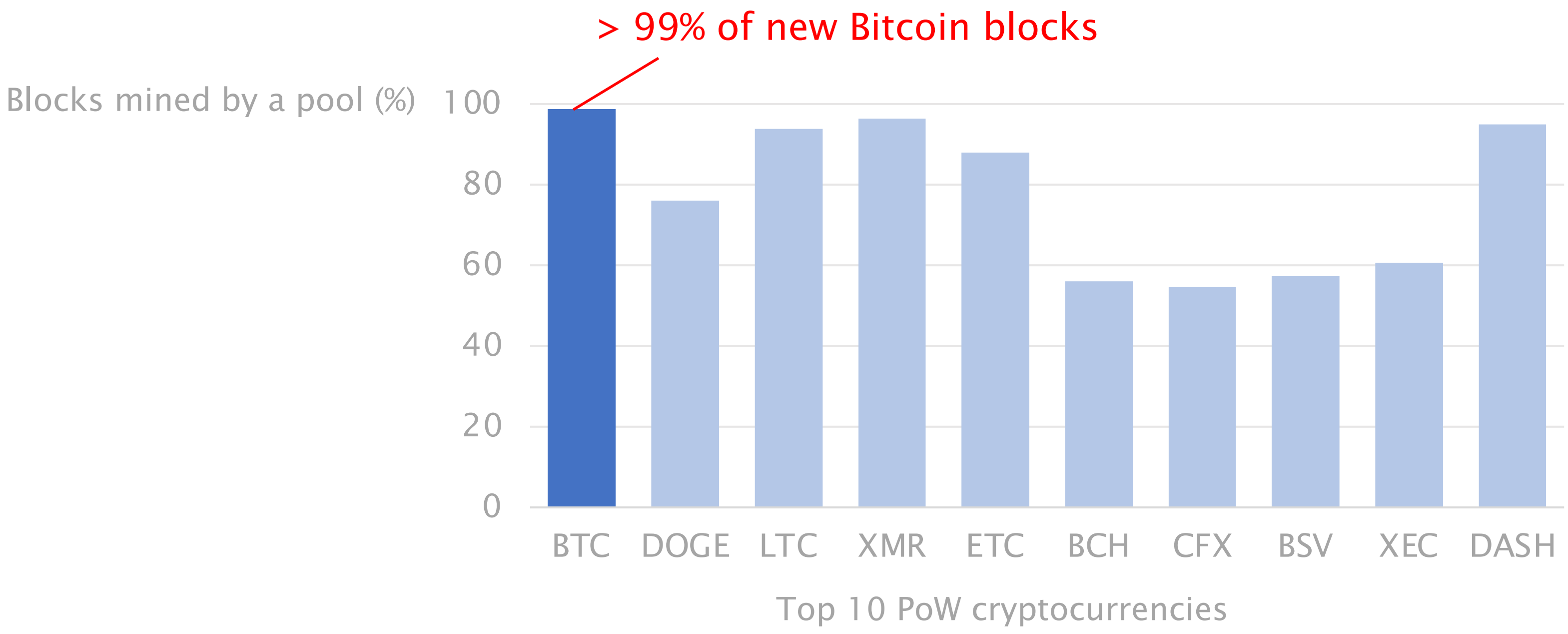
Mining pools competing to create new blocks for rewards in return



Mining pools account for most of new blocks



Mining pools account for most of new blocks



> 99% of new Bitcoin blocks

Introducing
the Erosion attacks

1 how to disrupt mining pools with routing attacks

2 how to create stealthier attacks with a new vulnerability

3 how to mitigate the attacks

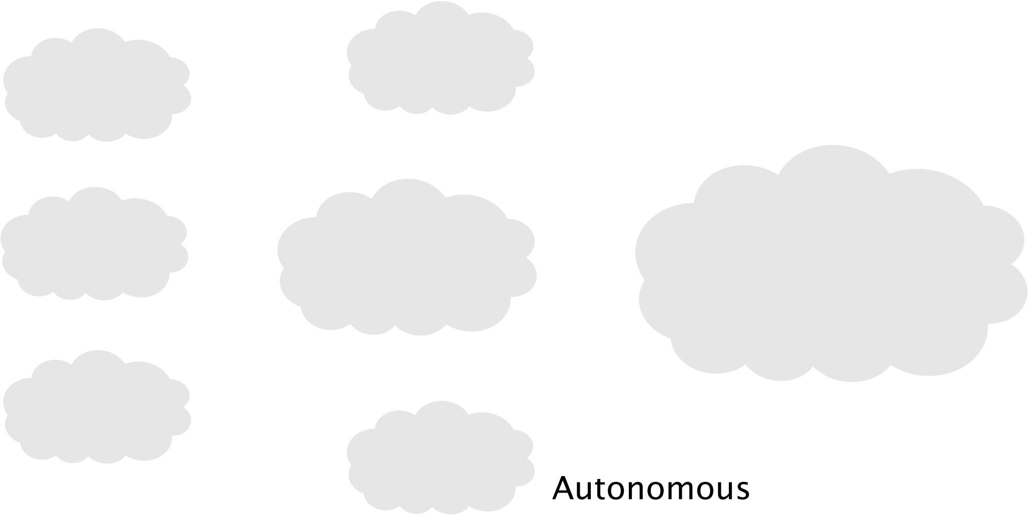
Introducing
the Erosion attacks

1 how to disrupt mining pools with routing attacks

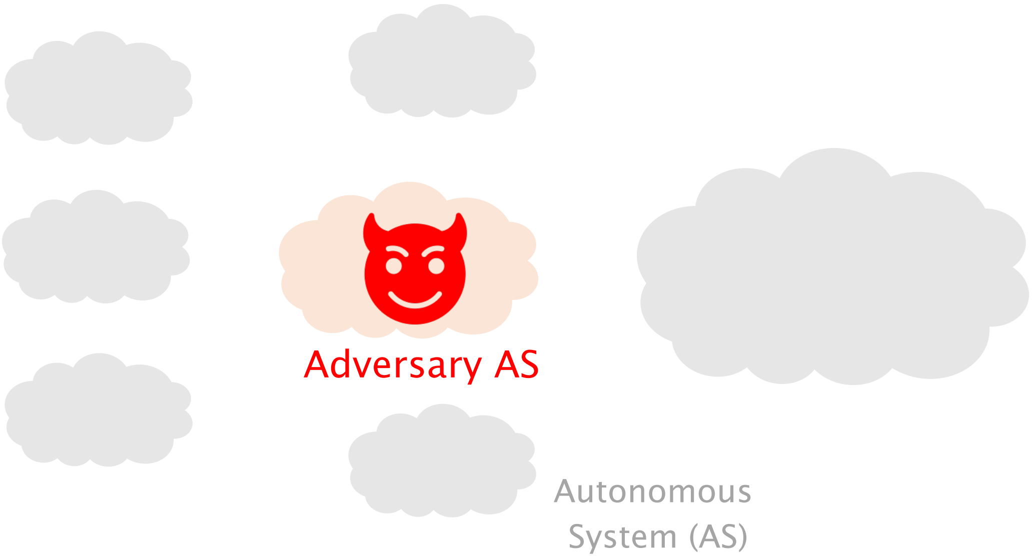
2 how to create stealthier attacks with a new vulnerability

3 how to mitigate the attacks

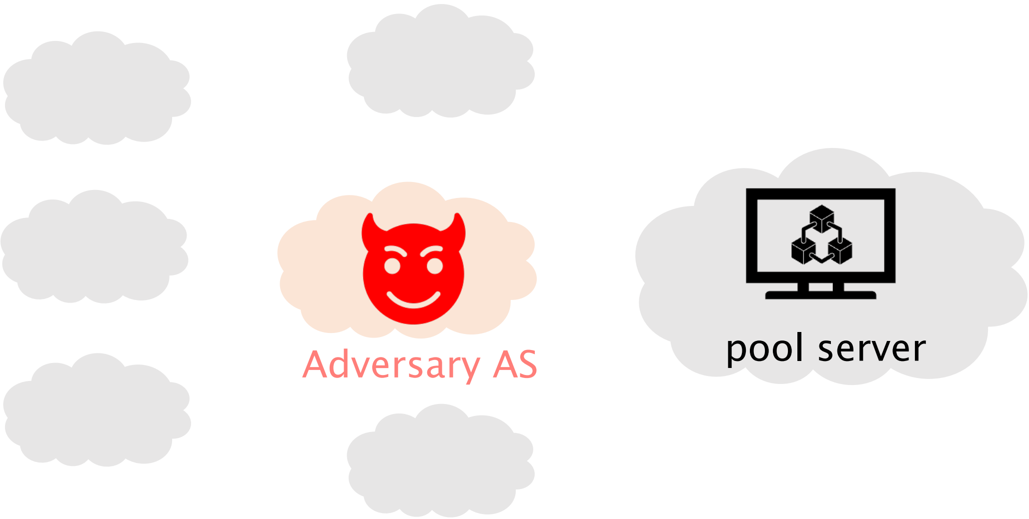
Threat model: the adversary controls a malicious AS



Threat model: the adversary controls a malicious AS

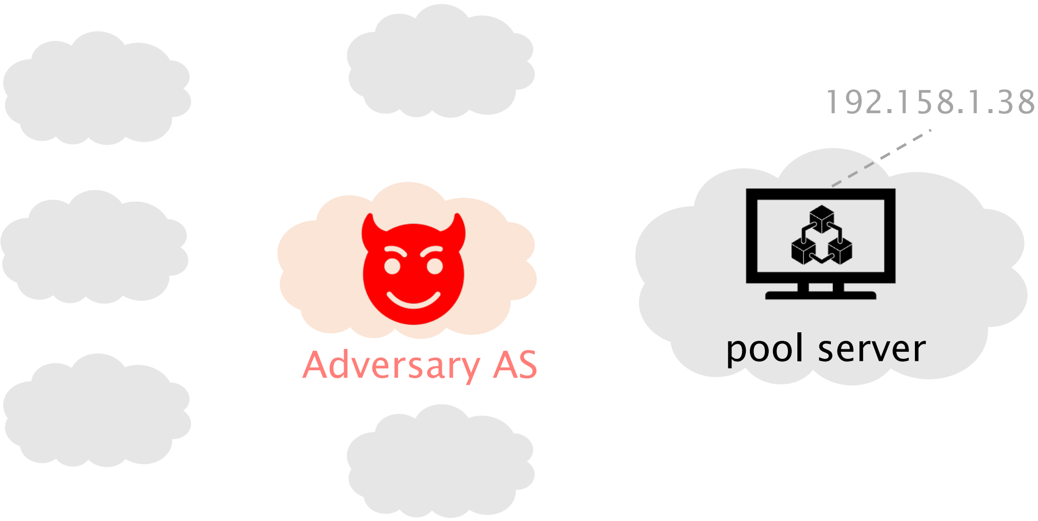


The adversary first identifies targeted pools



The adversary first identifies targeted pools

having accessible servers



55 active mining pools

10 top PoW cryptocurrencies

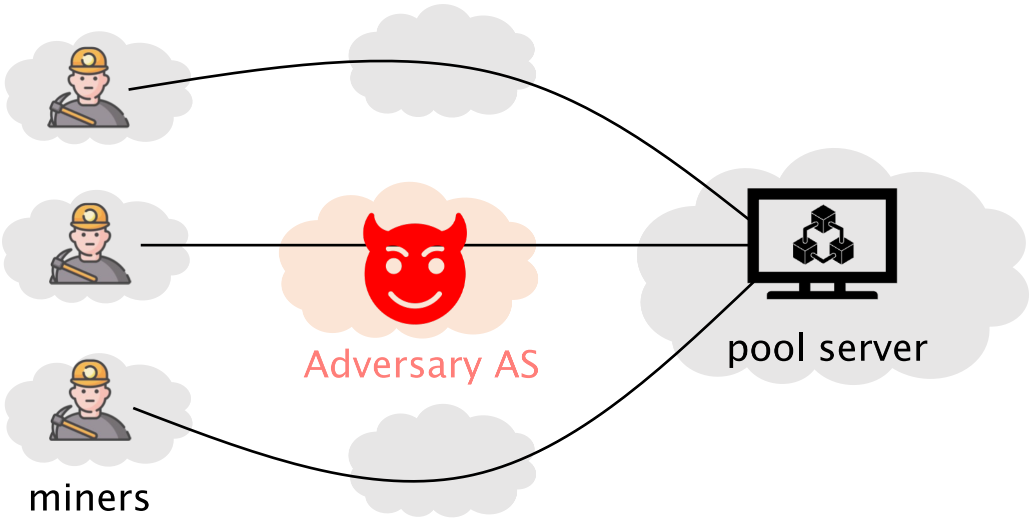
- 2Miners
- 666pool
- Antpool
- Binance Pool
- Braiins Pool
- BTC.com Pool
- C3Pool
- CrazyPool
- DxPool
- EMCD
- Ethermine
- Ezil
- F2Pool
- Flexpool
- Foundry USA Pool
- GNTL Monero Pool
- GorillaPool
- HashVault
- HeroMiners
- Hiveon Pool
- K1Pool
- Kryptex Pool
- KuCoin Pool
- LitecoinPool
- Luxor Mining Pool
- Mining-Dutch
- Mining Pool Hub
- MoneroHash
- MoneroOcean
- Nanopool
- NiceHash
- PEGA Pool
- POOL-MOSCOW
- Poolflare
- Poolin
- Prohashing
- SBICrypto Pool
- Sigmapool
- Skypool
- solomining.io
- SoloPool
- SupportXMR
- Toomim
- Ultimus Pool
- ViaBTC
- Volt mine
- WoolyPooly
- XMRPool
- Zergpool
- ZULUPooL
- HyperDonkey
- MaraPool
- p2p-spb
- P2Pool
- TAAL

91% mining pools can be targeted for attacks

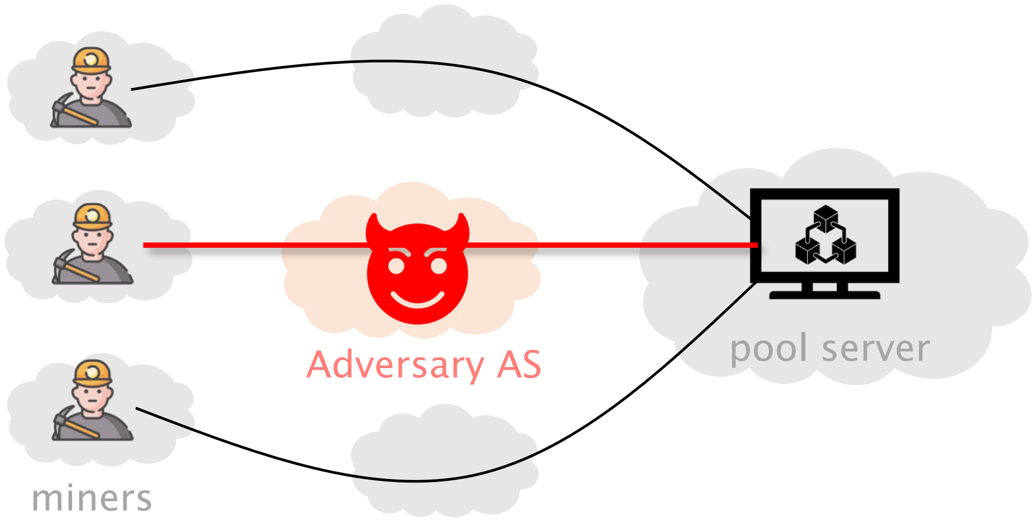
2Miners
666pool
Antpool
Binance Pool
Braiins Pool
BTC.com Pool
C3Pool
CrazyPool
DxPool
EMCD
Ethermine
Ezil
F2Pool
Flexpool
Foundry USA Pool
GNTL Monero Pool
GorillaPool
HashVault
HeroMiners
Hiveon Pool
K1Pool
Kryptex Pool
KuCoin Pool
LitecoinPool
Luxor Mining Pool
Mining-Dutch
Mining Pool Hub
MoneroHash
MoneroOcean
Nanopool
NiceHash
PEGA Pool
POOL-MOSCOW
Poolflare
Poolin
Prohashing
SBICrypto Pool
Sigmapool
Skypool
solomining.io
SoloPool
SupportXMR
Toomim
Ultimus Pool
ViaBTC
Volt mine
WoolyPooly
XMRPool
Zergpool
ZULUPooL

HyperDonkey
MaraPool
p2p-spb
P2Pool
TAAL

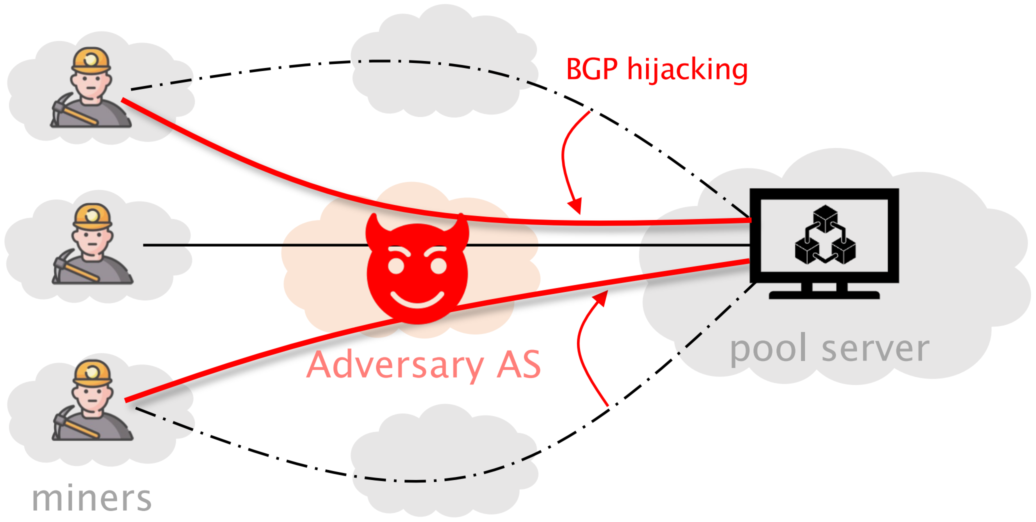
The adversary intercepts pool-miner connections



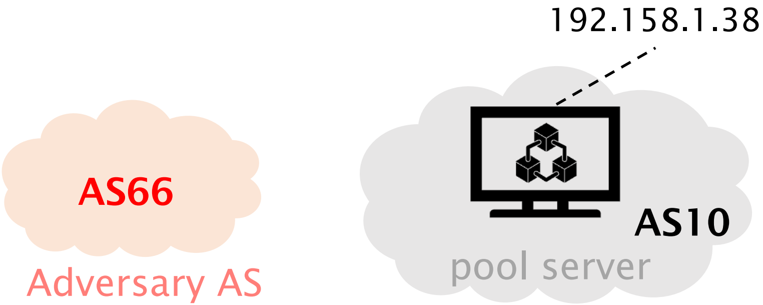
The adversary intercepts pool-miner connections naturally



The adversary intercepts pool-miner connections naturally or **using BGP hijacking**



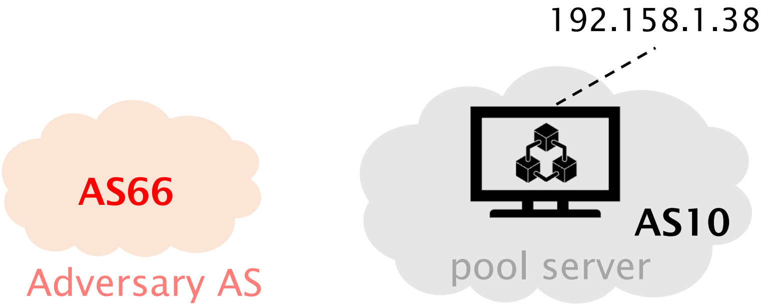
To hijack traffic, the adversary advertises bogus BGP messages



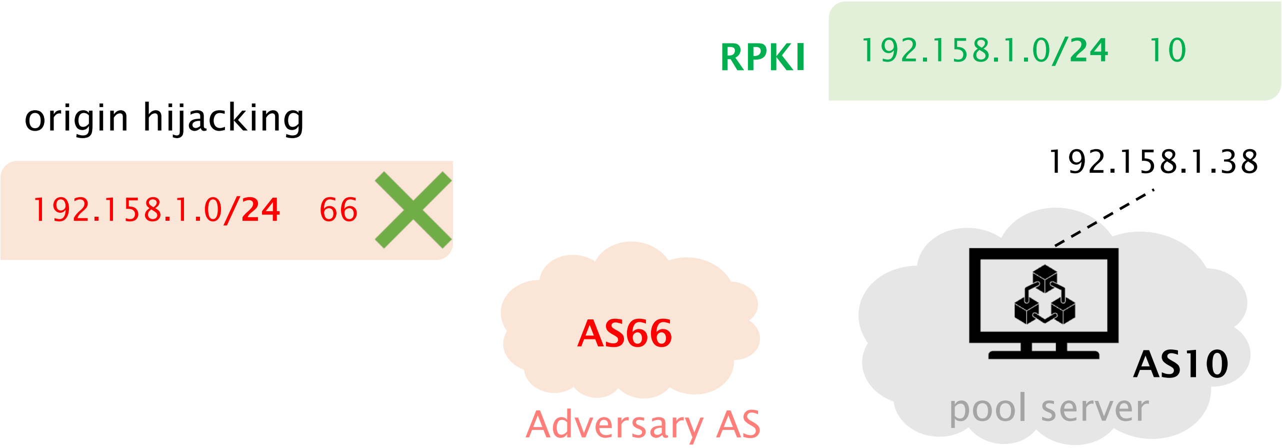
To hijack traffic, the adversary advertises bogus BGP messages

origin hijacking

192.158.1.0/**24** 66



To hijack traffic, the adversary advertises bogus BGP messages



RPKI 192.158.1.0/24 10

origin hijacking

192.158.1.0/24 66 ✗

192.158.1.38

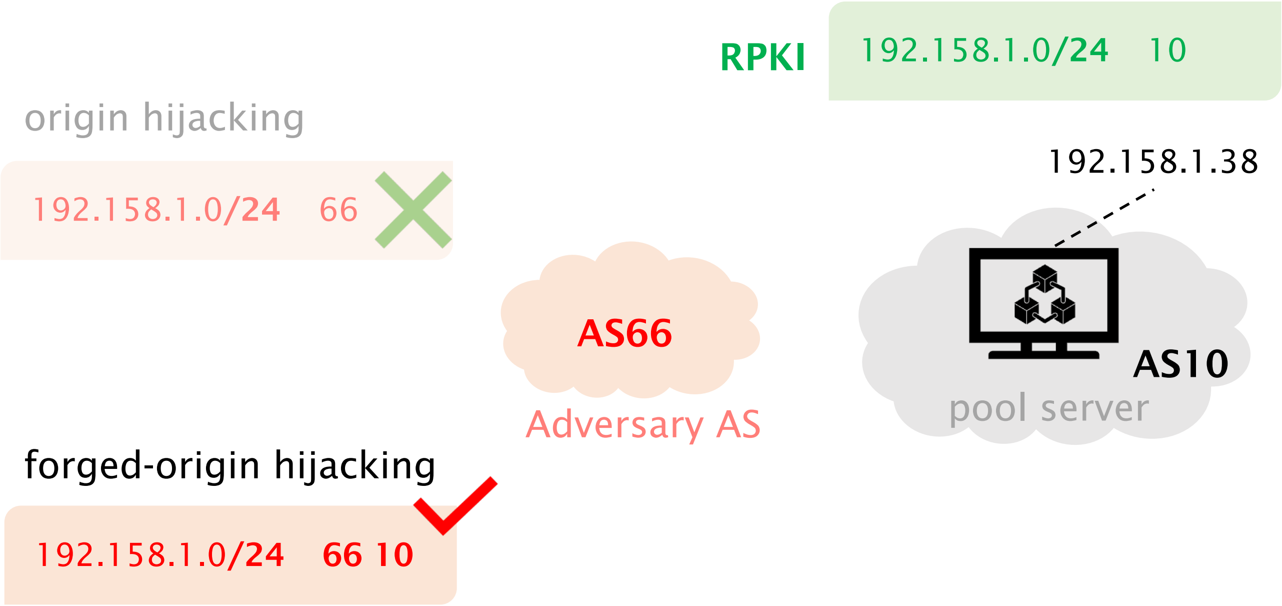
AS66

Adversary AS

AS10

pool server

To hijack traffic, the adversary advertises bogus BGP messages



RPKI

192.158.1.0/24 10

origin hijacking

192.158.1.0/24 66 ✗

forged-origin hijacking

192.158.1.0/24 66 10 ✓

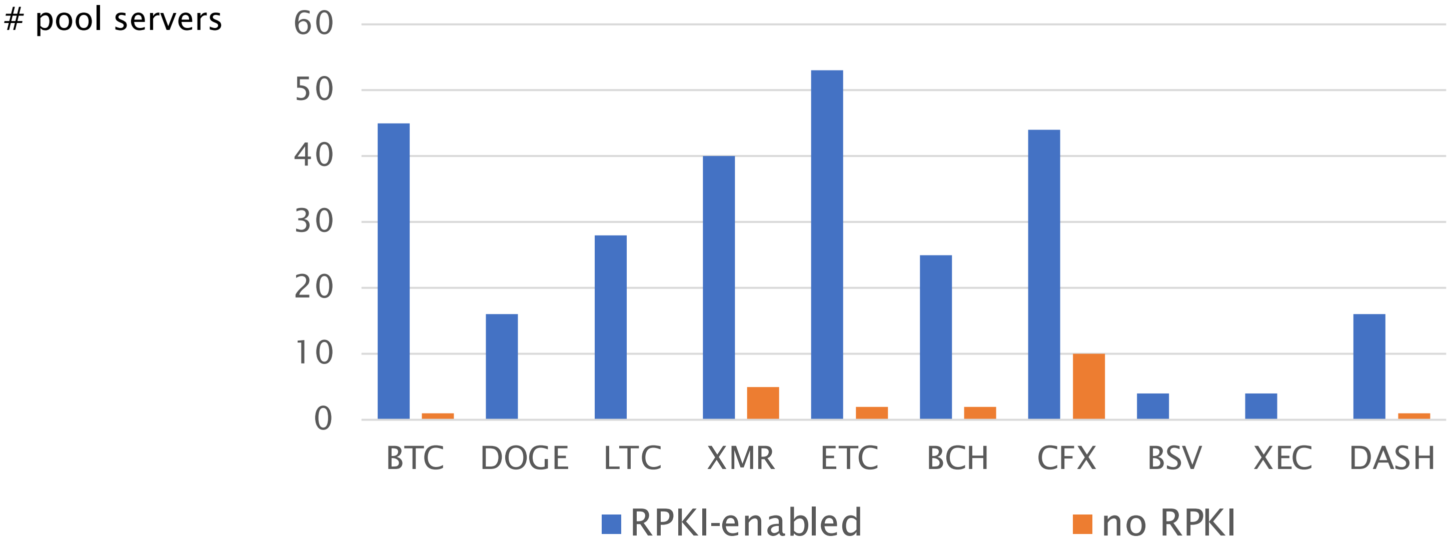
AS66

Adversary AS

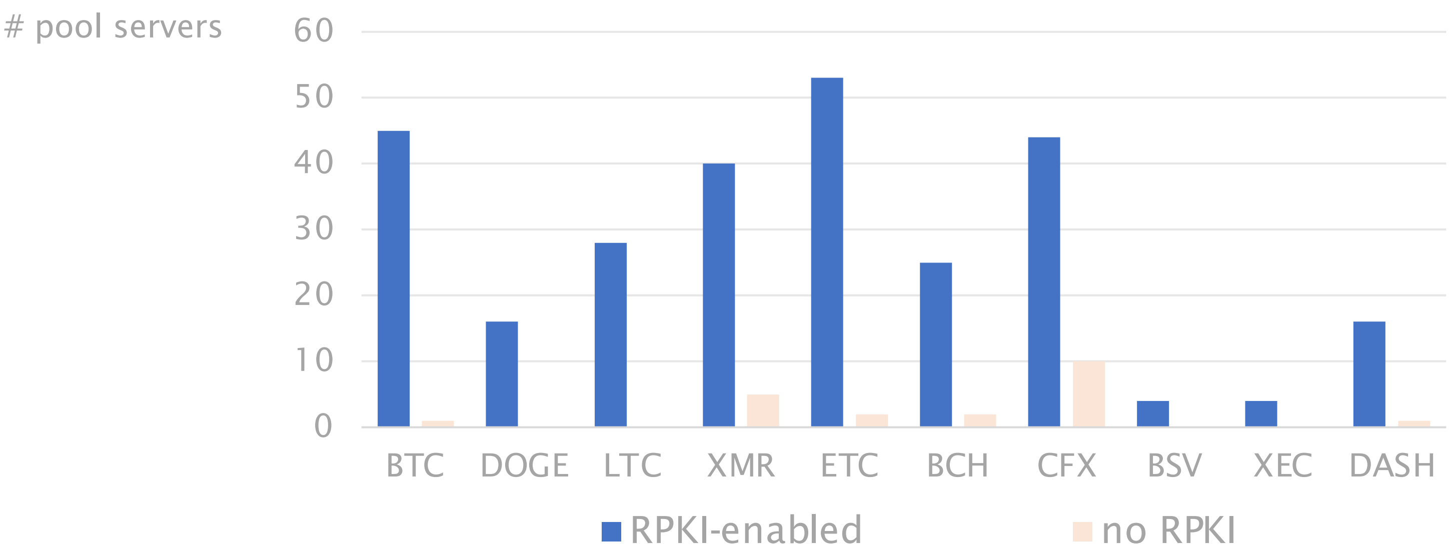
192.158.1.38

AS10

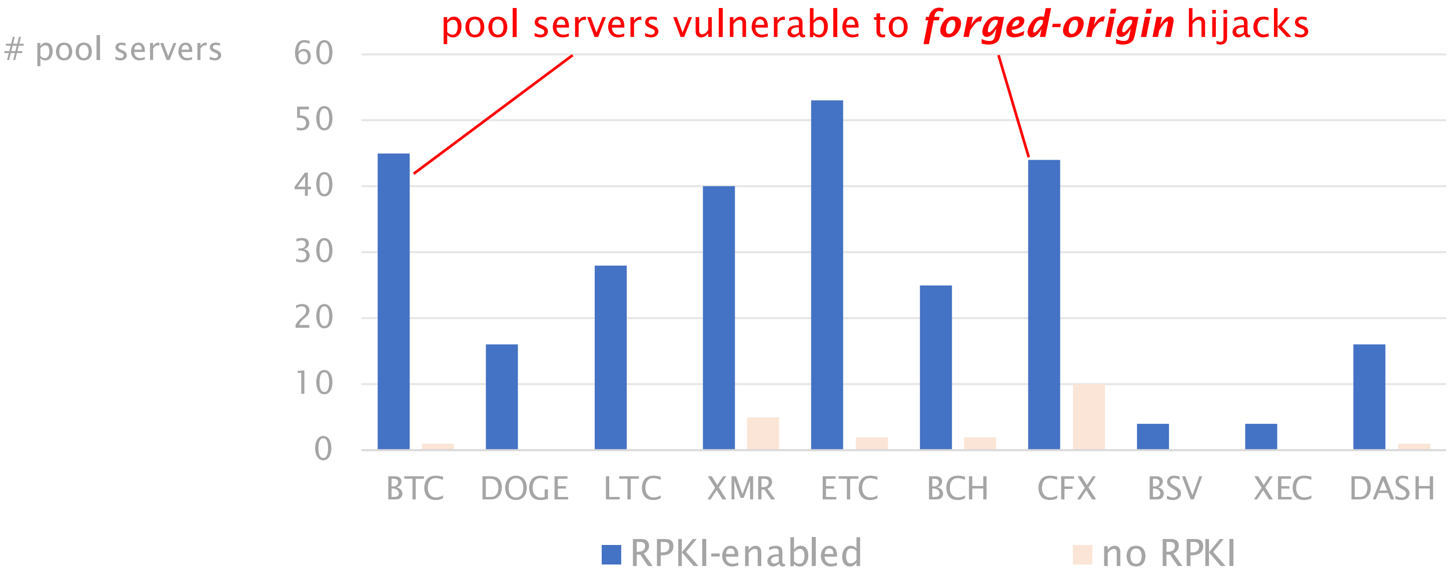
pool server


# pool servers
60
50
40
30
20
10
0
BTC
DOGE
LTC
XMR
ETC
BCH
CFX
BSV
XEC
DASH
RPKI-enabled
no RPKI

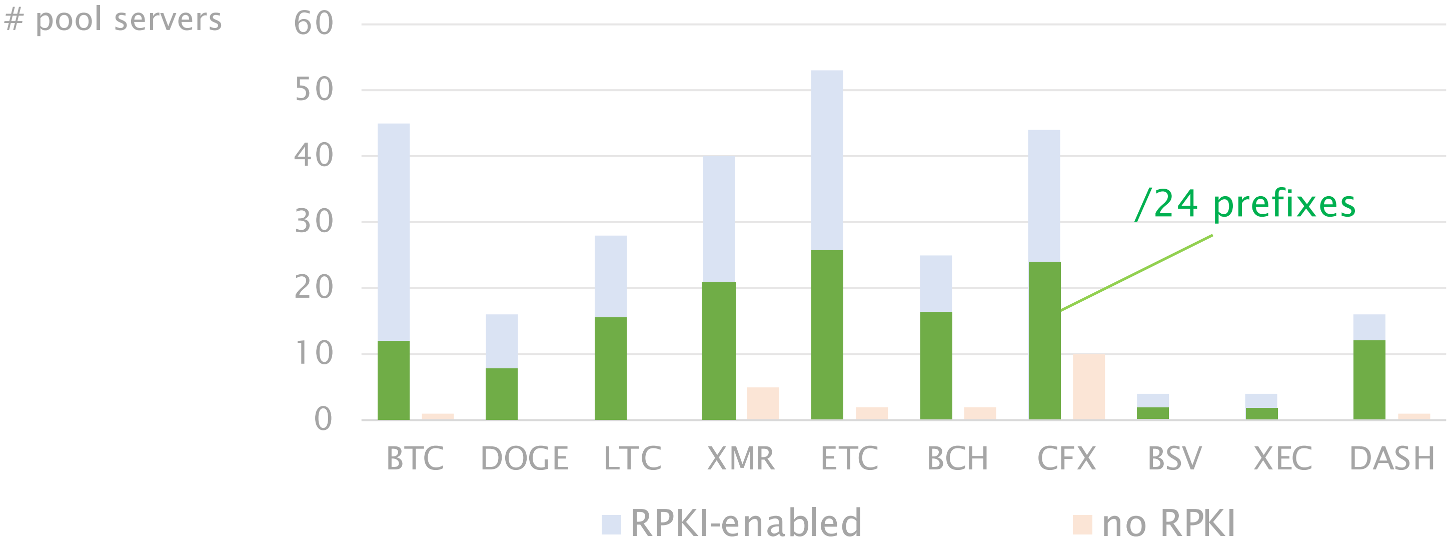
93% pool servers are protected by **RPKI**



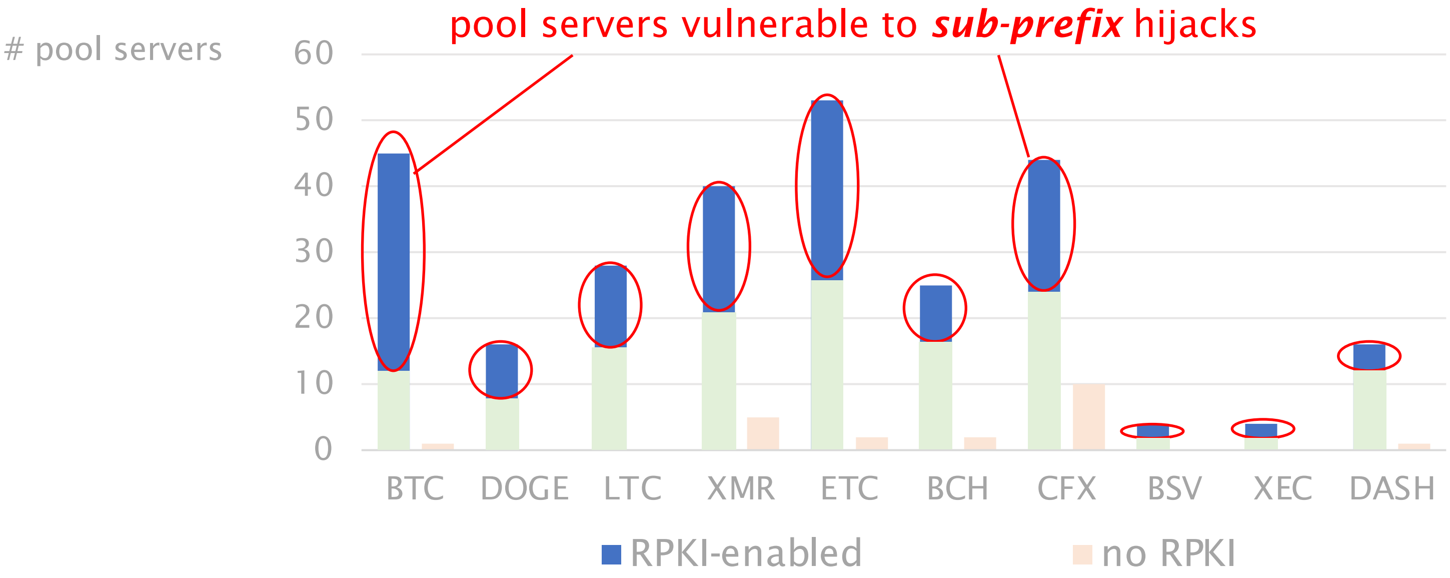
93% pool servers are protected by **RPKI**



52% pool servers are protected by **max-length prefixes**

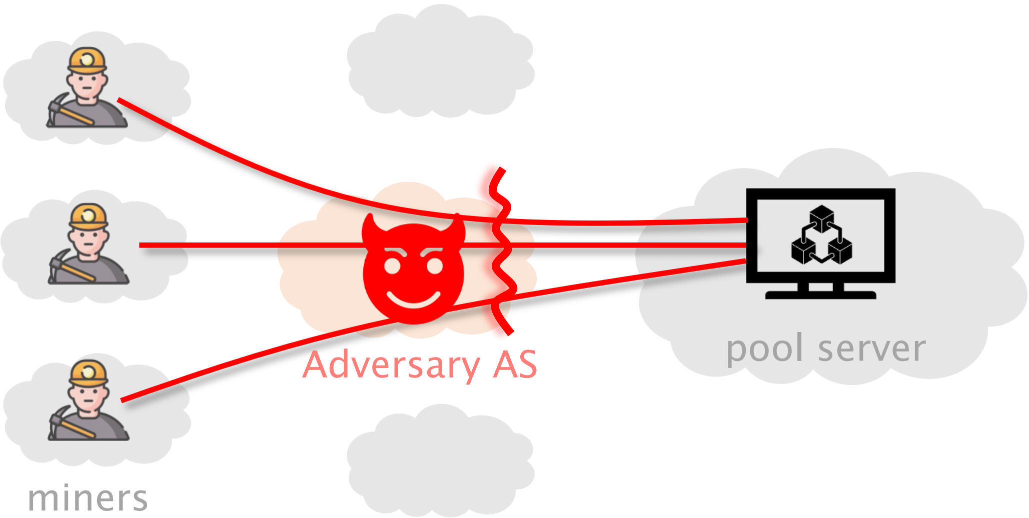


52% pool servers are protected by **max-length prefixes**

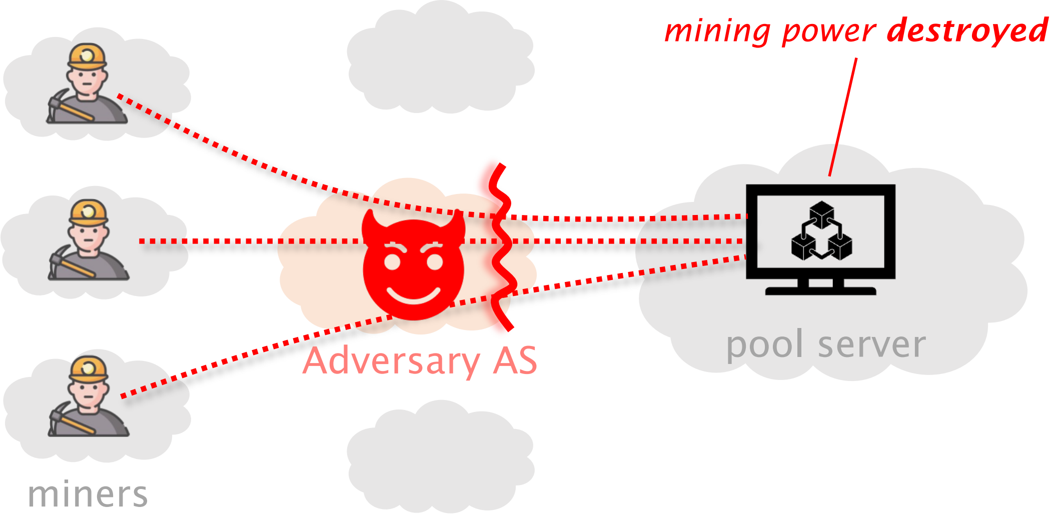


pool servers vulnerable to ***sub-prefix*** hijacks

The adversary then drops the intercepted pool-miner connections



The adversary then drops the intercepted pool-miner connections



Introducing
the Erosion attacks

1 how to disrupt mining pools with routing attacks

2 how to create stealthier attacks with a new vulnerability

3 how to mitigate the attacks

Hijacking and dropping mining pool traffic can be quite visible

Hijacking and dropping mining pool traffic can be quite visible

Long-term BGP hijacks cause attention

impactful attacks last from minutes to hours

Hijacking and dropping mining pool traffic can be quite visible

Long-term BGP hijacks cause attention

impactful attacks last from minutes to hours

Dropping packets alerts victims

> 1% packet loss rate is not normal

We discover a mining protocol’s **vulnerablity** that enables **stealthier** attacks

Long-term BGP hijacks cause attention

impactful attacks last from minutes to hours

Dropping packets alerts victims

> 1% packet loss rate is not normal

We discover a mining protocol's **vulnerablity** that enables **stealthier** attacks

Long-term BGP hijacks cause attention

impactful attacks last from minutes to hours

Dropping packets alerts victims

> 1% packet loss rate is not normal

Only ***minimal packet tampering*** needed

We discover a mining protocol’s **vulnerablity** that enables **stealthier** attacks

Long-term BGP hijacks cause attention

impactful attacks last from minutes to hours

Only ***short-lived*** BGP hijacks needed

Dropping packets alerts victims

> 1% packet loss rate is not normal

Only ***minimal packet tampering*** needed

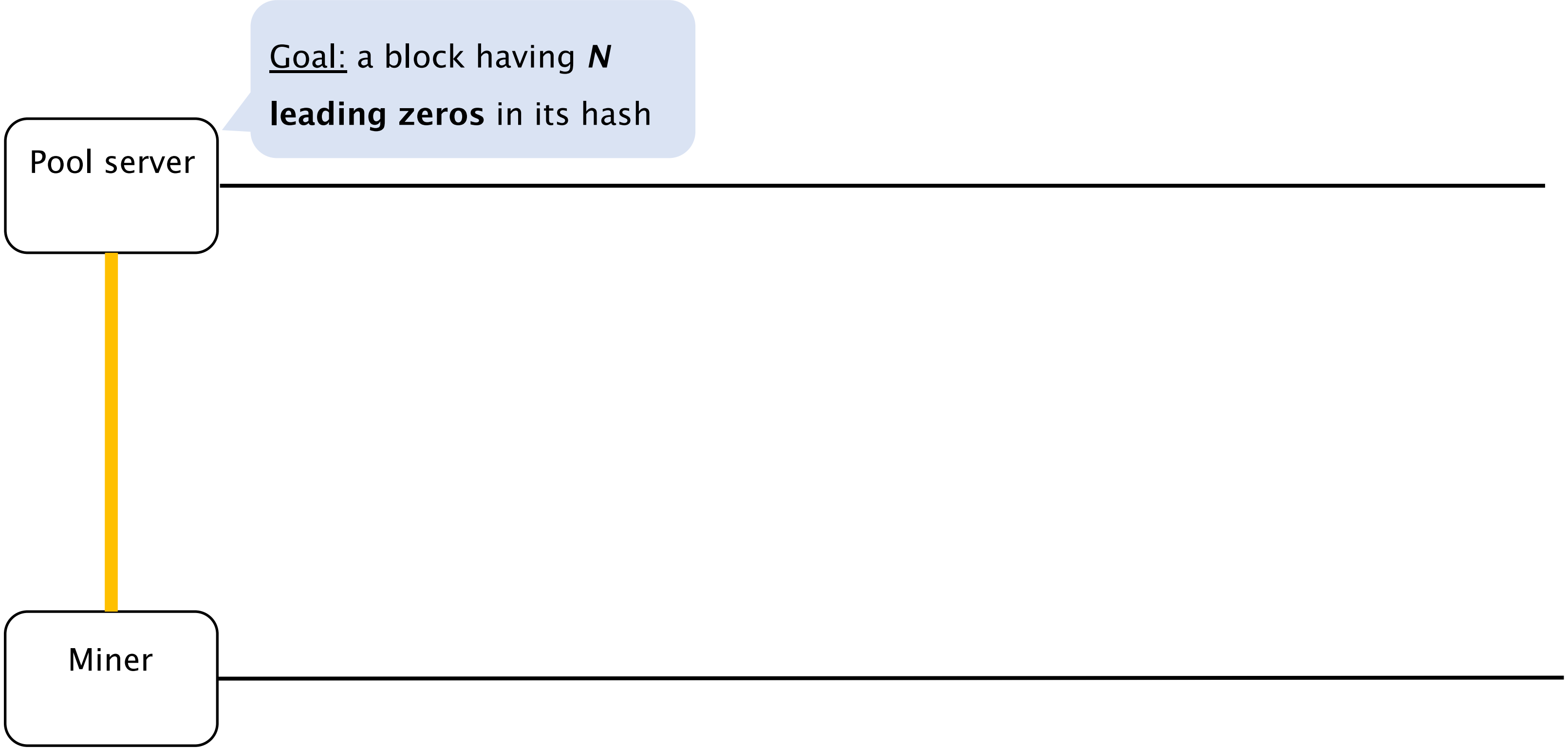
Stratum V1 has been the dominant mining protocol

Pool server

no encryption

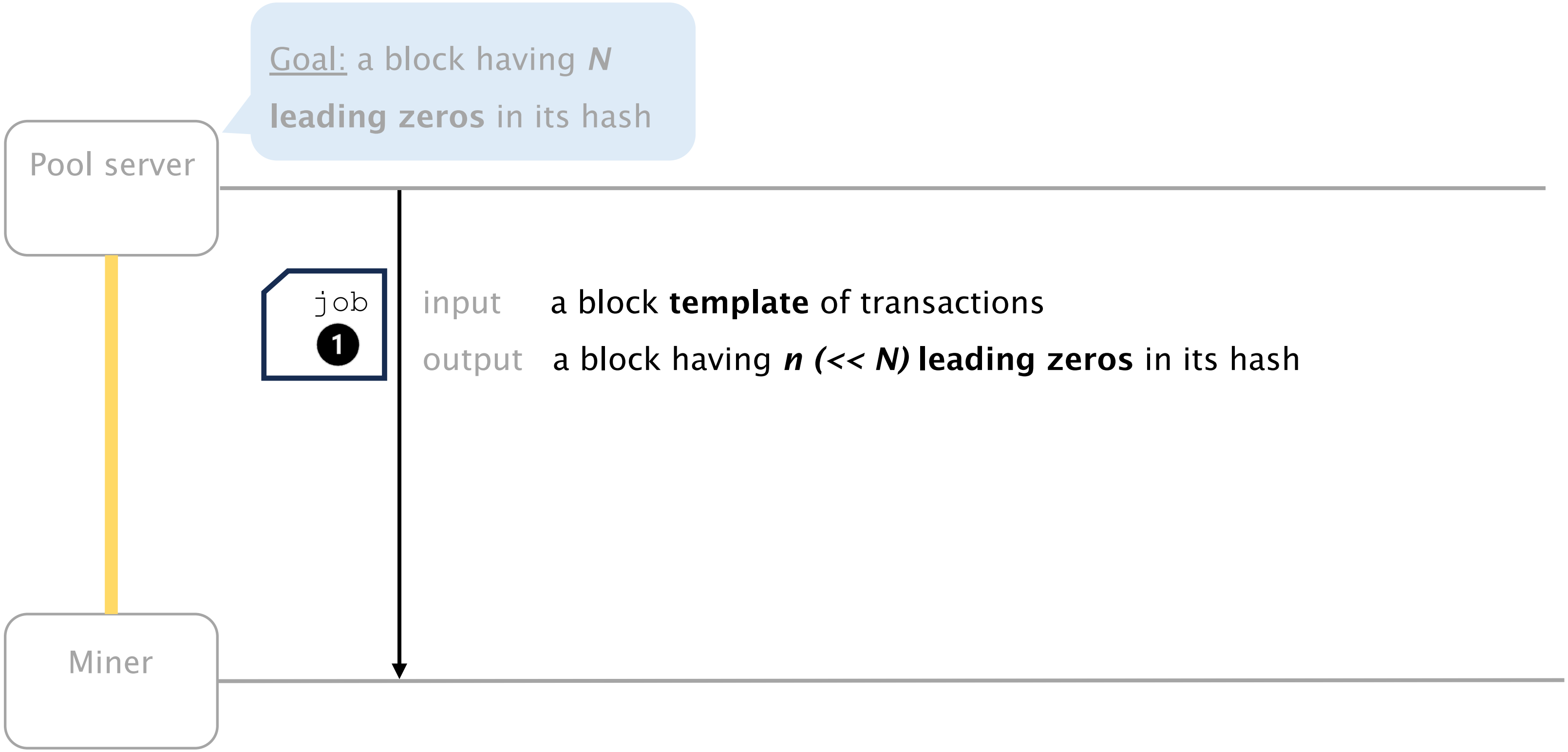
Miner

Stratum V1 has been the dominant mining protocol



Goal: a block having ***N*** **leading zeros** in its hash

Stratum V1 has been the dominant mining protocol

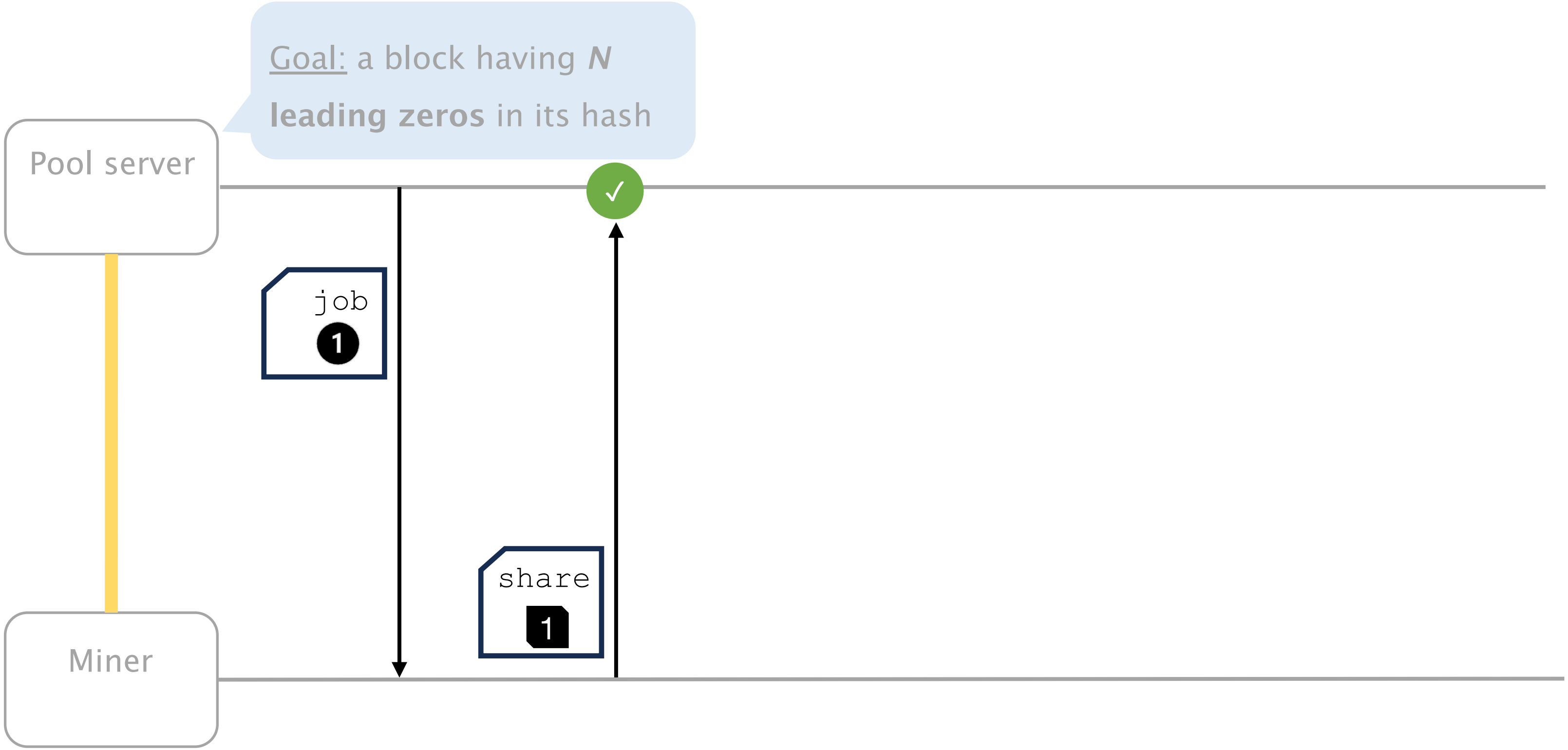


Goal: a block having ***N*** **leading zeros** in its hash

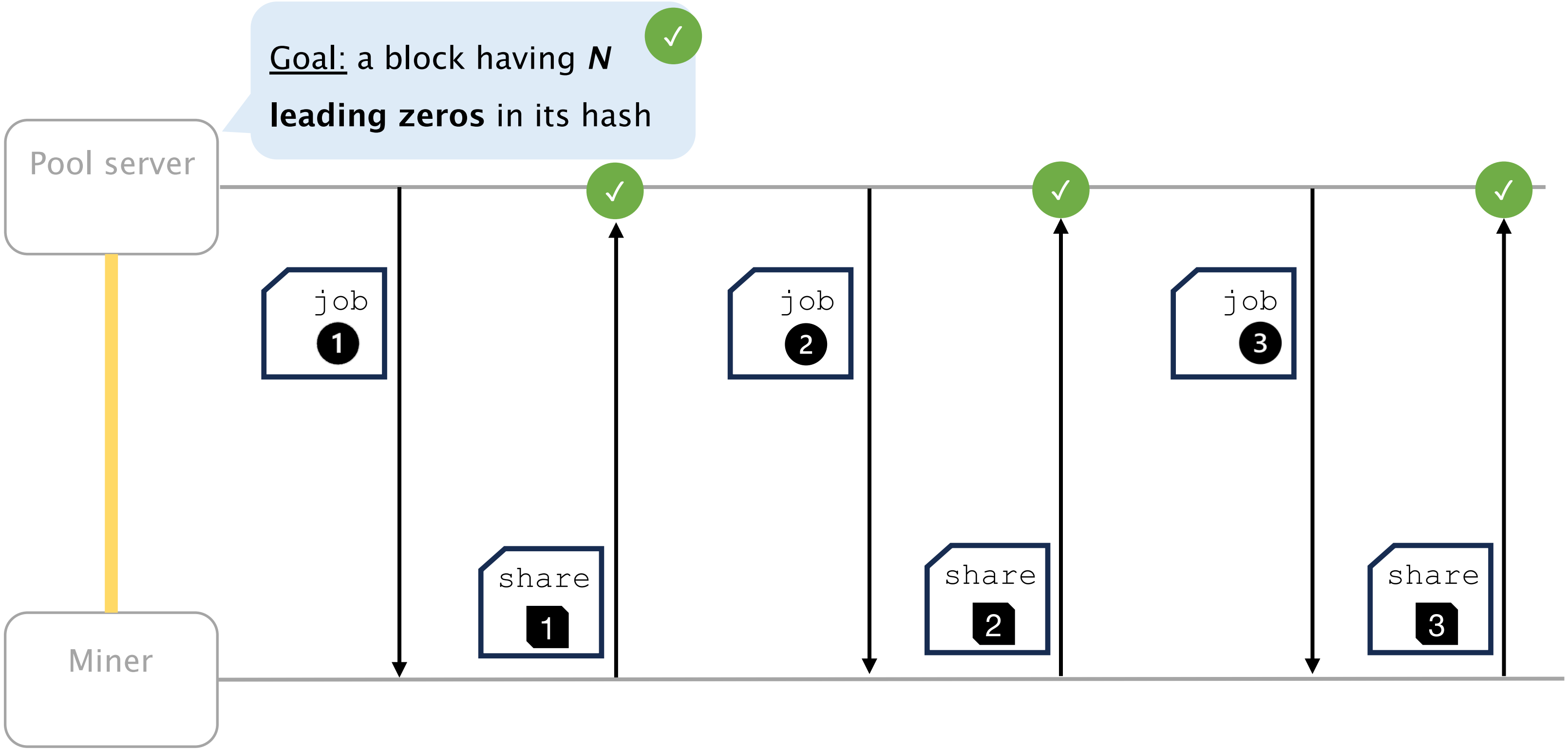
input a block **template** of transactions

output a block having ***n (<< N)*** **leading zeros** in its hash

Stratum V1 has been the dominant mining protocol



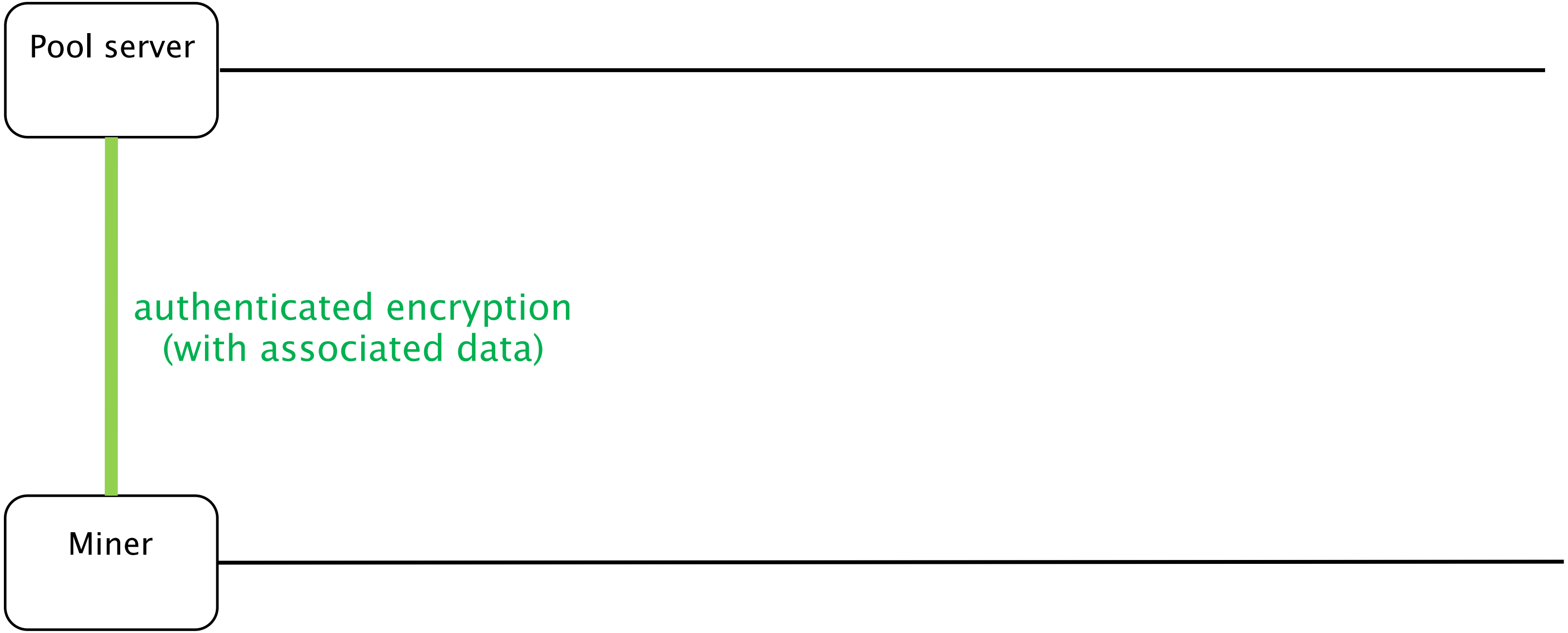
Stratum V1 has been the dominant mining protocol



Goal: a block having ***N*** **leading zeros** in its hash ✓

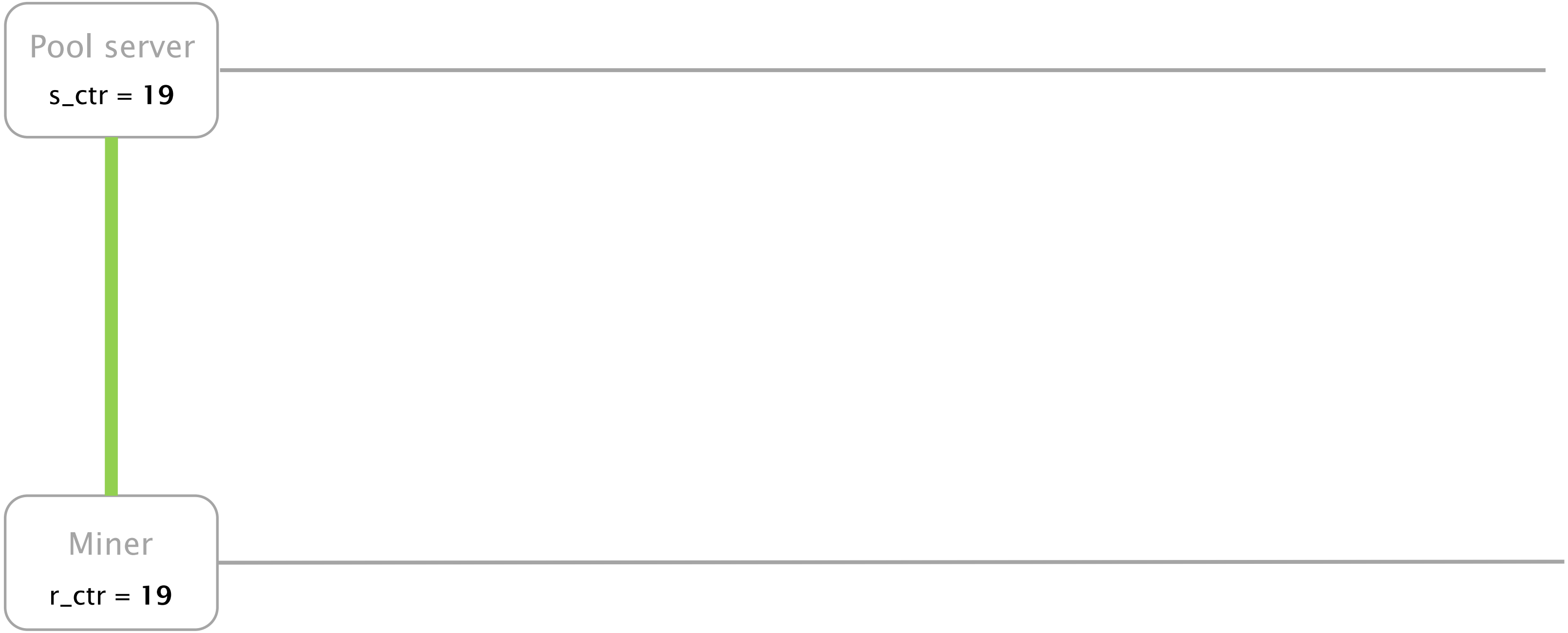
Stratum V2 supports encryption

and will become the standard mining protocol



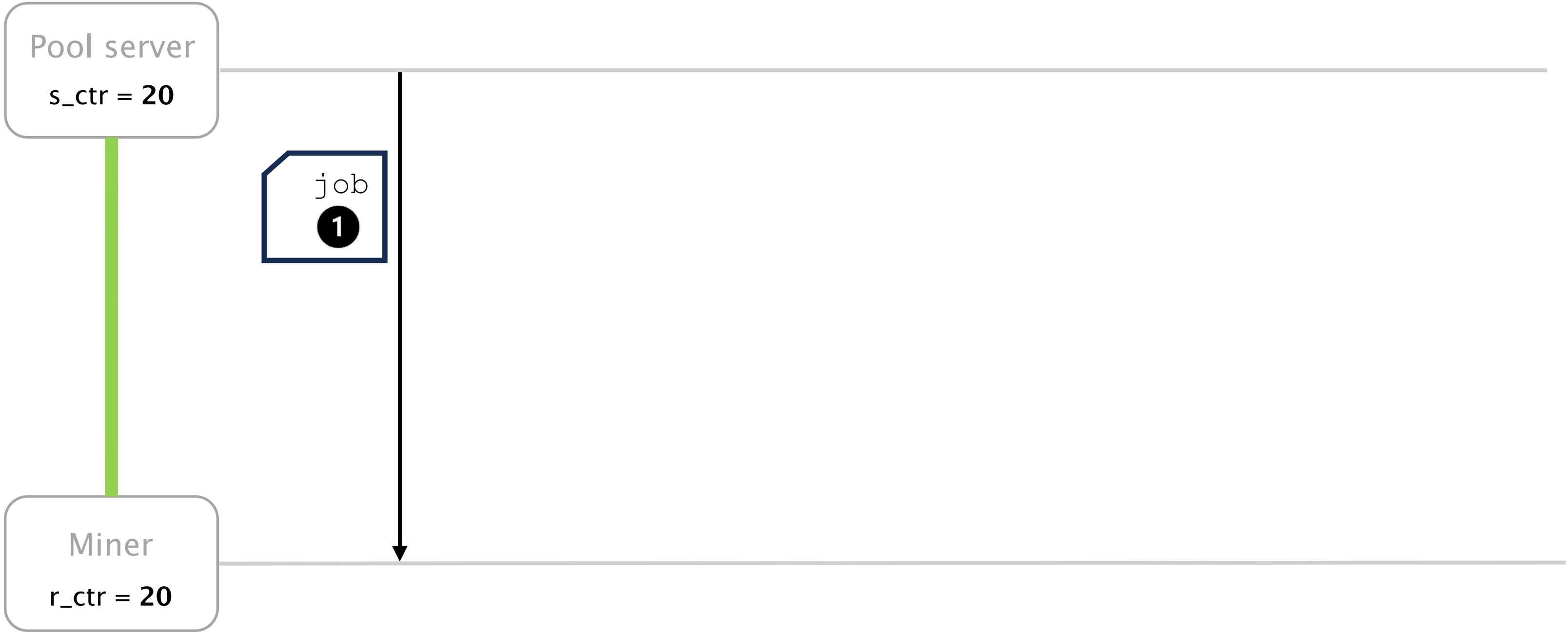
Stratum V2 supports encryption

and will become the standard mining protocol



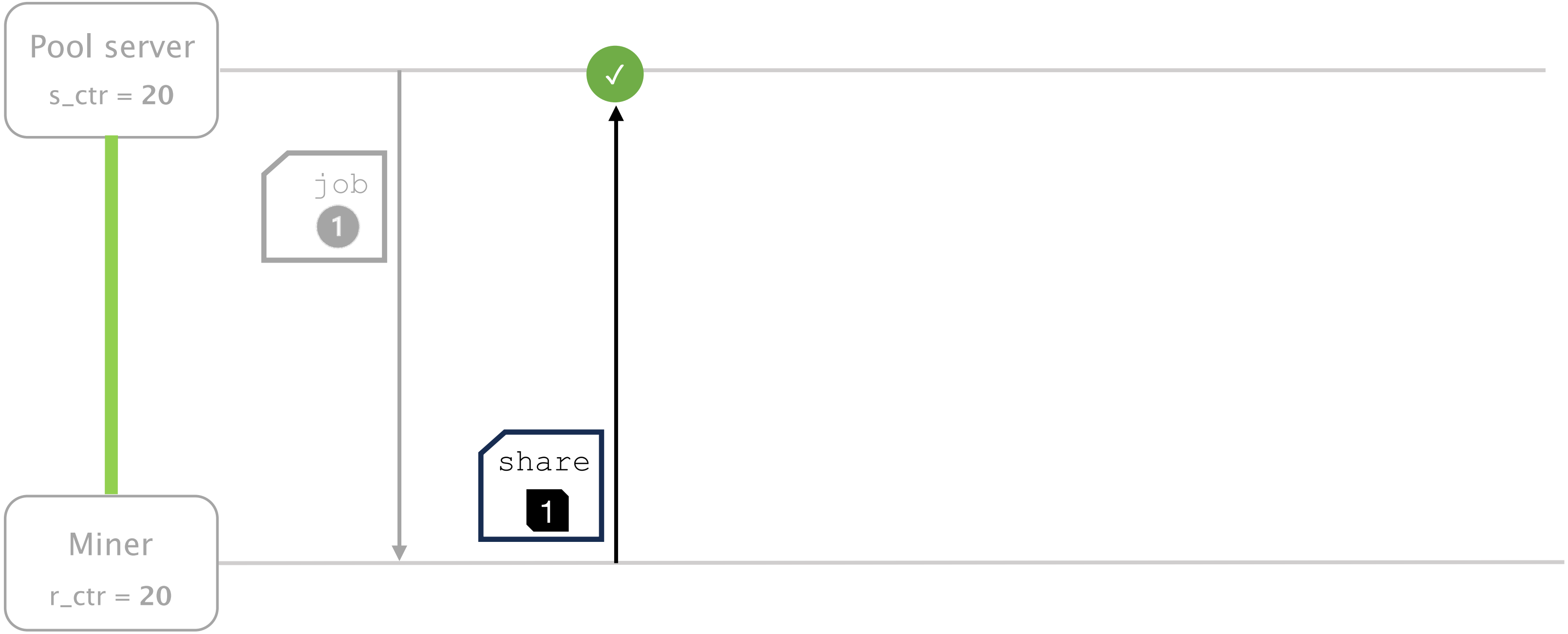
Stratum V2 supports encryption

and will become the standard mining protocol

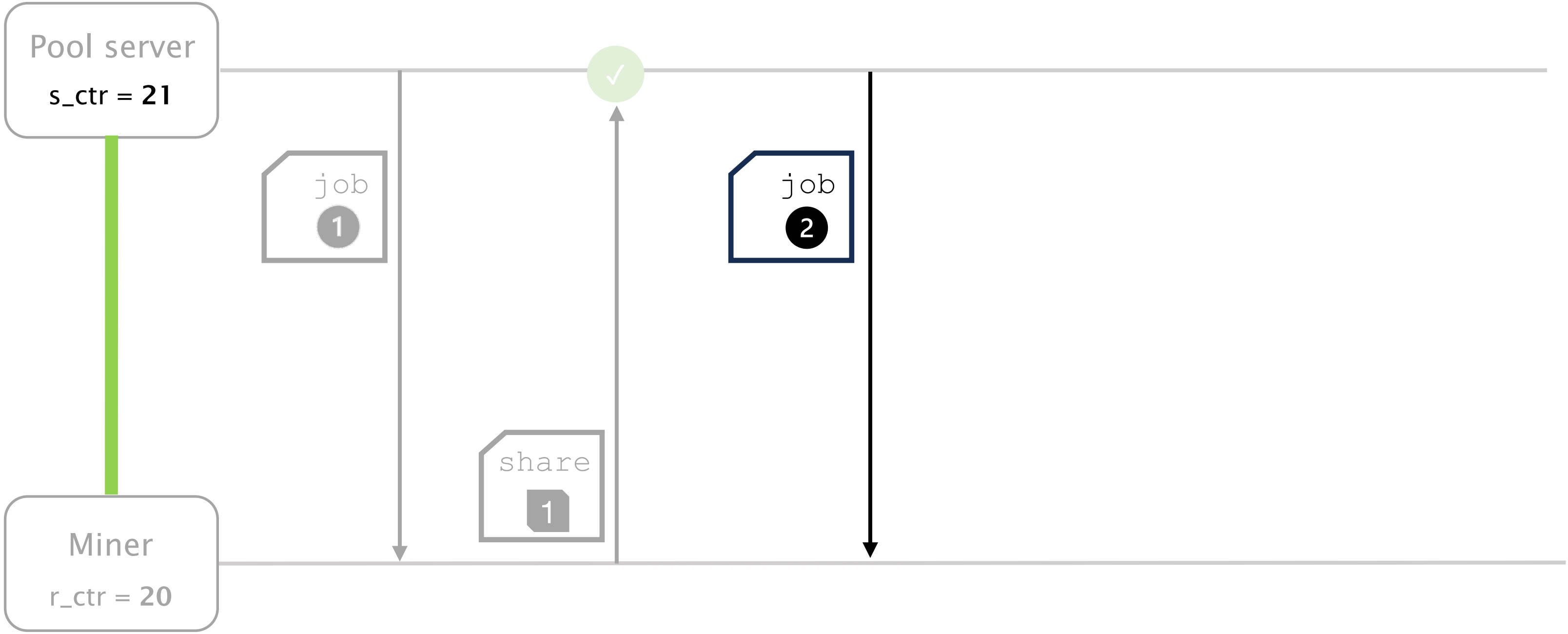


Stratum V2 supports encryption

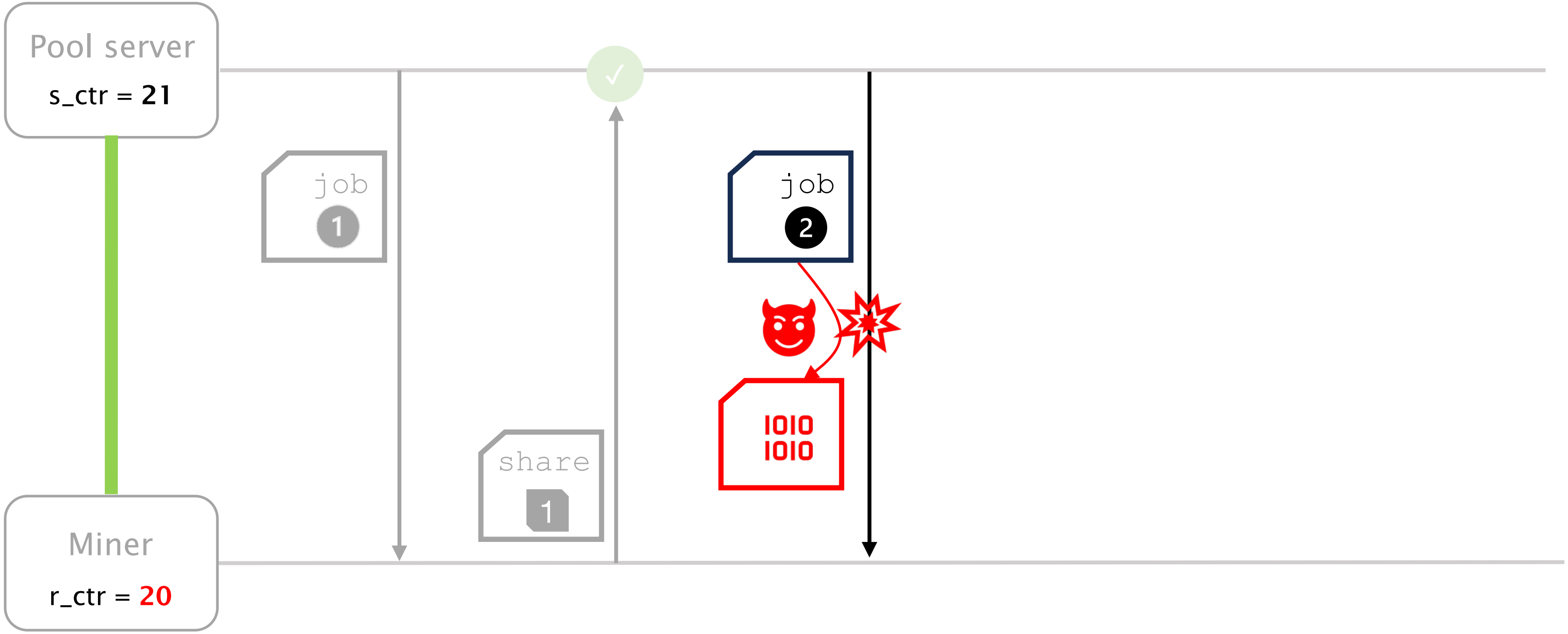
and will become the standard mining protocol



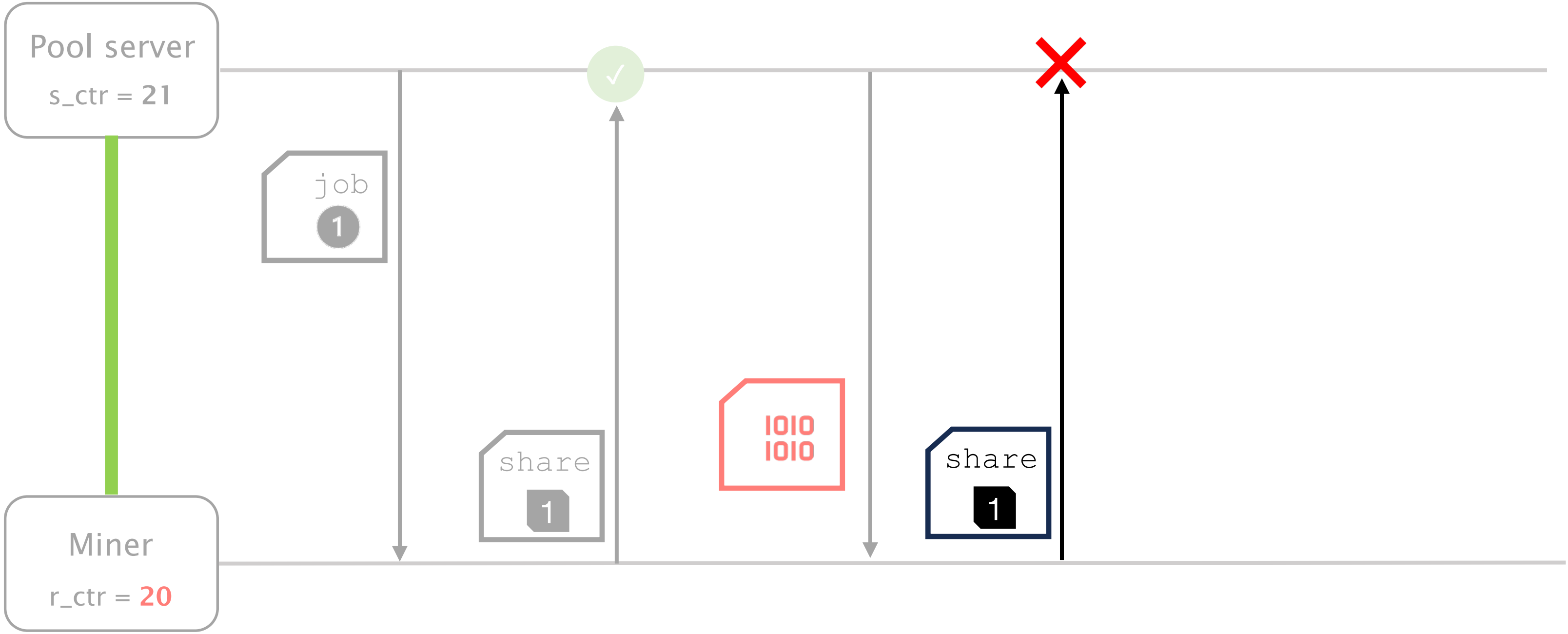
Stratum V2 has a vulnerability in handling decryption errors



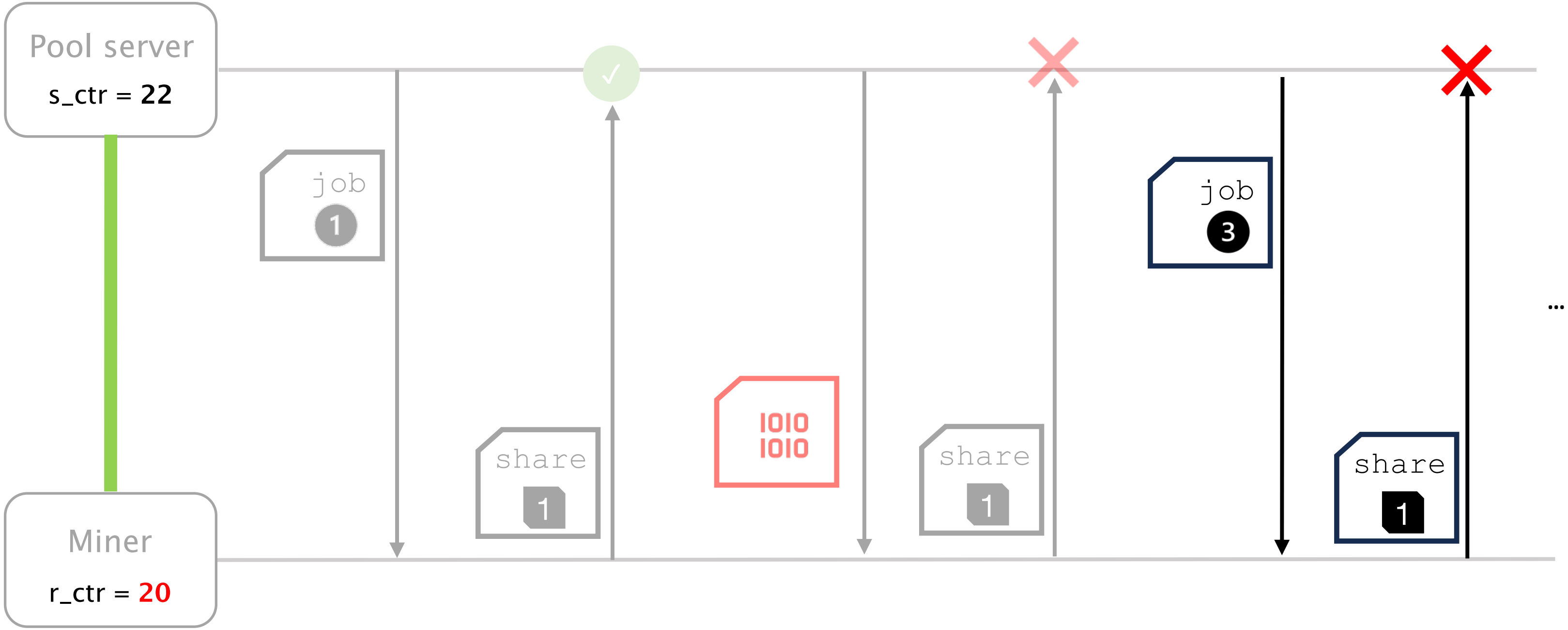
Stratum V2 has a vulnerability in handling decryption errors



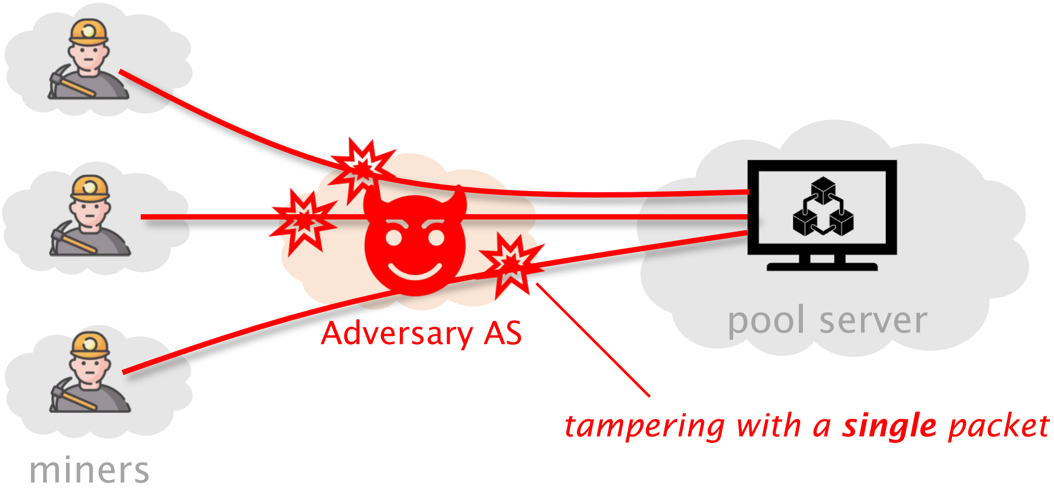
The vulnerability leads to rejected shares



The vulnerability leads to rejected shares
and persistent decryption failures

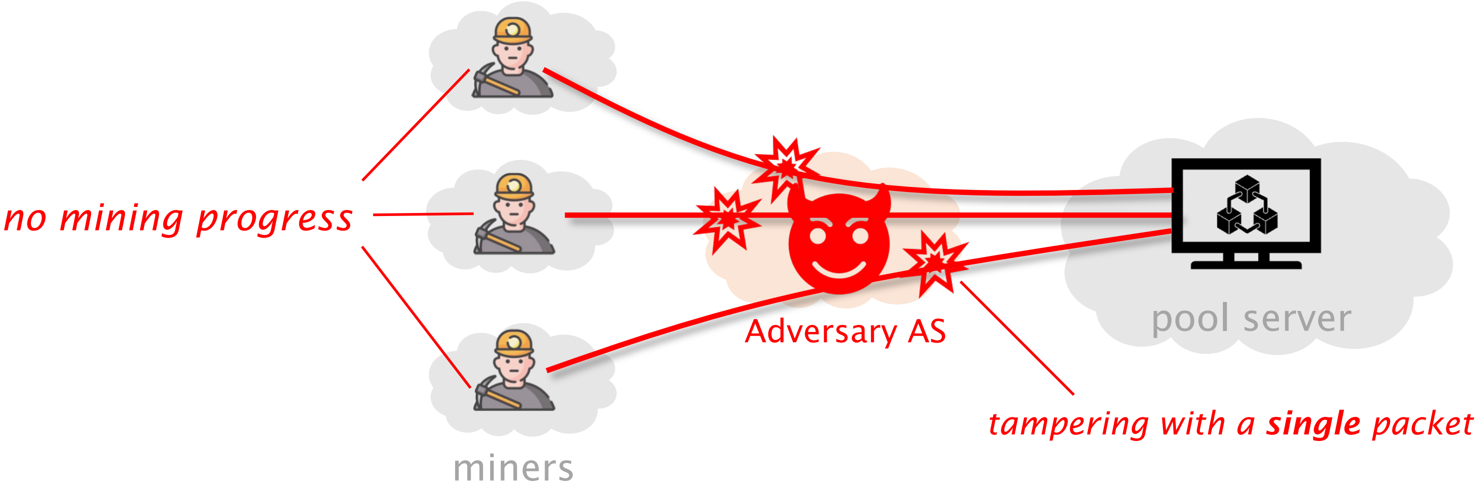


Thus, the adversary can **persistently disrupt** mining pools by tampering with (a few) packets

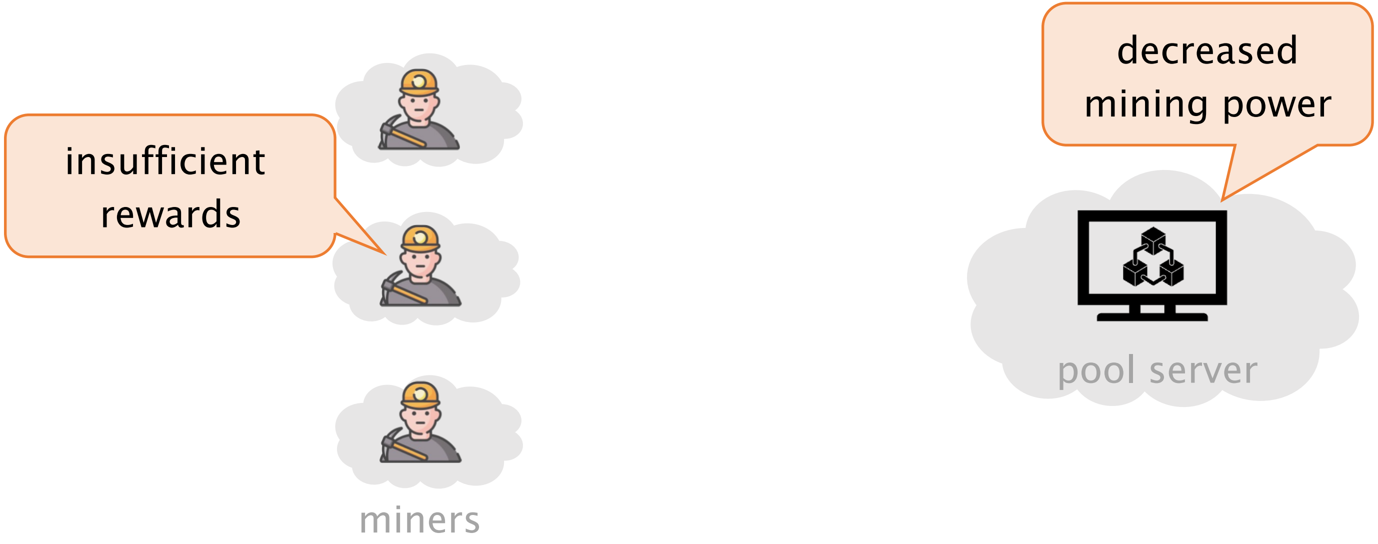


tampering with a ***single*** *packet*

Thus, the adversary can **persistently disrupt** mining pools by tampering with (a few) packets



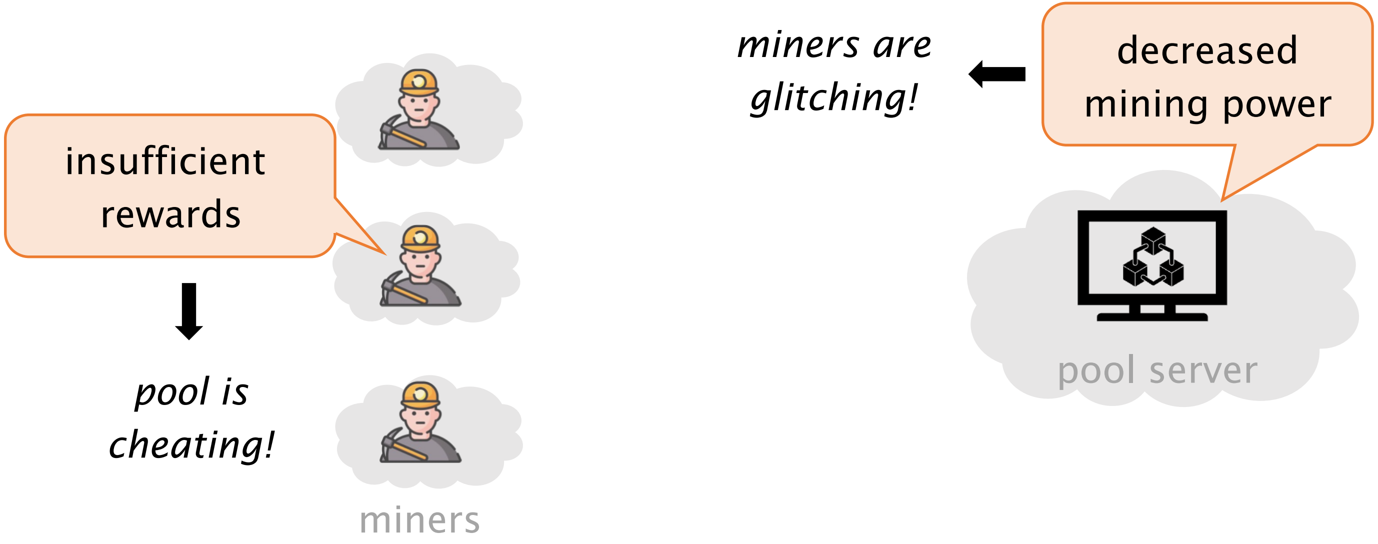
Pools and miners may observe attack effects



insufficient rewards

decreased mining power

Pools and miners may observe attack effects, but often blame each other due to the lack of trust



insufficient rewards

pool is cheating!

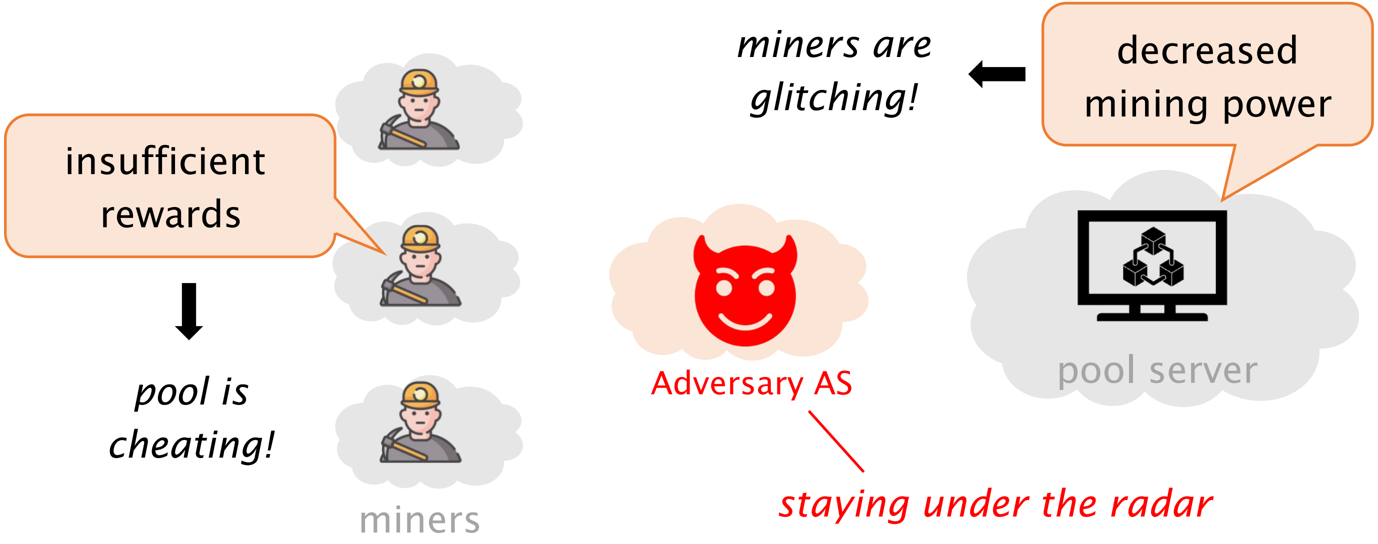
miners

miners are glitching!

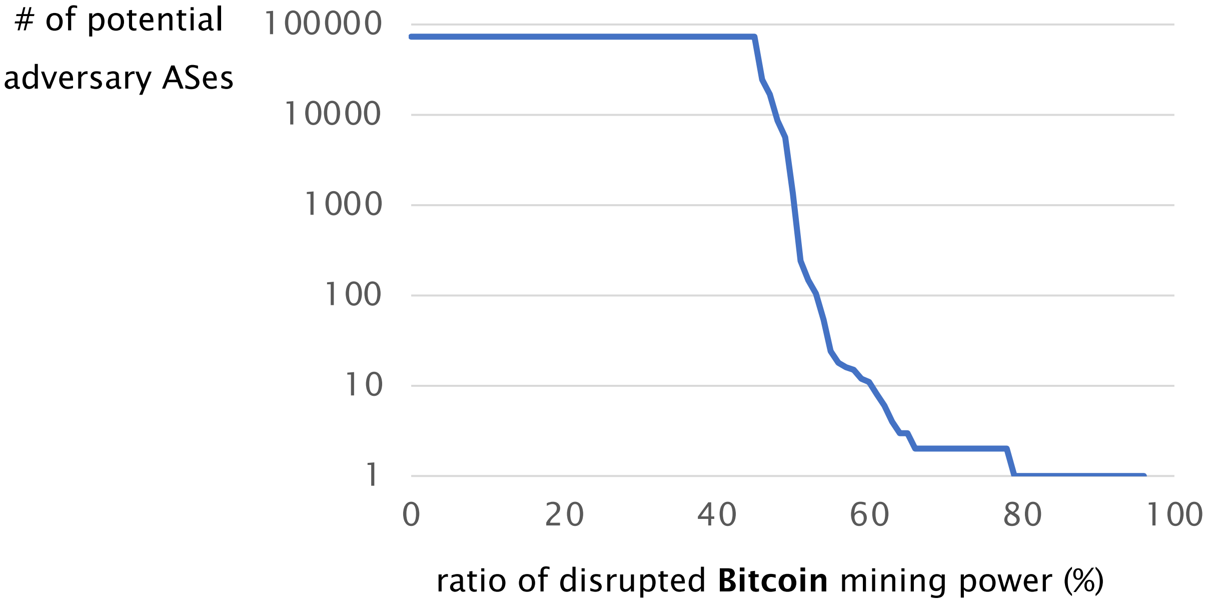
decreased mining power

pool server

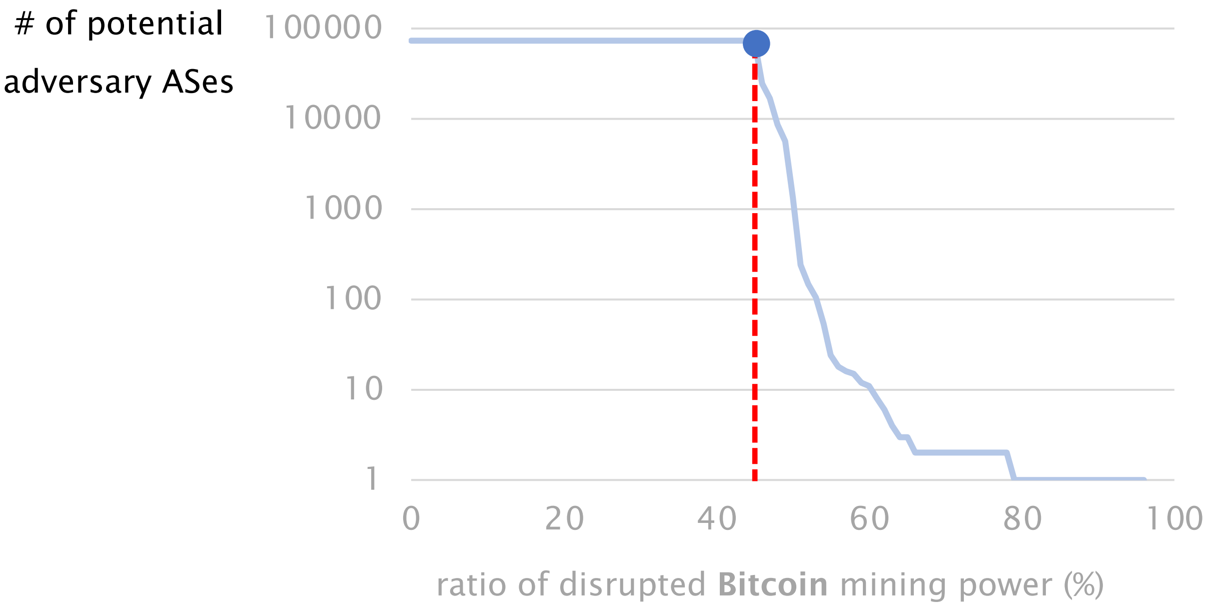
Pools and miners may observe attack effects, but often blame each other due to the lack of trust



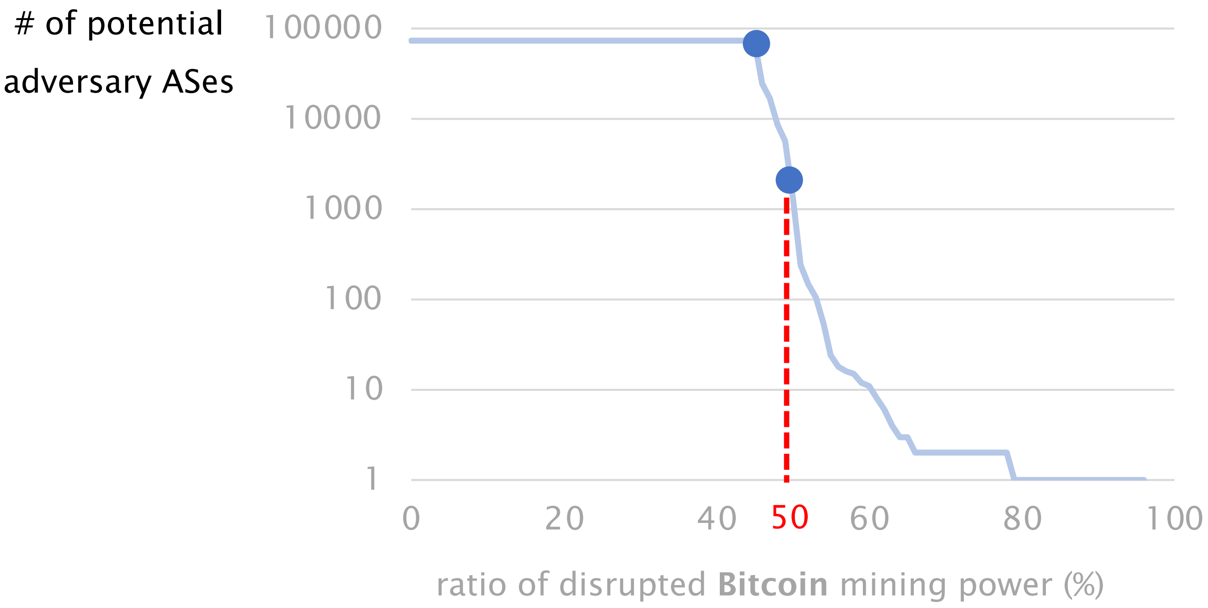
The adversary can create large-scale attacks against multiple mining pools



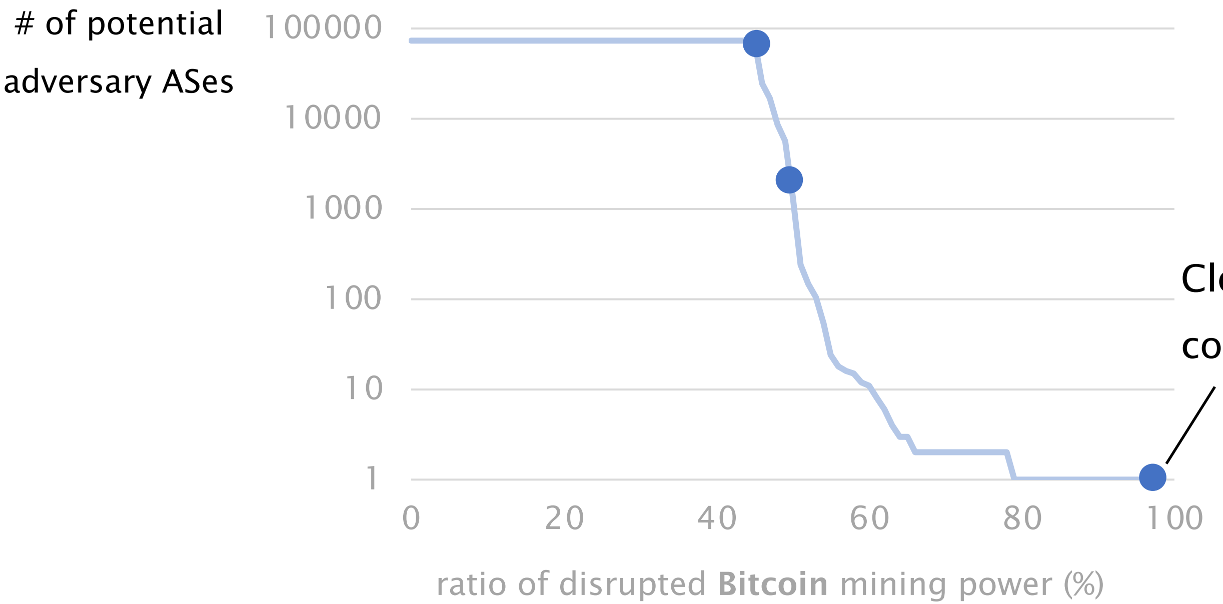
Most ASes can destroy **45%** Bitcoin mining power



> **1300 ASes** can destroy the **majority** of power



One AS can destroy **almost all** mining power



Cloudflare (AS13335) can control 96% mining power

Introducing
the Erosion attacks

1 how to disrupt mining pools with routing attacks

2 how to create stealthier attacks with a new vulnerability

3 how to mitigate the attacks

Patching the vulnerability:

Reseting the connection upon decryption failures

Date	05 February 2024
Subject	Re: Disclosing a new vulnerability in Stratum V2 protocol
Body	Yes, the bug is ***fixed*** and the fix has been ***merged*** in main […]

Short-term countermeasure:

more decentralization and secure routing

Short-term countermeasure:

more decentralization and secure routing

hosting on multiple ASes

Short-term countermeasure:

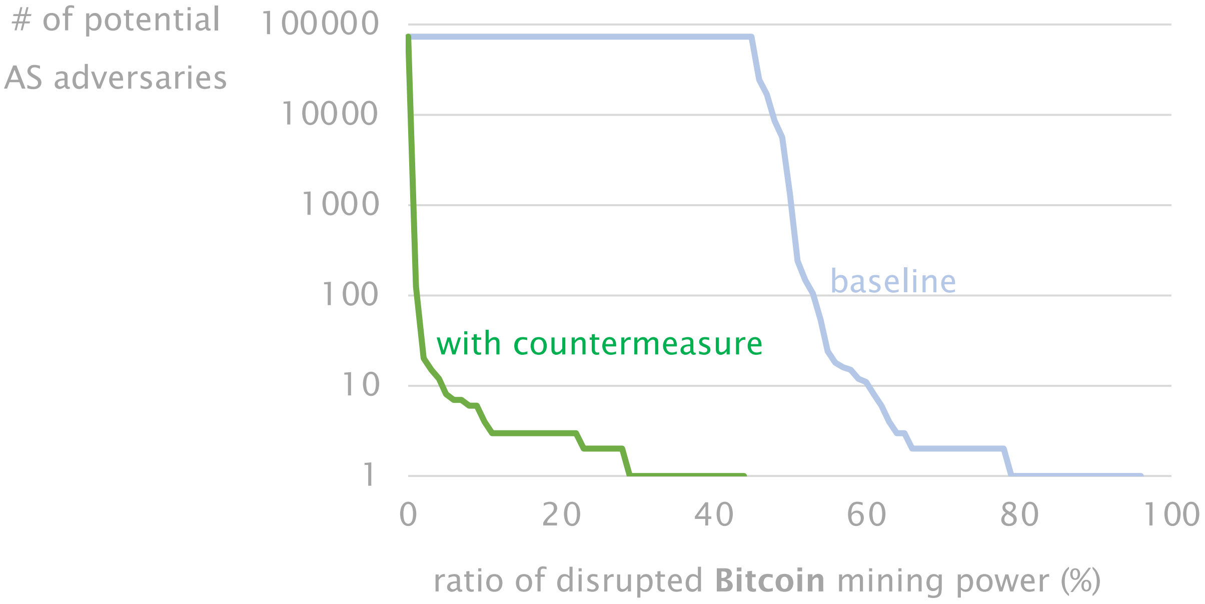
more decentralization and secure routing

hosting on multiple ASes

hosting on RPKI-enabled, max-length prefixes

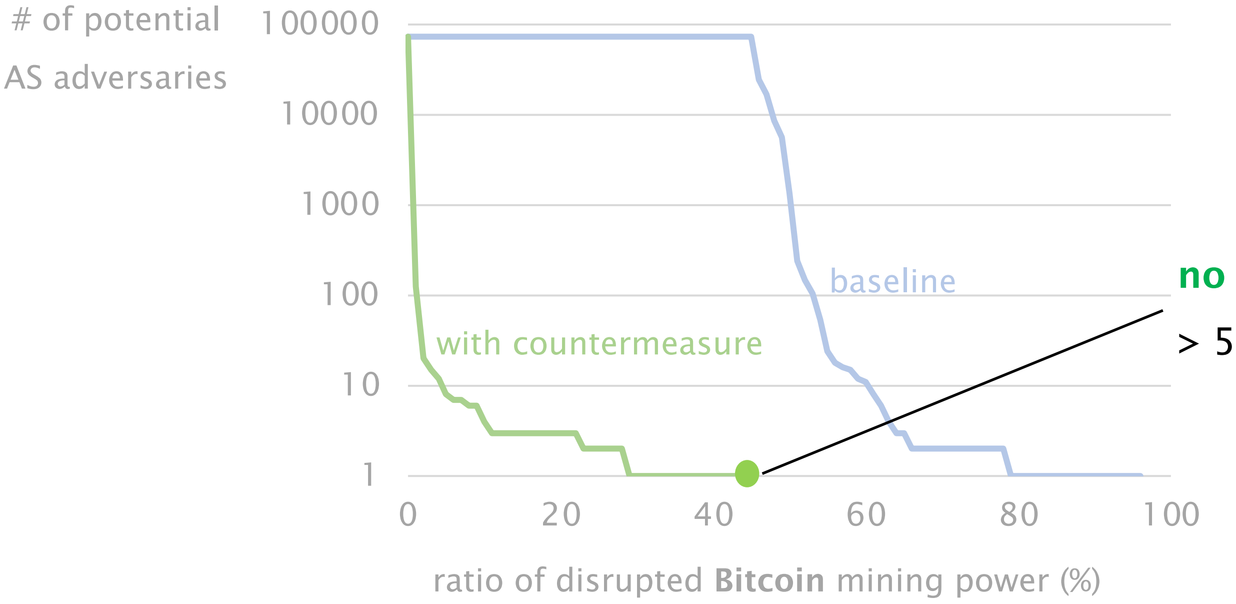
Short-term countermeasure:

more decentralization and secure routing



Short-term countermeasure:

more decentralization and secure routing



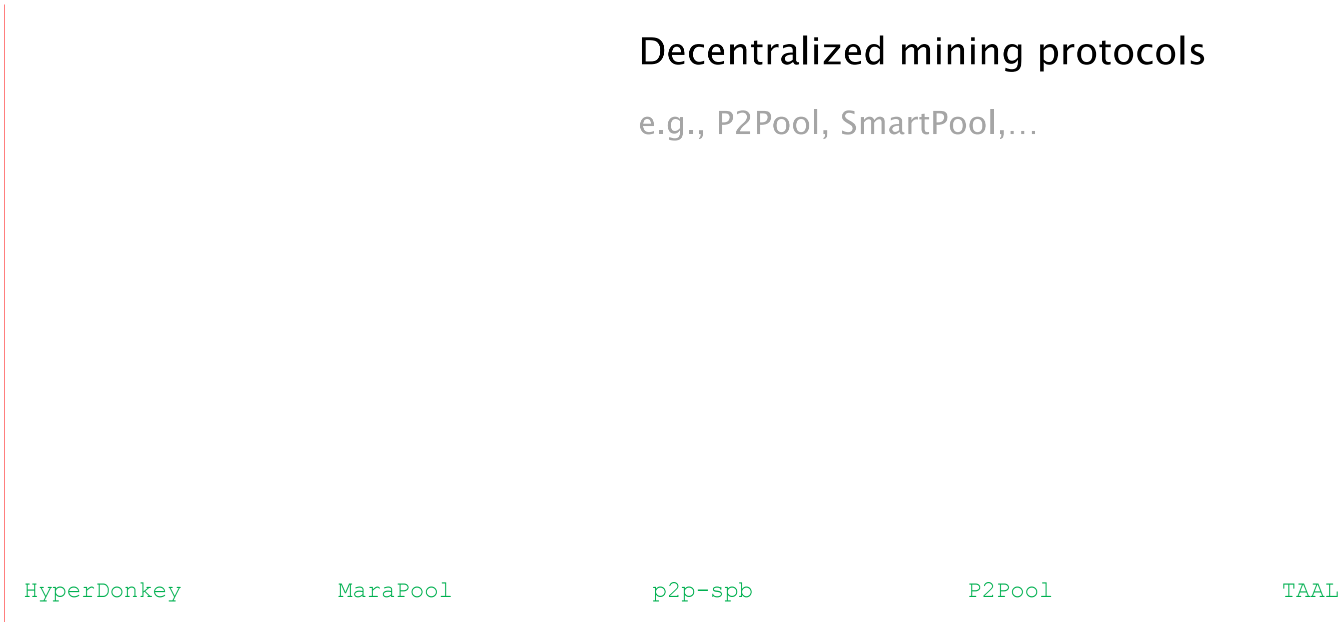
no adversary AS controls

> 50% mining power

Long-term countermeasure:

even more decentralization and secure routing

Long-term countermeasure:
even more decentralization and secure routing



Decentralized mining protocols

e.g., P2Pool, SmartPool,…

Long-term countermeasure:
even more decentralization and secure routing

Decentralized mining protocols

e.g., P2Pool, SmartPool, …

Routing-aware mining

e.g.,routing-awareness in pool-miner connections

Summary

Cryptocurrency mining pools are extremely **vulnerable** to routing attacks

We discover a protocol **vulnerability** that enables **stealthy** attacks against mining pools

Critical cryptocurrency services should embrace **decentralized architectures**

Routing attacks on Cryptocurrency Mining Pools

Stratum's erosion

Muoi Tran

dutran@ethz.ch

IEEE S&P

May 22 2024

ETH zürich