Aug 21, 2024. 2:30pm – 2:50pm
2024 IEEE International Conference on Blockchain

Effective Ethereum Staking in Cryptocurrency Exchanges

Yuto TAKEI
(Mercari, Inc. and Tokyo Institute of Technology, JAPAN)

Kazuyuki SHUDO
(Kyoto University, JAPAN)

mercari

Outline of the Presentation

1. Research Motivation
2. Related Work and Background
3. Briefs on Ethereum Architecture
4. Challenges to Solve
5. Proposed Techniques
6. Experiment and Results
7. Conclusion

Research Motivation

Cryptocurrency staking is an attractive option for exchanges.
Ethereum is one of the most major Proof of Stake (PoS) assets.

- Exchanges hold $100+ billion worth customer cryptocurrencies worldwide, where most of those assets are idle.
- Some jurisdictions allow exchanges to invest assets in custody into relatively low-risk instruments.
- PoS Ethereum adopts a very unique and complex architecture. It rewards successful validators, while penalize violators.

Related Work

Public Blockchain Consensus

- Acceleration or optimization of PoW-based mining
- Picking transactions with better fee (MEV-boosted)
- Mitigating various attacks against consensus.
- Solving scalability issues.

Other PoS Mechanisms

Variations of PoS exist.

- Proof of Importance (NEM)
- Delegated PoS (Solana, BNB)

BFT-like Consensus Algorithms

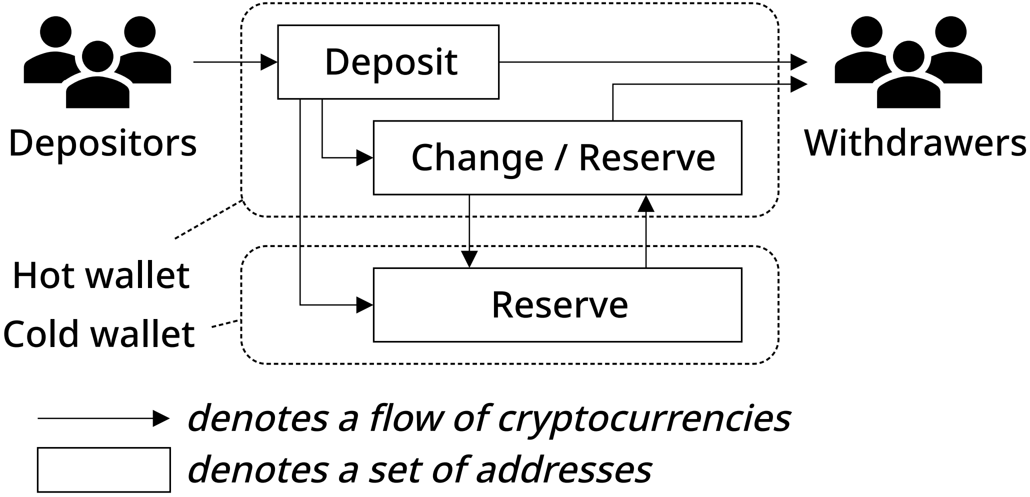
Paxos, PBFT or other voting based algorithms are studied to extend for blockchain context.

- Tendermint, HoneyBadgerBFT

Background: Wallets at Exchanges

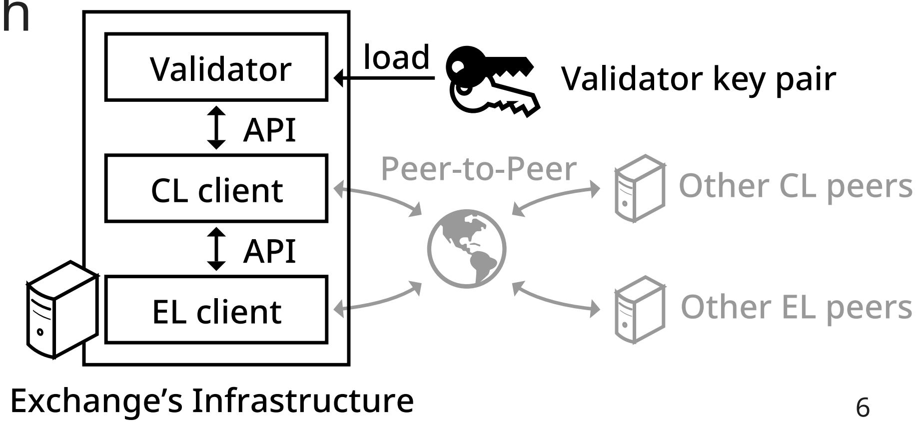
Most exchanges have multiple layers of wallets to accept incoming deposits, and initiate outgoing withdrawals.

- Deposit addresses are issued per customer.
- Cold wallets are useful to enhance security.
- Transactions between hot and cold are made to adjust balances.

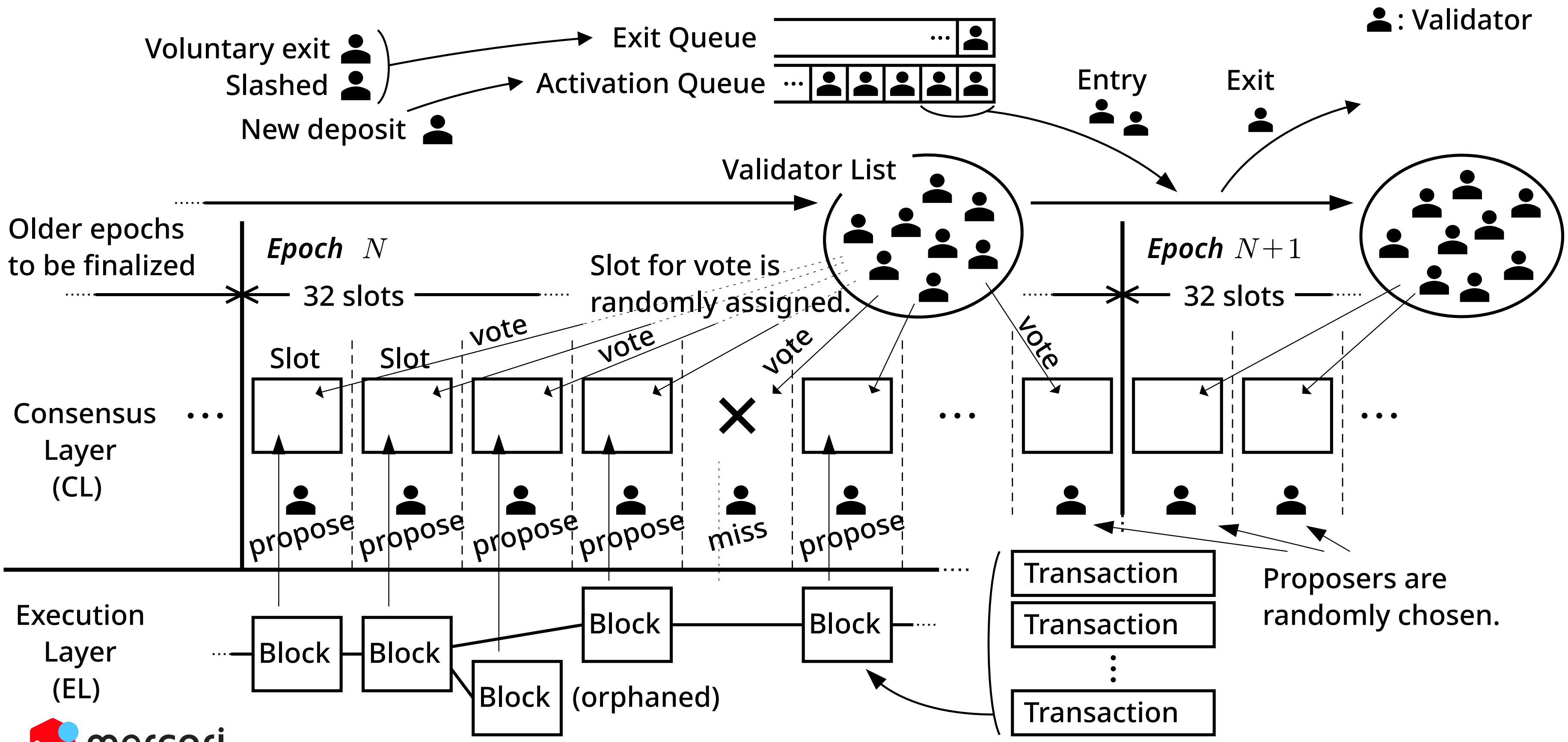


Background: Ethereum

- Asset with #2 market capitalization.
  - The second most popular cryptocurrency after Bitcoin.
  - Host of ERC-20 and other tokens (e.g. NFTs).
- Migrated from PoW to PoS after “The Merge”
  - Exchanges generally run two types of node in tandem.
  - Nodes can be replaced with Blockchain as a Service. (e.g. Infura, QuickNode, GCP Blockchain Engine)



Ethereum Mechanisms at Glance

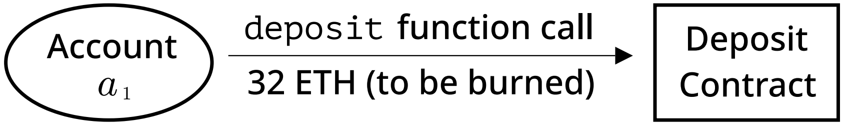


mercari

Deposit and Withdrawals of Ethereum Staking

Deposit (EL → CL)

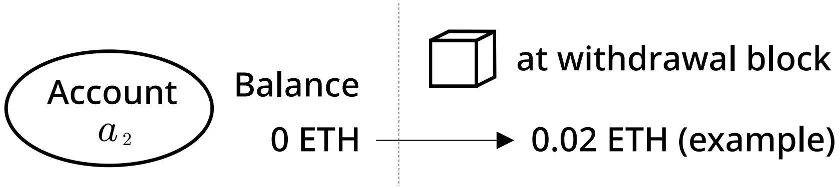
When depositing on EL:



Send 32 ETH to Deposit Contract with following parameters:

- BLS pubkey (= ETH2 account)
- Withdrawal EL address
- Signature by the BLS key

Withdrawal (CL → EL)



- **Partial**: Excess above 32 ETH is refunded periodically.
- **Full**: All amount is refunded and ETH2 account closed. (Voluntary exit or slashing)

Four Challenges to Consider

1. **Preserving Asset Liquidity**
   Keeping non-staked reserve for customer withdrawal

2. **Validator Key Management**
   Preventing BLS key compromise (leak) or loss

3. **Stable Validator Operation**
   Keeping validator nodes online and updated

4. **Increased Profits from Staking**
   Saving running cost, and proposing fee-rich transactions

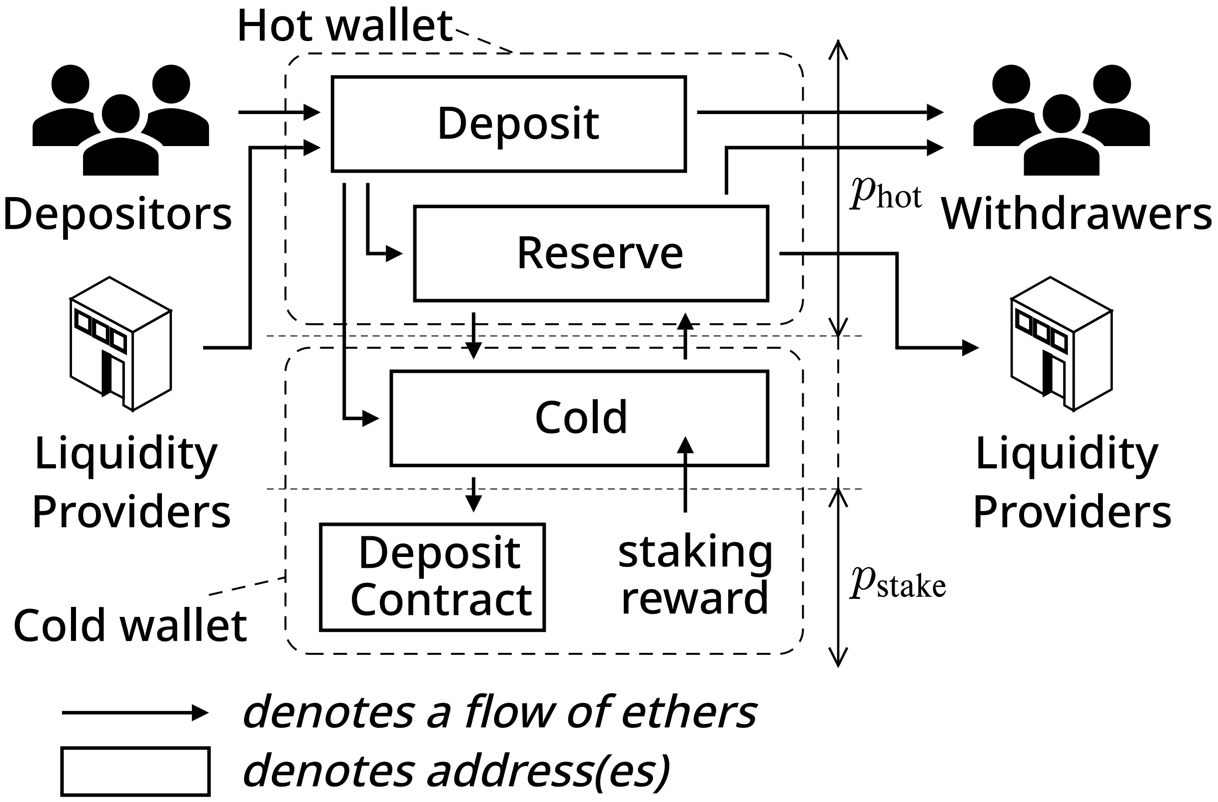
Proposed Techniques

- Staking-enabled Wallet Layers
- Security Considerations
- Infrastructure on Cloud
- MEV-boosting and Staking Pools

Wallet Layers for Ethereum Staking

(Solutions to Challenge 1)

- Staking initiated from cold wallet for security.
- Use of hot wallets minimized.
- Extra liquidity may be secured with liquid staking.



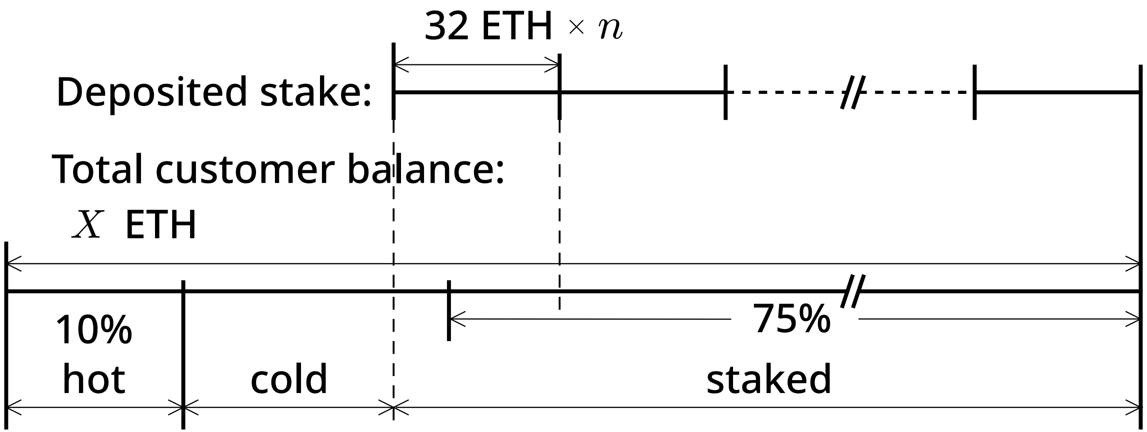
mercari

Wallet Allocation *(Solutions to Challenge 1)*

Set the target staking ratio (p_{stake}) and decide the number of 32 ETH units (n).

$$n = \left\lfloor \frac{X \cdot p_{\text{stake}}}{32} + 0.5 \right\rfloor$$

$$\text{if } X > \frac{16}{1 - (p_{\text{hot}} + p_{\text{stake}})}$$



The exchange need to regularly perform deposit or full withdrawal to maintain the asset distribution across wallet layers.

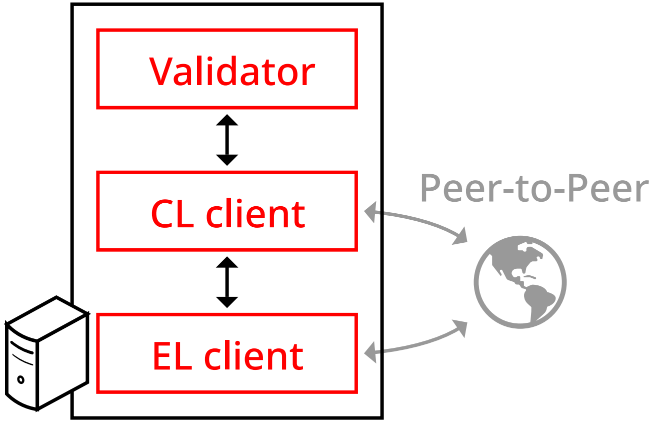
Software Security *(Solutions to Challenge 2)*

Nodes run online, and key protection becomes important.

- Client software must be kept up to date.
- Security audit may be required according to risk control.

Node diversity should also be considered.

- Instability caused by specific software may impact the operation.



Exchange's Infrastructure

Staking with Cloud Infrastructure
(Solutions to Challenge 3)

Following advantages can be considered:

- Easy to scale in and out. Easy to provision new nodes.
- Higher bandwidth with fast network backbone.
- Built-in security functions at various layers.

Similar infrastructure stack can be built across Azure / GCP / AWS.

- Some differences do exist. (e.g. VM’s state / IAM / logging)
- Multi-cloud approach may be better to avoid vendor lock-in.

Experiment on Holesky Testnet

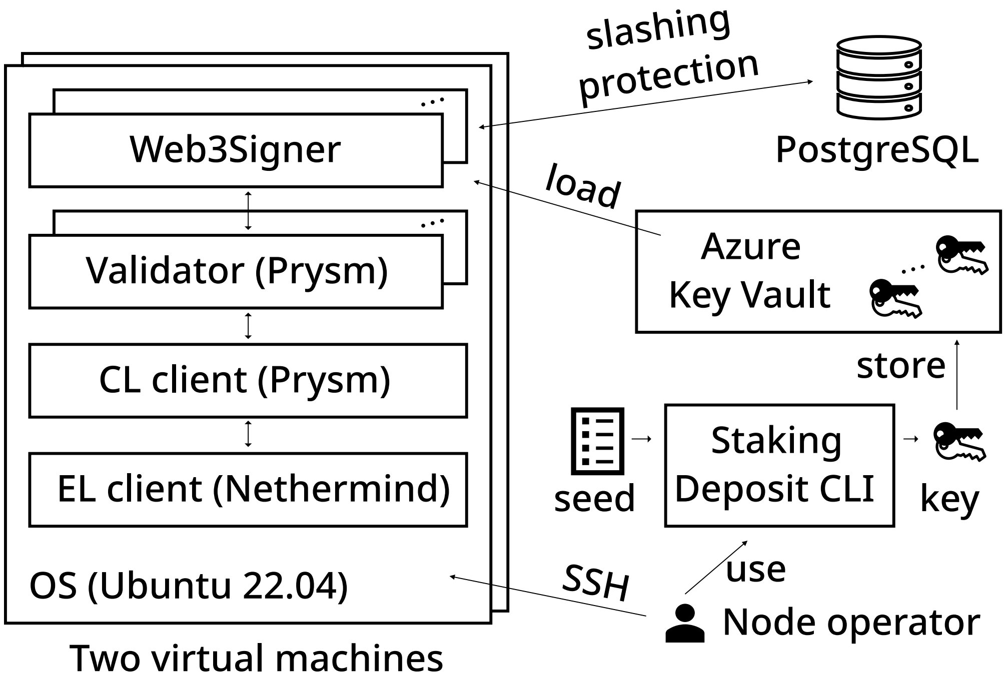
Testing staking with cloud infrastructure

- Performance Results
- Operational Results
- Profitability Evaluations

Staking Architecture on Cloud

We built Solo-Staking infrastructure on Microsoft Azure.

- VM #1 : 4 validators
  VM #2 : 16 validators
- Employed Web3Signer with PostgreSQL to prevent slashing.
- BLS keypair generated by Staking Deposit CLI on an isolated VM.



Performance Result

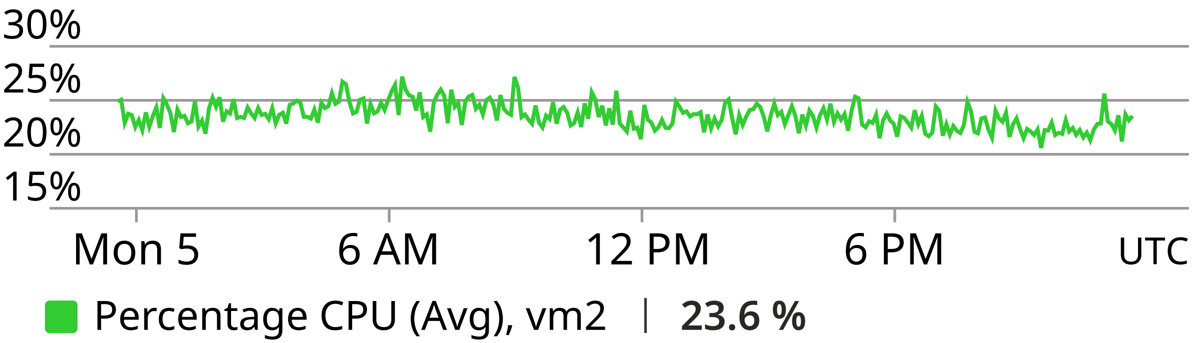
- CL/EL consume high resources regardless of # of validators.
  High network bandwidth requirements.

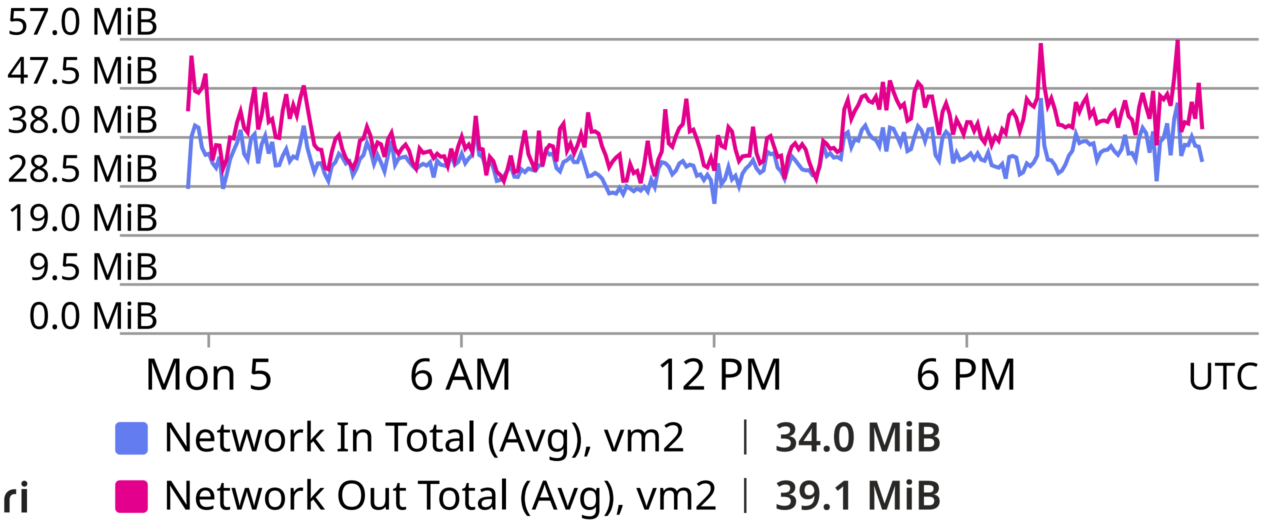
- Validators consume very few resources. Multiple instances can be deployed on a single machine.

Total CPU Utility (95th percentile)	0.32 vCPU (minimum) 0.84 vCPU (maximum) 0.48 vCPU (average)
Memory usage (average)	8.93 GiB (Nethermind, EL client) 2.54 GiB (Prysm, CL client) 0.04 GiB (Prysm, per each validator)
Storage used	85 GiB (Nethermind, EL client) 55 GiB (Prysm, CL client)
Total storage IO per minute (average)	170 MiB (write) 20 MiB (read)
Total network usage per minute (average)	39 MiB (incoming) 43 MiB (outgoing)

mercari

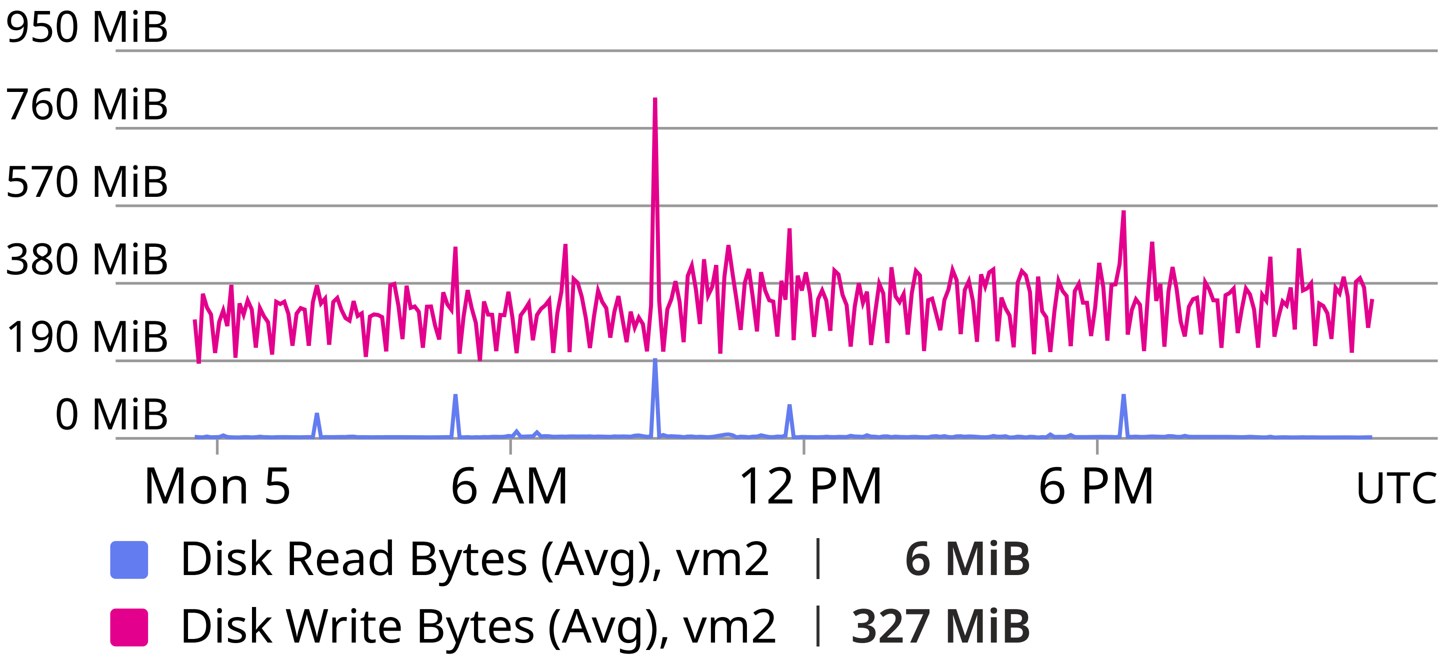
Performance Result (CPU & Network)





mercari

Performance Result (Disk IO)



mercari

Operational Results

In-place upgrade

Update OS / node software.

- **Result**: < 6 min. offline. 1 – 2 attestation misses.
- Switch-over to a replica node may have further reduced misses.

Unplanned migration

Simulates disaster recovery.

- **Result**: 1 – 2 attestation misses in hot standby.
- Slashing protection must be configured properly.
- Cold standby case may require 5+ hours bootup. (approx. 50 epochs)

Profitability Evaluation

- Hosting multiple (n) validators on a single VM.
- Expected reward can be estimated from # of active validators, or otherwise calculated from the past statistics.
  (Does not include MEV reward)

Daily operational cost: x USD / VM
Daily staking reward: y ETH / validator
Exchange rate: z USD / ETH
# of validators on VM: n

Annual Percentage Yield:

$$A = \frac{365(y - x/nz)}{32}$$

Further Improvements Identified

- **Other infrastructure options**
  On-premises may be more cost-effective in some cases.
  For example, large-scale staking or use of special hardware.
- **Reducing attestation misses**
  Attestation misses observed unrelated to node stability.
  Cause is unknown, but presumed to be specific to testnet.
- **Finding appropriate staking ratio in asset distribution**
  Higher staking ratio can increase profits, but having lower hot ratio may impact the exchange operations.

Conclusion

- Exchanges can invest ETHs with a low-risk profile by staking.
  - A wallet architecture must consider operability.
  - Cloud environment eases staking for exchanges.
- Experiment on Holesky demonstrated 2.84% APY w/o MEV.
  Next step: large-scale test on Mainnet.
- Further investigations required: reducing attestation misses, increasing node diversity, profitable asset distribution.