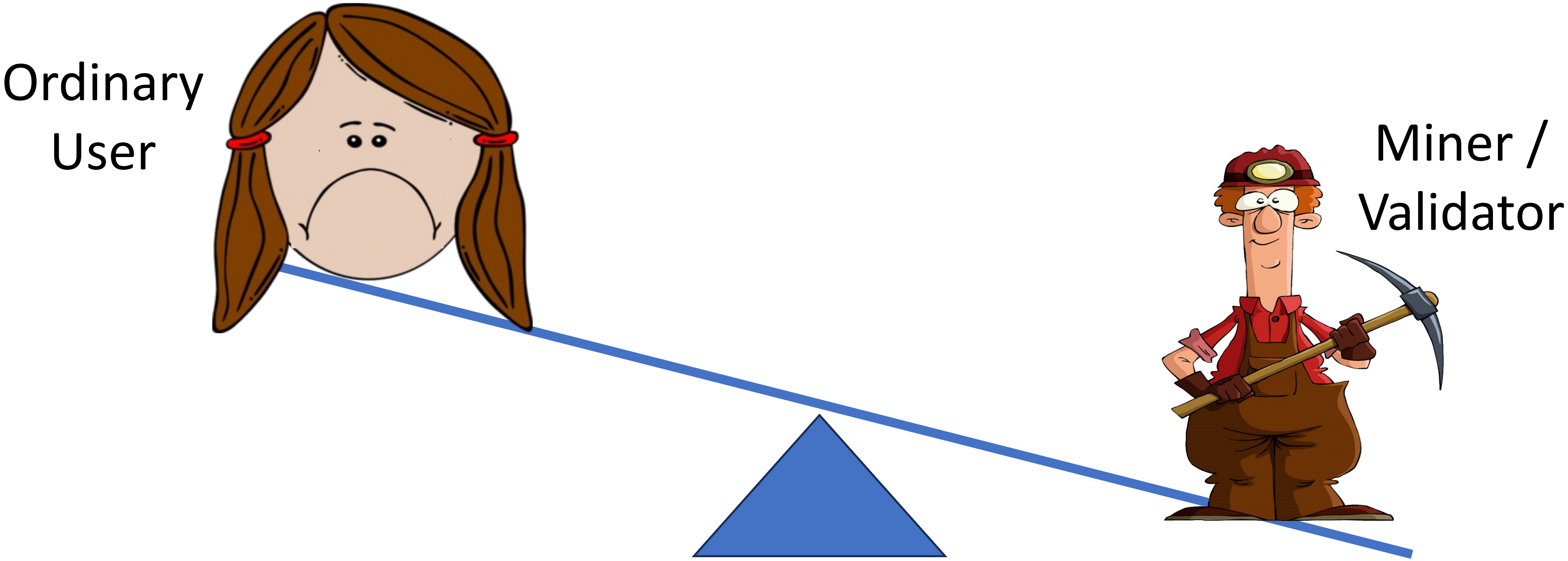
How has the community dealt with MEV?

Systematization of Value Extraction

- Assume that extraction is inevitable as validators are rational agents
- But some validators have more capability than others
- Systematically give every validator access to the most profitable block *possible*
- Proposer Builder Separation (PBS)

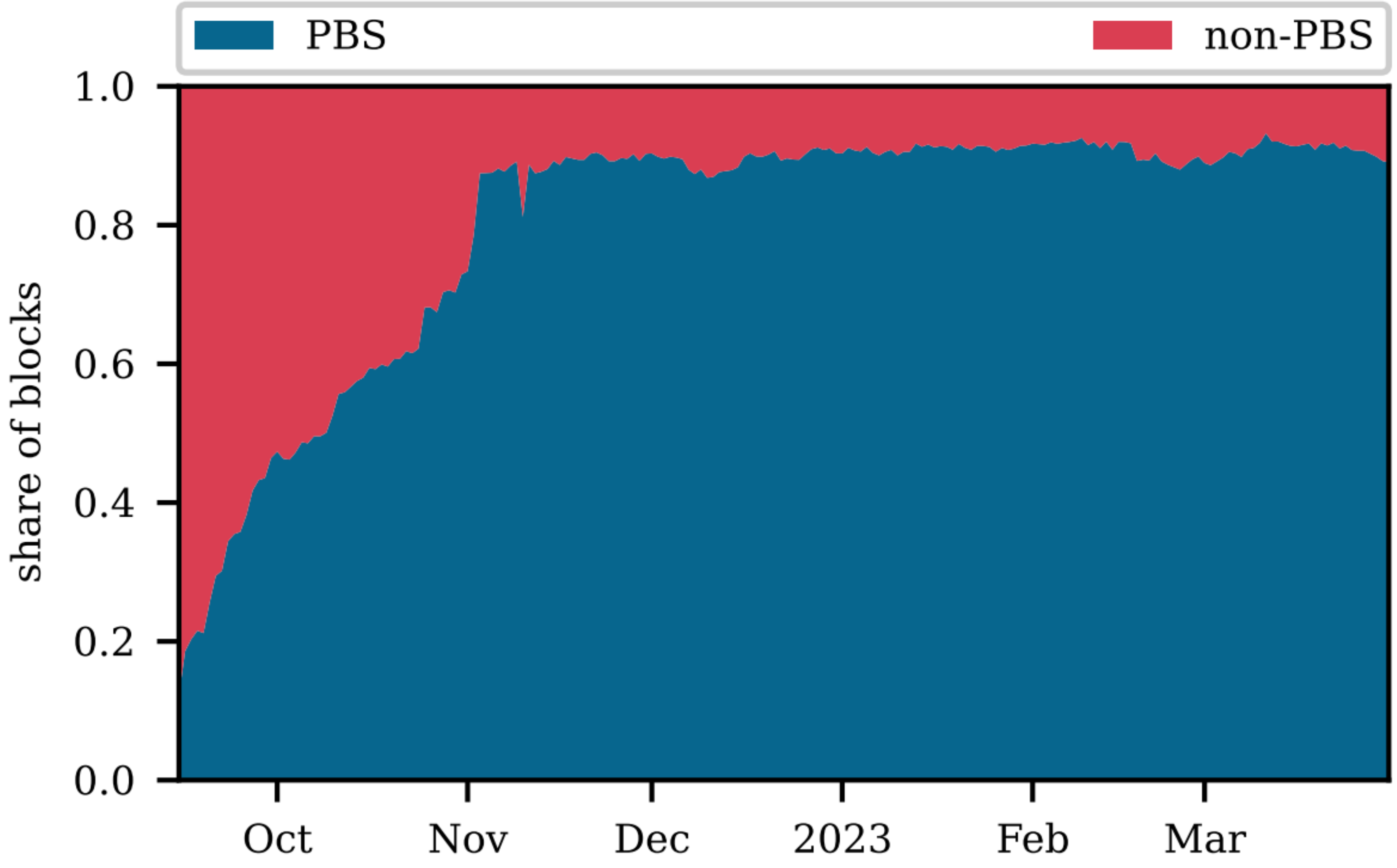
- **Often the profits to validators come at the expense of ordinary users, leaving ordinary users vulnerable to systematic extraction**

Systematization of Value Extraction



Systematization of Value Extraction

- Widespread in industry
- Validation of the rational model



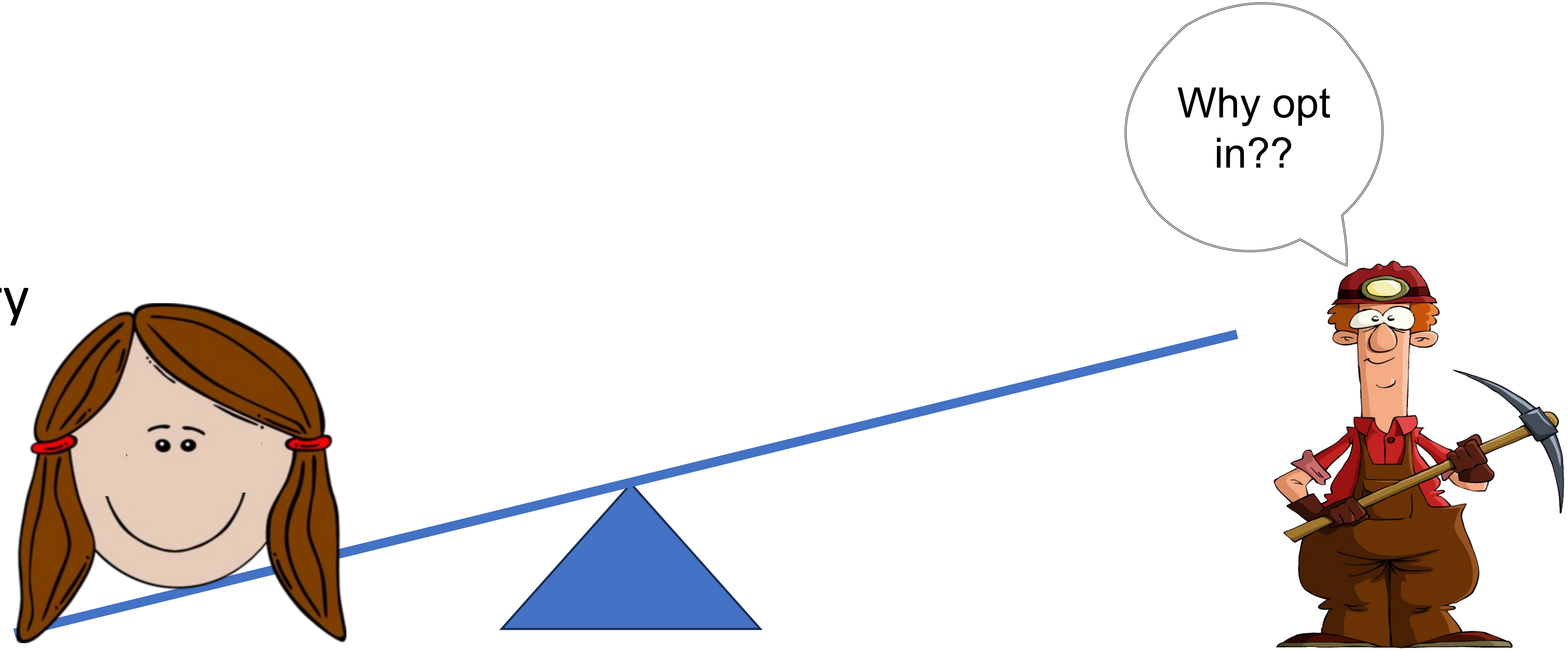
[HKTW23] Ethereum's Proposer-Builder Separation: Promises and Realities

Fair Ordering

- Temporal Fair Ordering
  - (Receive Order Fairness) “If sufficiently many (at least $\boldsymbol{\gamma}$-fraction) nodes receive a transaction *tx1* before another transaction *tx2* , then all honest nodes must output *tx1* before *tx2*” [KZGJ20]
- Blind Ordering
  - Ordering policy does not consider transaction contents (except transaction fees). Can be enforced through threshold encryption, Trusted Execution Environments (TEEs)
- A large body of *academic* literature
- **Protection for users**
- Why would a **rational** validator opt in, unless protocol is revamped?

Fair Ordering

Ordinary User



Miner / Validator

Externality: Latency racing for the top of the block

A practical question

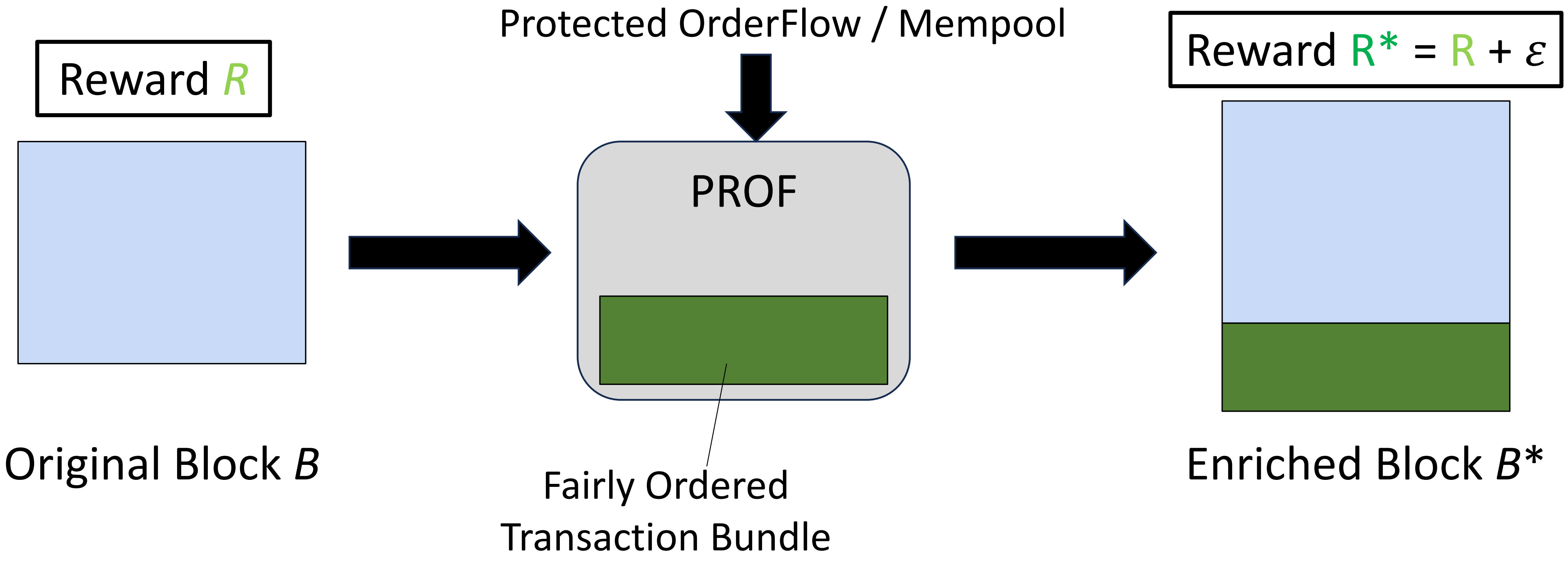
Can users get protection against the most pernicious forms of MEV while accounting for rational validators?

PROF: Protected Order Flow in a Profit-Seeking World

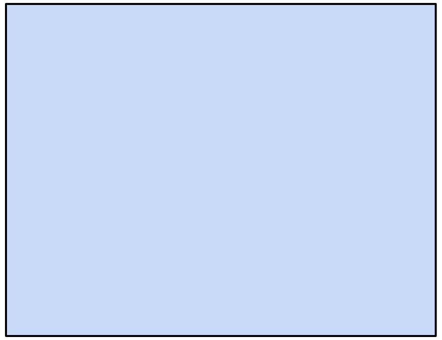
PROF Mechanism

- Simple
- Backward Compatible
- Protects Users without service degradation
- Accounts for Rational Validators

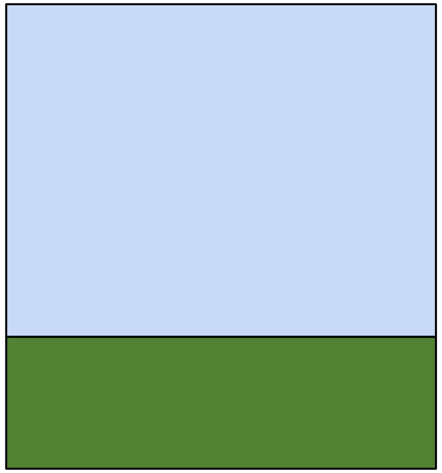
PROF Design Summary



Validator’s perspective



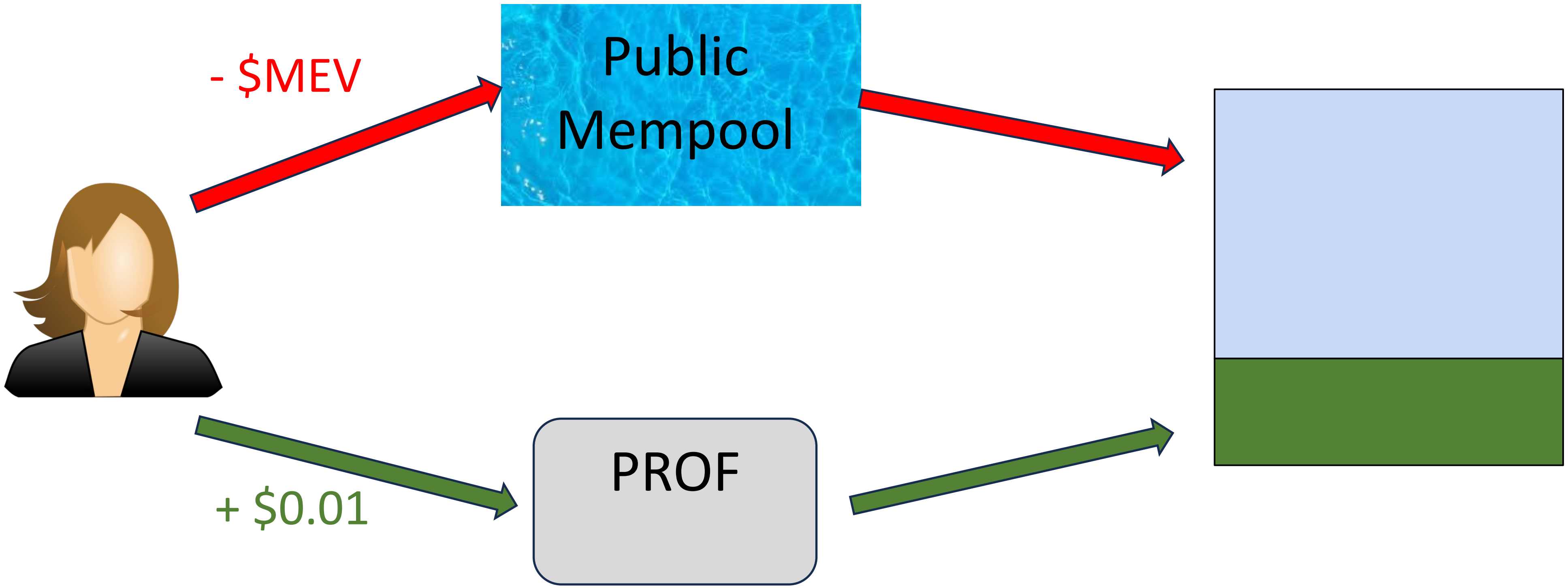
Which block does the validator choose?



Block B
Reward R

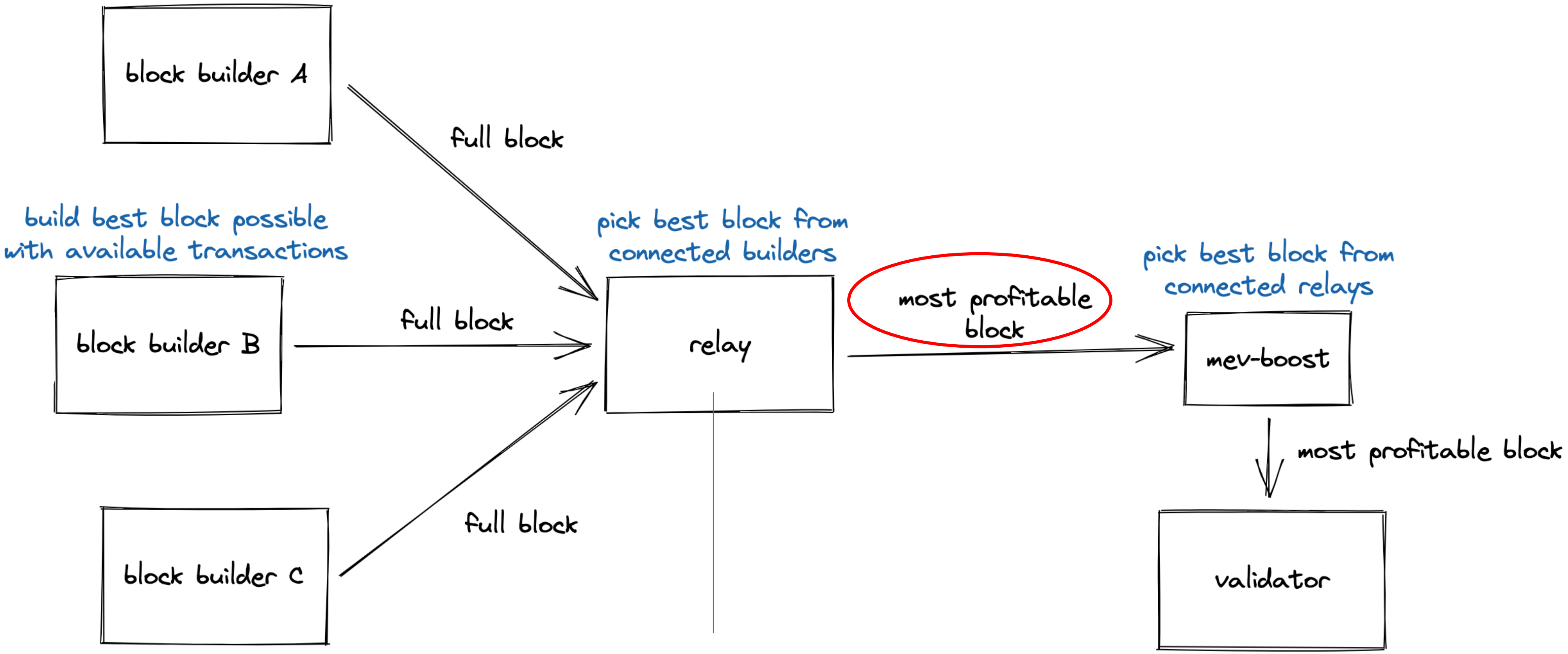
Block B^*
Reward $R^* = R + \varepsilon$

User’s perspective



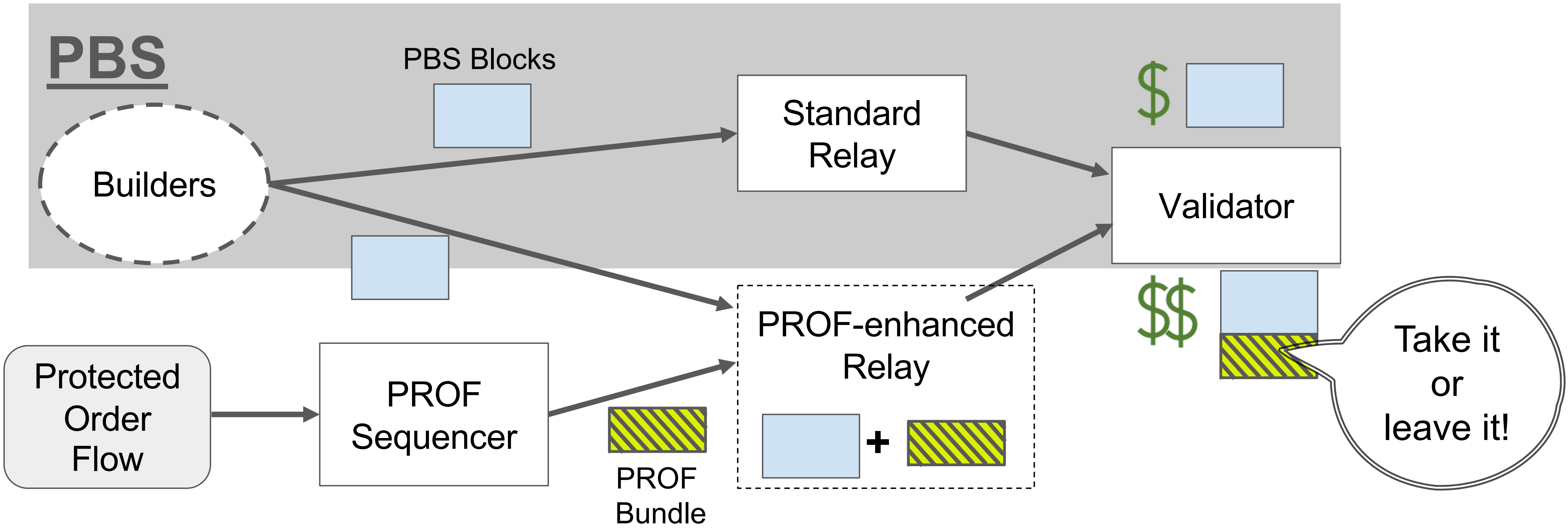
Which path does the user choose?

Proposer Builder Separation (PBS)



Trusted Auctioneer

PROF Key Insight

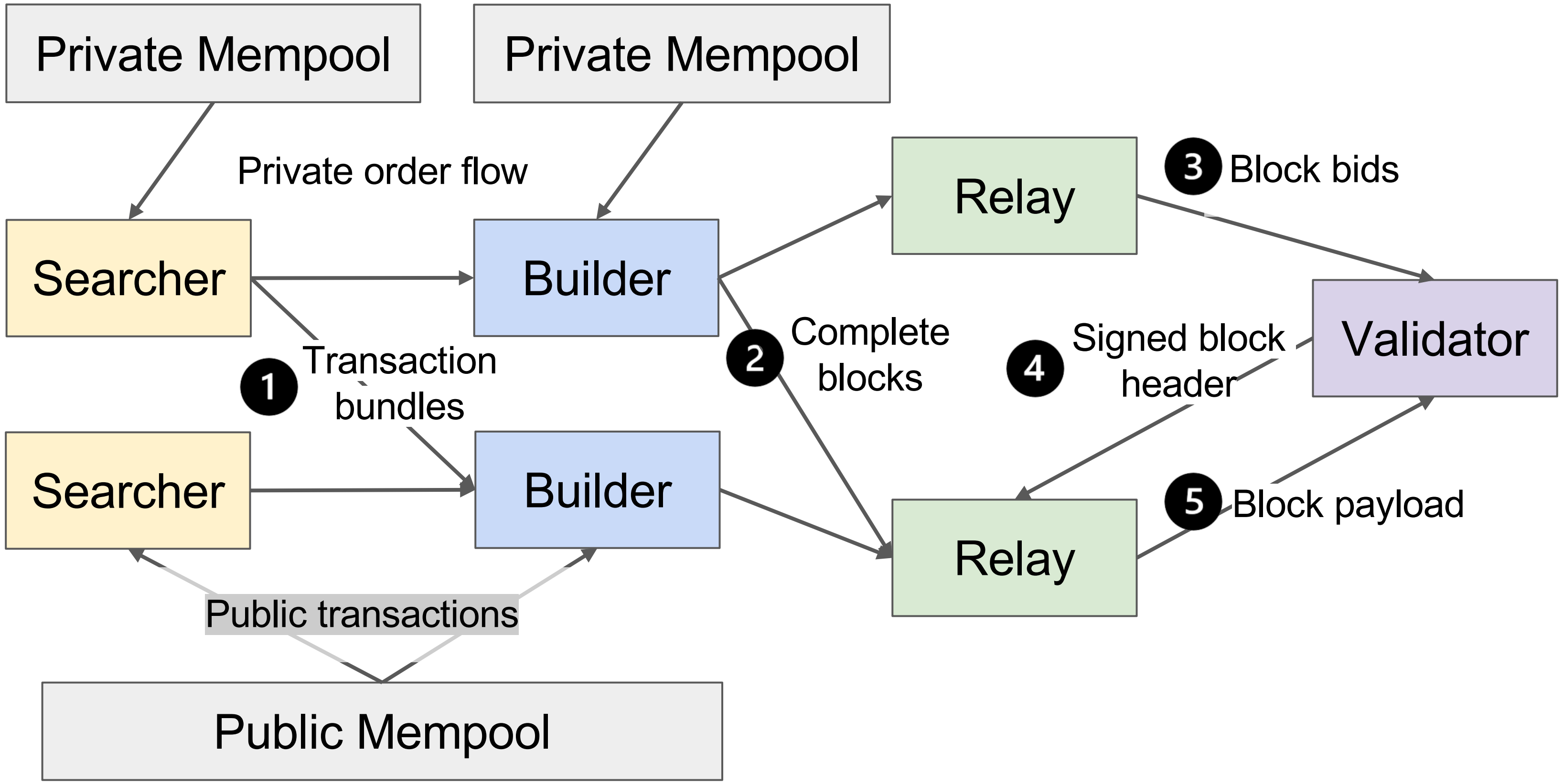


Learn practically nothing about PROF transactions if you *leave-it*

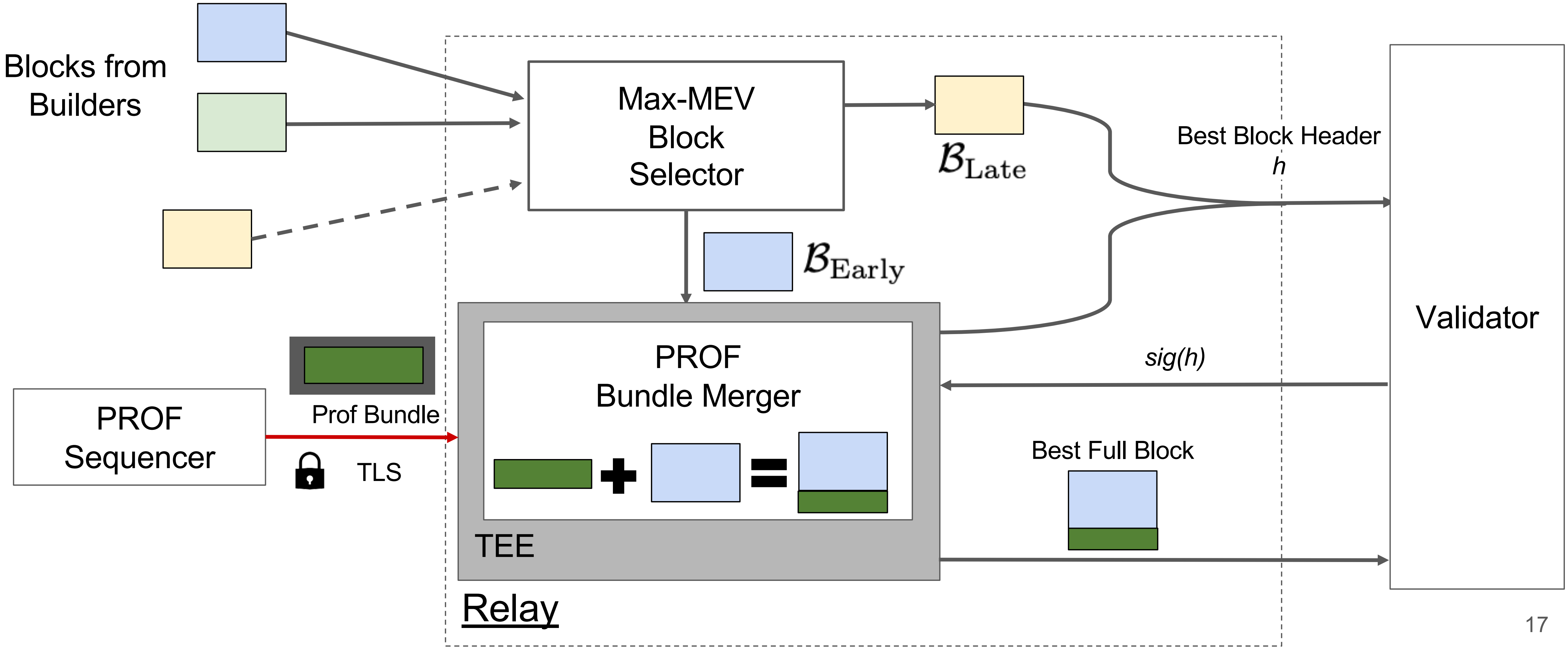
Why should relays adopt PROF?

- Relays compete to have their blocks accepted
- All else equal, a PROF-enhanced relay is more competitive than a regular relay
- Workflow for builders remains unchanged

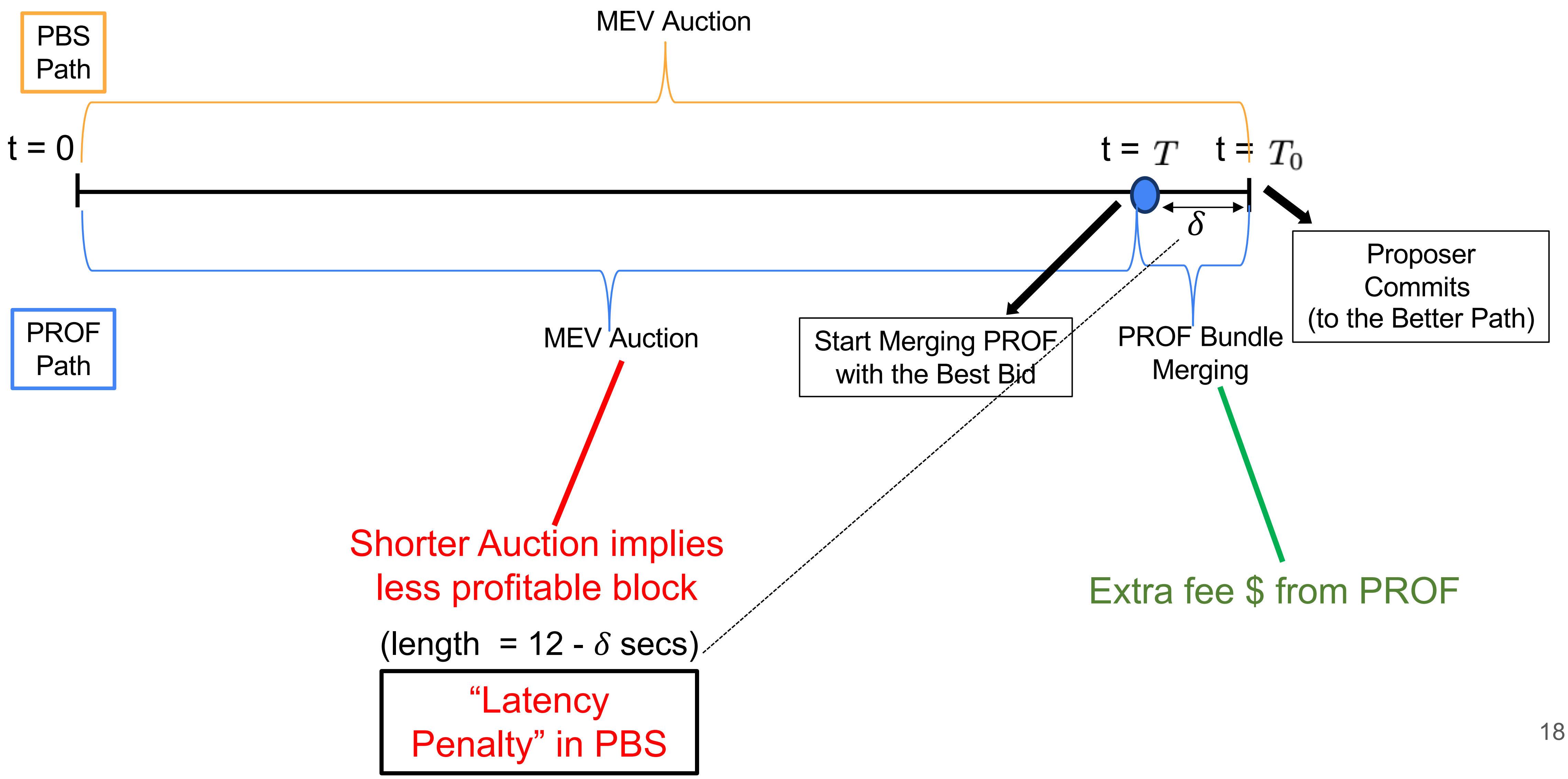
PBS Workflow



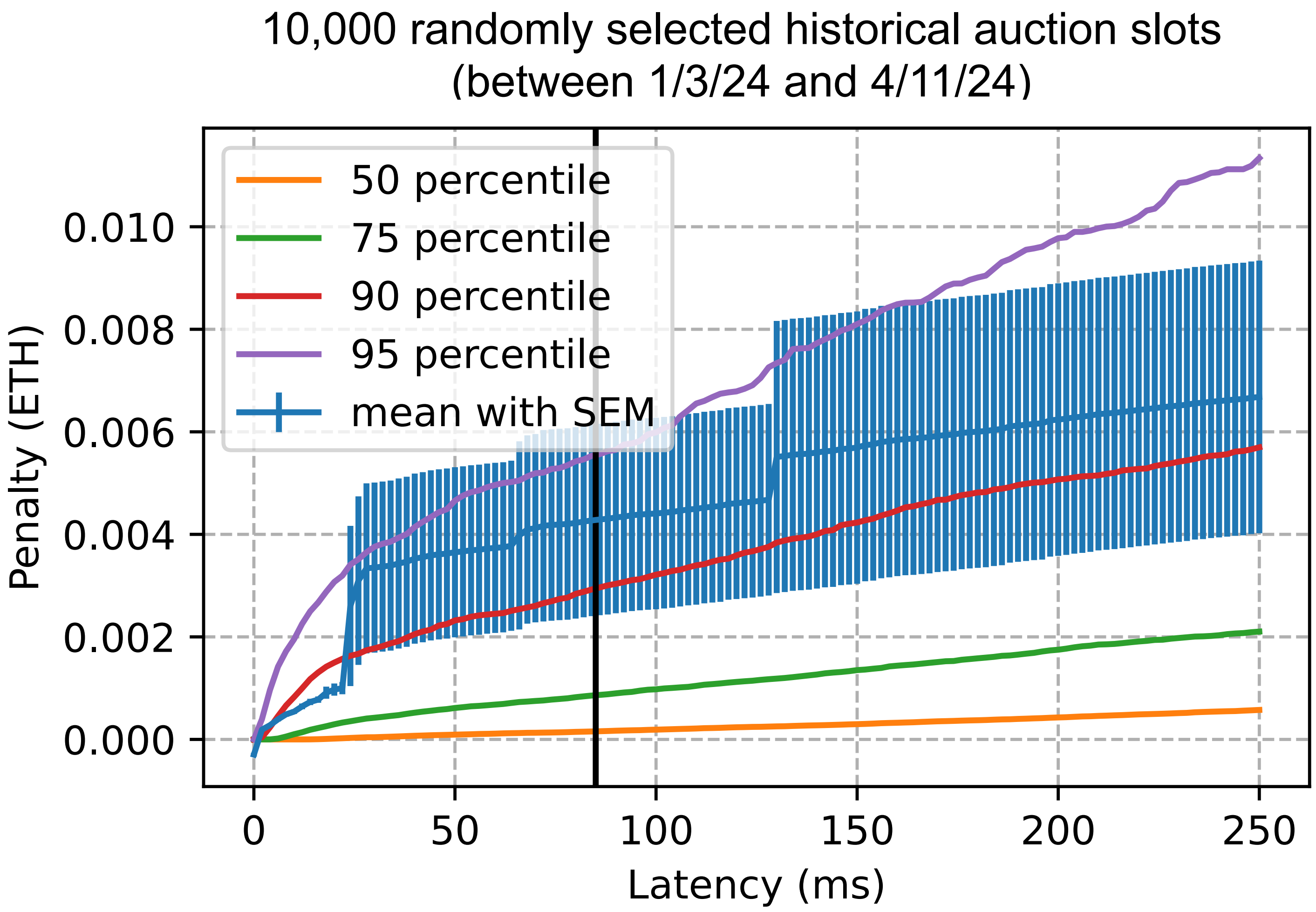
PROF Design Details



PROF Timeline



Latency Penalty in PBS Auction



Percentiles of slots for a particular latency and penalty

Example: If auction were ended 85ms earlier, 90% of slots would give ~0.003 ETH less

Inclusion Likelihood

$$\alpha = \Pr[\text{Fees}(\theta_{\text{PROF}}) > \underbrace{\max(\text{Bids}(T_0)) - \max(\text{Bids}(T_0 - \delta))}_{\text{Latency Penalty}(\delta)}].$$

Inclusion Likelihood

$$\alpha = \Pr[g\gamma f > \text{Latency Penalty}(\delta)].$$

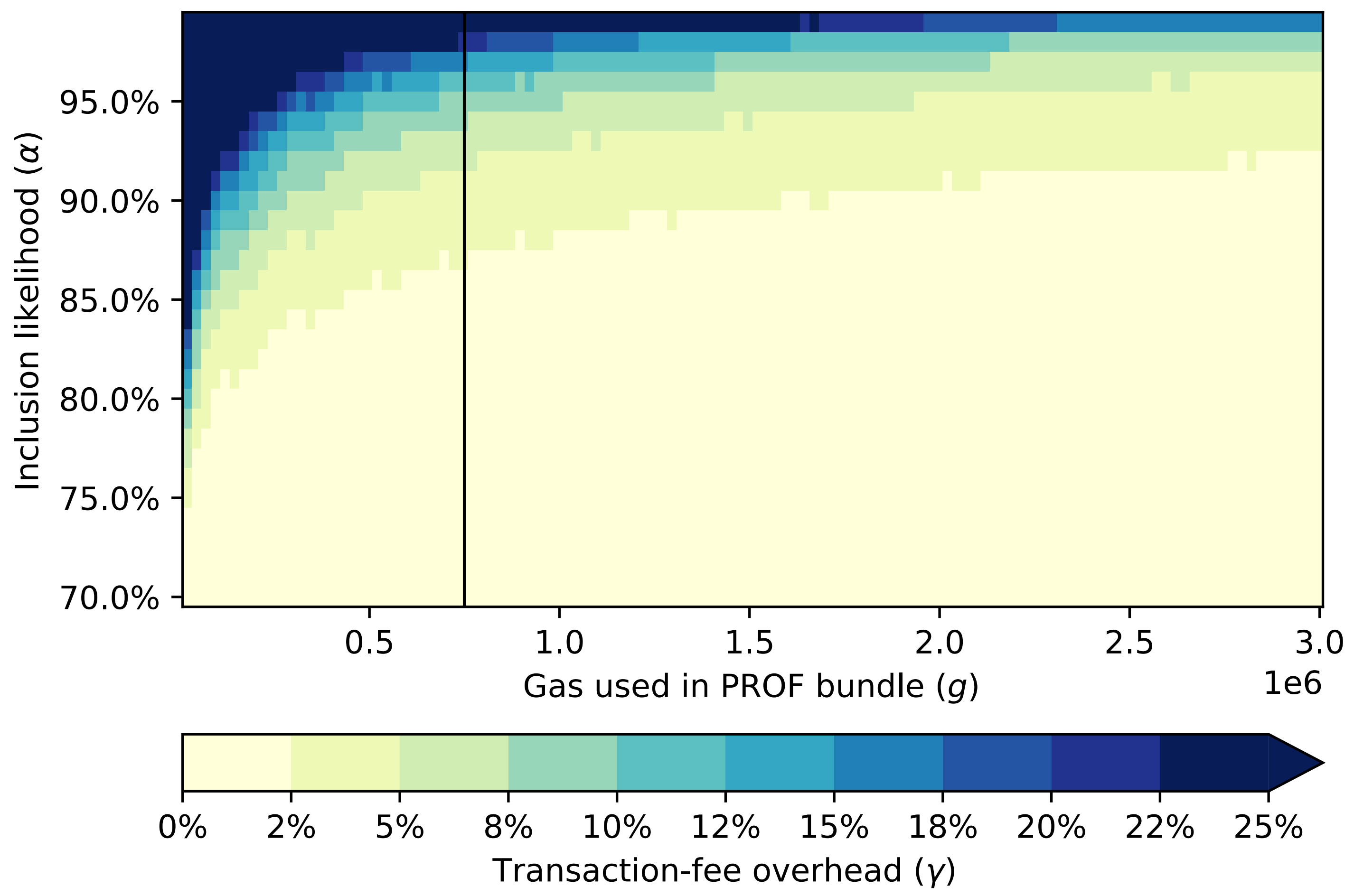
Gas used in PROF bundle

Overhead as a multiple of `"base fee" *f*

Depends on gas used *g*

Relationship between α, g , γ

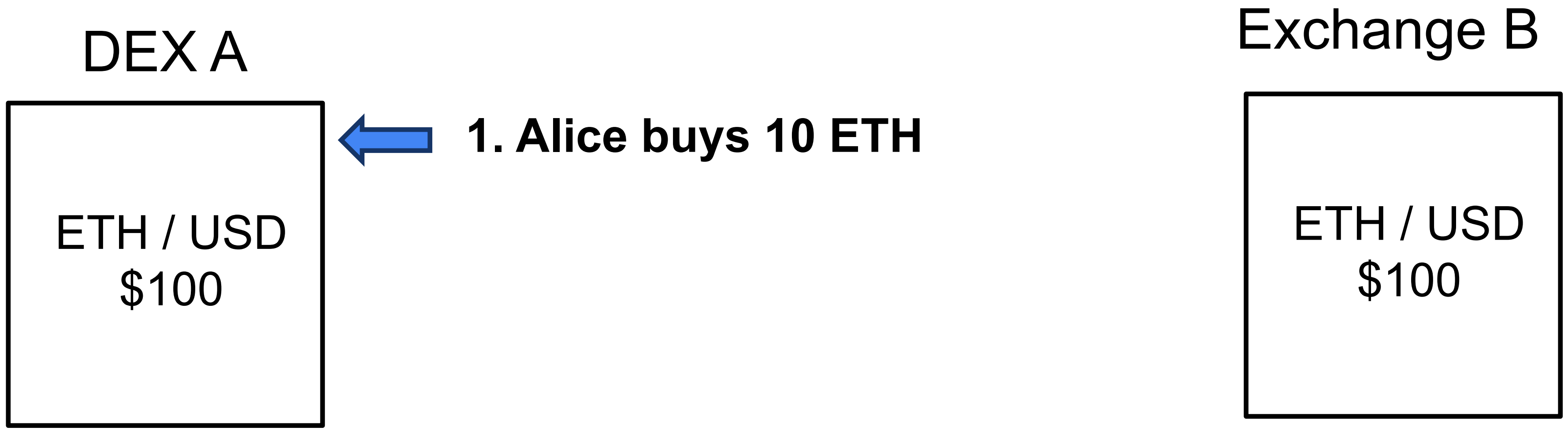
Inclusion Likelihood



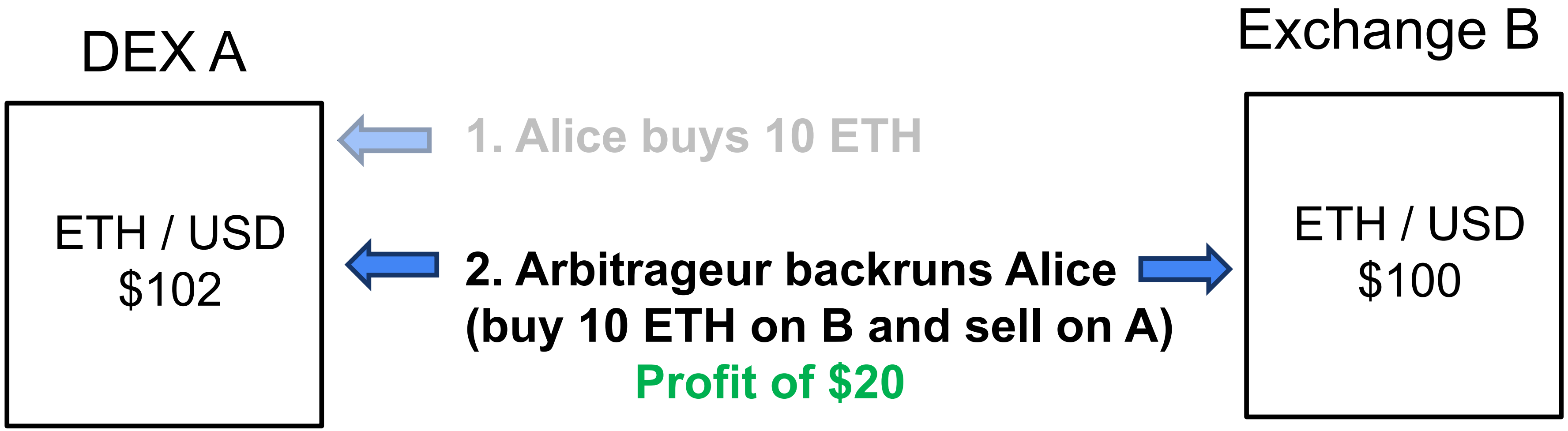
Takeaway:

High Inclusion Likelihood of PROF for minimal fee

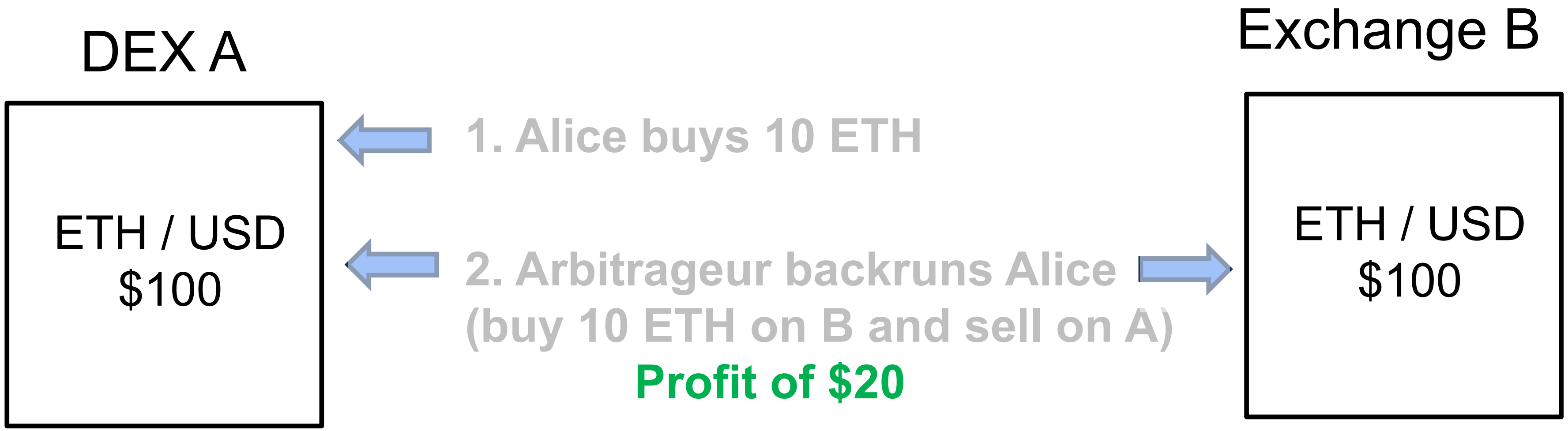
A Step Further: Redistribution of MEV to Users



A Step Further: Redistribution of MEV to Users



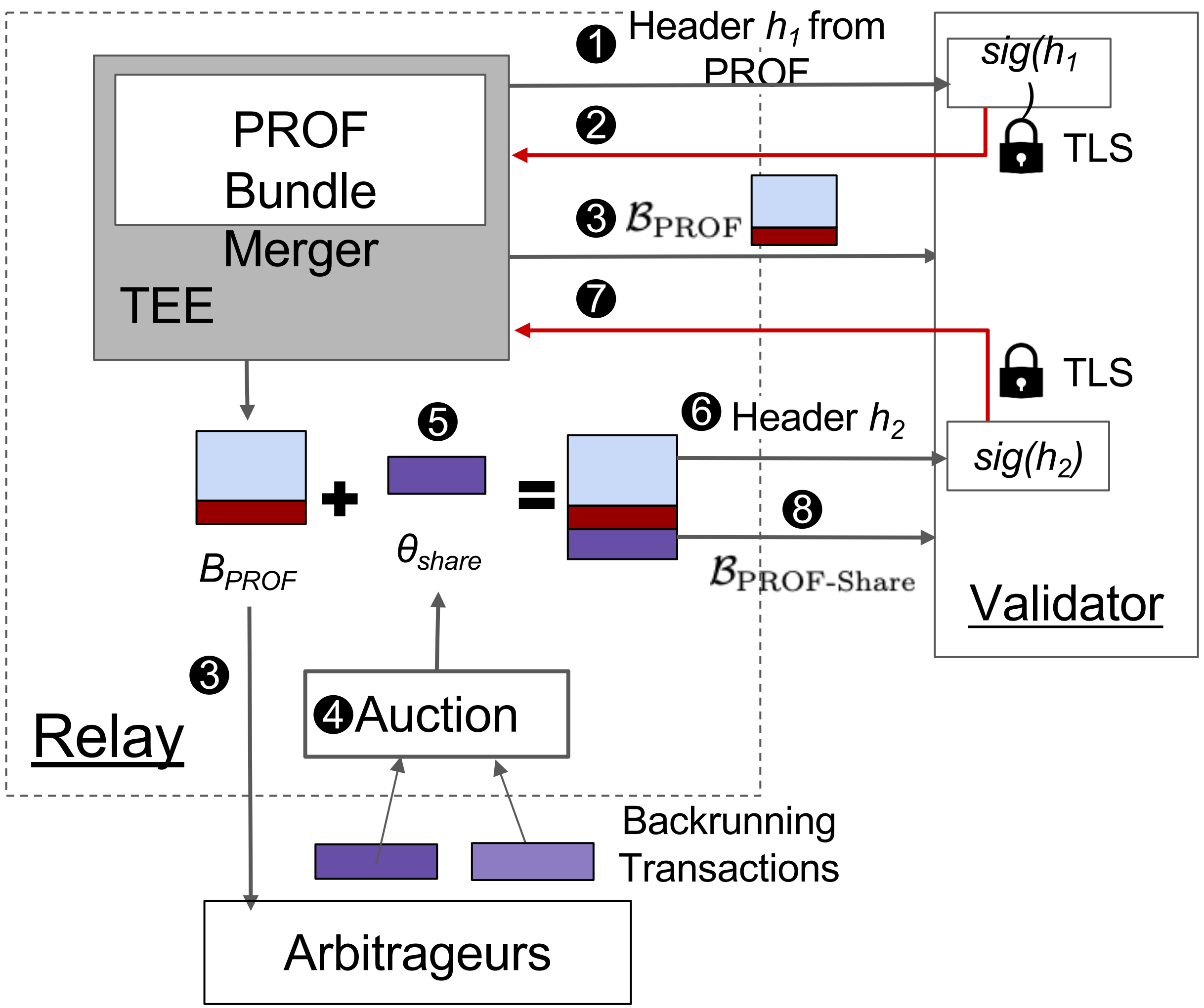
A Step Further: Redistribution of MEV to Users



Share $X with Alice, $20-X divided up between validator and arbitrageur

PROF-Share : A Step Further

- Redistribute any MEV opportunity created by PROF users back to them
- For instance, arbitrage from backrunning of DEX trades



Related Redistribution Mechanisms

- MEV-Share and MEV-Blocker
- Attempts to prevent frontrunning through a trusted intermediary
- Yet, needs to leak hints about transaction contents for attracting and facilitating backrunning and redistribution
- Widespread in industry : Revenue to the validator from MEV-Share and MEV-Blocker is pivotal in deciding the winner of a majority of auctions!

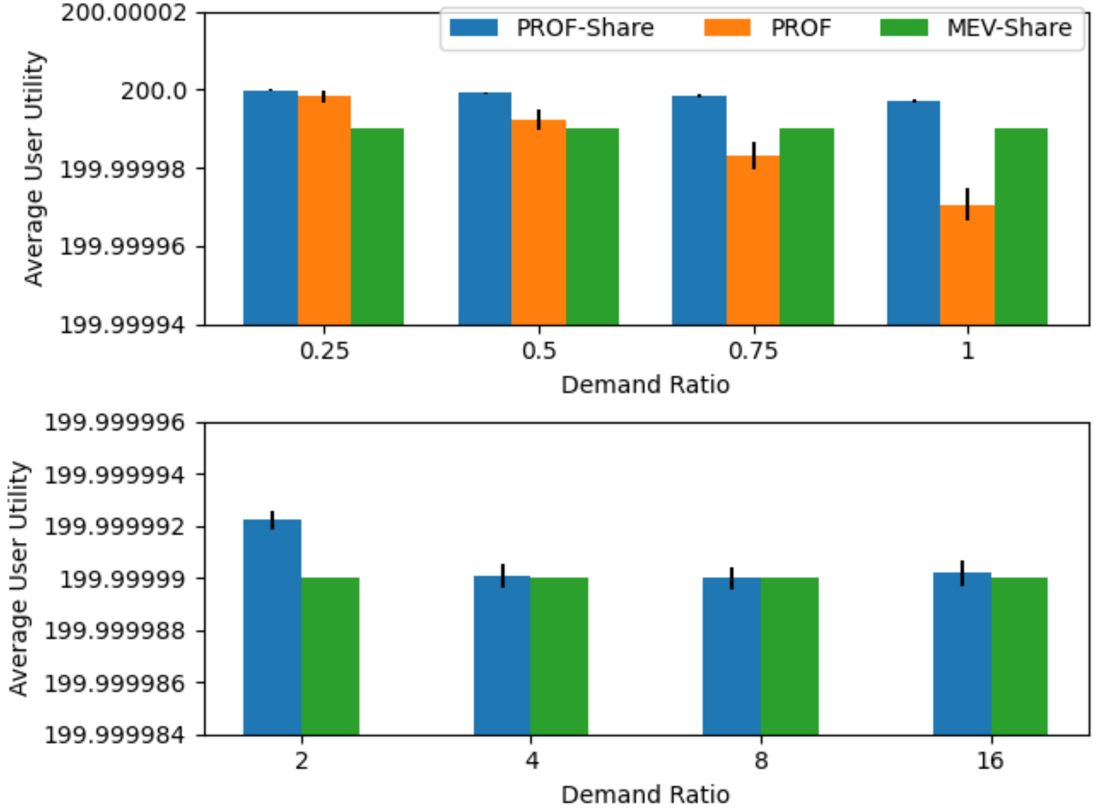
Other benefits of PROF-Share

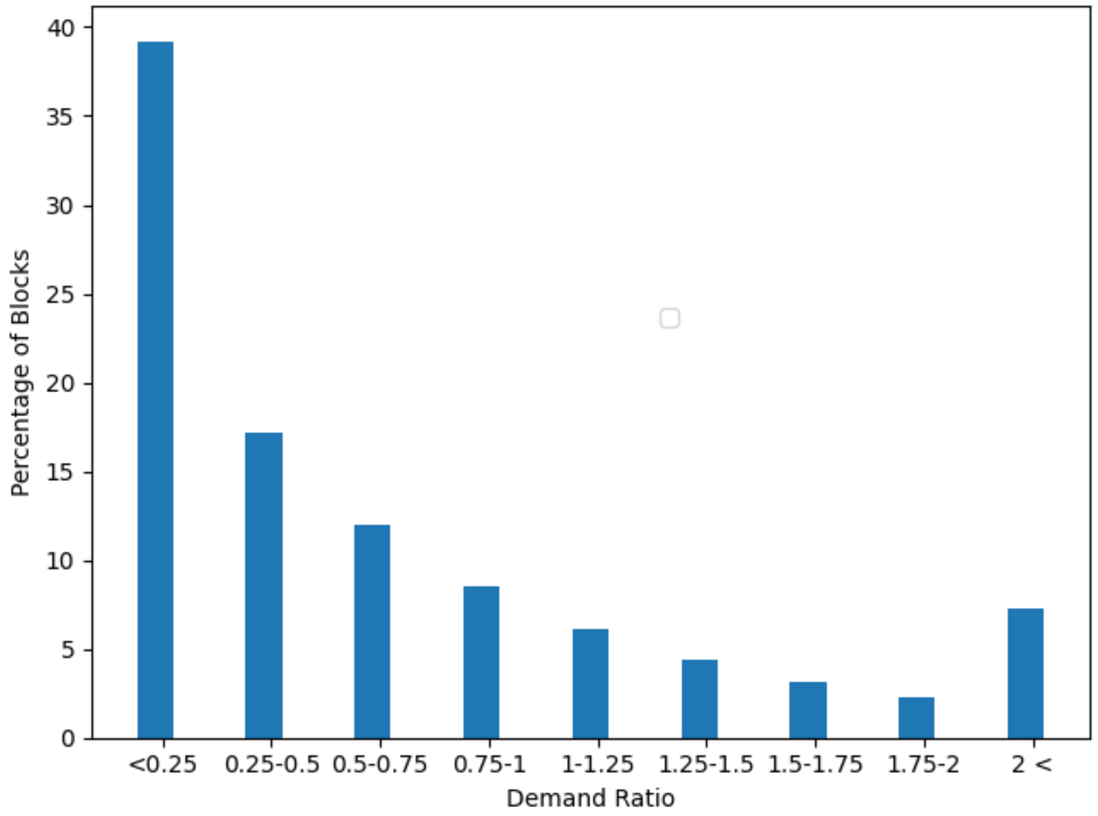
- PROF-Share transactions are completely private until the validator commits to including them, and then are completely released for backrunning
- As a result:
- More efficient backrunning compared to backrunning based on hints (gas savings as state is known offchain)
- PROF-Share users get to keep *almost all* of the backrunning profits rather than sharing it with validators (as in MEV-Share)
- Organic backrunning between transactions of a PROF bundle – one PROF user could be a "backrunner" of another user if they trade in opposite directions

Economic Utility Analysis

- Compare different protection mechanisms
- PROF v/s PROF-Share v/s MEV-Share
- Model:
  - DEX : A constant product AMM
  - An external infinite liquidity market for arbitragers (Centralized Exchanges) – constant price P
  - Start out with AMM price of P
  - Each user trades a unit quantity in randomly either direction
  - Demand Ratio (informally) : A maximum cap on how much volume of trades are in one direction compared to a baseline of net 0 buy and 0 sell

Economic Utility Analysis

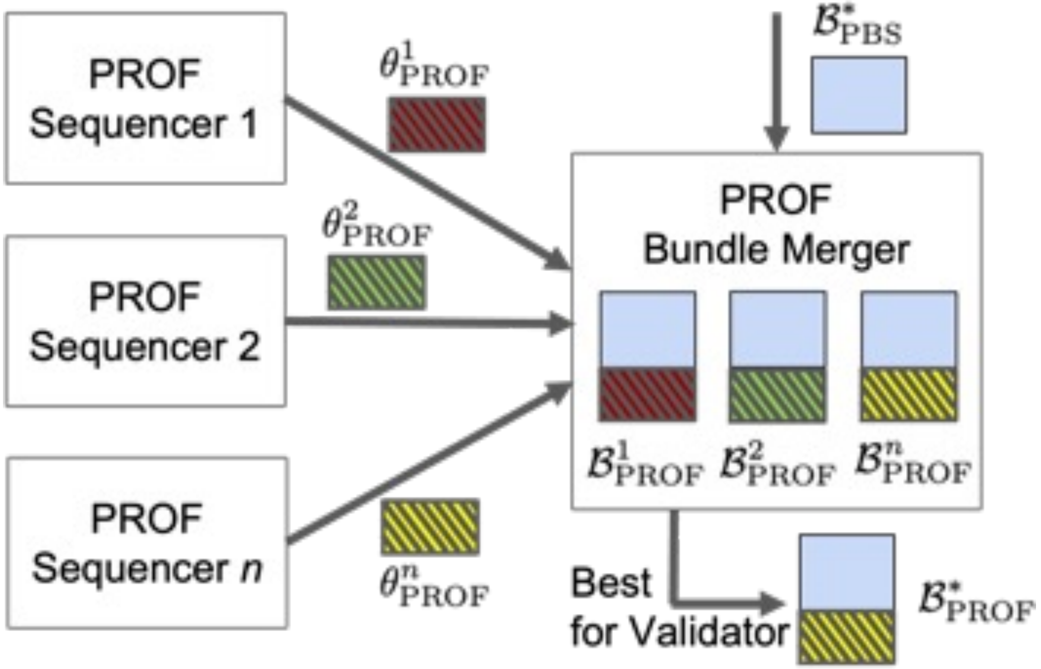


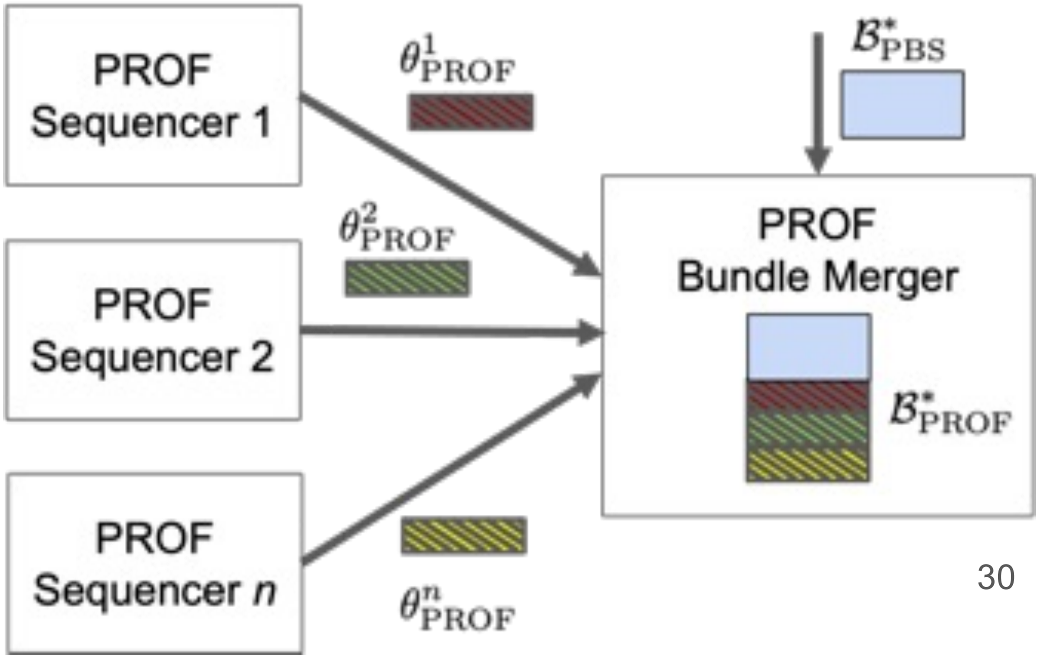


- Takeaway1 : PROF-Share always delivers the highest value of users
- Takeaway2: In times of low net demand, PROF delivers higher value even without redistribution benefits (MEV-Share), thanks to organic backrunning

Flexibility in PROF

- Multiple Sequencers
- PROF Sequencer here is a black-box
    - Centralized / Decentralized
    - PROF supports any ordering policy





Conclusion

- PROF: A simple backward-compatible system designed for protecting users from harmful MEV extraction, while accounting for the profit-maximizing nature of validators
- PROF Endgame Thesis: Transactions that want top of the priority can go through the gauntlet of MEV auctions*. All other transactions should go through PROF to enjoy protection from MEV

*nullifies the externality of latency racing in fair and blind ordering

To Learn More

- Visit the website: prof-project.github.io (FAQs)
  - Watch the demo of PROF-enriched blocks landing at validators
- Uniswap RFP: $50k for maturing PROF implementation
- Announcements @PROF_MEV
- Contact: babel@cs.cornell.edu
- PROF paper just released!

PROF: Protected Order Flow in a Profit-Seeking World

Kushal Babel[†§], Nerla Jean-Louis[‡§], Yan Ji[†§], Ujval Misra[‖§], Mahimna Kelkar[†§], Kosala Yapa Mudiyanselage[¶], Andrew Miller[‡§], Ari Juels[†§]

[†]*Cornell Tech*, [‡]*UIUC*, [‖]*UC Berkeley*, [§]*IC3*, [¶]*Fidelity Center for Applied Technology*

https://arxiv.org/abs/2408.02303