extractable value (aka MEV)

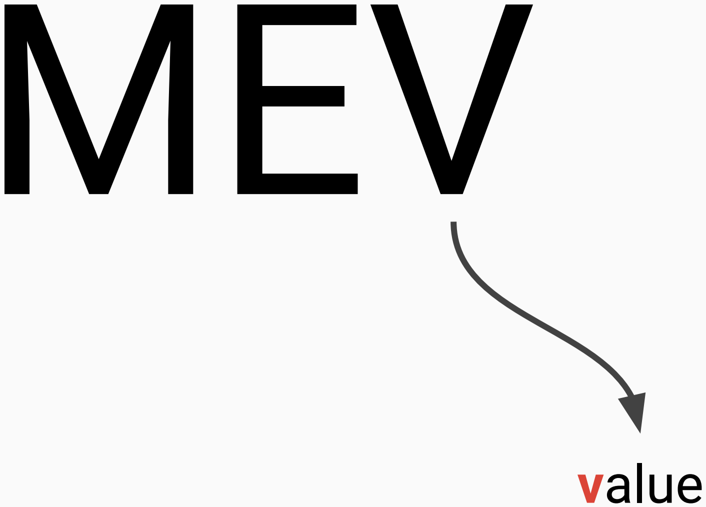
cryptographic opportunities

incentives shape outcomes

"show me the incentive and I'll show you the outcome"

—Charlie Munger

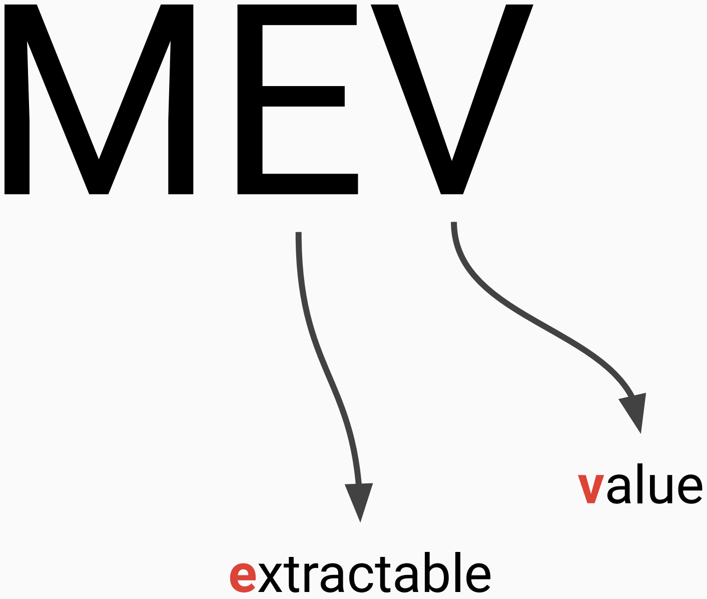
MEV



MEV

value

MEV

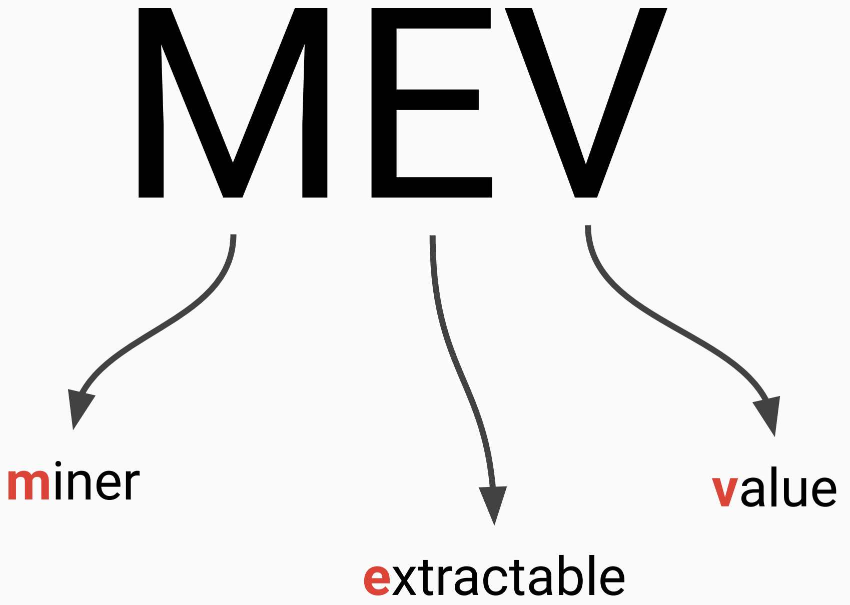


MEV

value

extractable

MEV



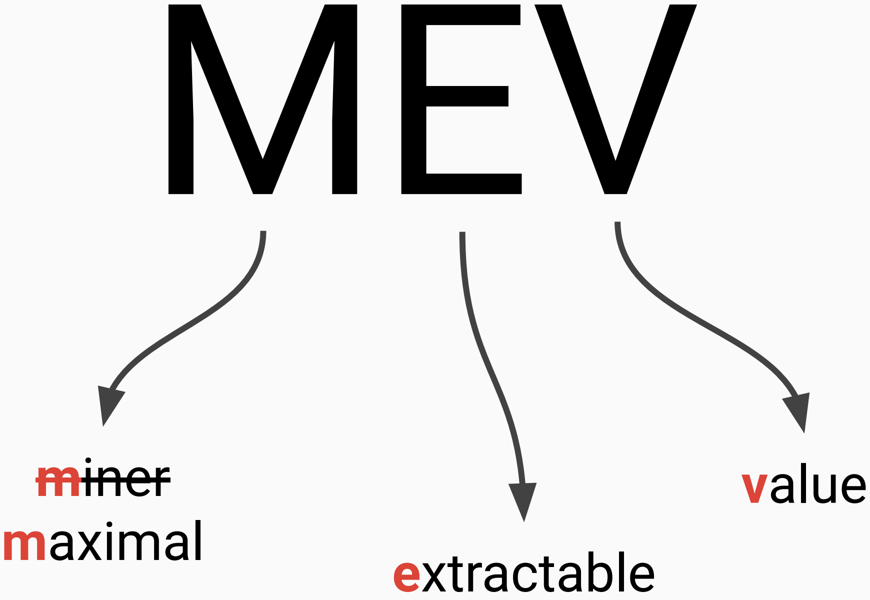
MEV

miner

extractable

value

MEV



MEV

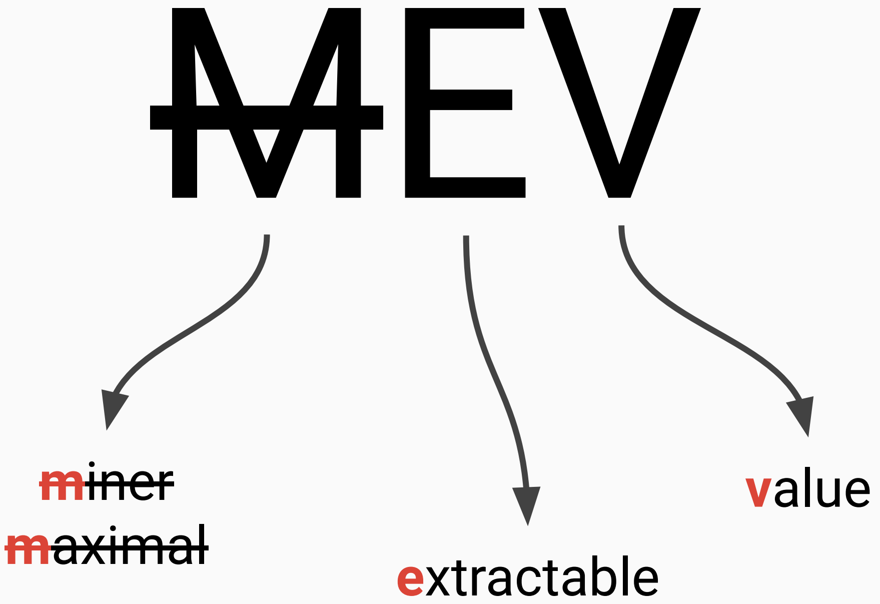
~~miner~~

maximal

extractable

value

MEV



~~M~~EV

~~miner~~

~~maximal~~

extractable

value

types of MEV

issuance

💦

fees

💵

carrots

🥕

types of MEV

issuance

💦

fees

💵

carrots

🥕

proposer rewards

attester rewards

types of MEV

issuance

- proposer rewards
- attester rewards

fees

- base fees
- tips

carrots

types of MEV

issuance

💦

proposer rewards

attester rewards

fees

💵

base fees

tips

carrots

🥕

arbitrage

liquidations

sandwiches

MEV amounts

issuance

💦

$55M/day

~15K ETH/day

fees

💵

carrots

🥕

MEV amounts

issuance	**fees**	**carrots**
💦	💵	🥕
$55M/day	**$40M/day**	
~15K ETH/day	cryptofees.info	

MEV amounts

issuance

💦

$55M/day

~15K ETH/day

fees

💵

$40M/day

cryptofees.info

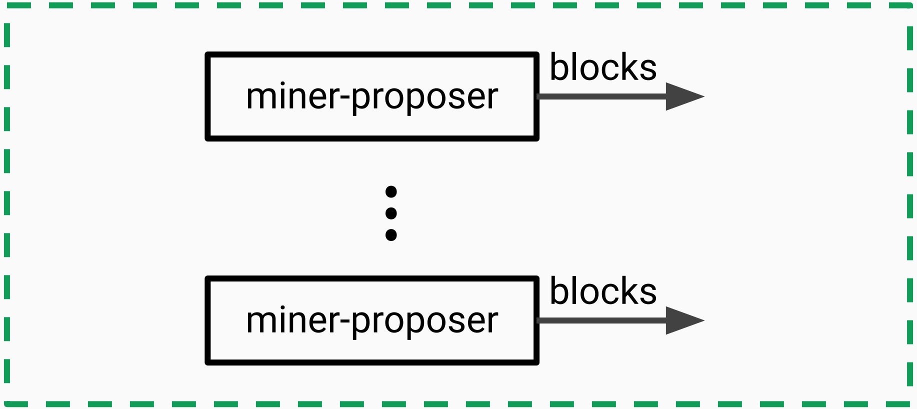
carrots

🥕

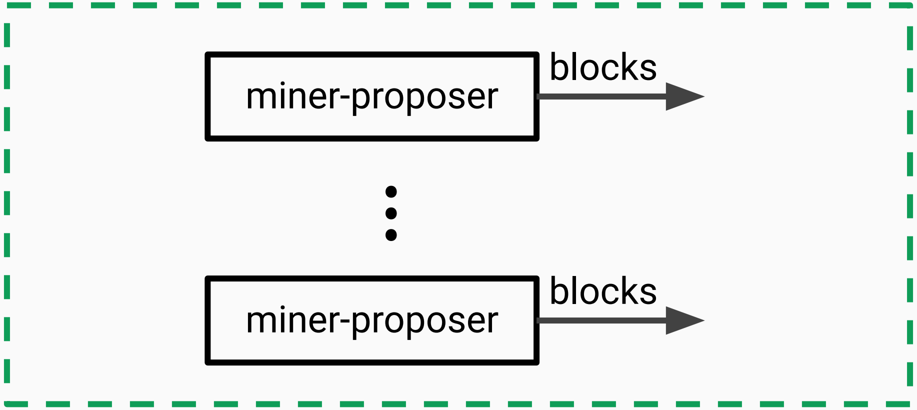
$1M/day

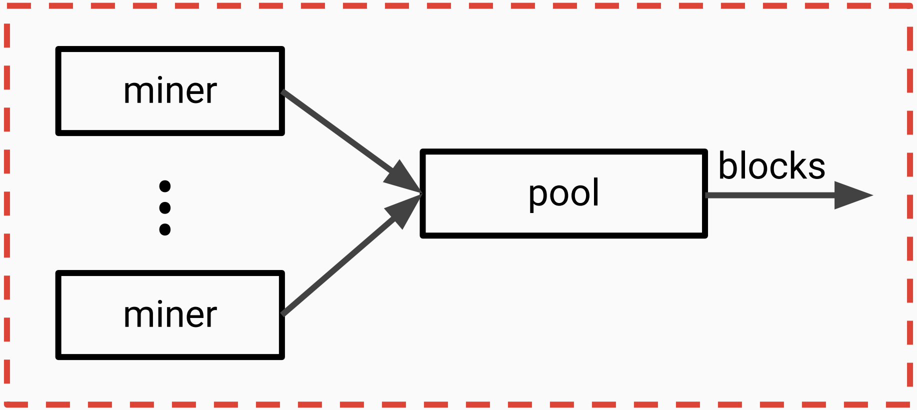
dashboard.flashbots.net

miner pooling

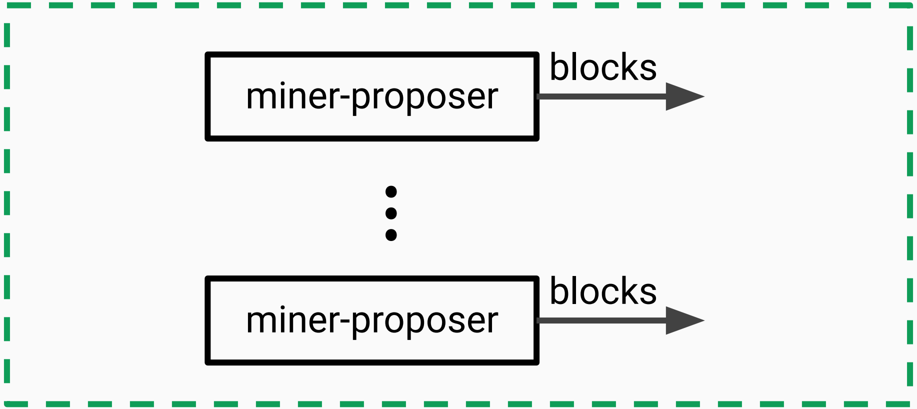


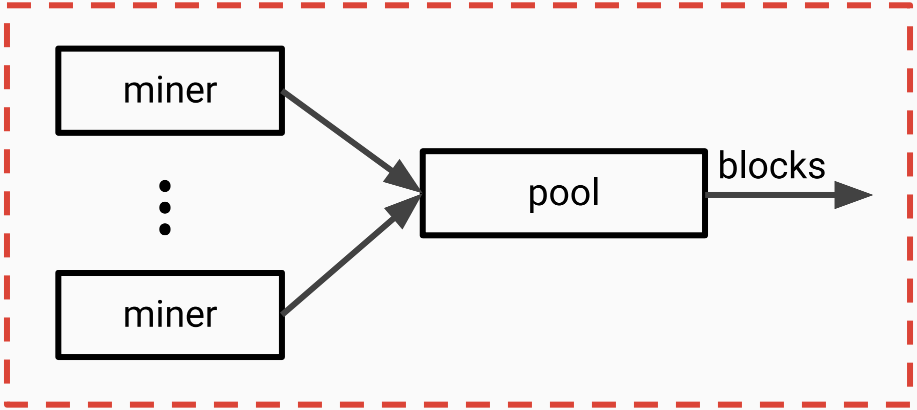
miner pooling

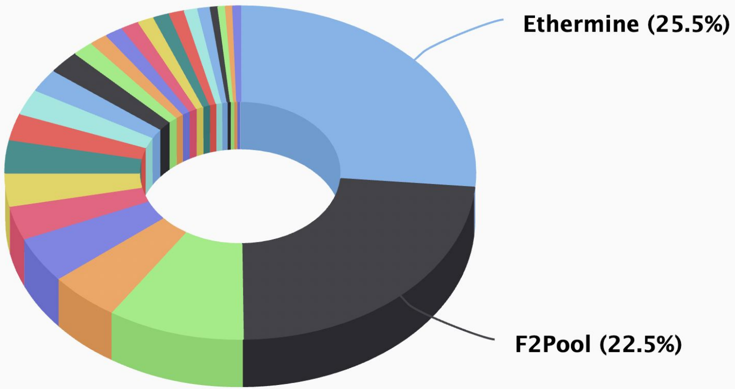




miner pooling







fee burn

fees

💵

~75% base fees 🔥

~25% tips

fee burn

fees

💵

~75% base fees 🔥

~25% tips

Ethereum economic utility

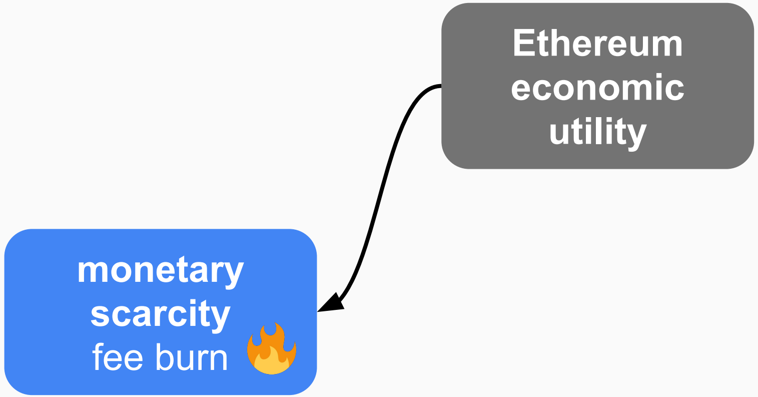
fee burn

fees

💵

~75% base fees 🔥

~25% tips



Ethereum economic utility

monetary scarcity
fee burn 🔥

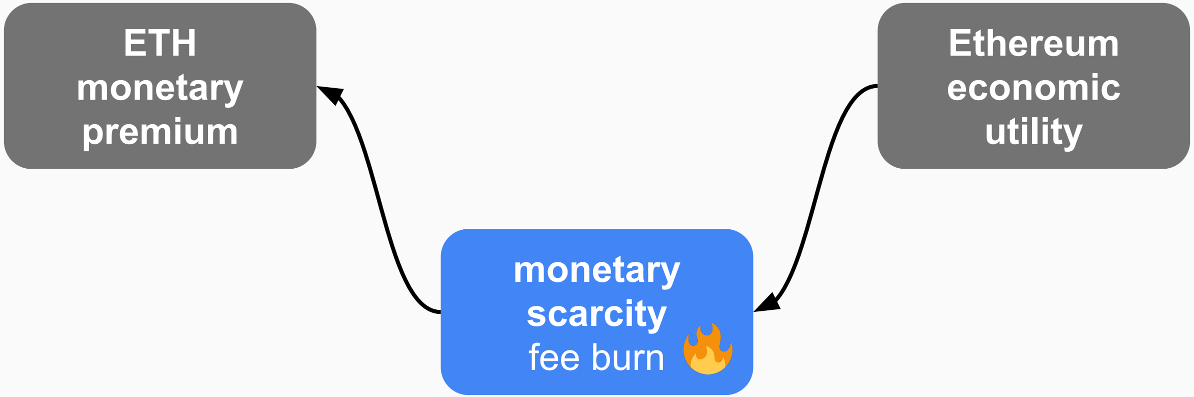
fee burn

fees

💵

~75% base fees 🔥

~25% tips



ETH monetary premium

Ethereum economic utility

monetary scarcity
fee burn 🔥

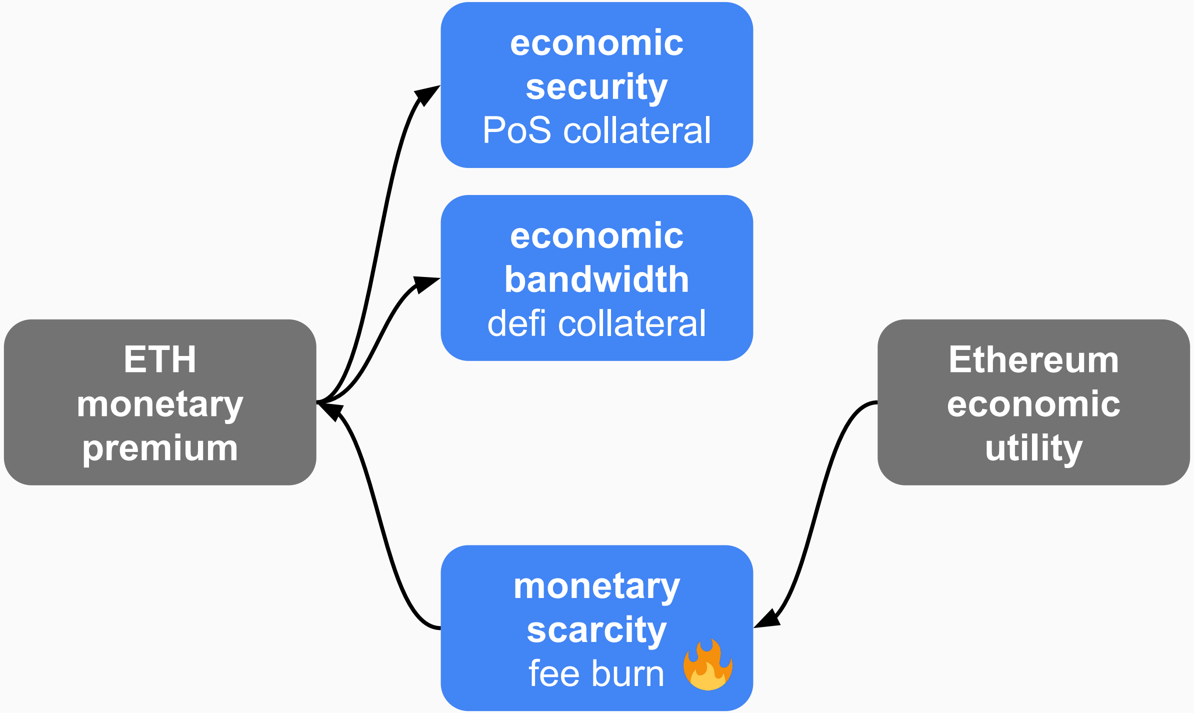
fee burn

fees

💵

~75% base fees 🔥

~25% tips



ETH monetary premium

economic security
PoS collateral

economic bandwidth
defi collateral

monetary scarcity
fee burn 🔥

Ethereum economic utility

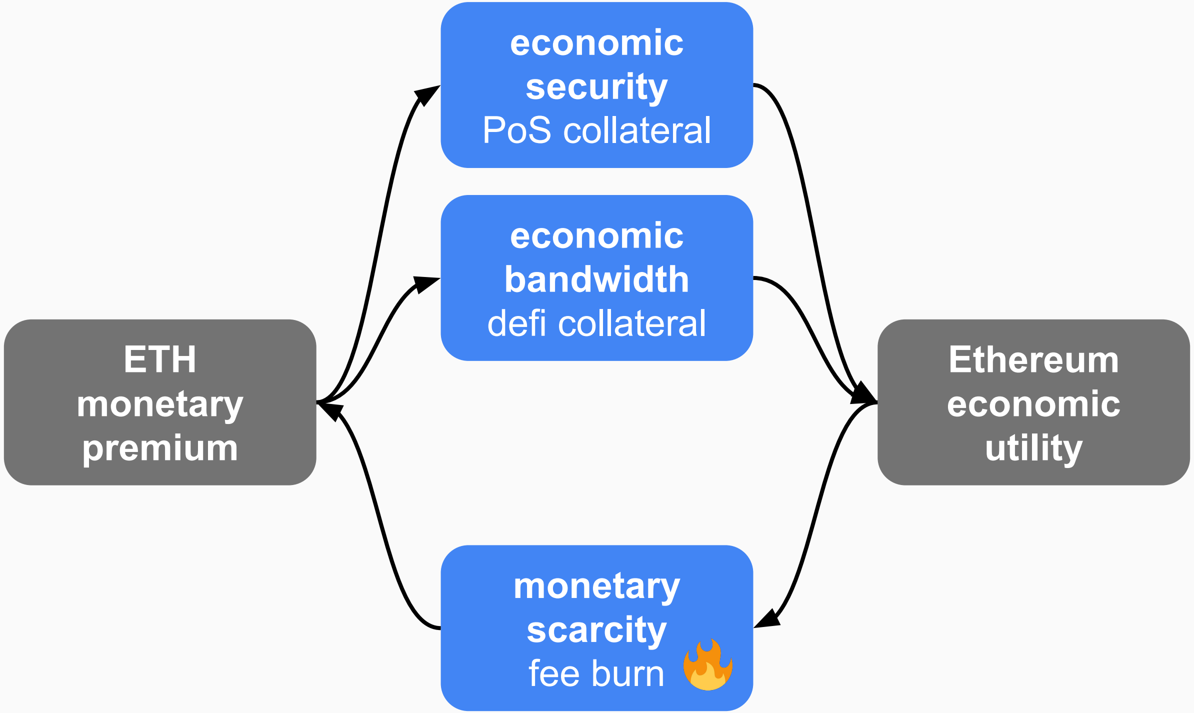
fee burn

fees

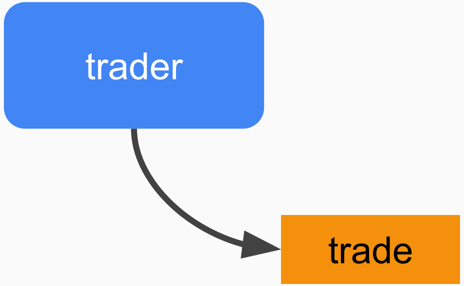
💵

~75% base fees 🔥

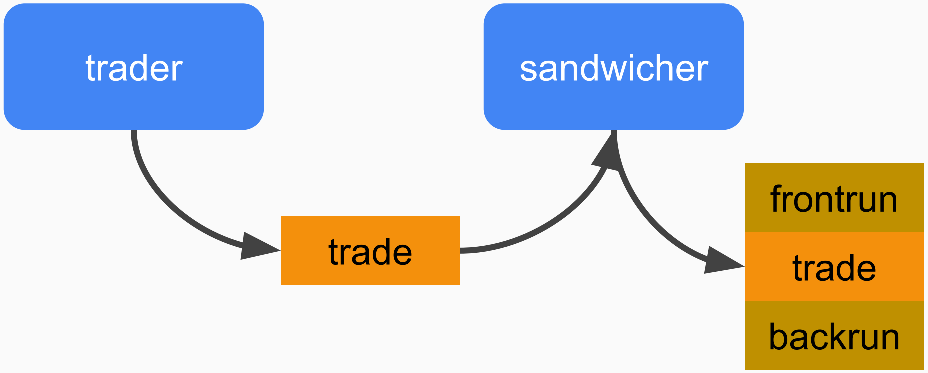
~25% tips



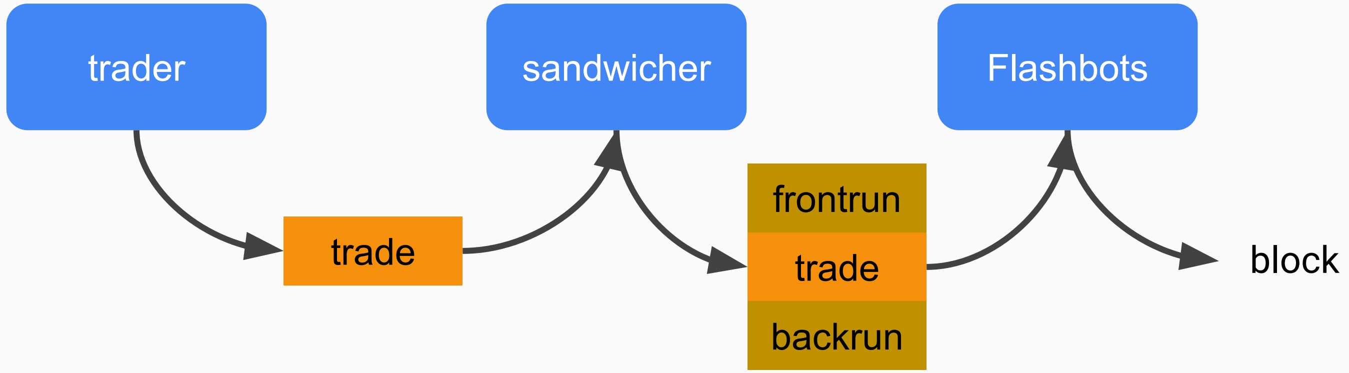
Flashbots



Flashbots



Flashbots


trader

trade

sandwicher

frontrun

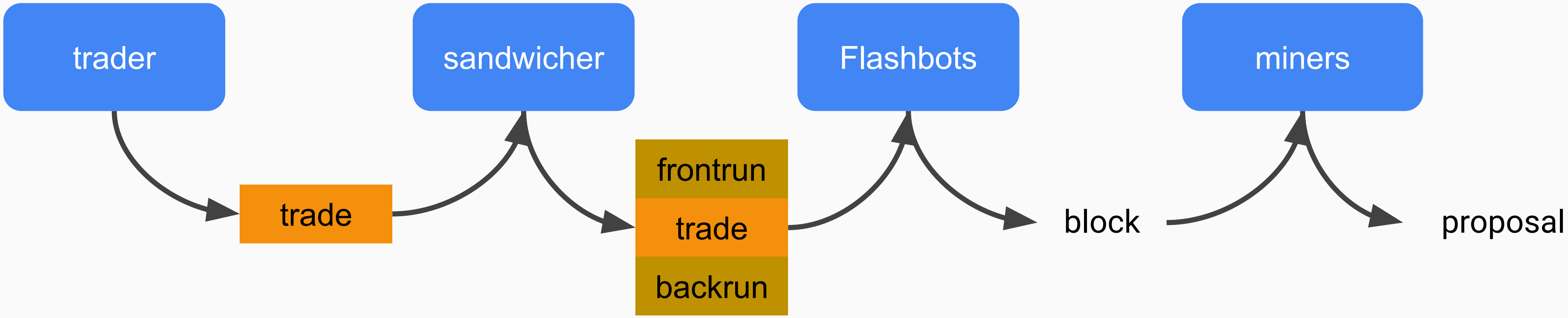
trade

backrun

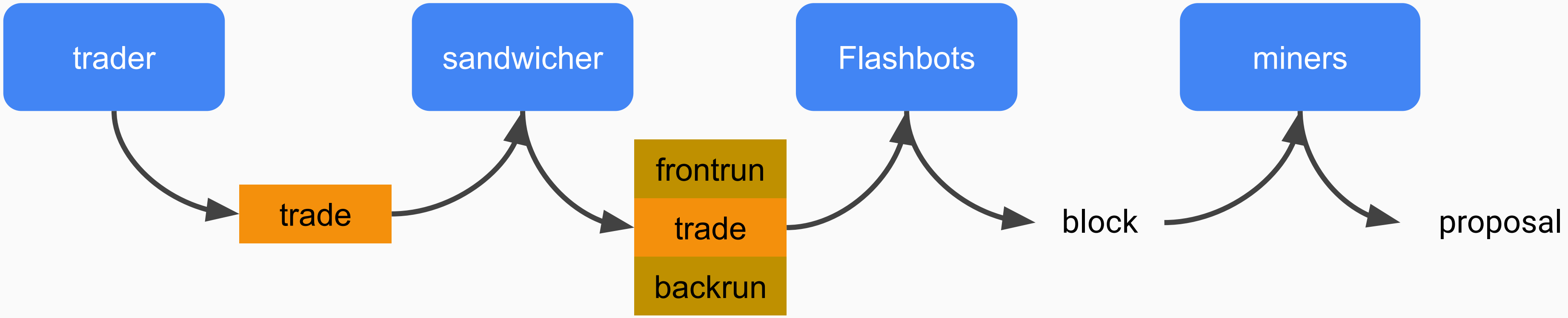
Flashbots

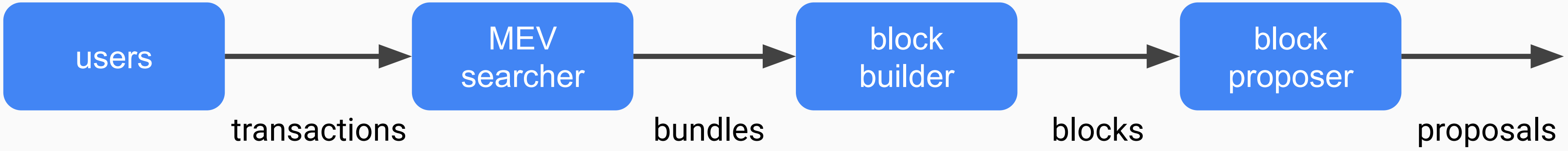
block

Flashbots


trader
trade
sandwicher
frontrun
trade
backrun
Flashbots
block
miners
proposal

Flashbots


trader
sandwicher
Flashbots
miners
trade
frontrun
trade
backrun
block
proposal


users
MEV searcher
block builder
block proposer
transactions
bundles
blocks
proposals

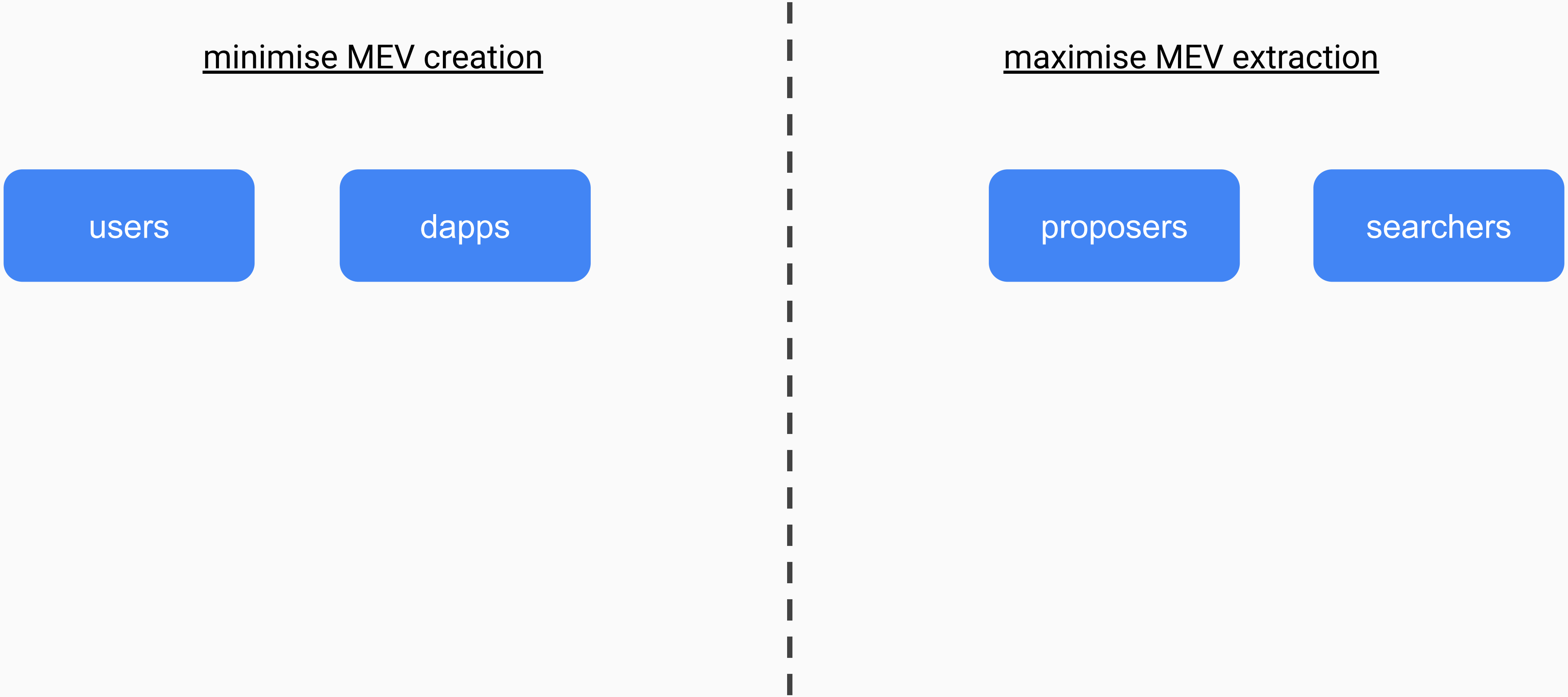
MEV creators and extractors

minimise MEV creation

users

dapps

MEV creators and extractors



minimise MEV creation

users

dapps

maximise MEV extraction

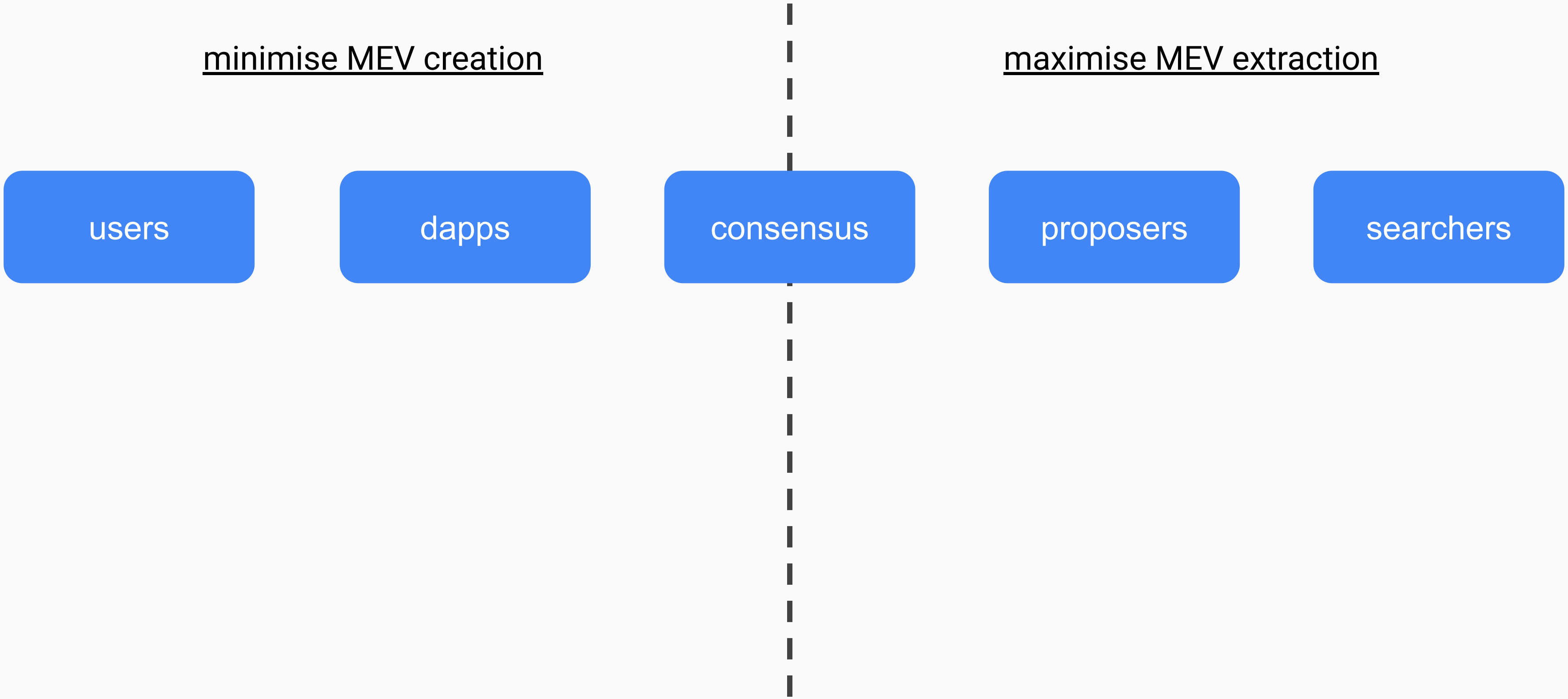
proposers

searchers

MEV creators and extractors

minimise MEV creation

maximise MEV extraction



users

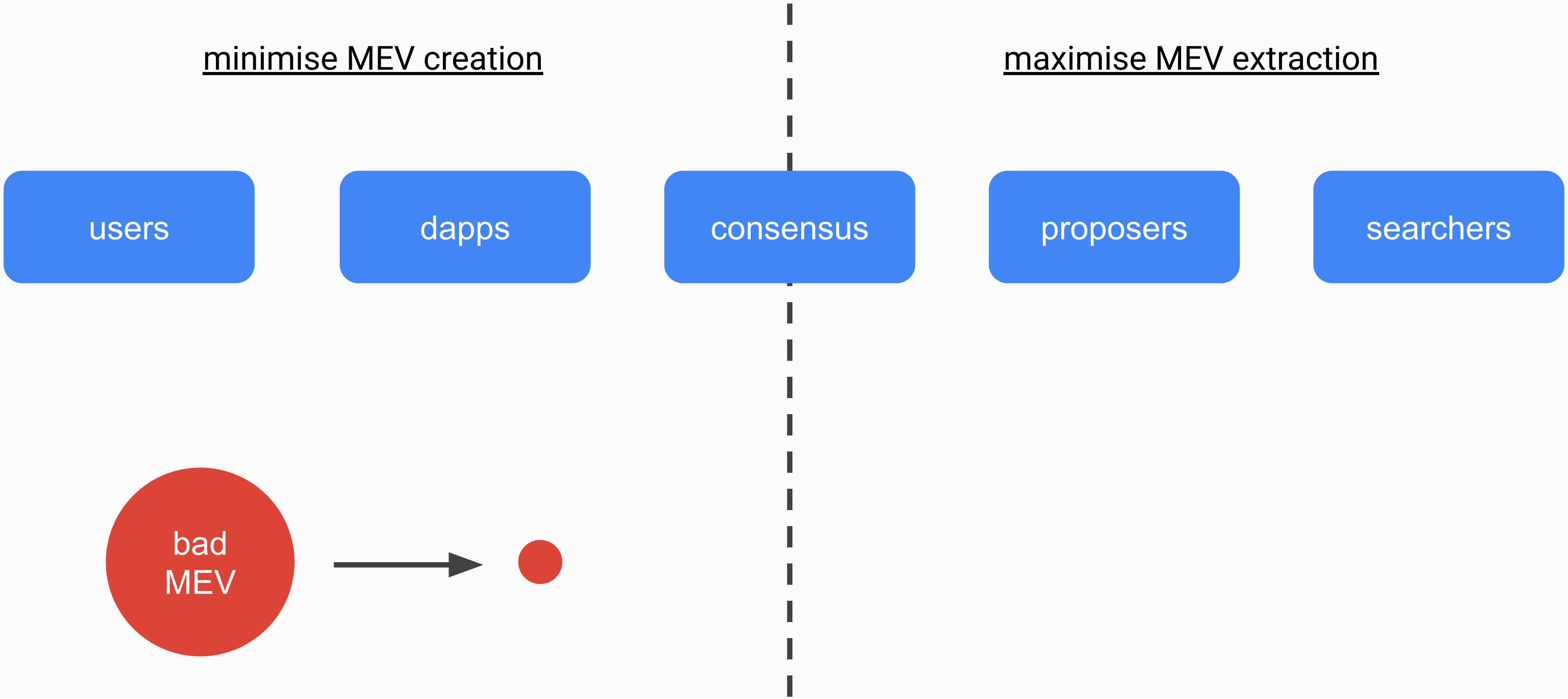
dapps

consensus

proposers

searchers

MEV creators and extractors



minimise MEV creation

maximise MEV extraction

users

dapps

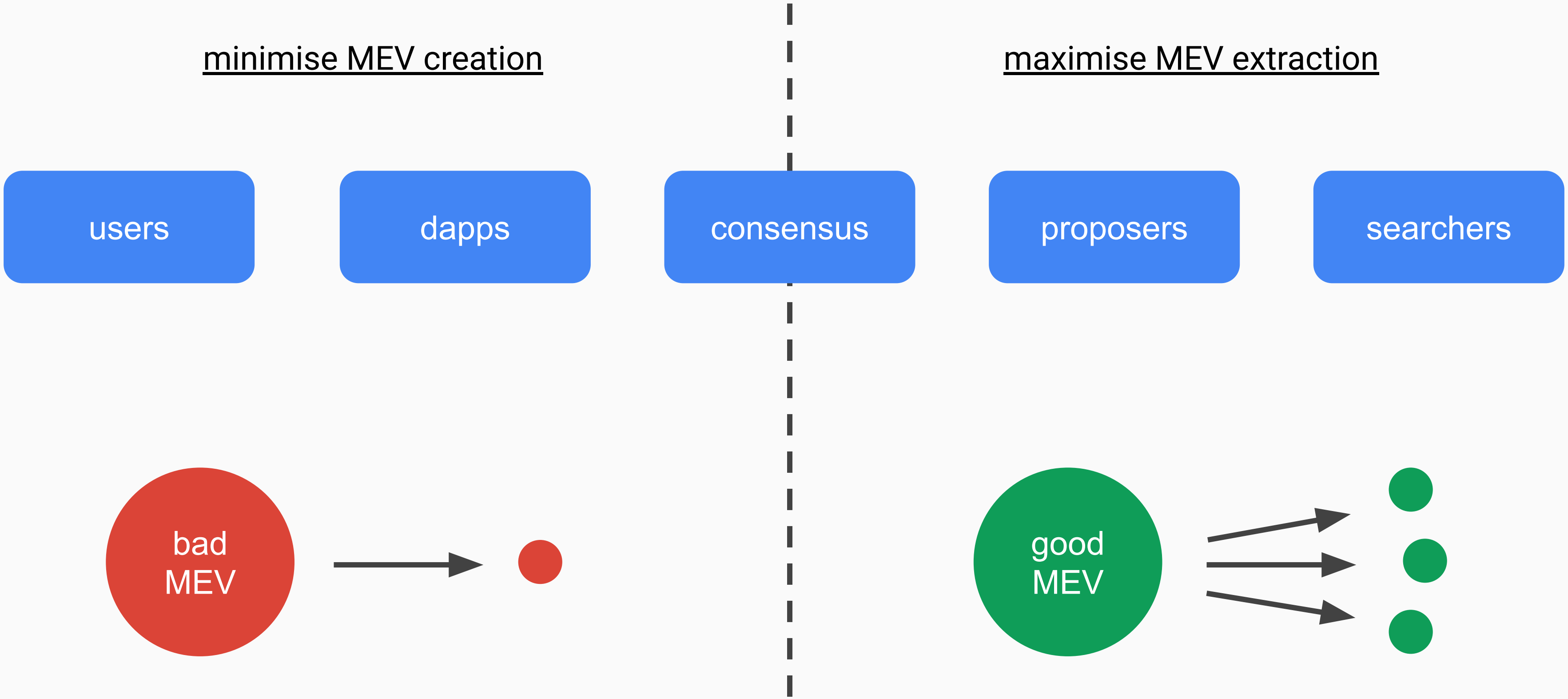
consensus

proposers

searchers

bad MEV

MEV creators and extractors



minimise MEV creation

maximise MEV extraction

users

dapps

consensus

proposers

searchers

bad MEV

good MEV

undesirable MEV outcomes

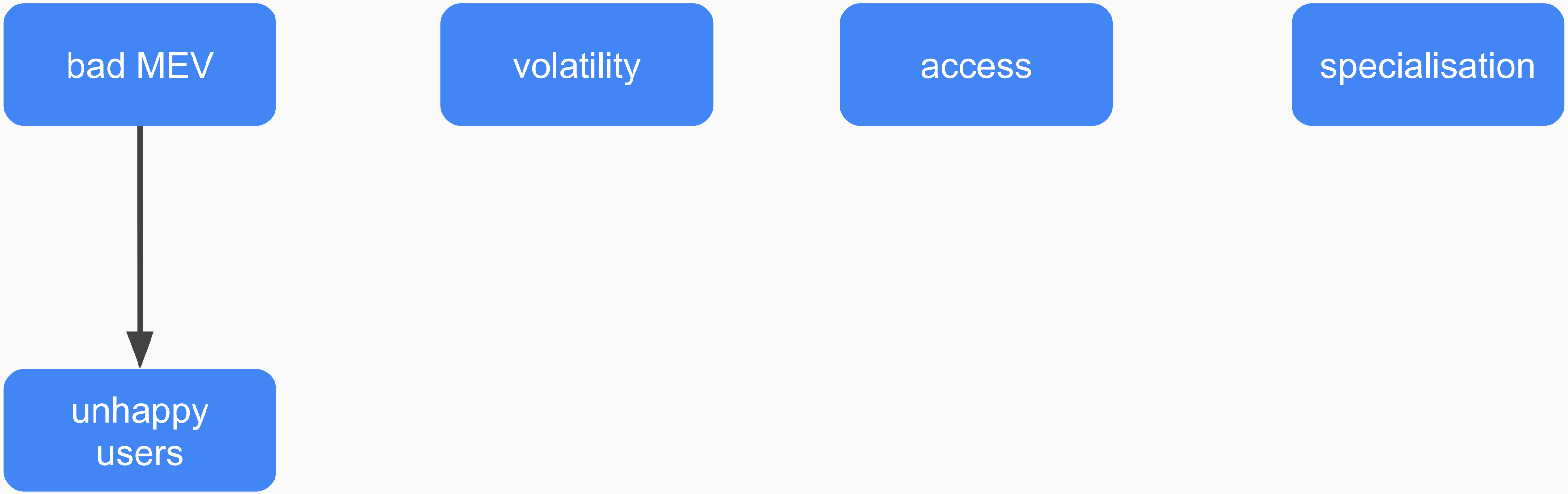
bad MEV

volatility

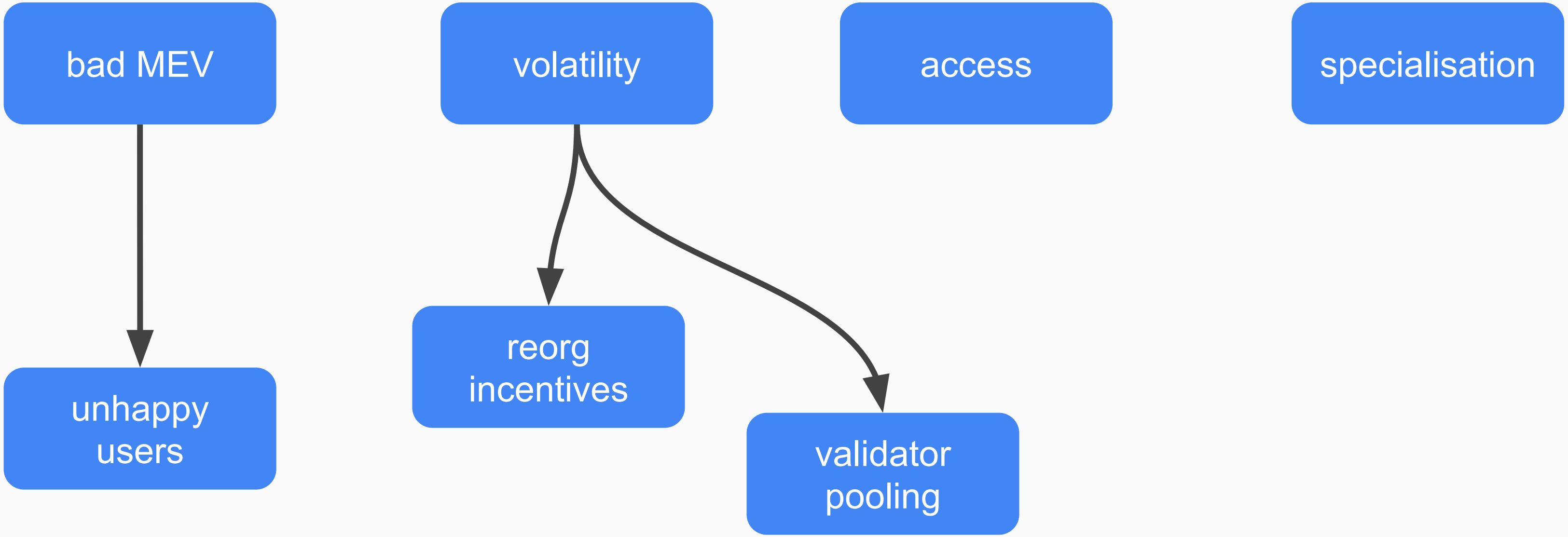
access

specialisation

undesirable MEV outcomes



undesirable MEV outcomes



bad MEV

unhappy users

volatility

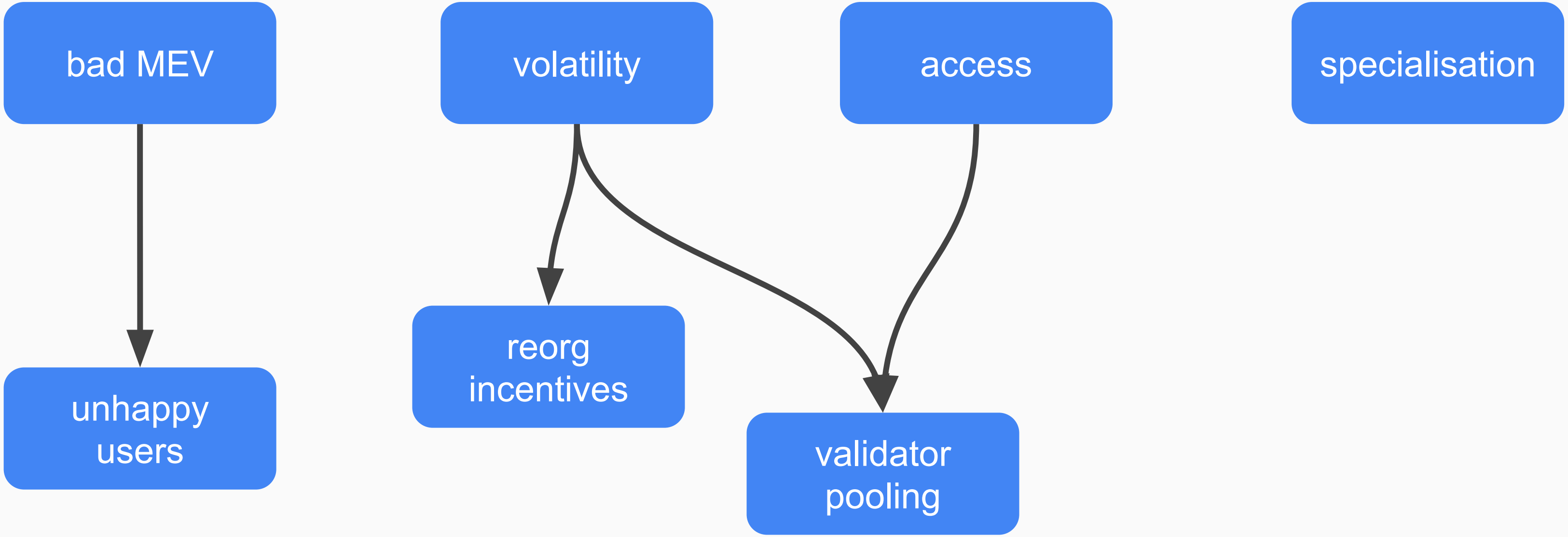
reorg incentives

validator pooling

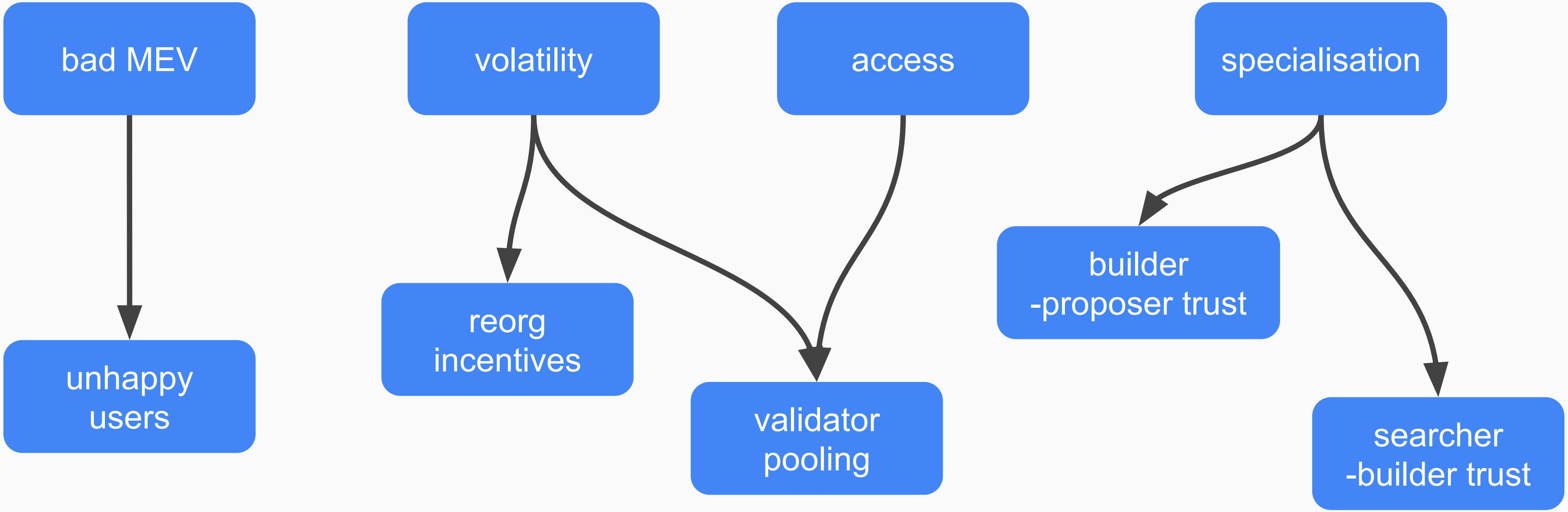
access

specialisation

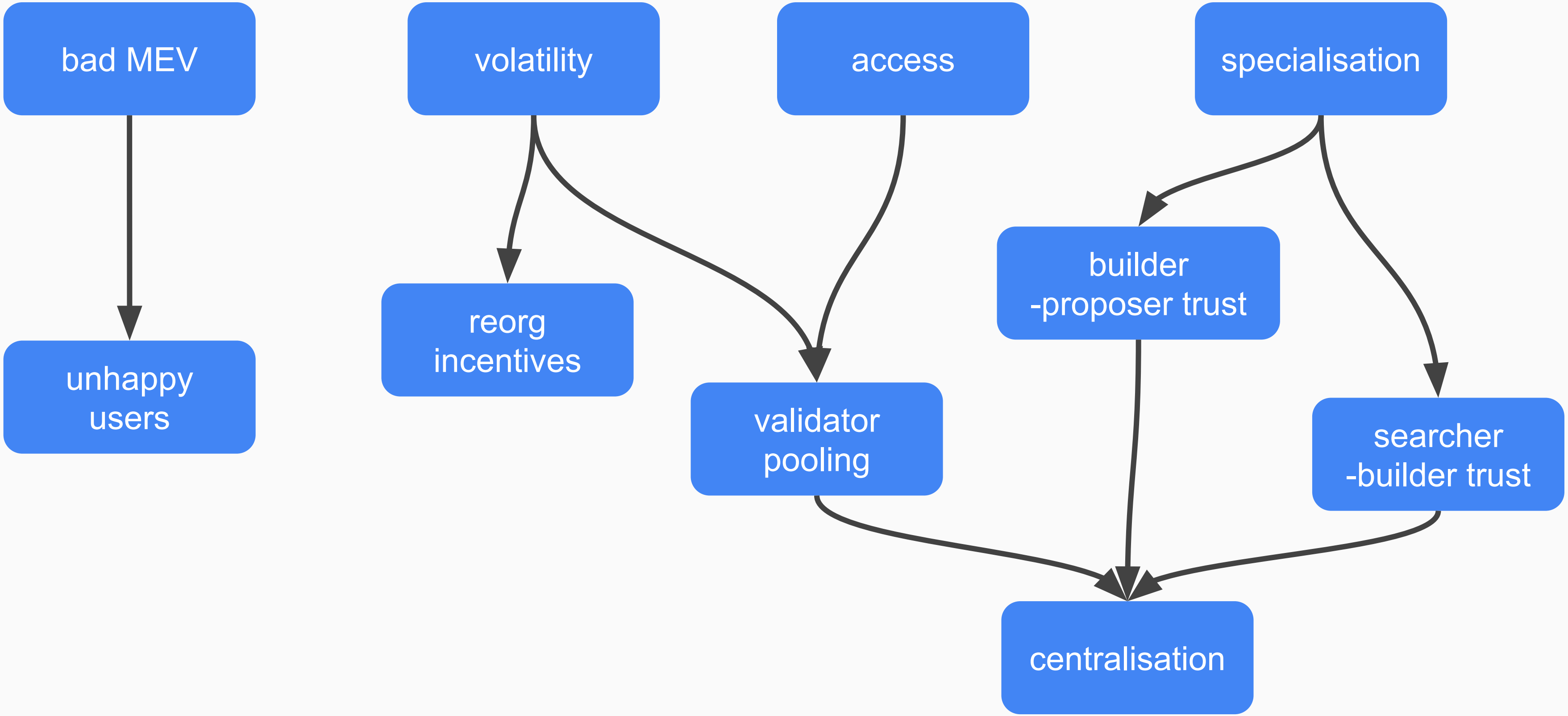
undesirable MEV outcomes



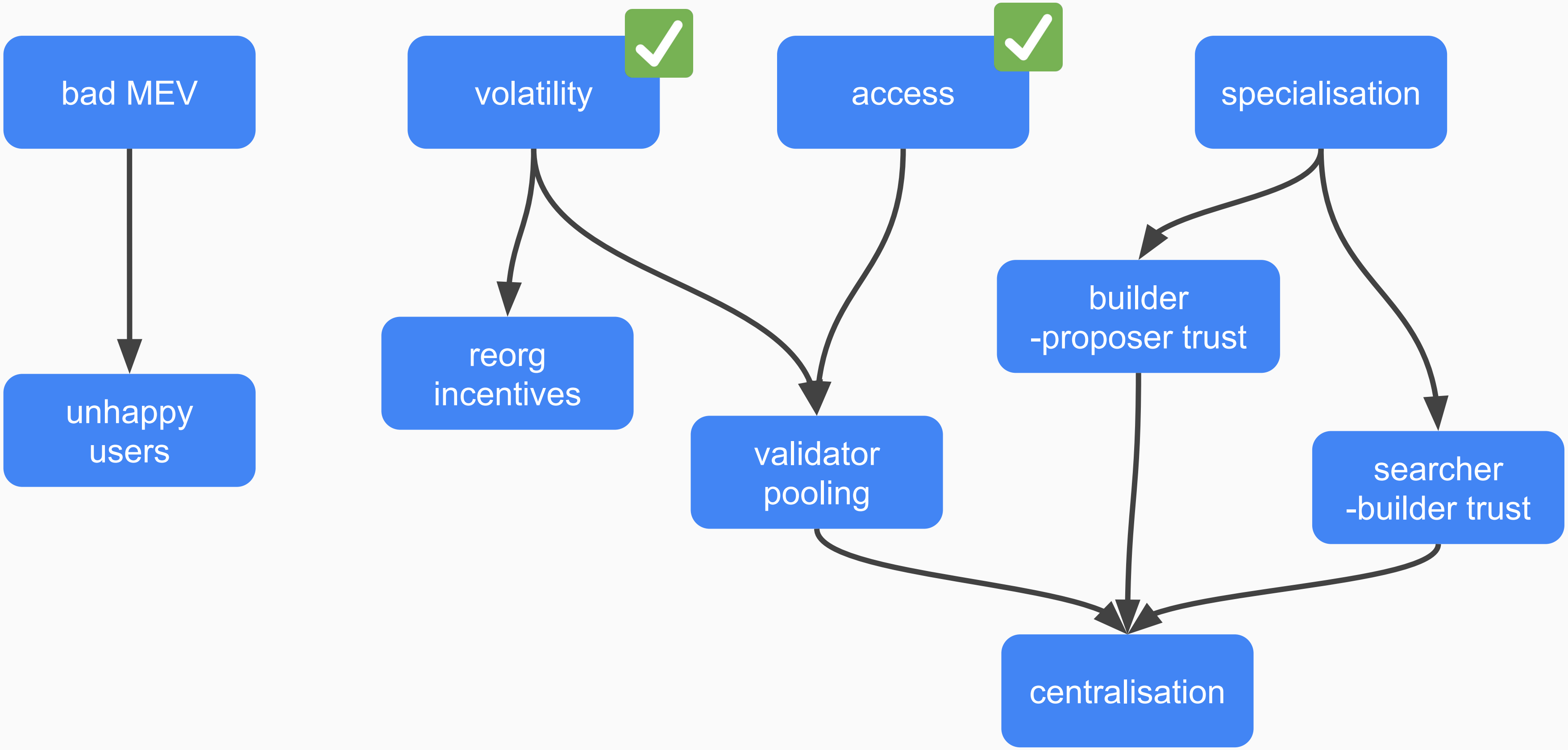
undesirable MEV outcomes



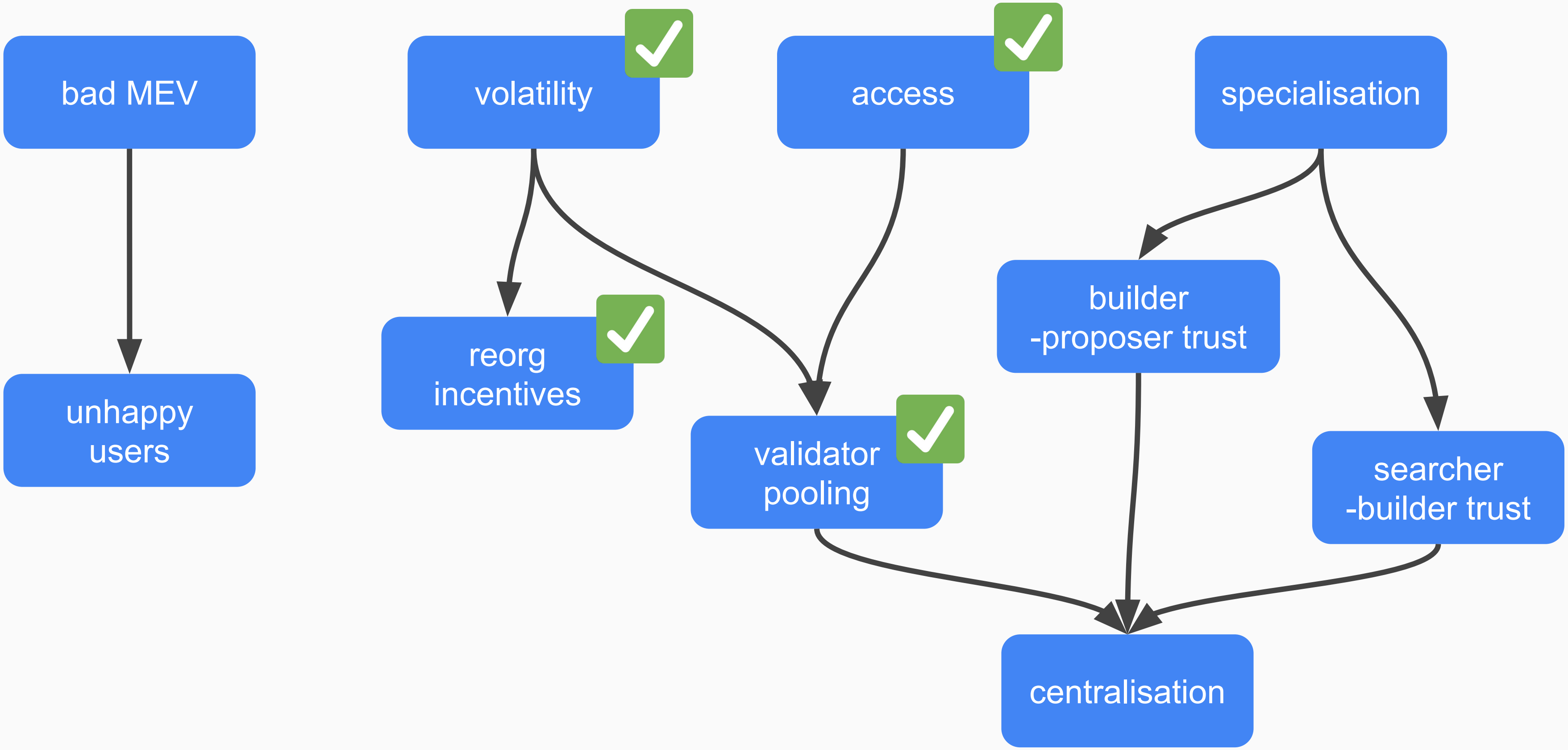
undesirable MEV outcomes



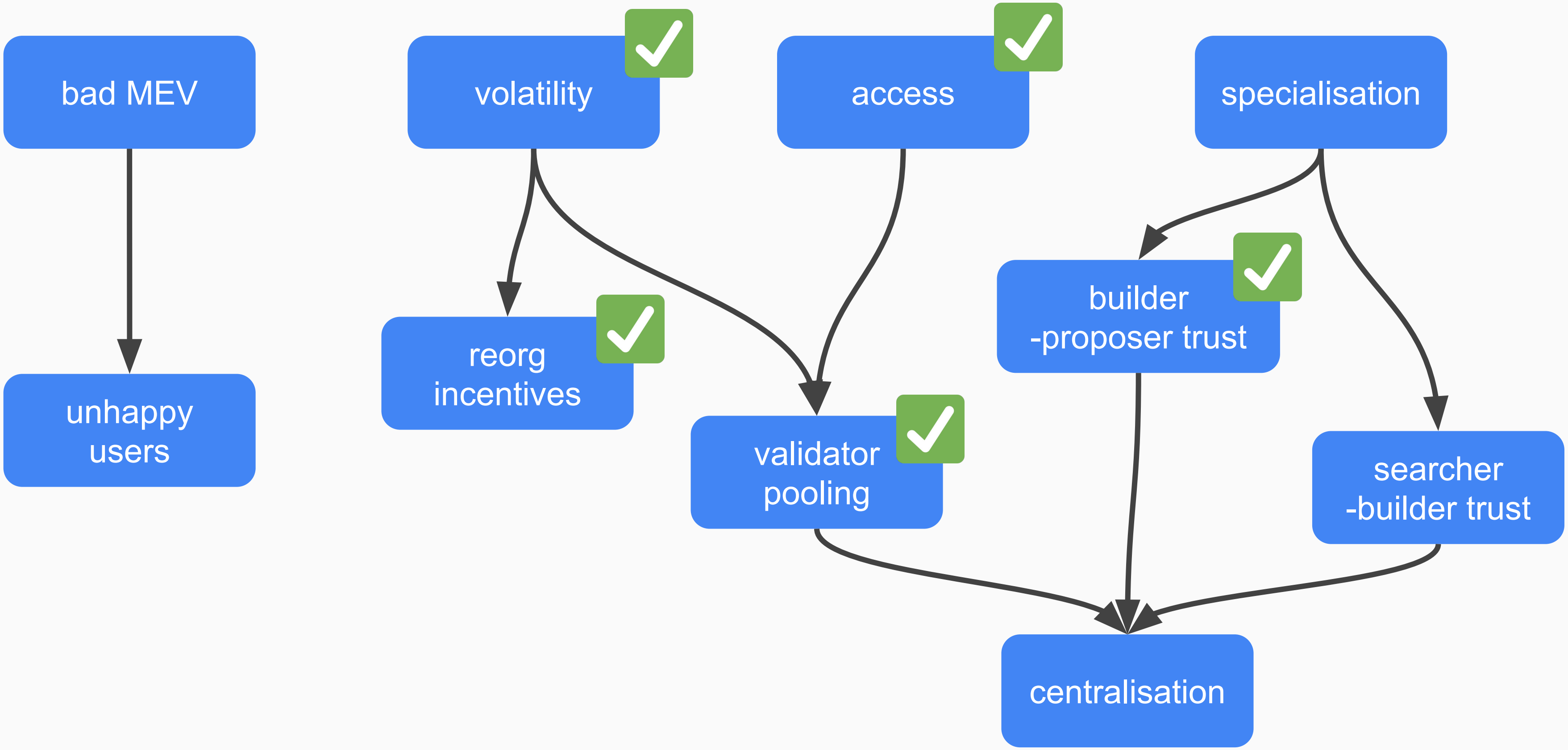
undesirable MEV outcomes



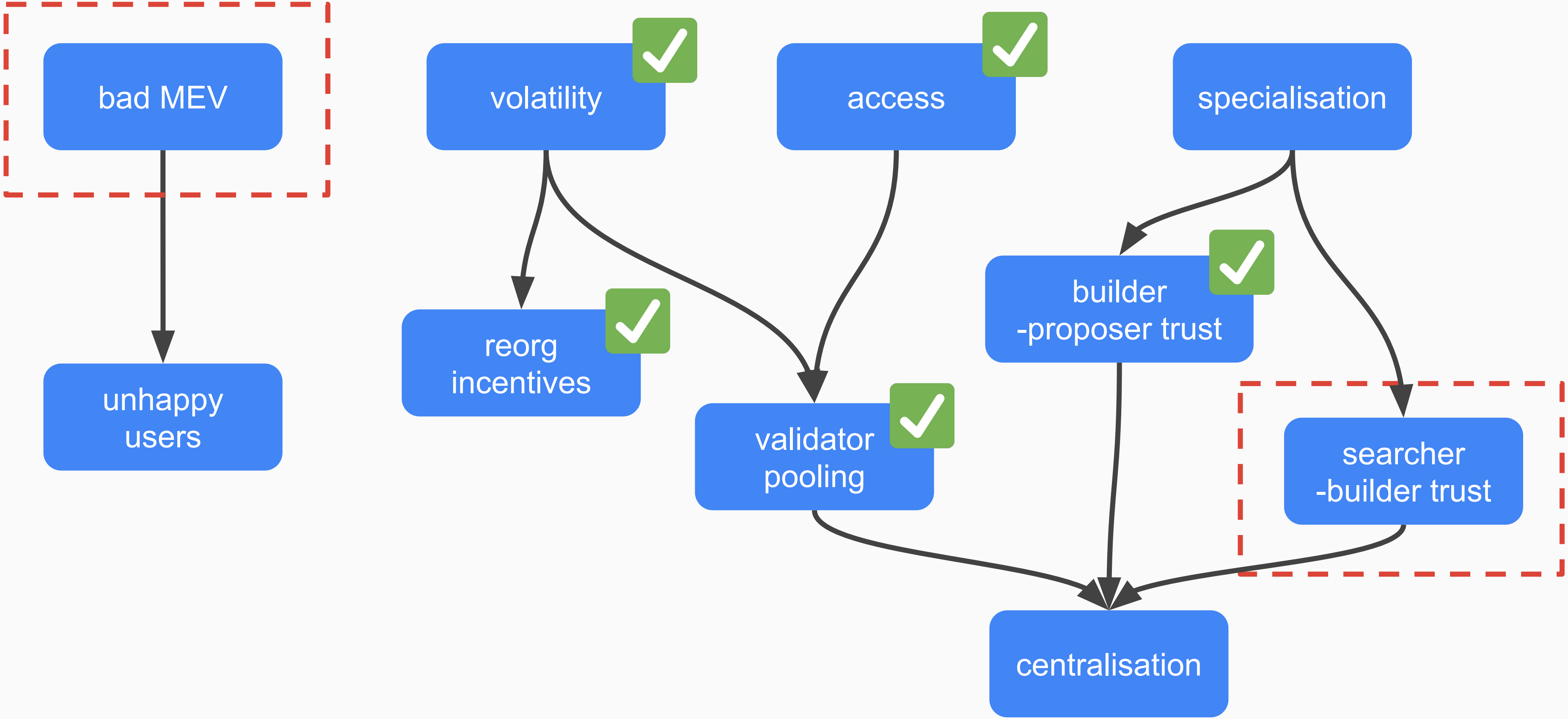
undesirable MEV outcomes



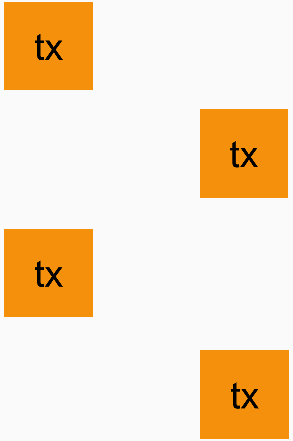
undesirable MEV outcomes



undesirable MEV outcomes



encryption with guaranteed decryption



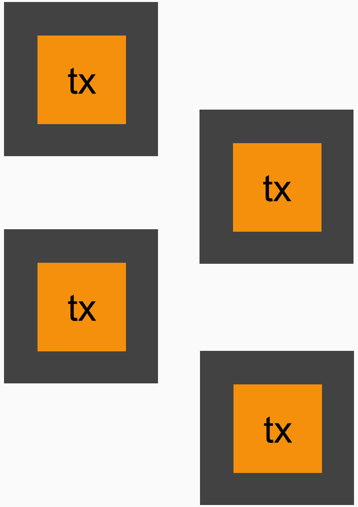
tx

tx

tx

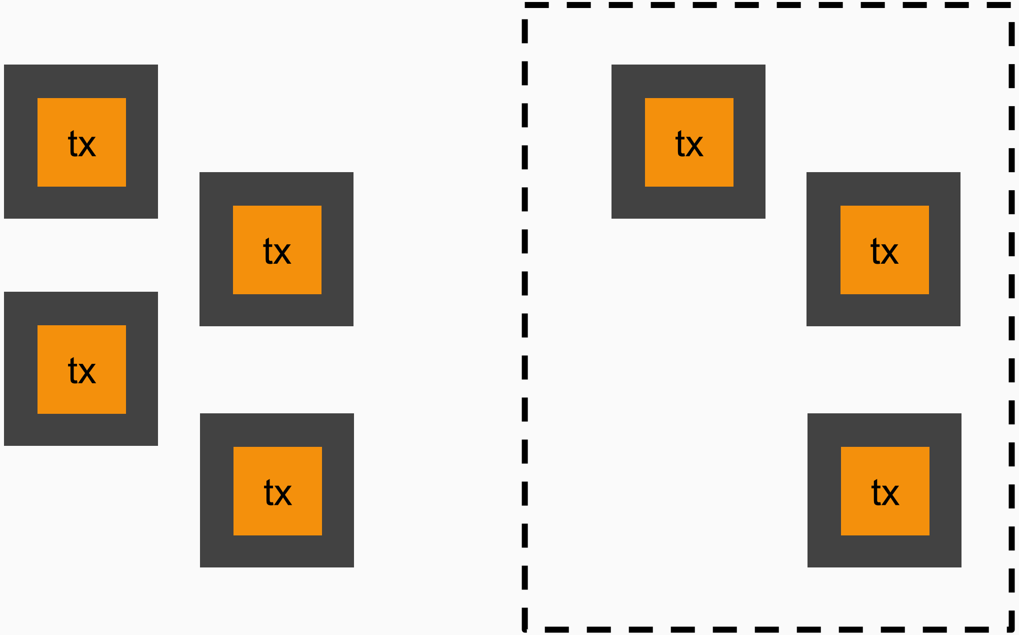
tx

encryption with guaranteed decryption



- user encrypts
- user broadcasts

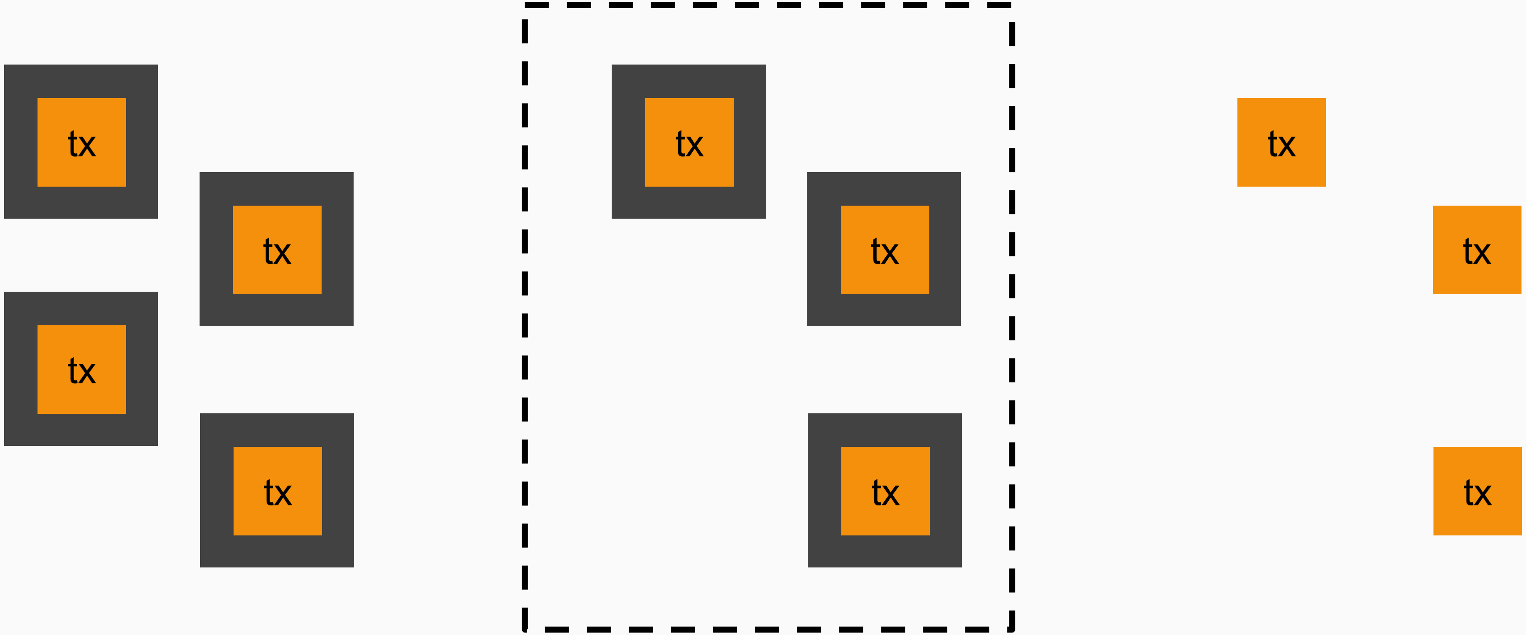
encryption with guaranteed decryption



- user encrypts
- user broadcasts

- on-chain inclusion

encryption with guaranteed decryption



- user encrypts
- user broadcasts

- on-chain inclusion

- guaranteed decryption
- on-chain execution

guaranteed decryption candidates

threshold decryption

→ federated trust

→ per-message verification cost

Sikka

Shutter

Drand

guaranteed decryption candidates

threshold decryption

→ federated trust
→ per-message verification cost

Sikka Shutter Drand

timelock puzzles

→ per-message decryption cost
→ new sequentiality assumptions

Starkware VDF Alliance

guaranteed decryption candidates

threshold decryption

→ federated trust
→ per-message verification cost

Sikka Shutter Drand

timelock puzzles

→ per-message decryption cost
→ new sequentiality assumptions

STARKWARE

Starkware VDF Alliance

delay encryption

→ only one construction known
→ large trusted setup

- 50GB/sec of delay

guaranteed decryption candidates

threshold decryption

→ federated trust
→ per-message verification cost

Sikka Shutter Drand

timelock puzzles

→ per-message decryption cost
→ new sequentiality assumptions

Starkware VDF Alliance

edit: there are also homomorphic timelock puzzles

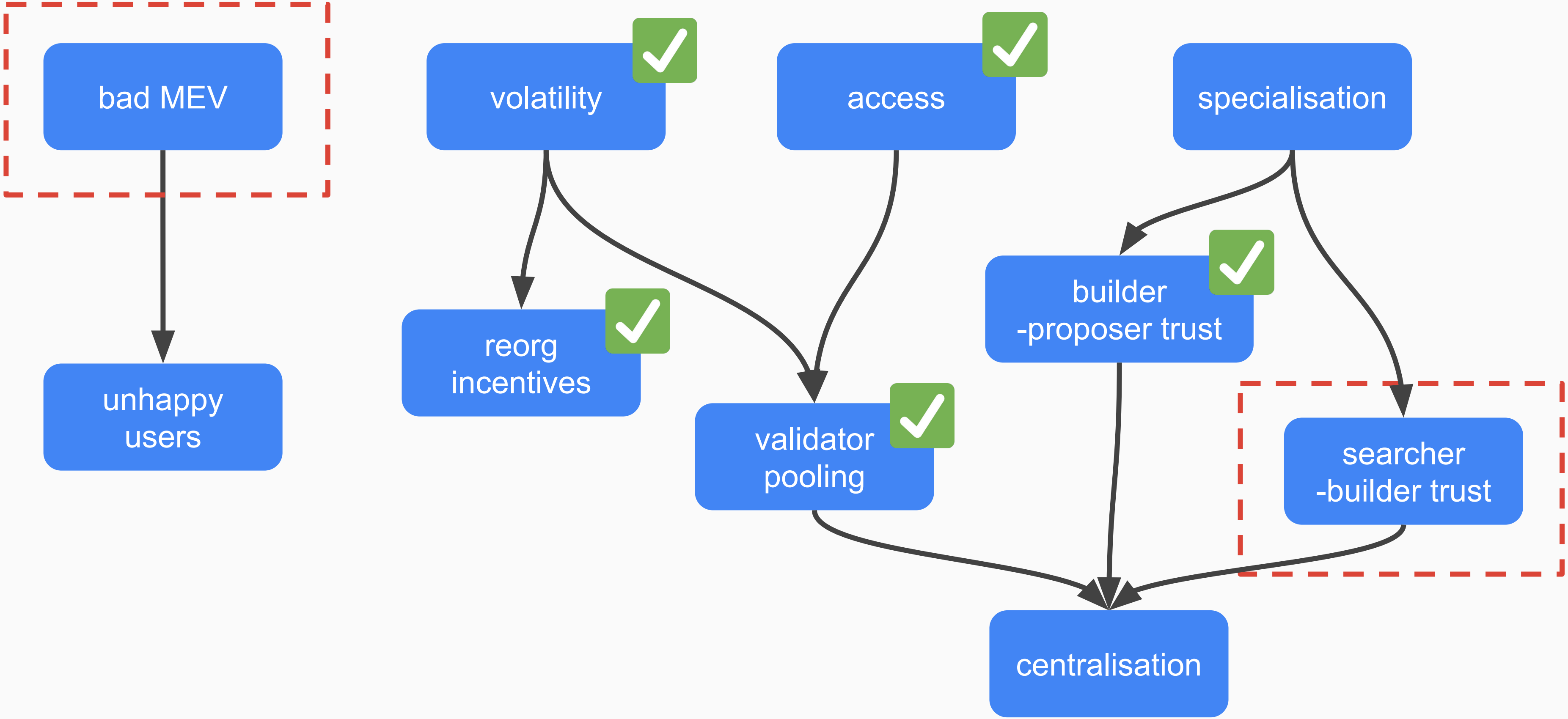
delay encryption

→ only one construction known
→ large trusted setup
- 50GB/sec of delay

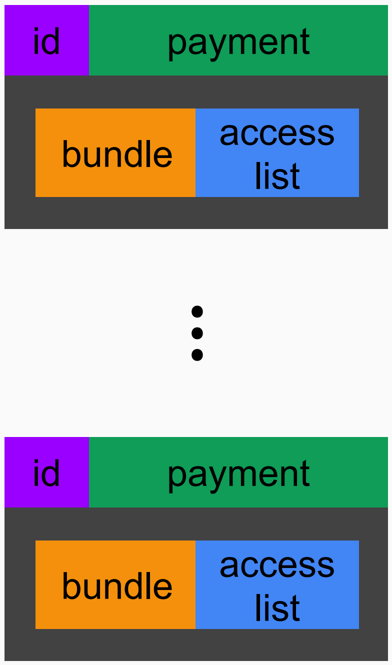
witness encryption

→ not practical

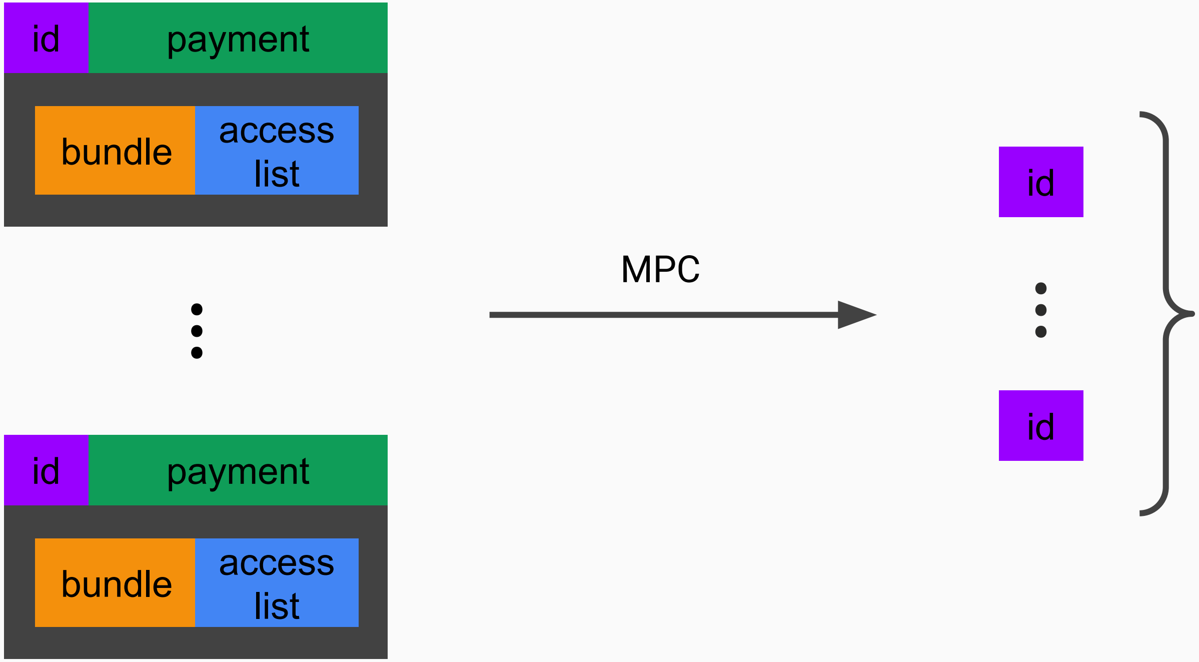
undesirable MEV outcomes



private disjoint bundle aggregation



private disjoint bundle aggregation



- order bundles
- disjoint access lists
- maximise payments

thanks :)

justin@ethereum.org