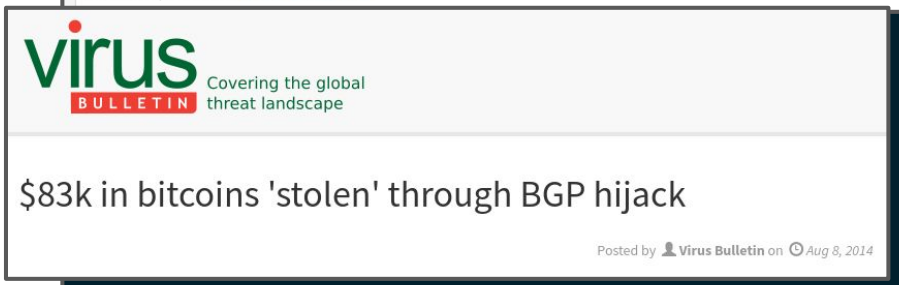
PRINCETON
UNIVERSITY

Routing Attacks on PoS Ethereum: A Systematic Exploration

Financial Cryptography and Data Security 2026

Constantine Doumanidis, Maria Apostolaki

Motivation: Routing attacks are practical



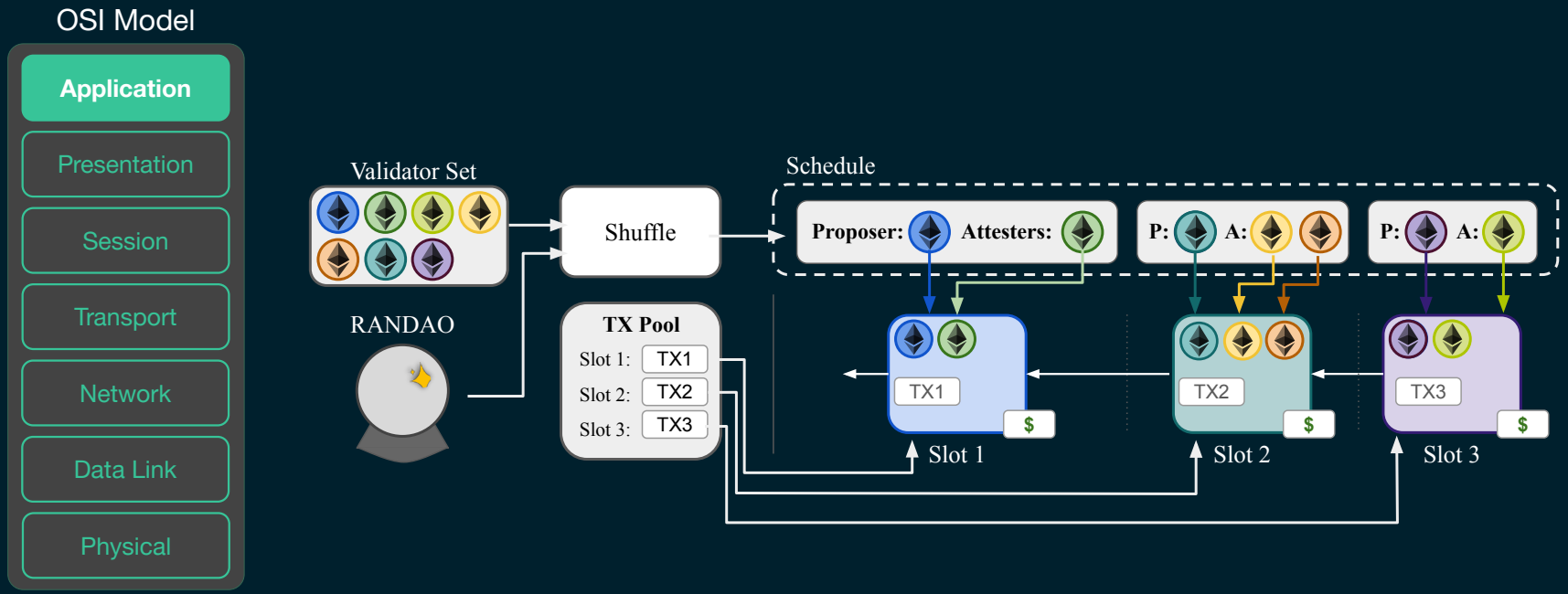
Motivation: Ethereum is a valuable target

Market data

Market cap.	24H volume	Circulating supply	Total Supply
$238.24B	$11.63B	120.69M ETH	120.69M ETH

Source: crypto.com

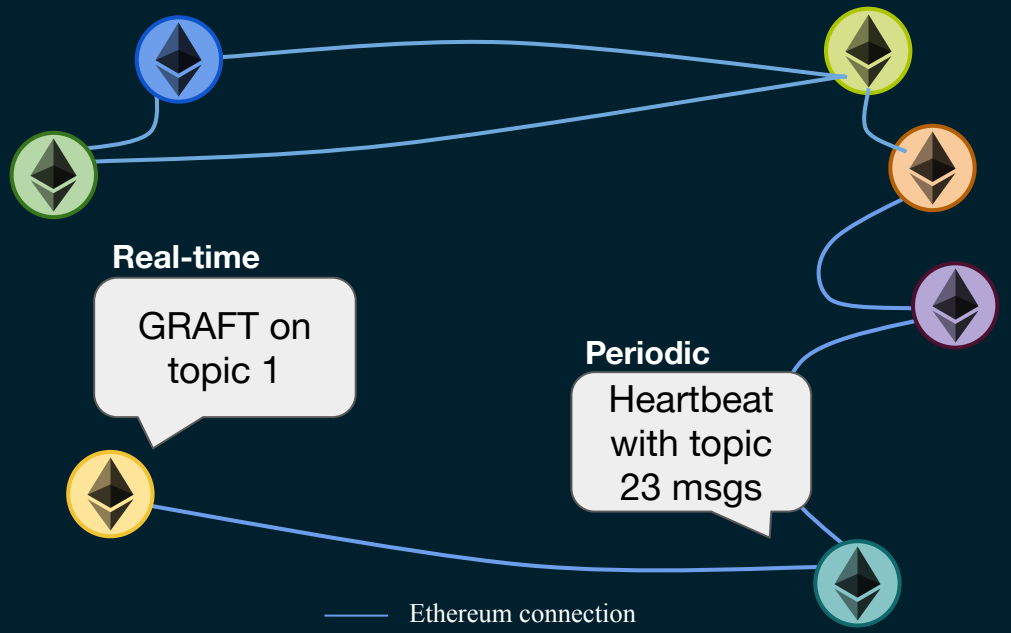
Background: The chain is extended using Proof-of-Stake



Background: Ethereum relies on a P2P overlay

OSI Model

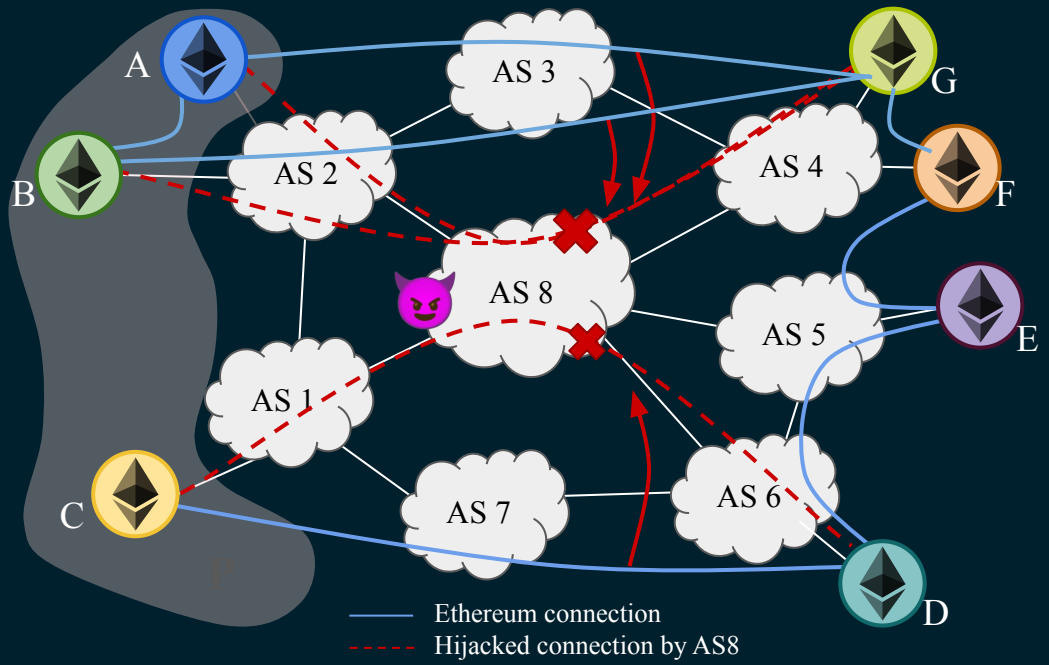
- Application
- **Presentation**
- **Session**
- **Transport**
- Network
- Data Link
- Physical



Background: P2P traffic is routed over the Public Internet

OSI Model

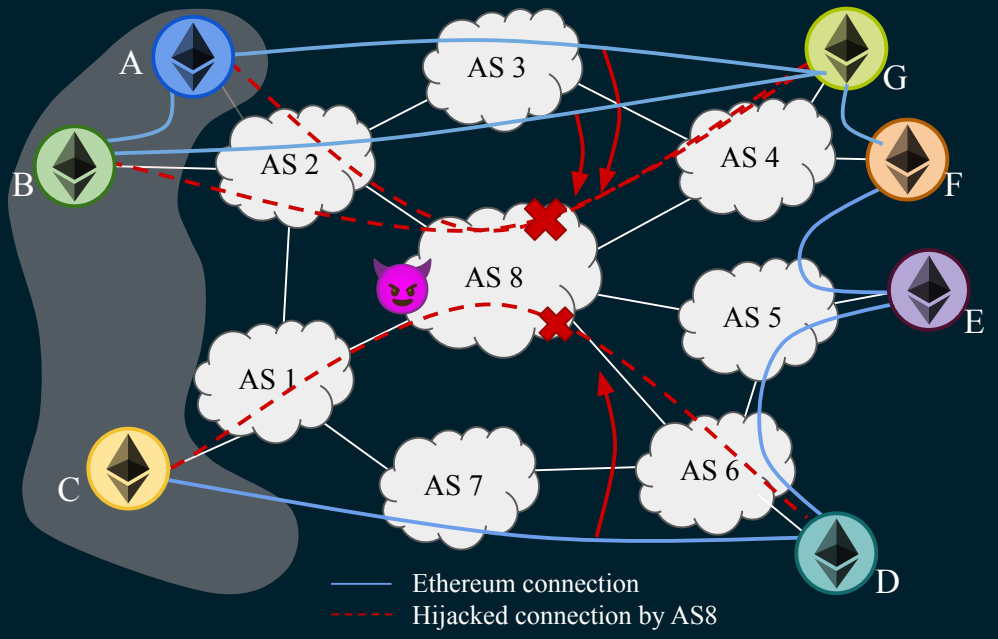
- Application
- Presentation
- Session
- Transport
- **Network**
- Data Link
- Physical

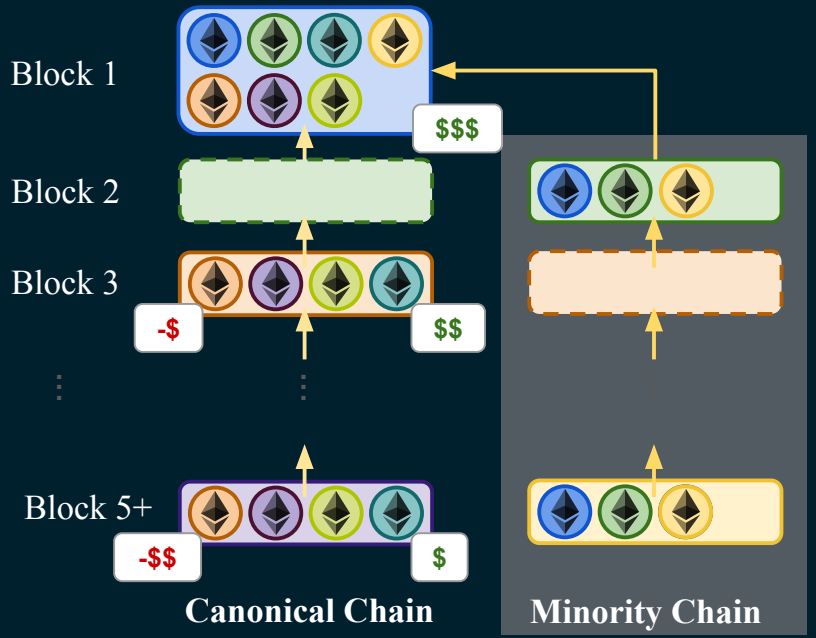


We propose two practical attacks that exploit routing and PoS mechanisms

	Target	Effect	Method	Tools
StakeBleed			Many long hijacks	BGP Router
KnockBlock	1x 		One short hijack	BGP Router Validator

StakeBleed prevents validator participation in consensus





StakeBleed halts finality and damages validators

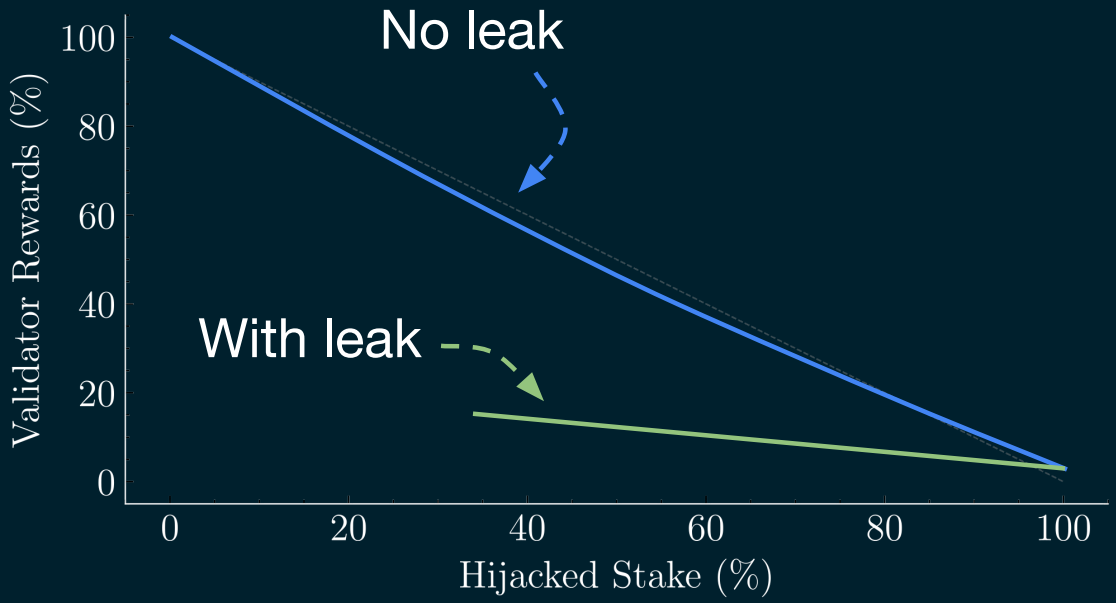
Lack of Finality

- Applications stall
- Users lose trust

Financial Damages

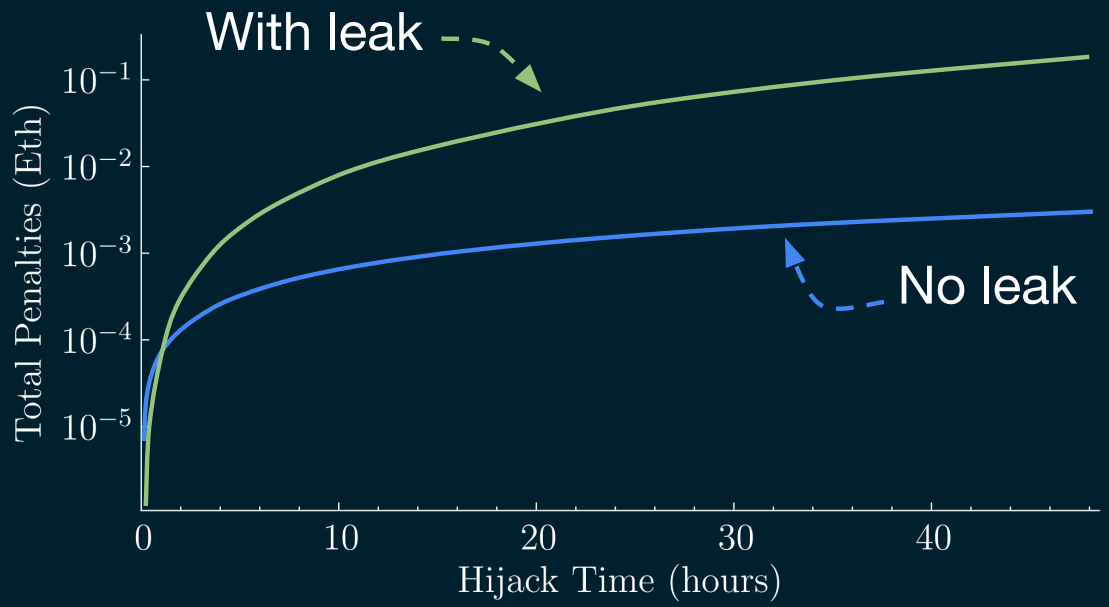
- Hijacked validators lose rewards and receive penalties
- Non-hijacked validators lose rewards

Non-hijacked Validators lose part of their rewards



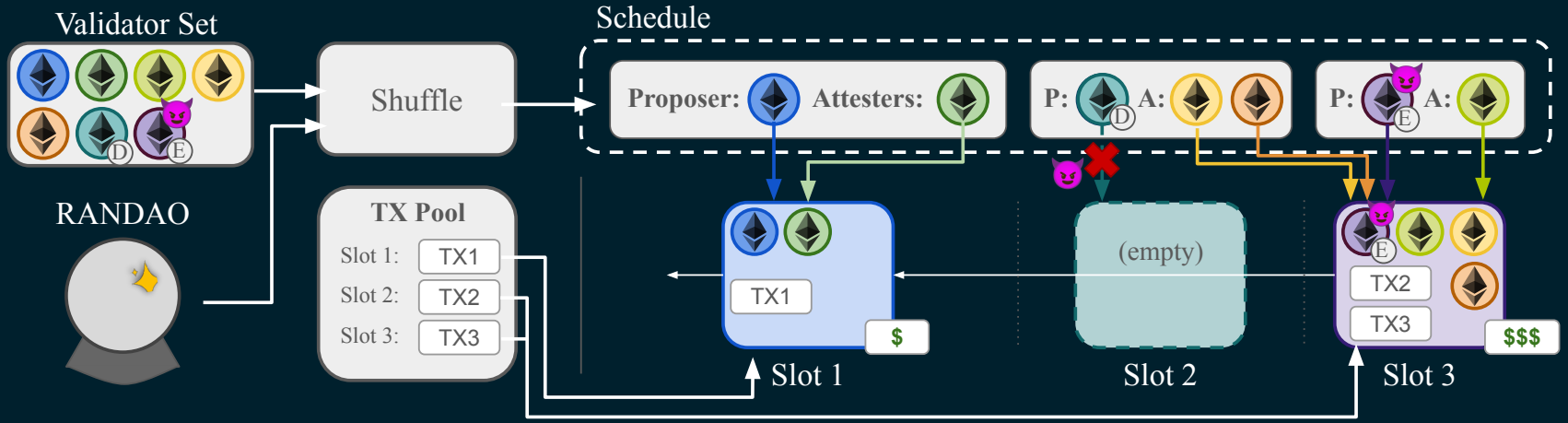
Validators lose over 80% of their expected revenue when the leak is triggered.

Hijacked Validators suffer increasing penalties



The inactivity penalty grows quadratically over time as the attacker maintains the partition that keeps the chain in the leak state.

KnockBlock prevents validators from proposing



KnockBlock yields higher proposer rewards and damages other validators

Higher rewards

- Proposal rewards from attestations
- MEV rewards from wider TX Pool

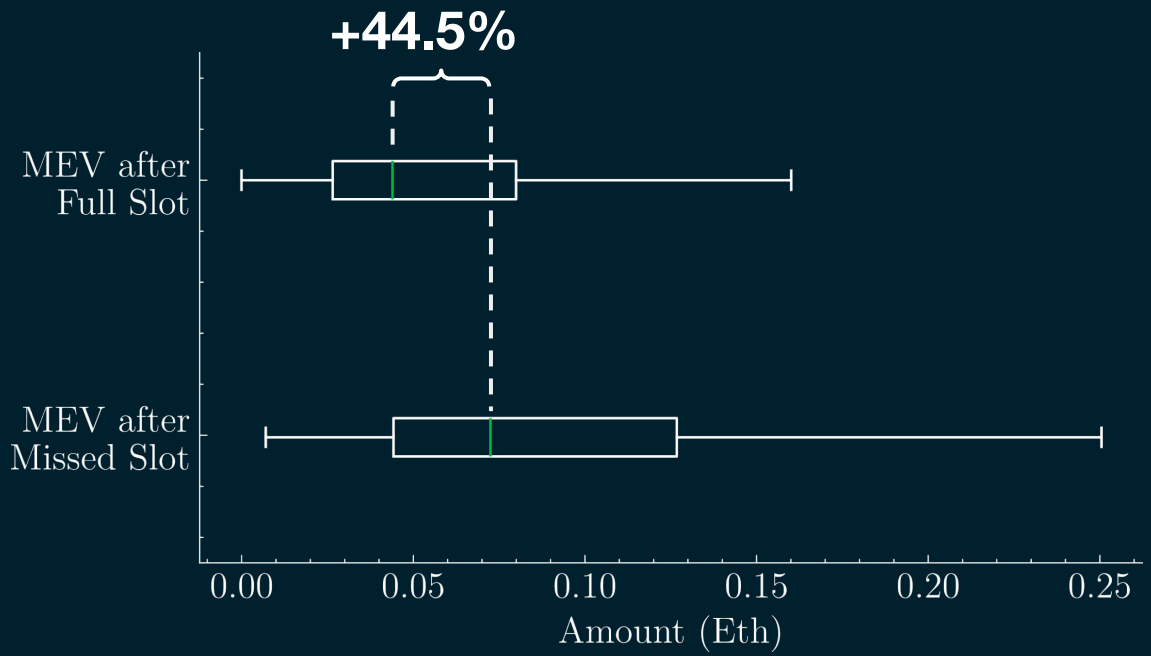
Financial Damages

- Hijacked proposers: lose proposal rewards
- Validators: lose rewards from late attestations

KnockBlock yields higher proposer rewards

Normal Block:	91 USD
KnockBlock Block:	**500 USD**

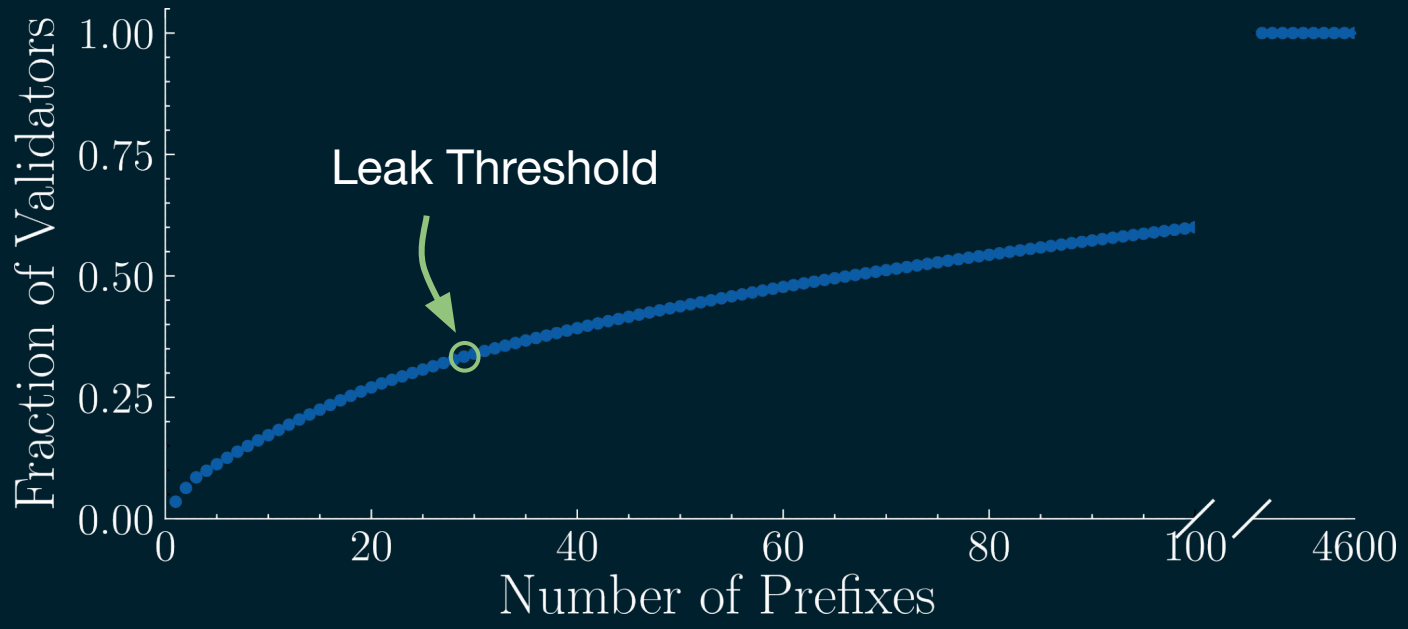
KnockBlock attackers extract higher MEV



Proposals after an empty slot on average extract 44.5% higher MEV.

Our attacks are possible because we can map blockchain identities to network identities

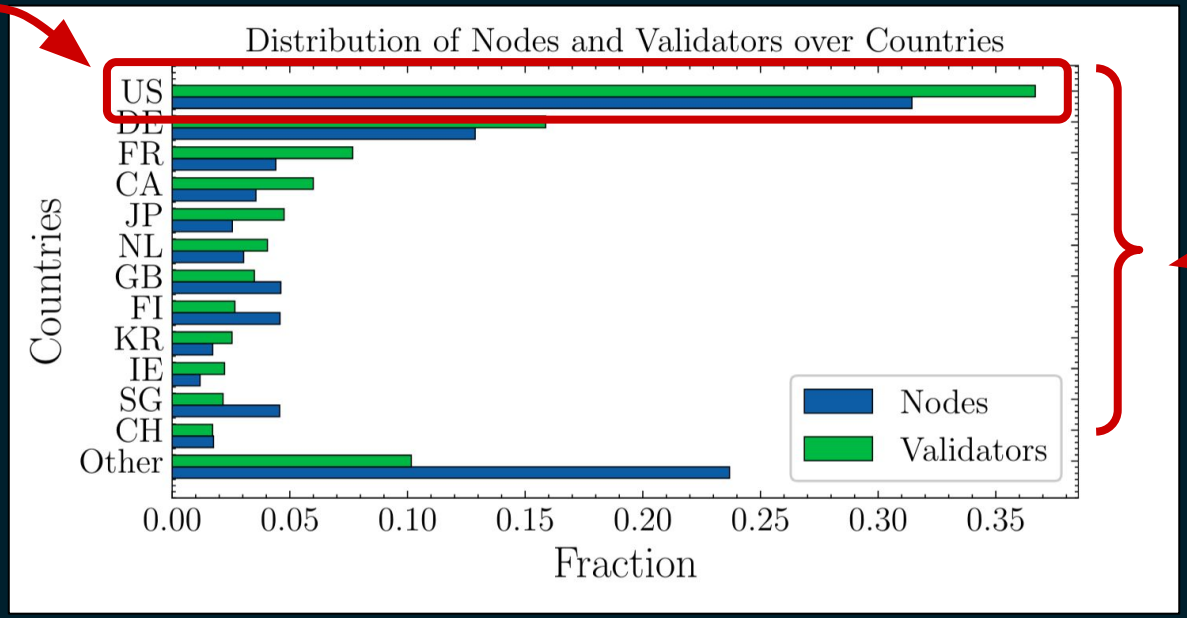
Validators are concentrated in few IP prefixes



> 1/3 of validators are hosted in just 29 prefixes.

Validators are concentrated geographically

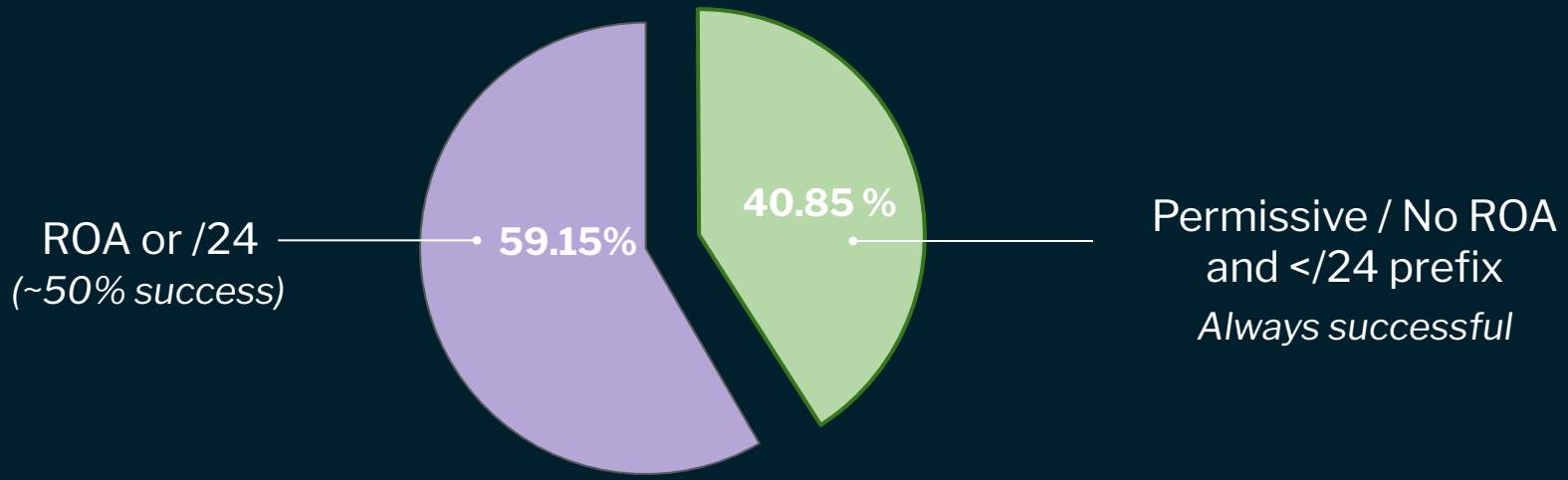
> 36%



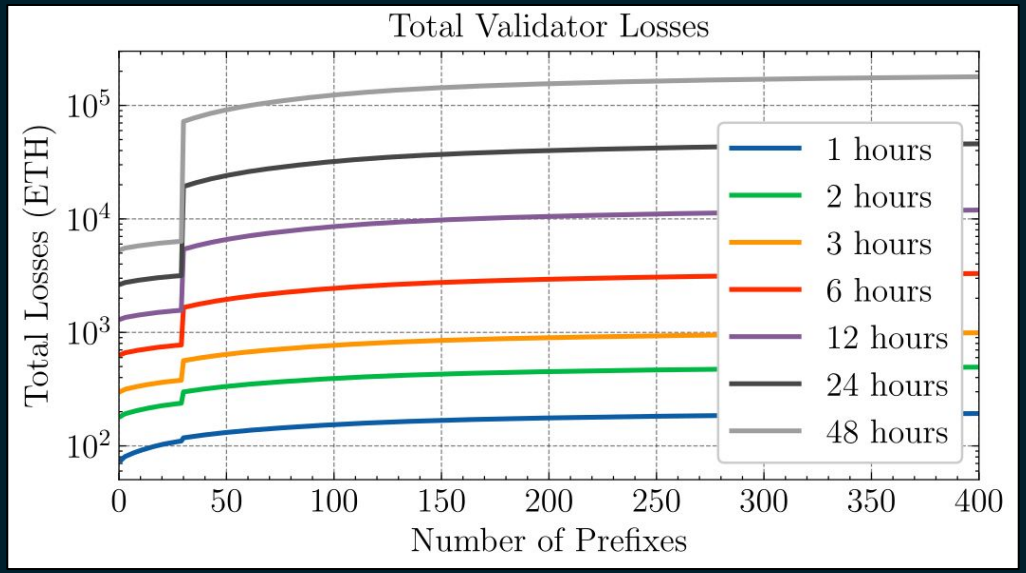
~ 90%

The United States host more than 36% of Ethereum's validators.

Validator nodes are vulnerable to routing attacks



StakeBleed is practical because of validator centralization



Hijacking 29 prefixes for 2 hours can trigger an leak inflict damages worth ~300 ETH. Even without a leak, hijacking 29 prefixes for 3 hours can cause a 379 ETH loss.

KnockBlock is practical and stealthy because of proposer schedule predictability and short hijacks

Prediction lookahead:	~12.8 minutes
Prediction accuracy:	99.97%
BGP Hijack Time-to-Effect:	**~90 seconds**
BGP Hijack Effective Duration:	**12 seconds**

Routing Attacks on PoS Ethereum: A Systematic Exploration

Conclusion

✅ We can map validators to Network IDs

✅ Routing Attacks are practical, stealthy, and profitable

🔎 Research is needed in cross-layer blockchain security

Paper

PRINCETON UNIVERSITY

DECENTER

NETΣyn

@c_smokeson

doumanidis@princeton.edu

netsyn.princeton.edu

@k05ta5