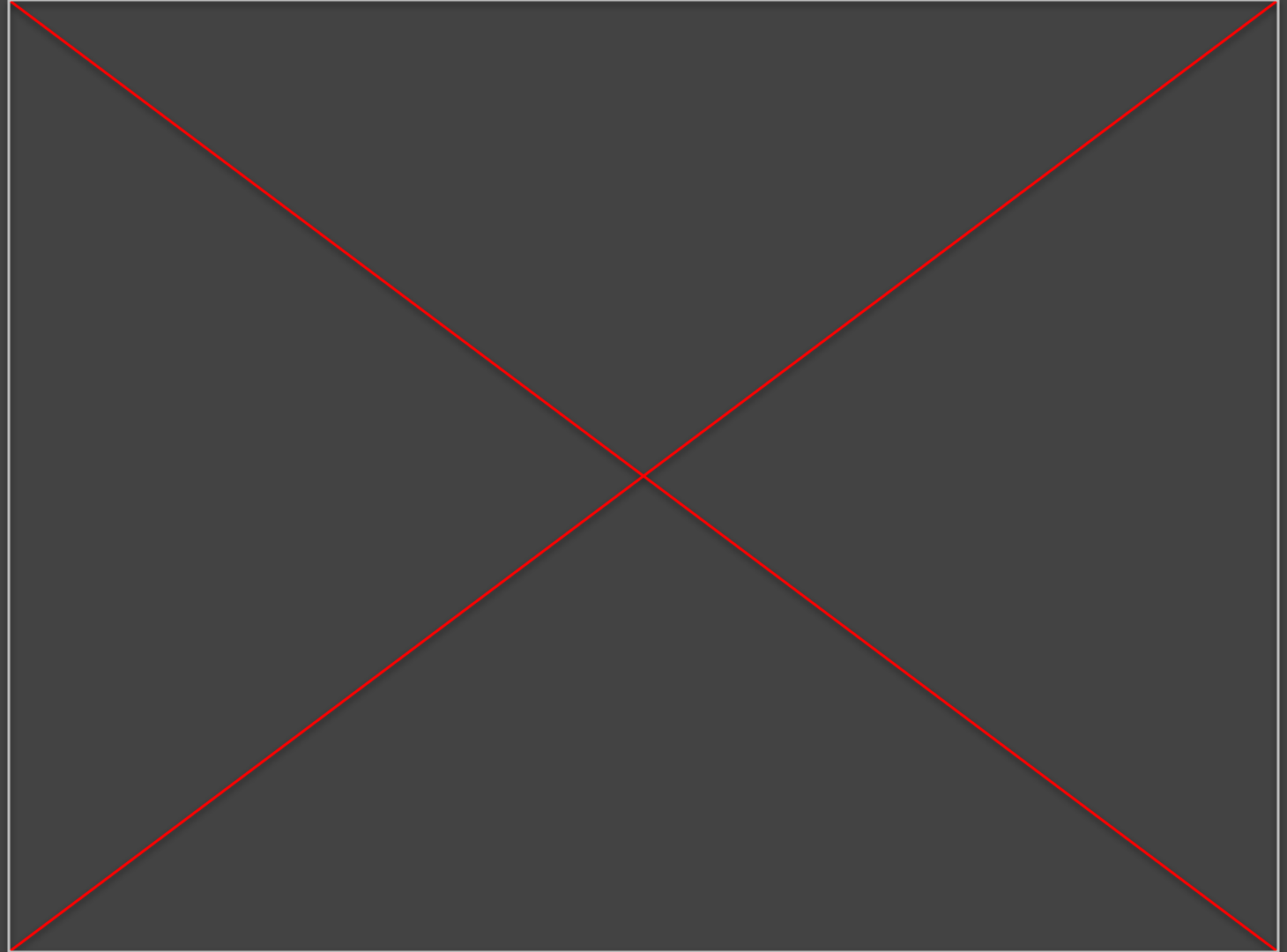
Solo staking in the dark forest

An attacker's gym

Qianchen "Q" Yu

Decentralized Technology Architect, HOPR Association

hopr



Thank you.

This work was supported by Ethereum Foundation Grant
“Transport privacy exploration of the Validator-Relayer Builder API”

Research report: Release soon on ethresear.ch

Discussion: Nov 15th, 13:30 | Blue Discussion Corner, L1

Qianchen “Q” Yu
Decentralized Technology Architect qianchen.yu@hoprnet.org

hoprnet.org | github.com/hoprnet | x.com/hoprnet

hopr

Appendix

What did we learn?

- Everyone is vulnerable, everyone is a suspect
- MEV isn’t just mempool re-ordering, e.g. skipped-slot MEV…
- Attacks are feasible and cheap
- Decentralizing MEV infrastructure actually leads to worse trust assumptions

hopr

Appendix

hopr

Appendix

What we want

- **Privacy protection**, plz
  - At least for Builder **HTTP API calls** on the validators side:

    ```
    POST /eth/v1/builder/blinded_blocks
    GET  /eth/v1/builder/header/{slot}/{parent_hash}/{pubkey}
    POST /eth/v1/builder/validators
    ```

  - Integrating network-level metadata privacy protection protocols directly into the **networking layer** of Ethereum clients when designing PBS
- Despacito
  Less latency-sensitive p2p layer for privacy protection, fairer MEV (re-)distribution of MEV, and enhanced network resilience.
  => protecting solo stakers

hopr

Appendix

Skipped-slot MEV

[ˈskɪpt - ˈslät]

Adversaries can target and interfere with block production processes to prevent certain transactions or even entire blocks from being processed.

hopr

Appendix

Ethereum network negative consequences - Skipped-slot MEV

- **Solo stakers are more vulnerable to DDOS attack**
  - K-tailed RANDAO takeover: victim of RANDAO manipulation
  - Fail in attesting to data availability sampling (DAS)
- **Selectively attack multi-block MEV**

hopr

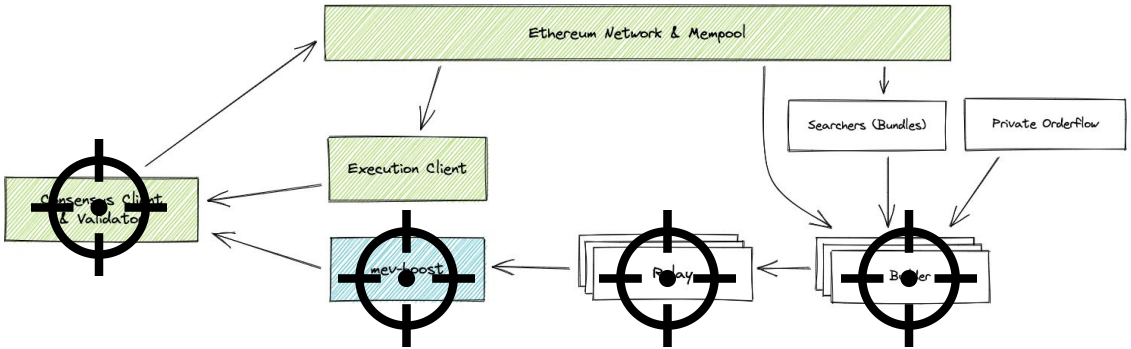
Appendix

Ethereum network negative consequences - P2P

- **Recently bootstrapped sparsely-connected beacon nodes, esp. home stakers, are more vulnerable to “covert flash attack”:**

  *Sybils of an attacker connect to the victim and behave properly long enough to build up score in GossipSub protocol before executing a coordinated eclipse attack when the victim needs to propose a block.

- **All parties can become a victim**



hopr