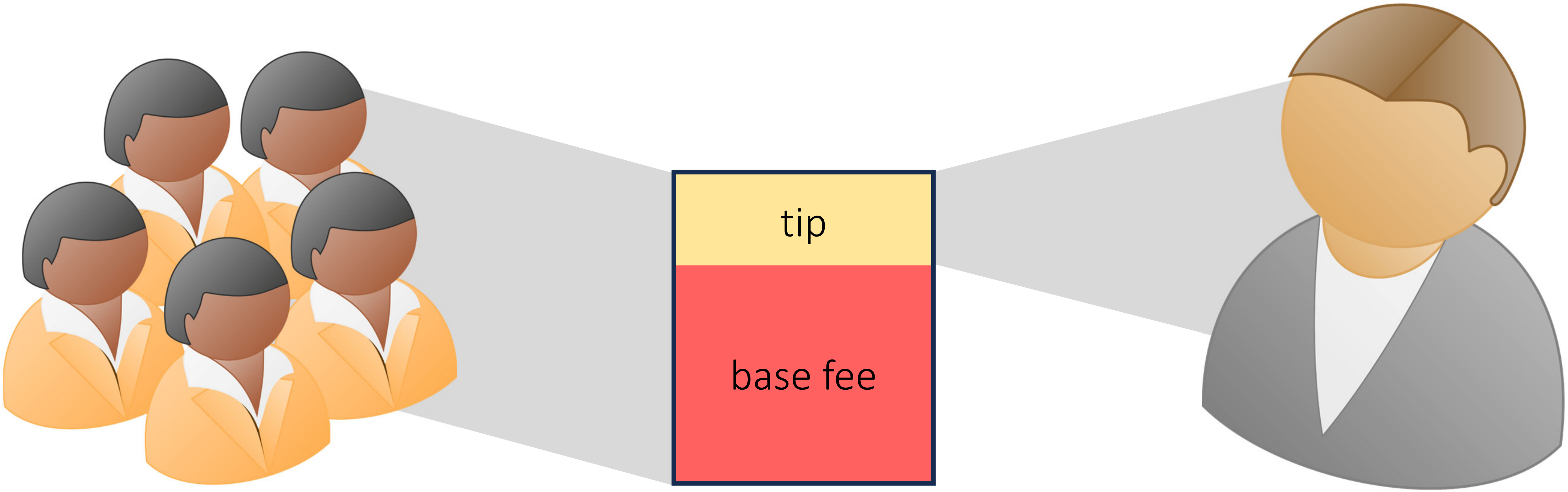
Base Fee Manipulation In Ethereum's EIP-1559 Transaction Fee Mechanism



Sarah Azouvi, Guy Goren, **Lioba Heimbach** and Alexander Hicks

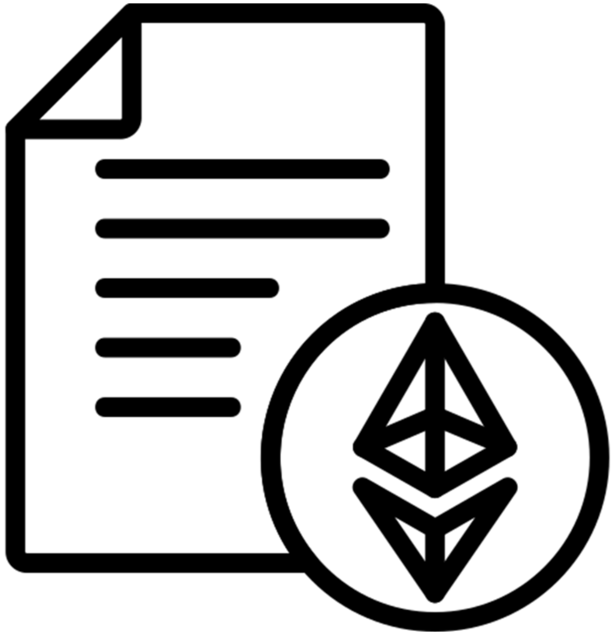
Protocol Labs, ETH Zurich and UCL

International Symposium on Distributed Computing (DISC) 2023

Ethereum

market capitalization:
US$ 200 billion

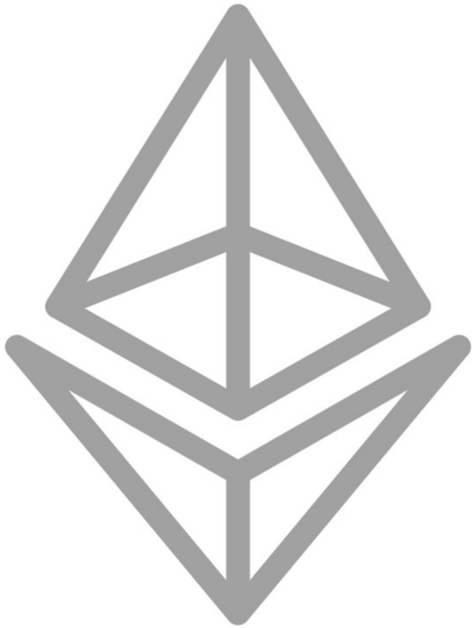
Ethereum



market capitalization:
US$ 200 billion

leading smart contract
and DeFi platform

Ethereum

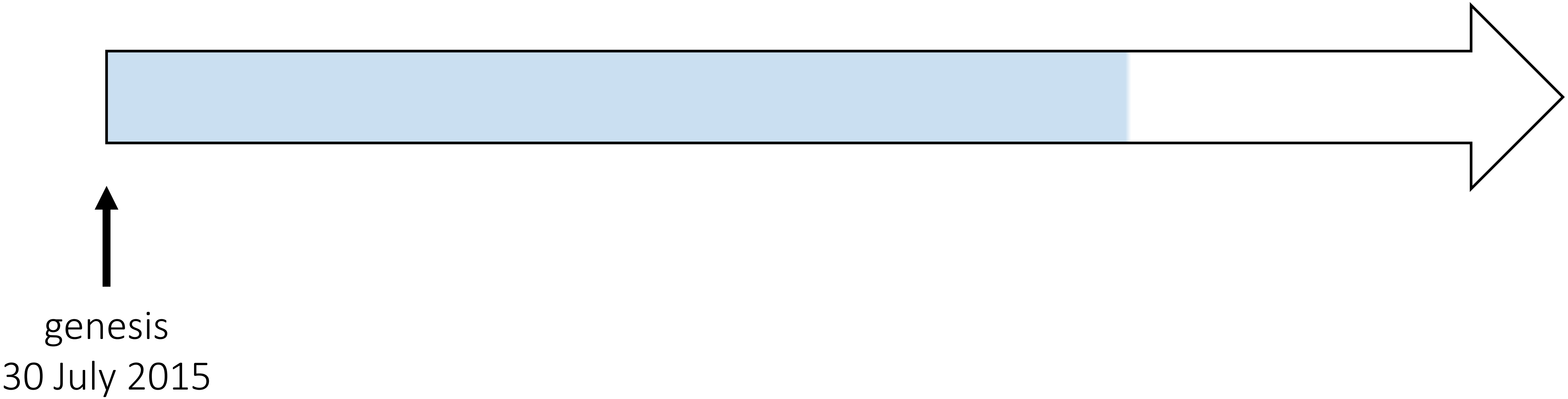


market capitalization:
US$ 200 billion

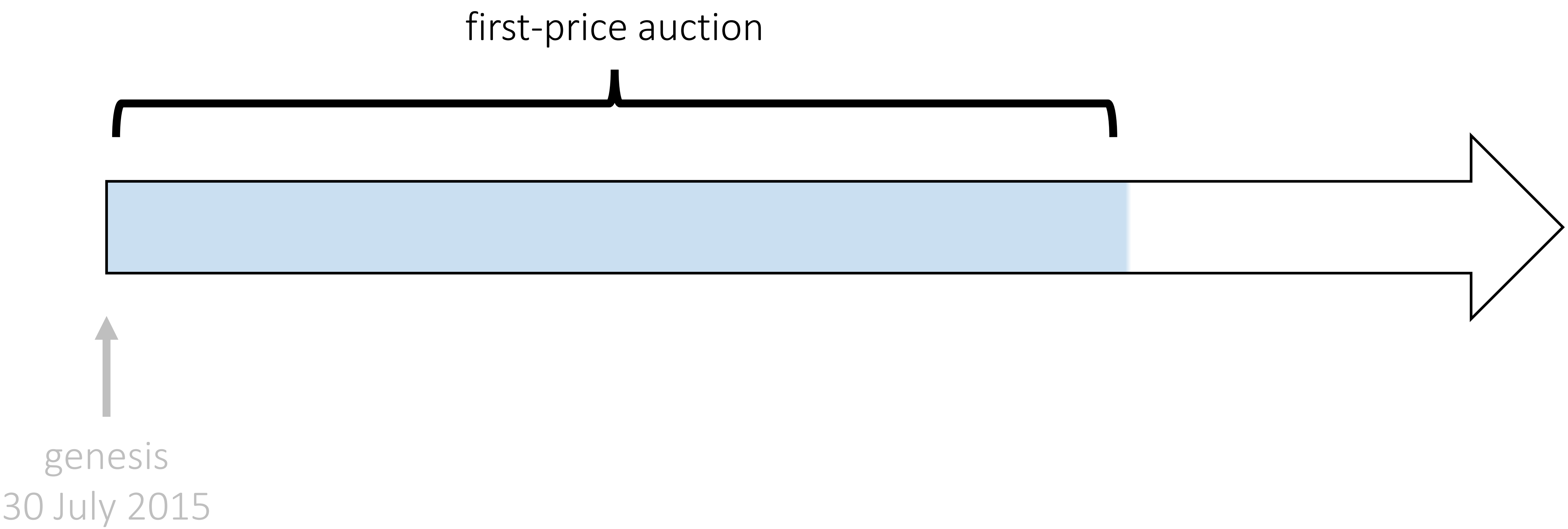
leading smart contract
and DeFi platform

daily transaction fees:
US$ 3 million

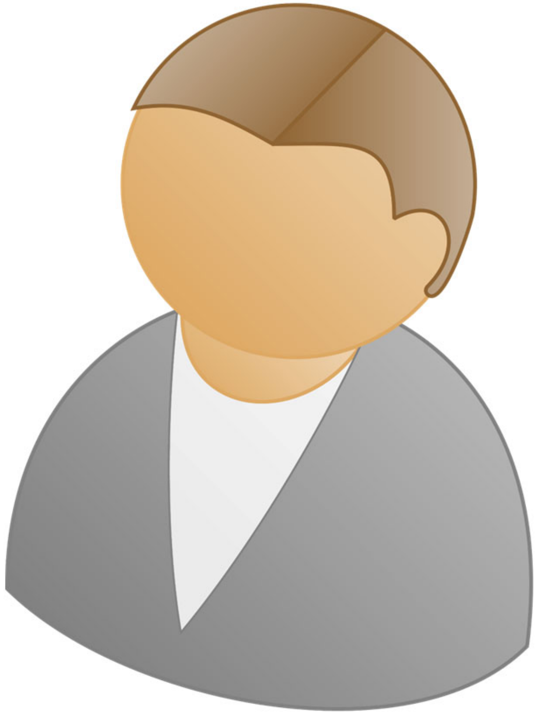
History of Ethereum transaction fees

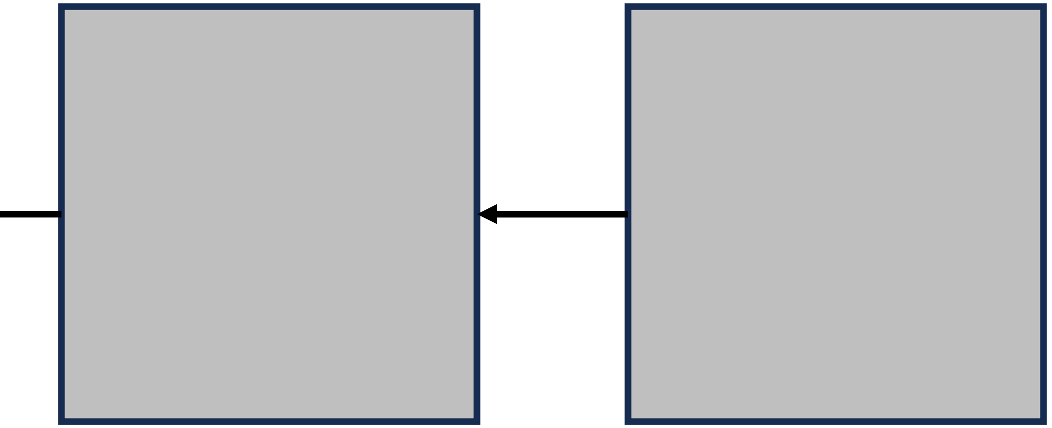


History of Ethereum transaction fees

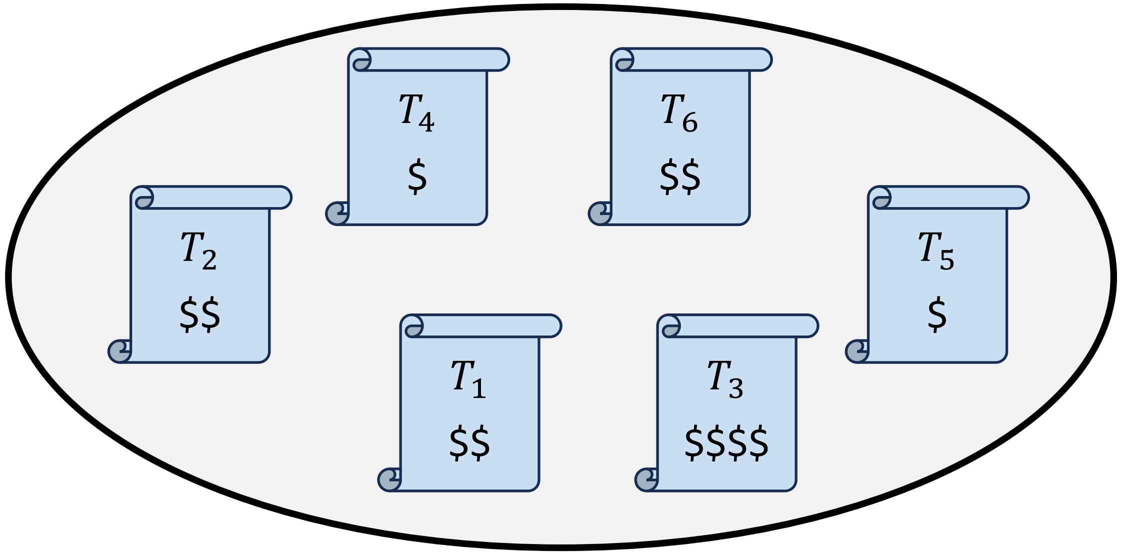


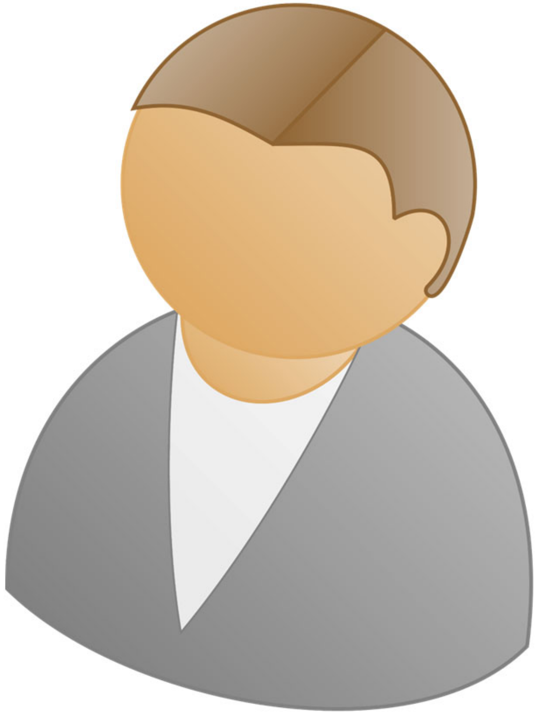
First-price auction

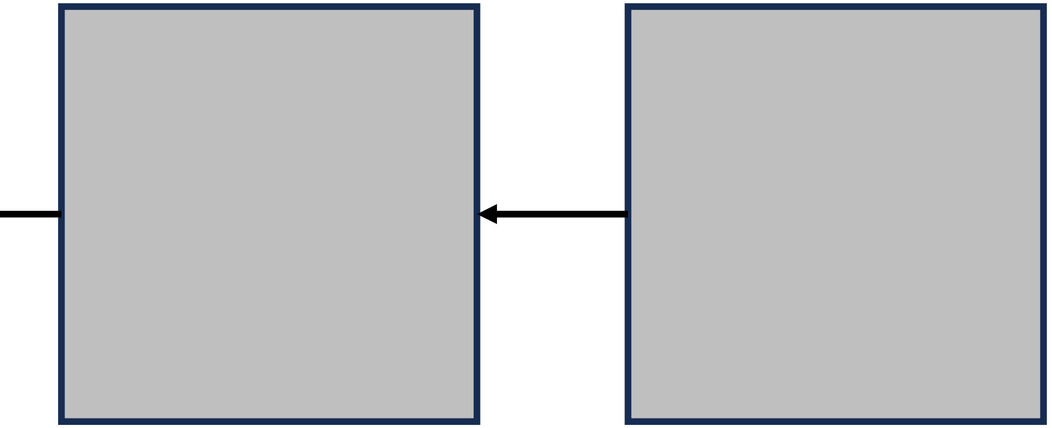




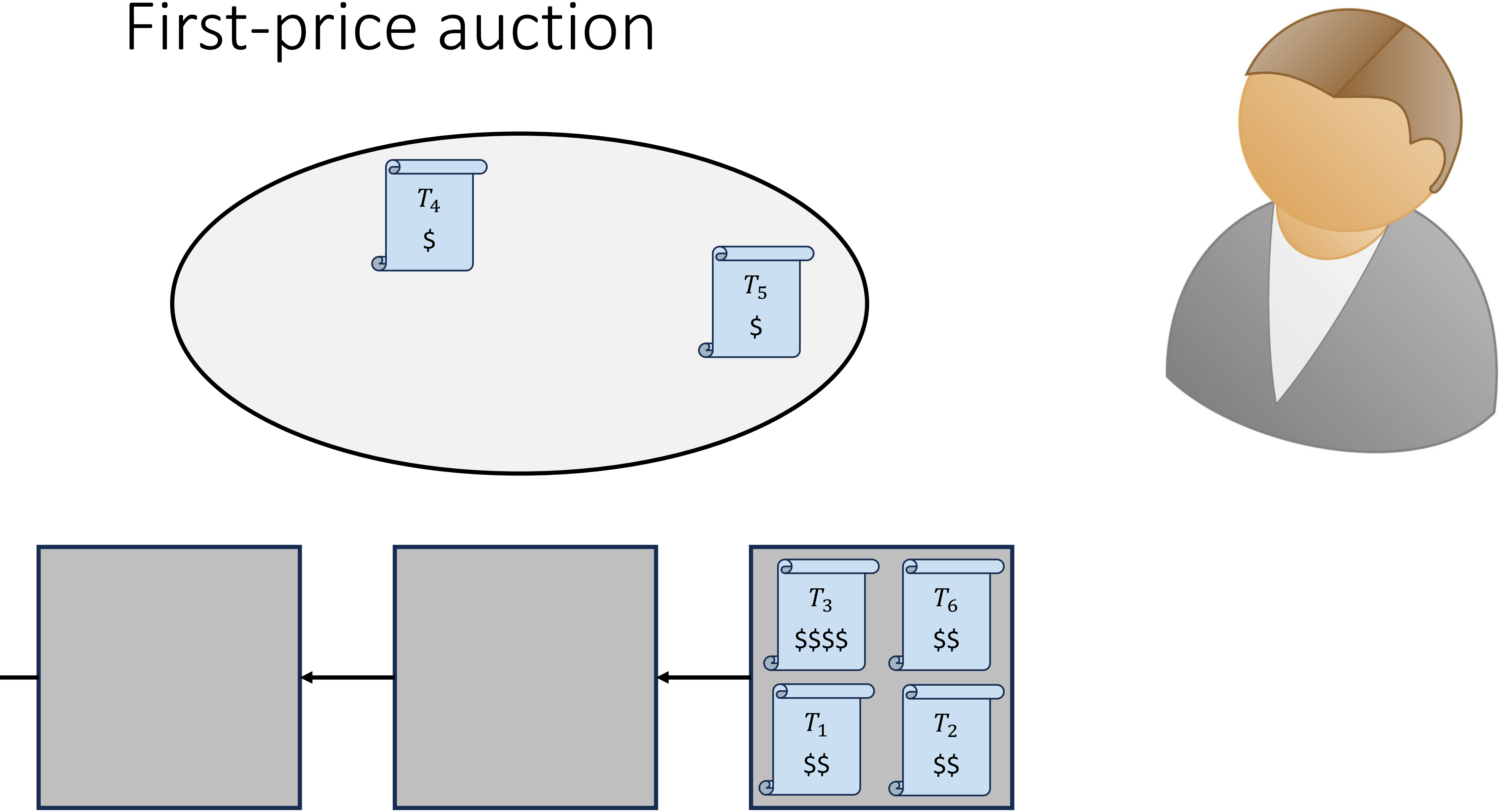
First-price auction



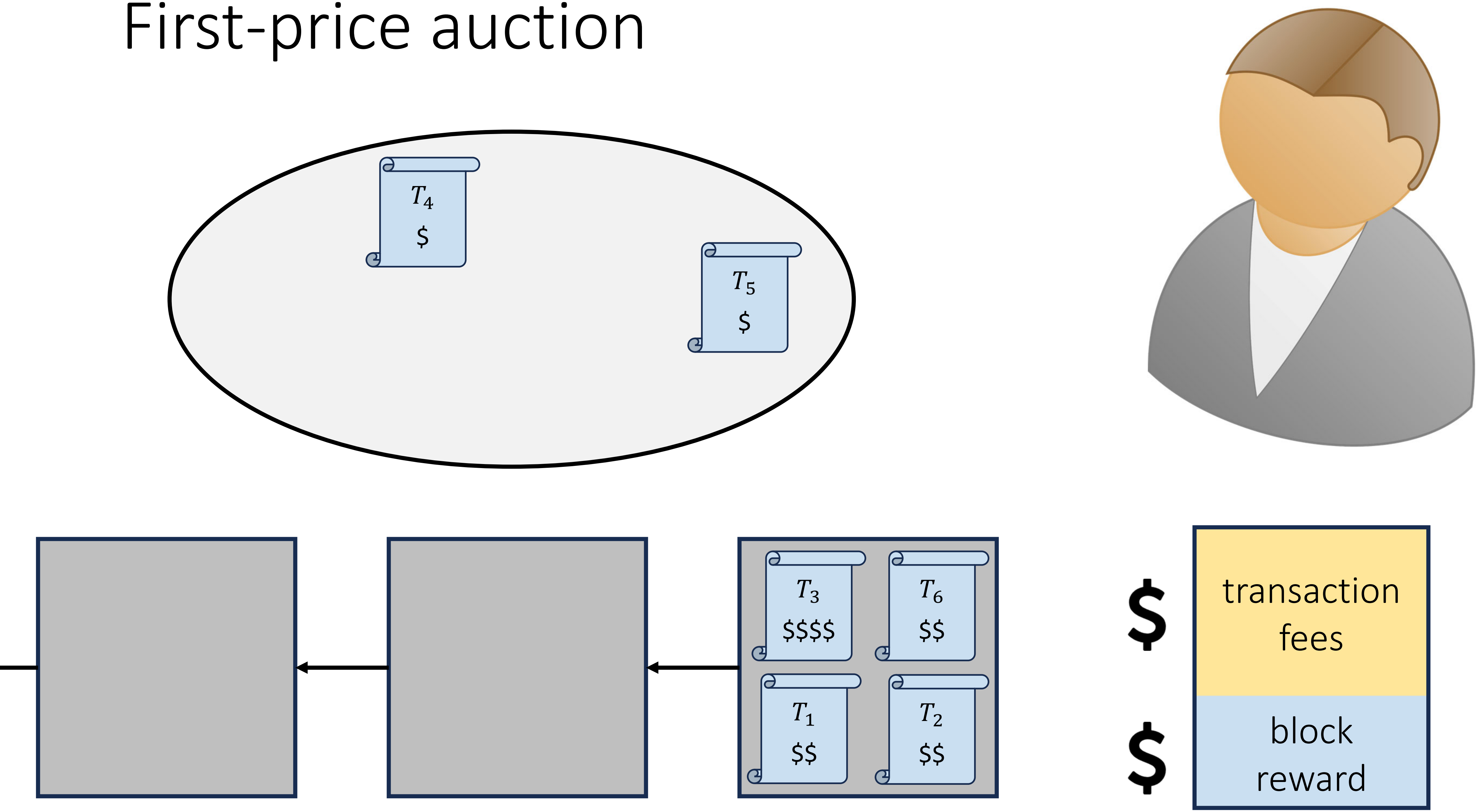




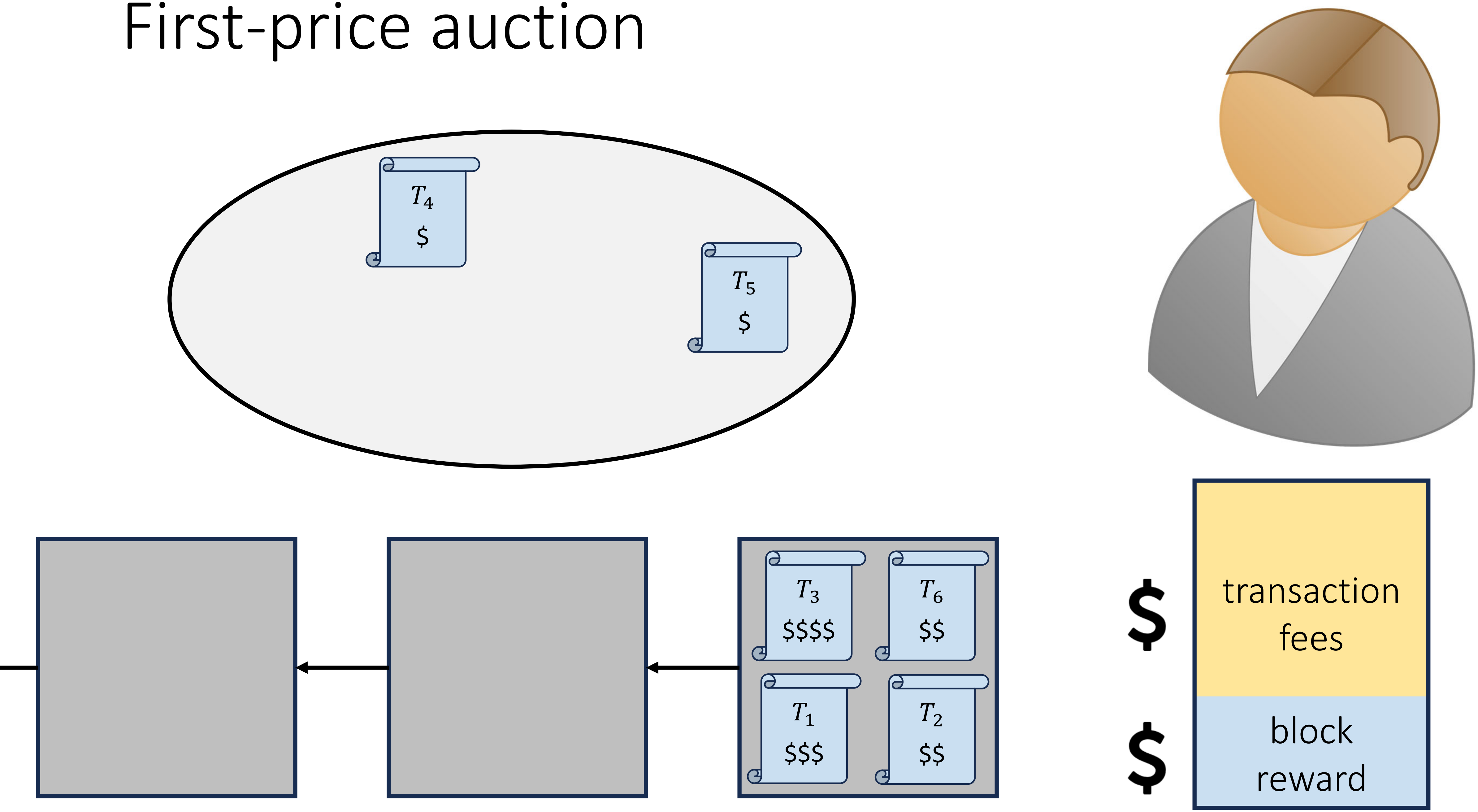
First-price auction



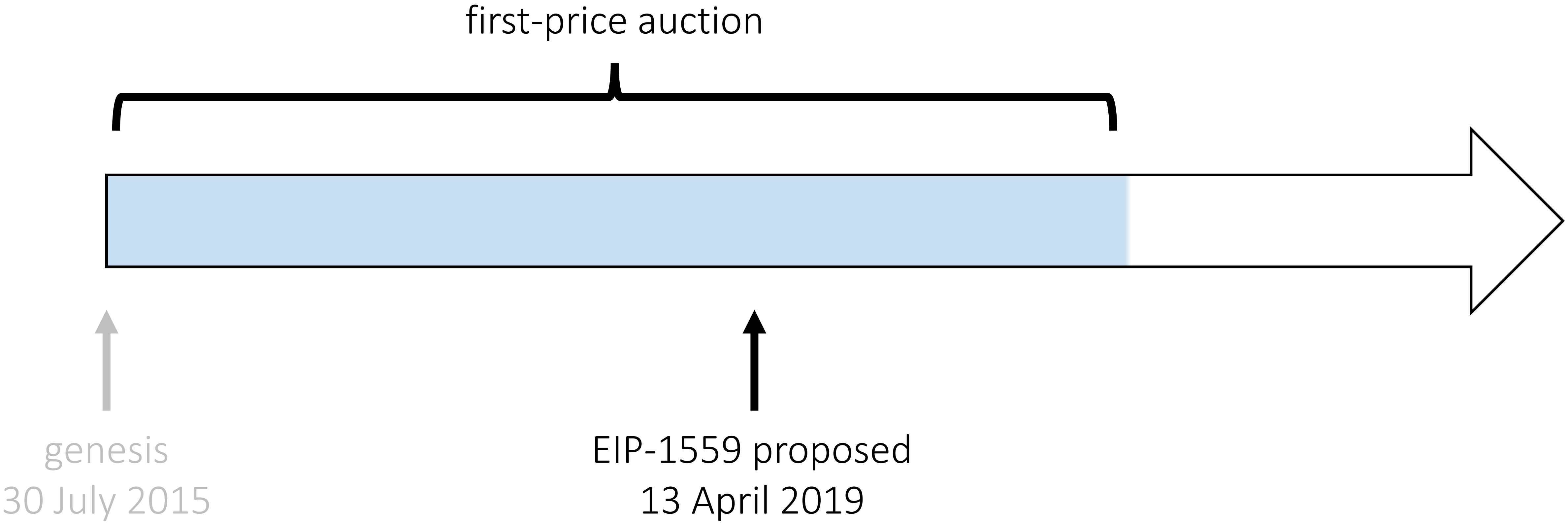
First-price auction



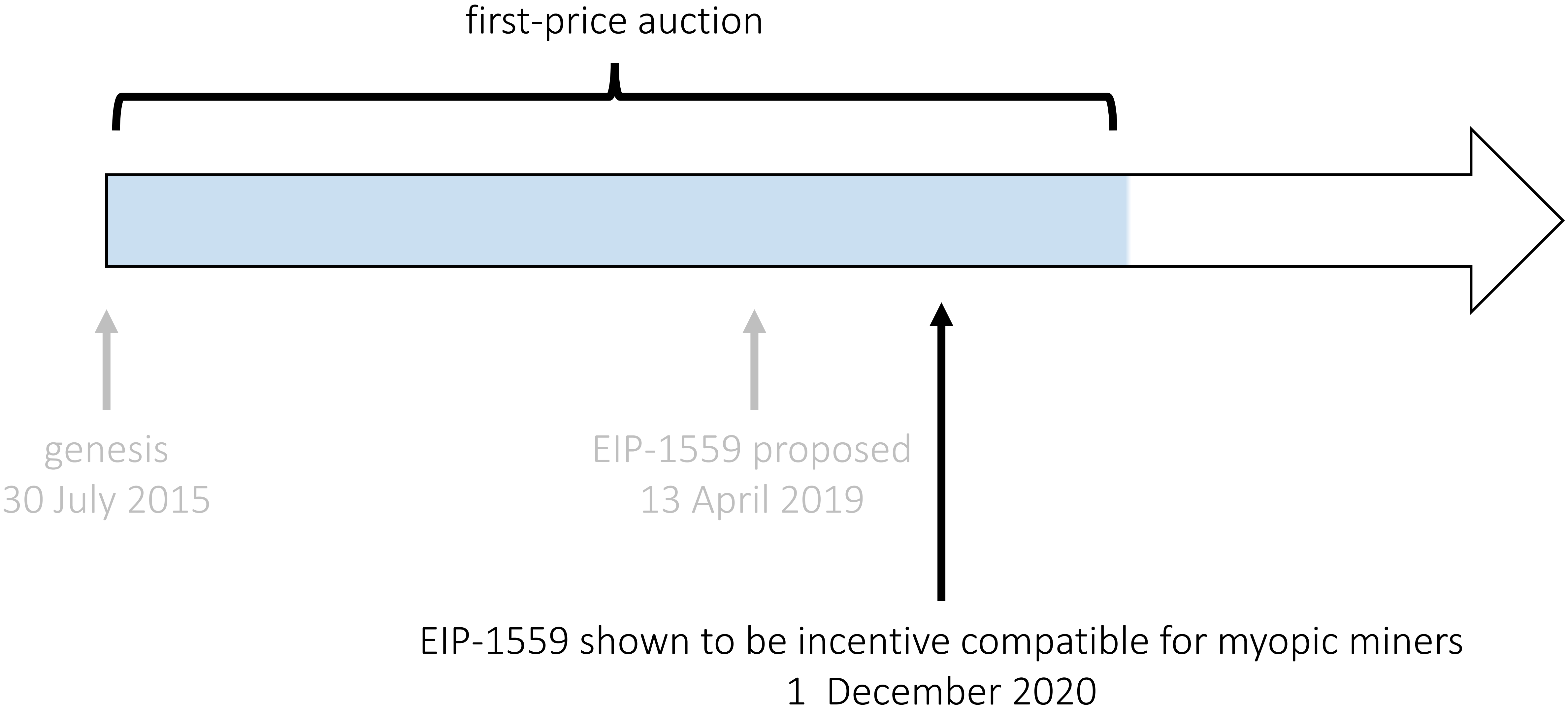
First-price auction



History of Ethereum transaction fees



History of Ethereum transaction fees



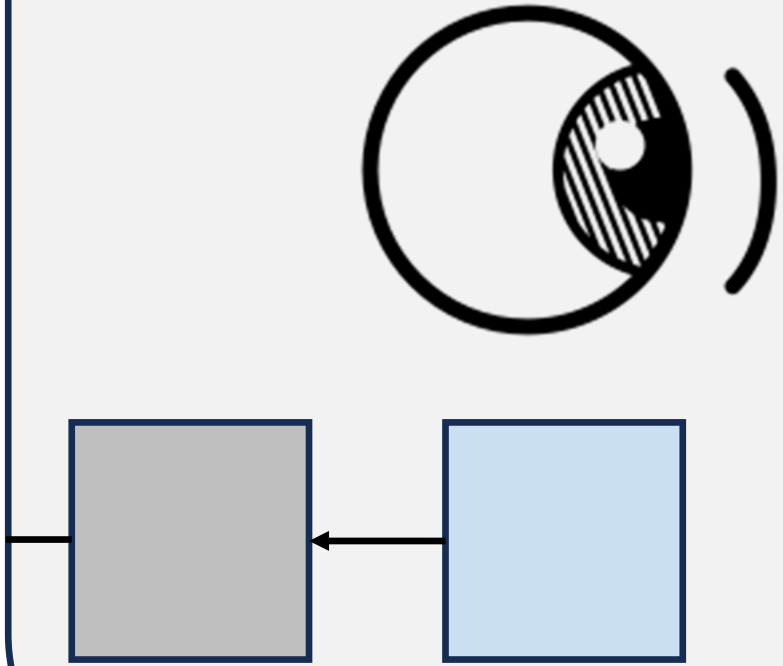
Myopic vs. non-myopic miners

Myopic miners

Non-myopic miners

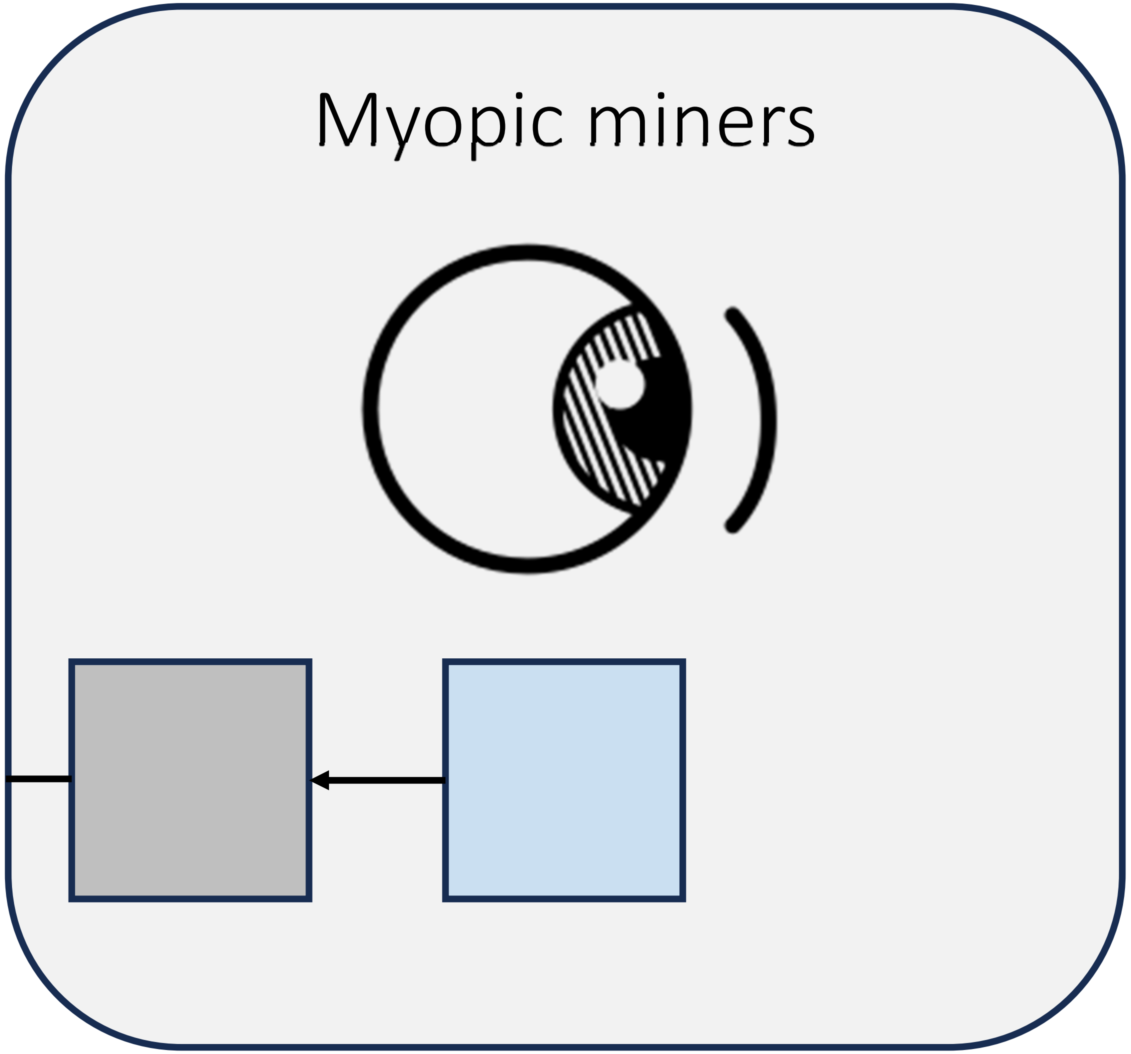
Myopic vs. non-myopic miners

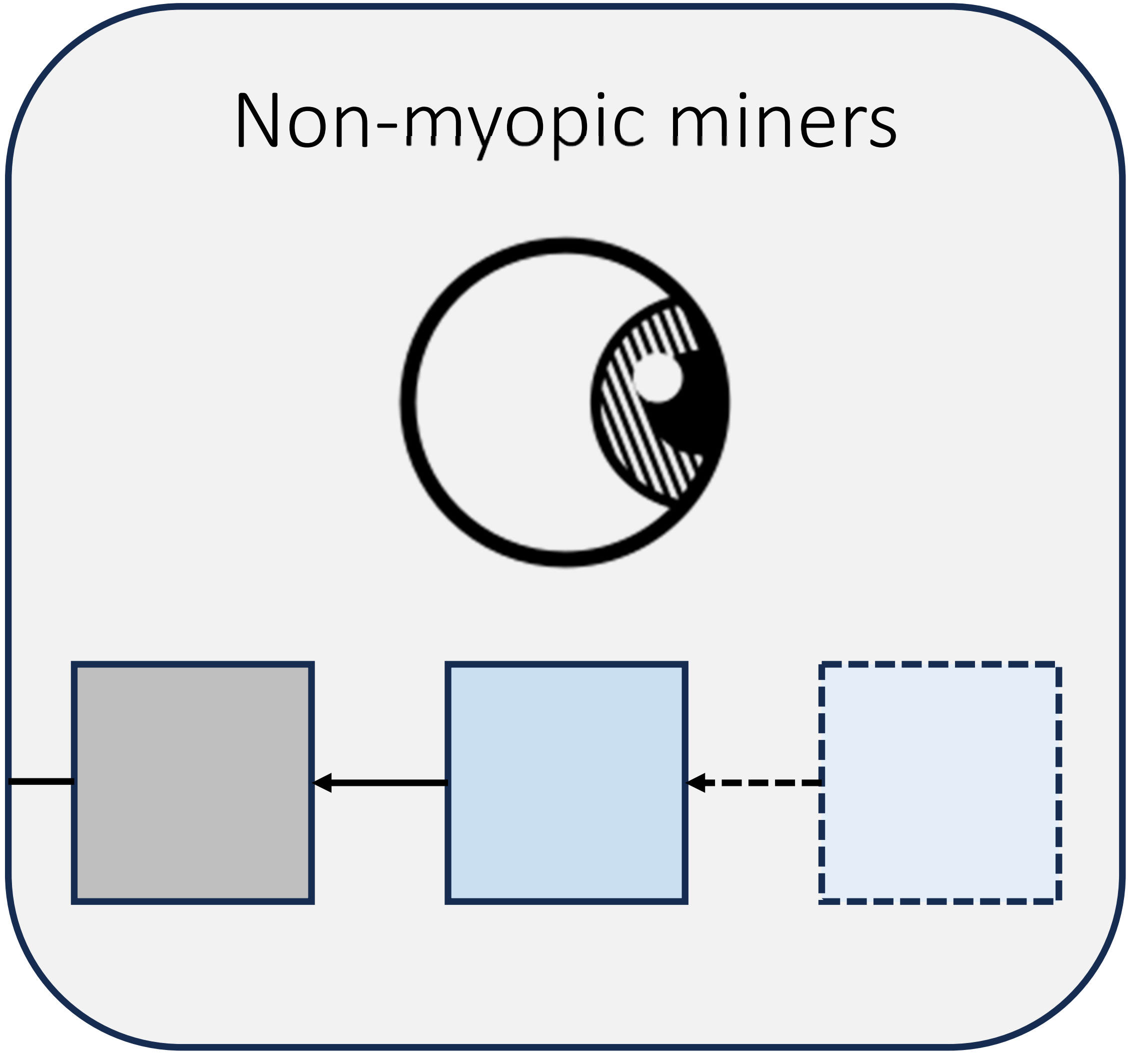
Myopic miners



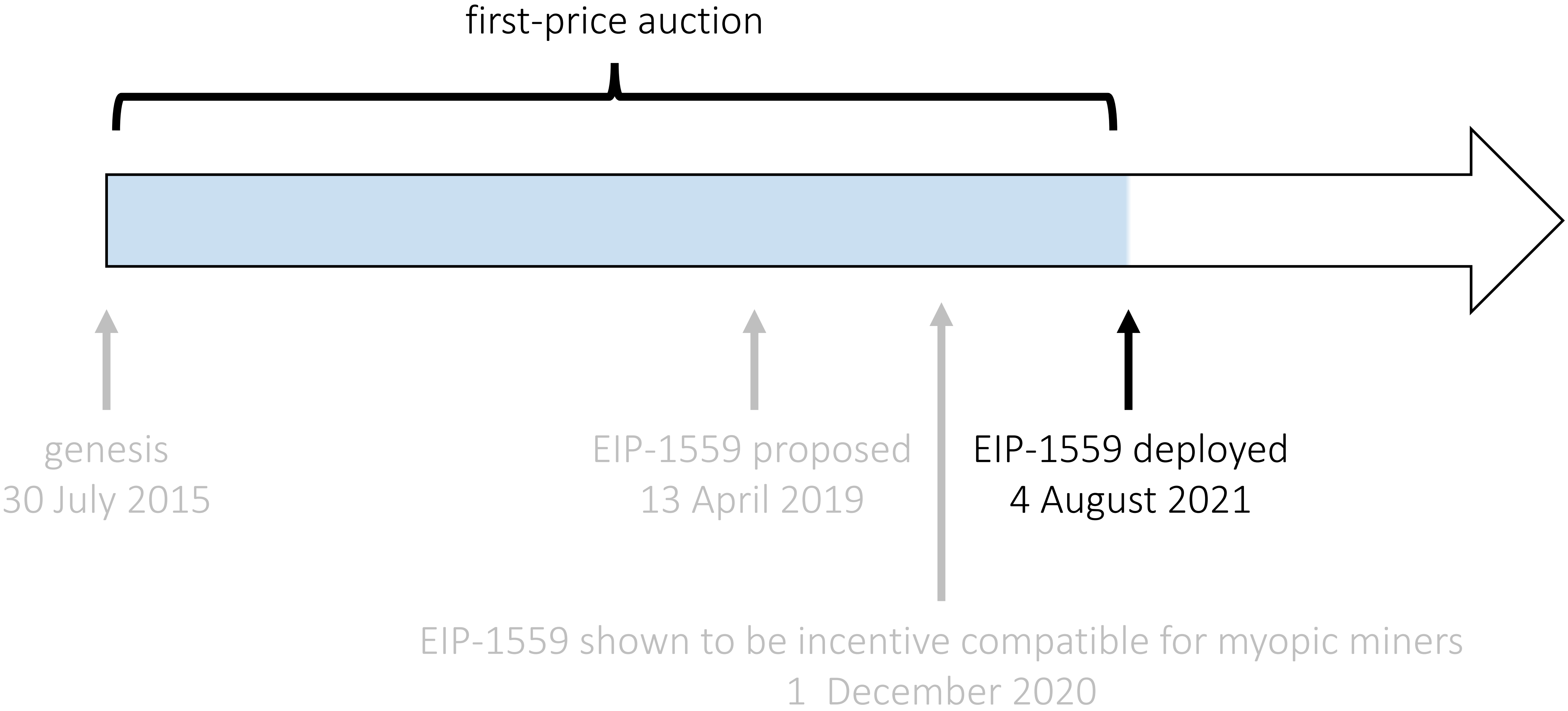
Non-myopic miners

Myopic vs. non-myopic miners

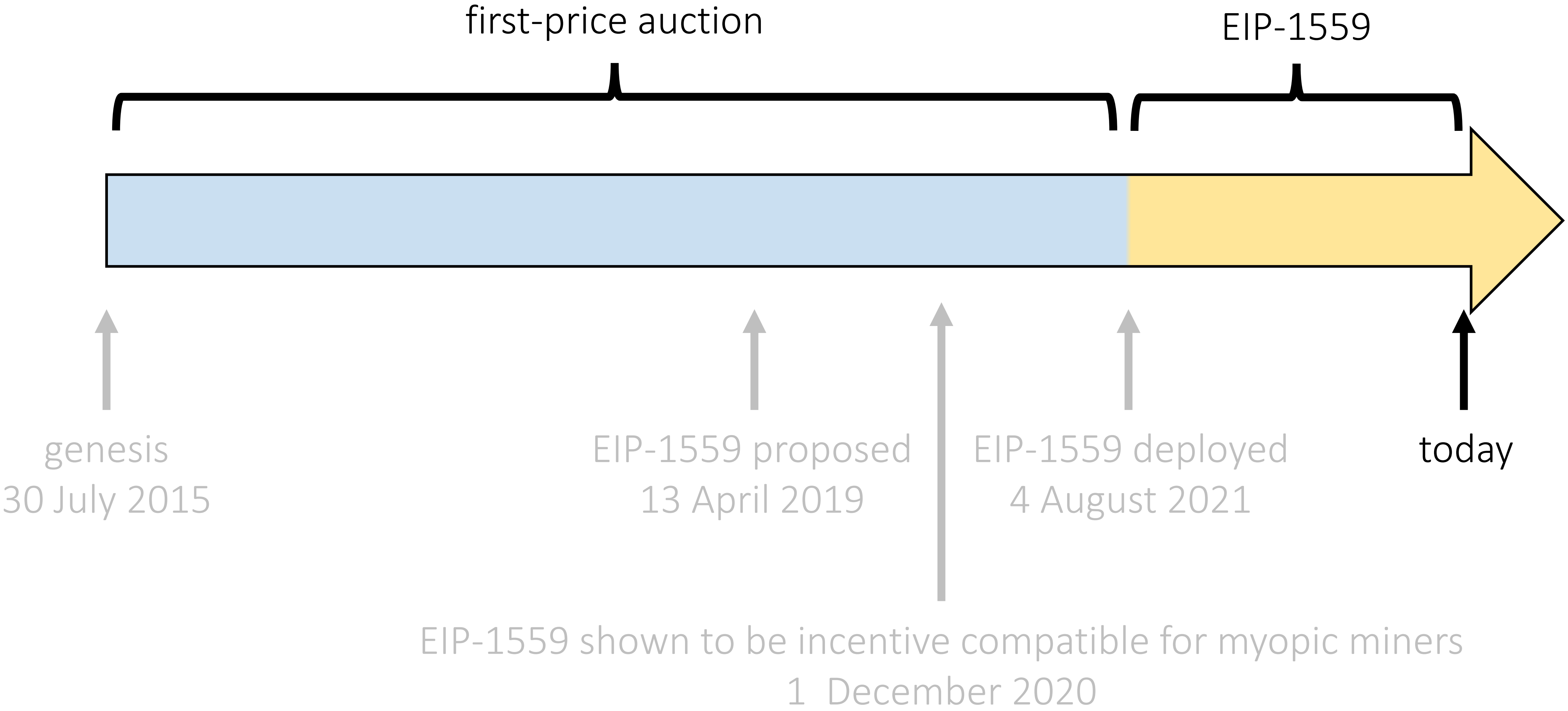




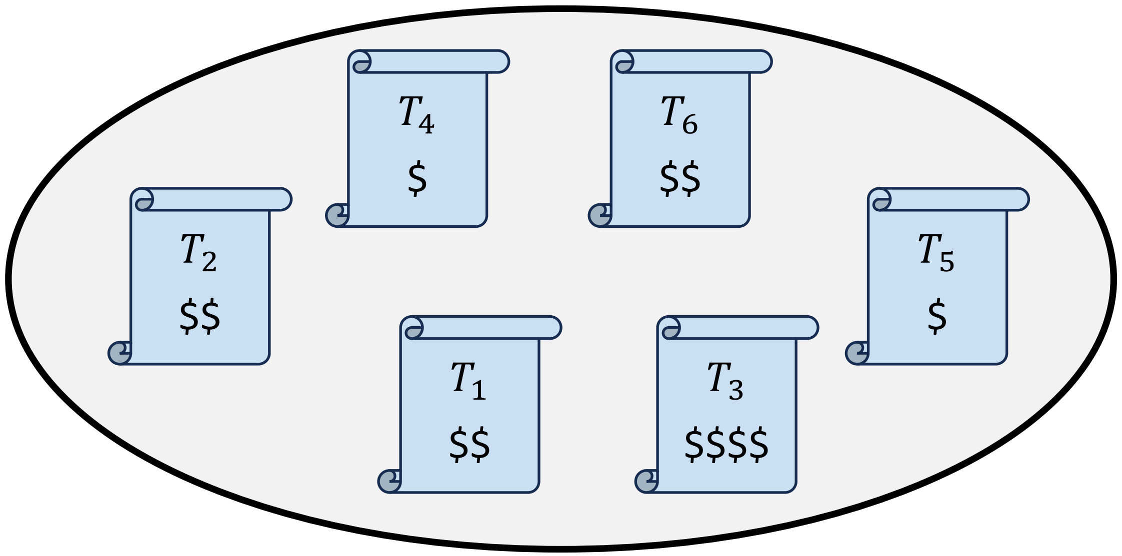
History of Ethereum transaction fees

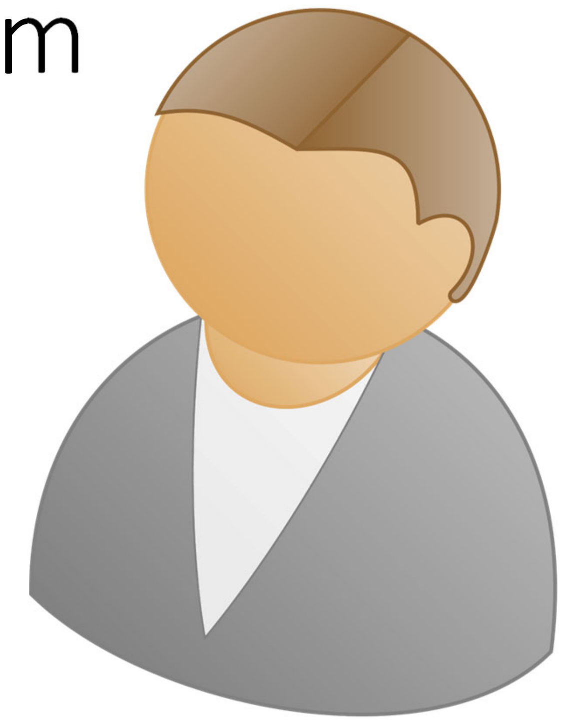


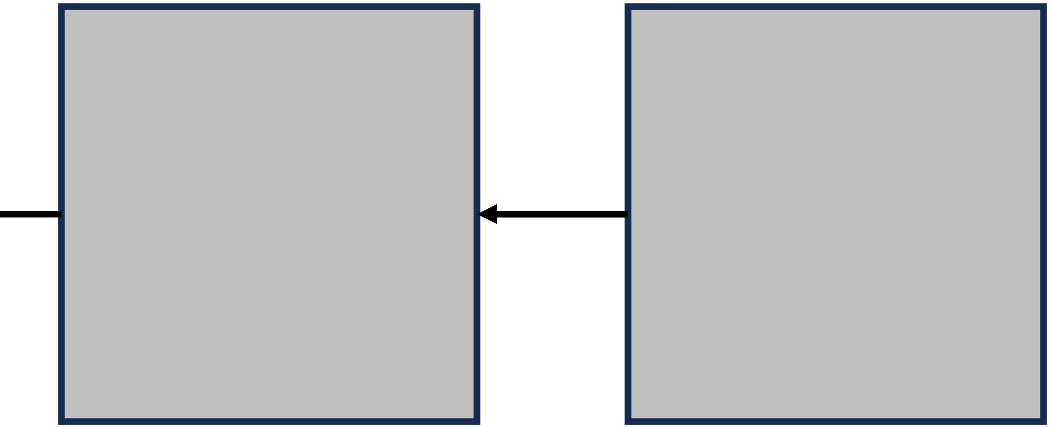
History of Ethereum transaction fees



EIP-1559 transaction fee mechanism

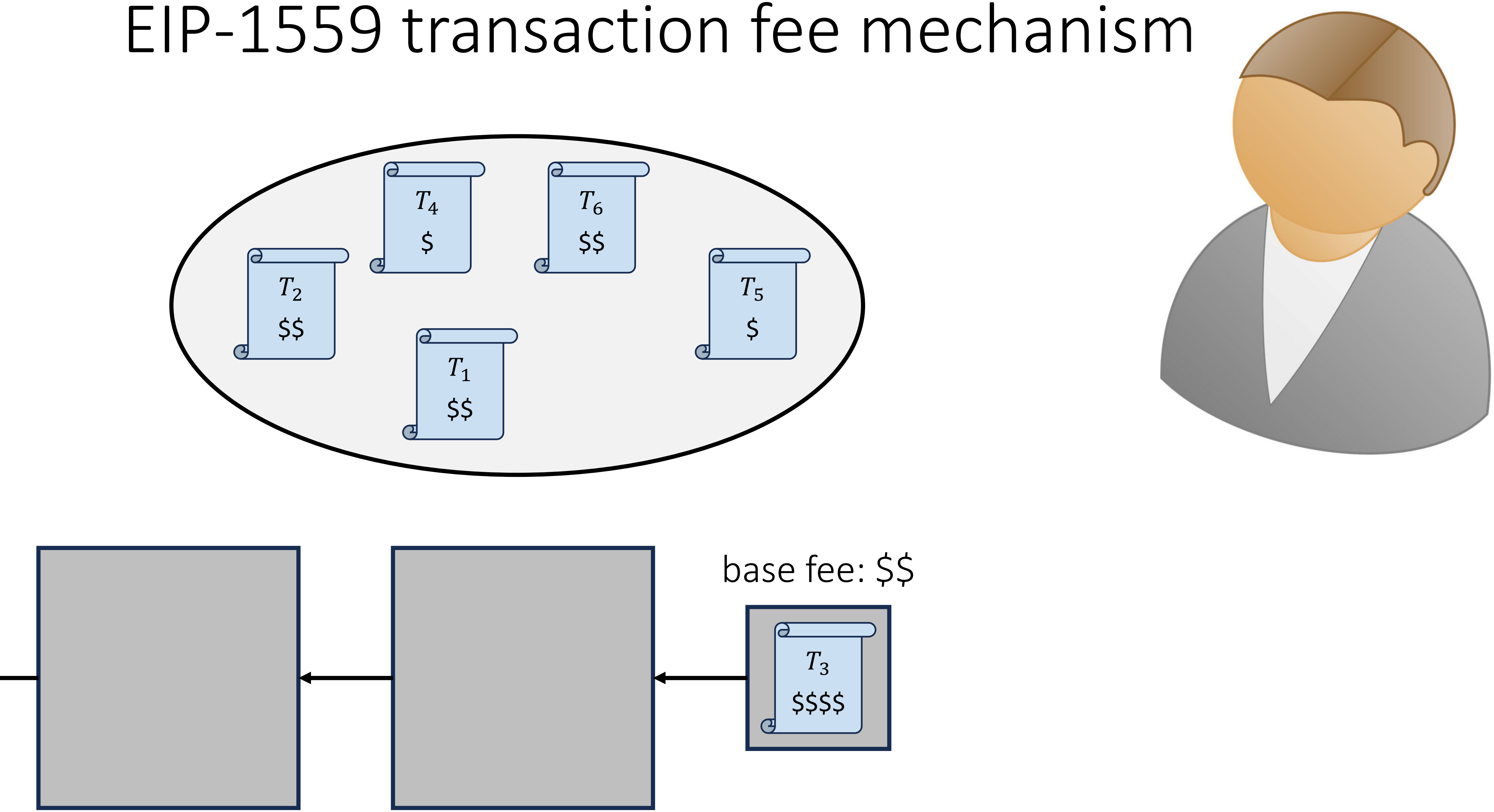




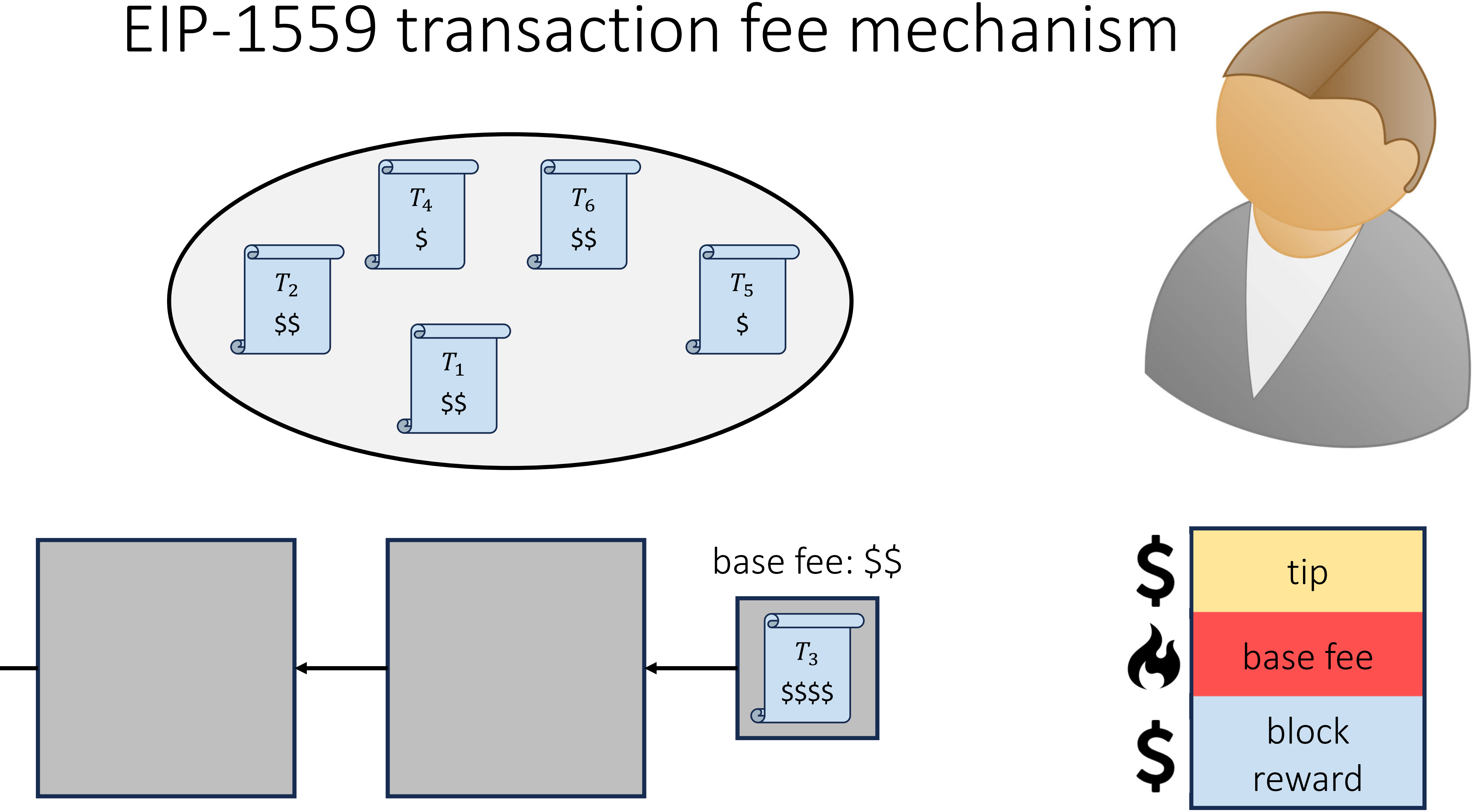


base fee: $$

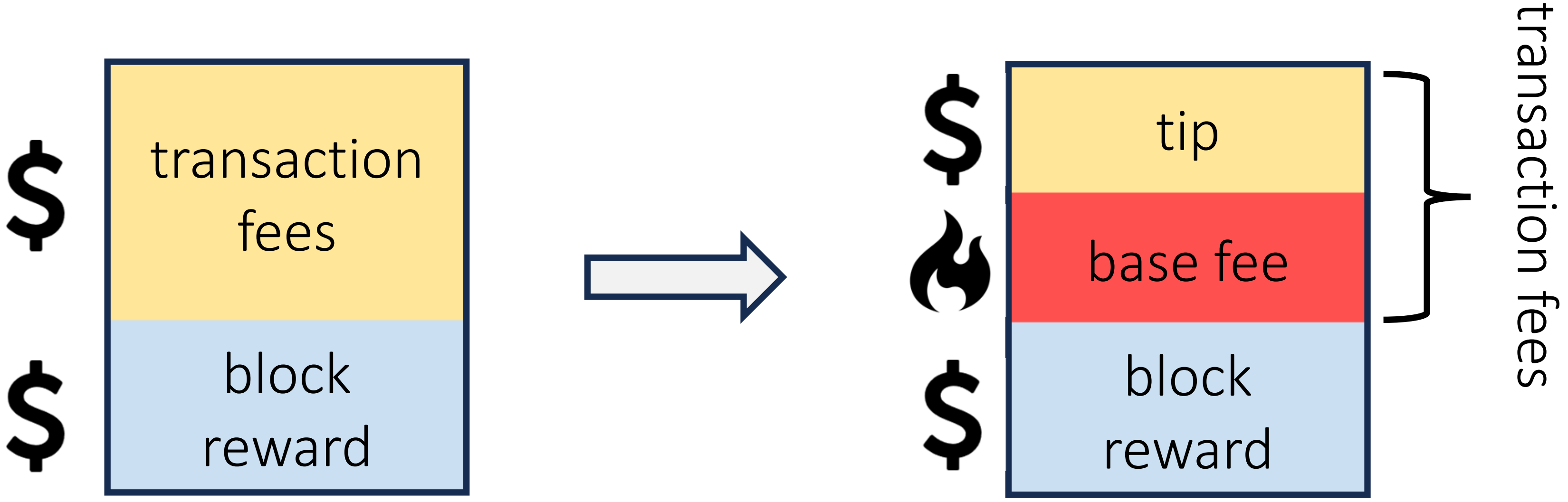
EIP-1559 transaction fee mechanism



EIP-1559 transaction fee mechanism



EIP-1559 transaction fee mechanism



base fee is burned and not received by the miner

EIP-1559 transaction fee mechanism

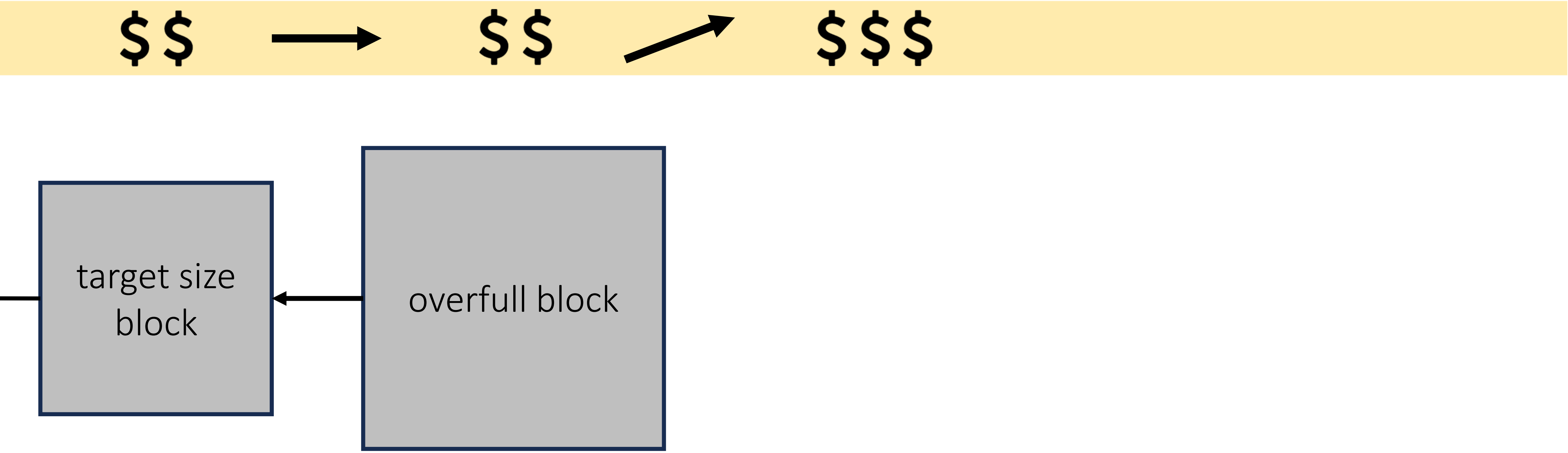
$$

base fee is dynamically adjusted

EIP-1559 transaction fee mechanism

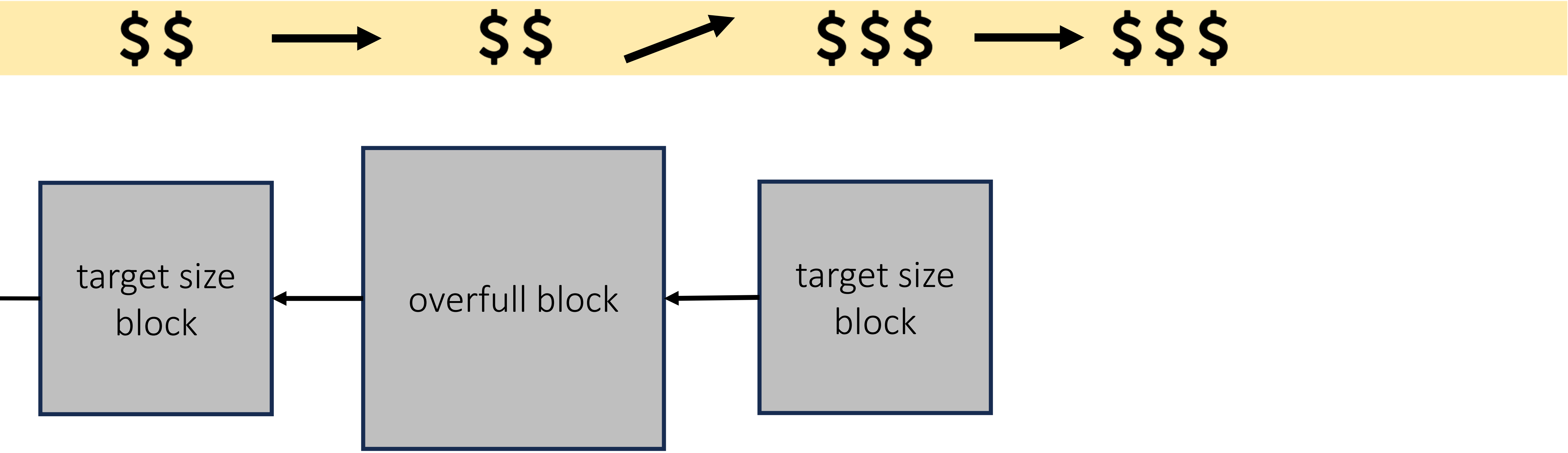
base fee is dynamically adjusted

EIP-1559 transaction fee mechanism



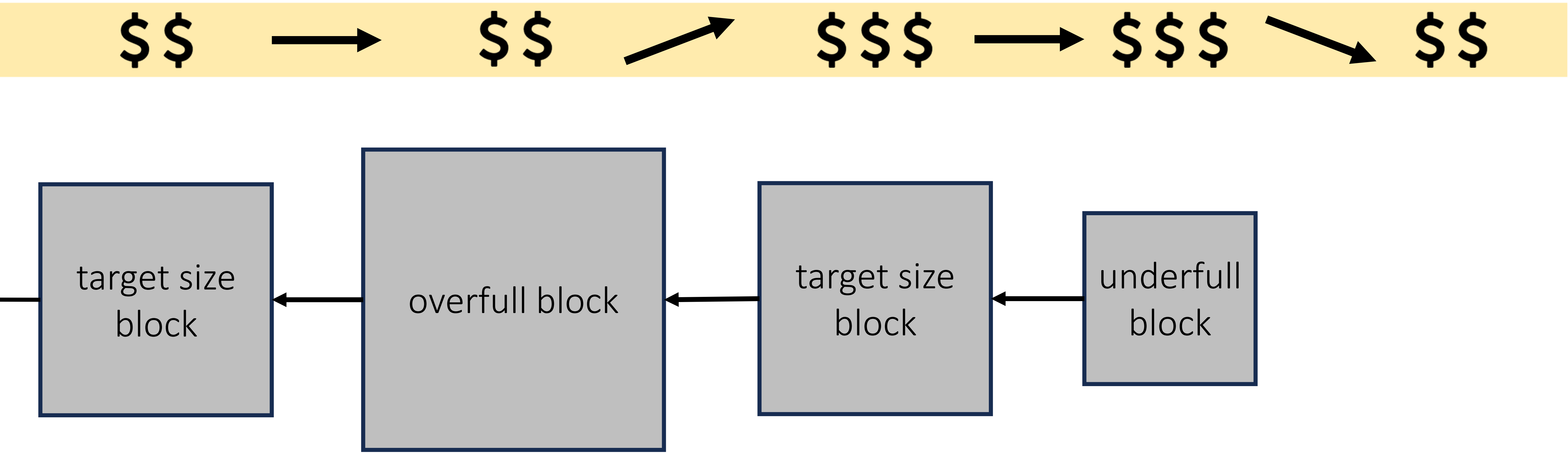
base fee is dynamically adjusted

EIP-1559 transaction fee mechanism



base fee is dynamically adjusted

EIP-1559 transaction fee mechanism

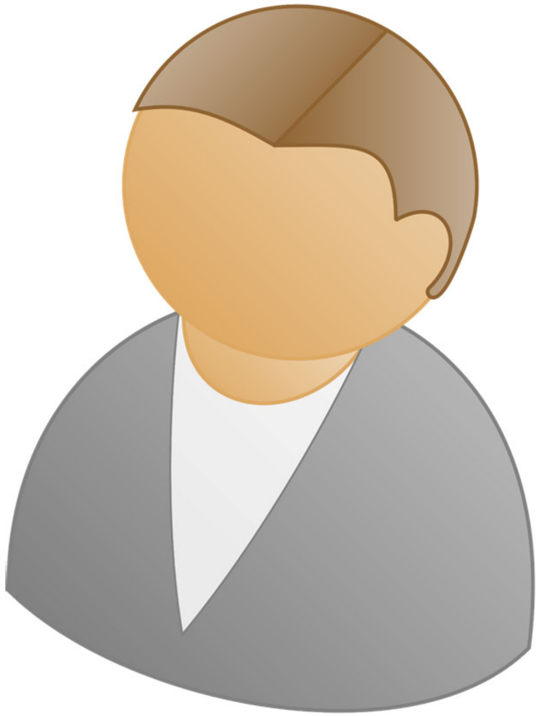


base fee is dynamically adjusted

Is EIP-1559 incentive-compatible?

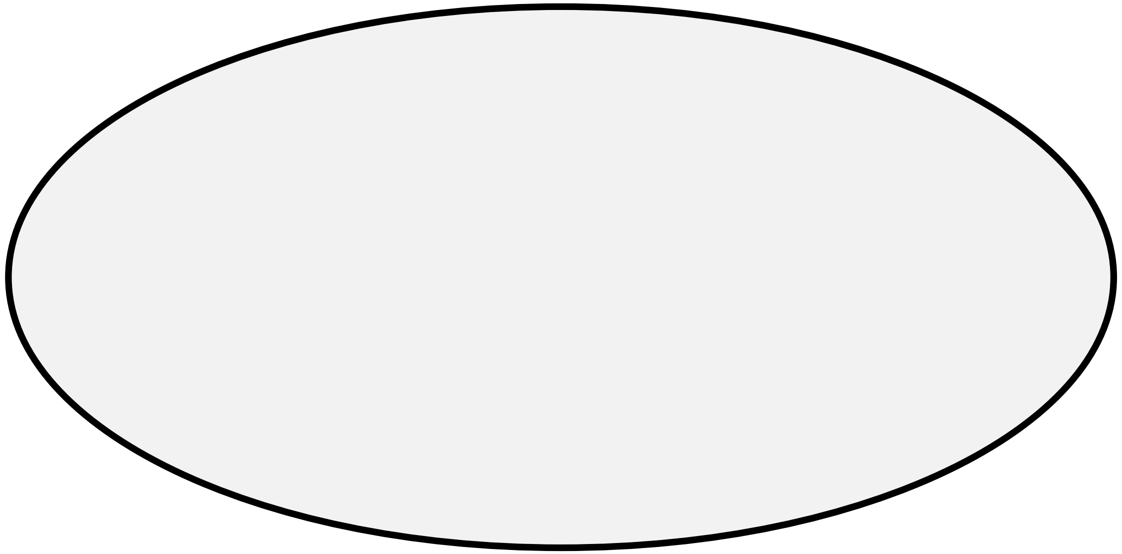
Model

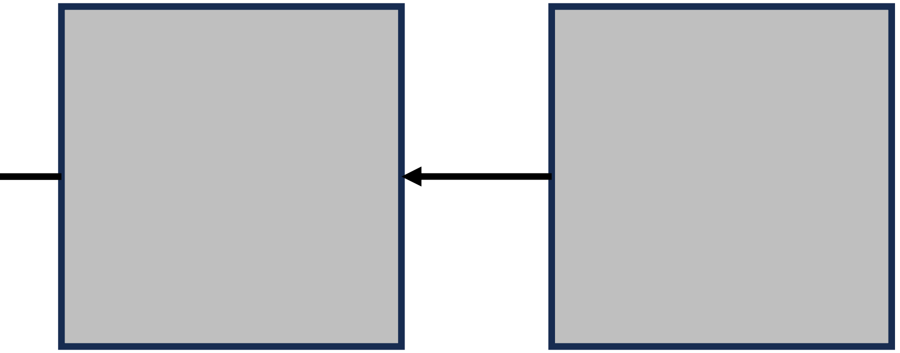
user



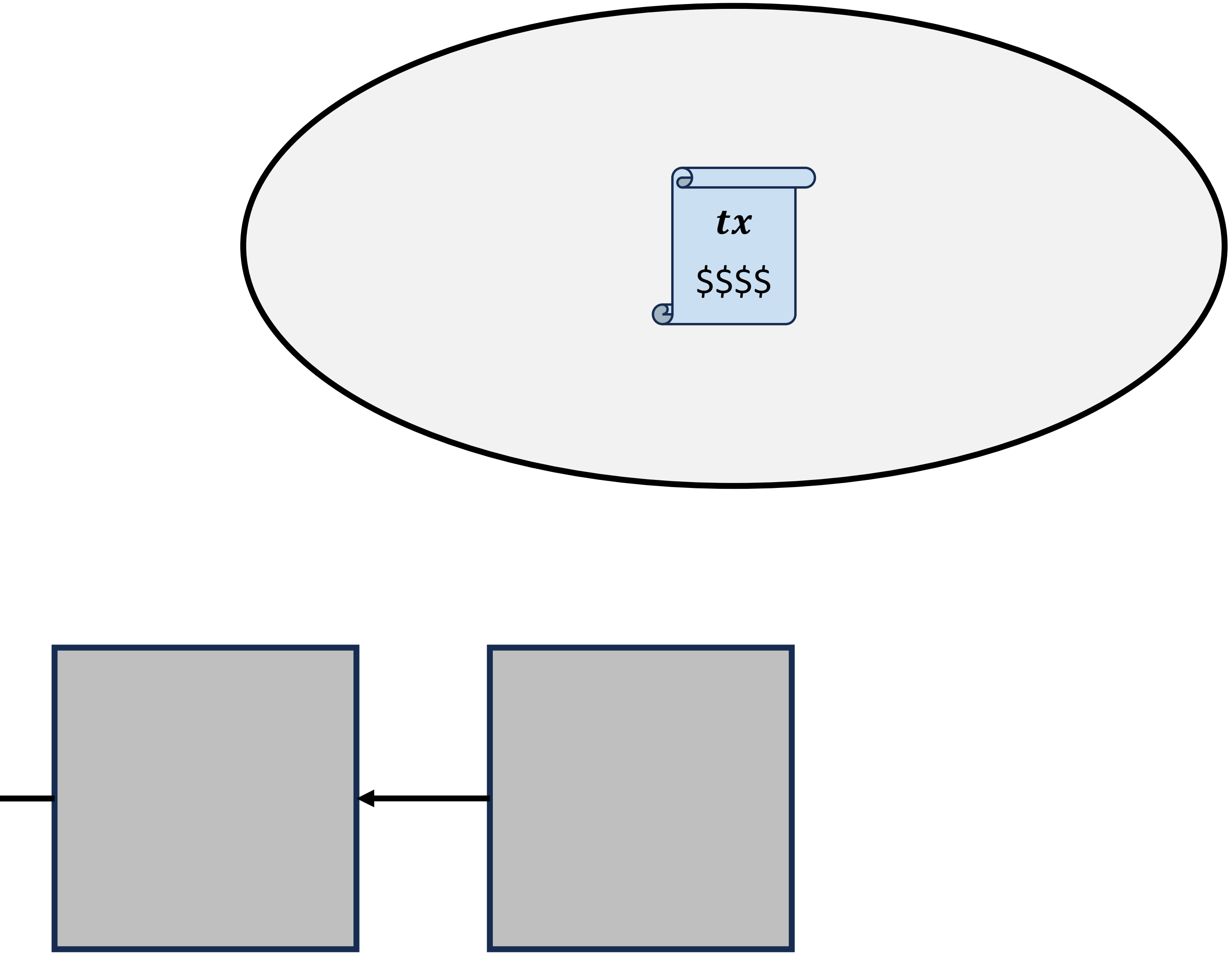
miner

User

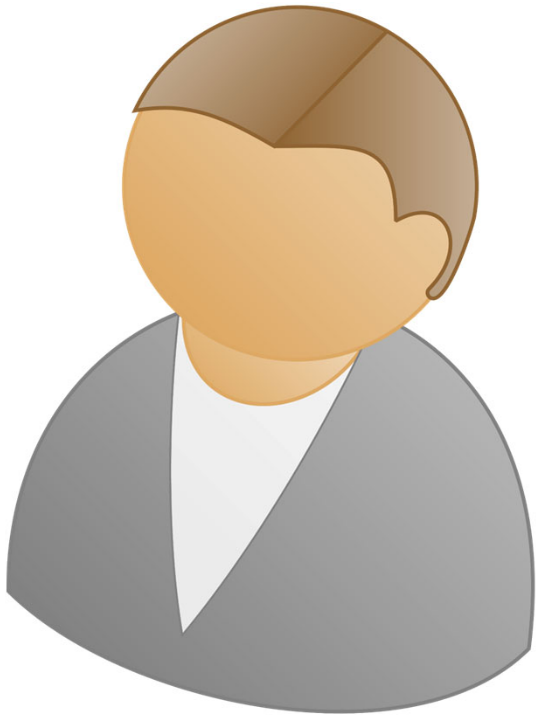


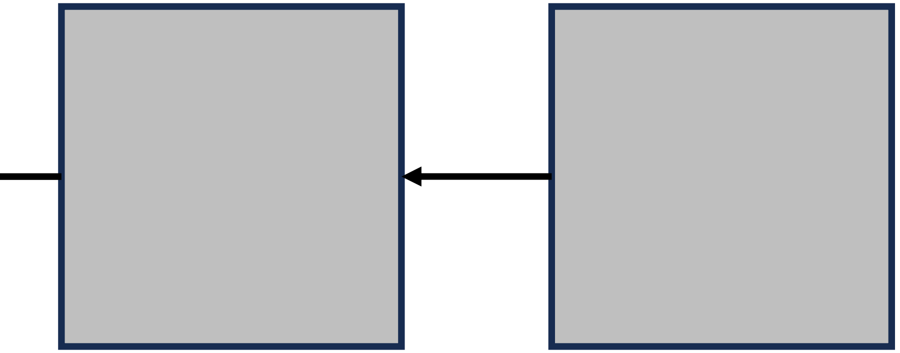


User

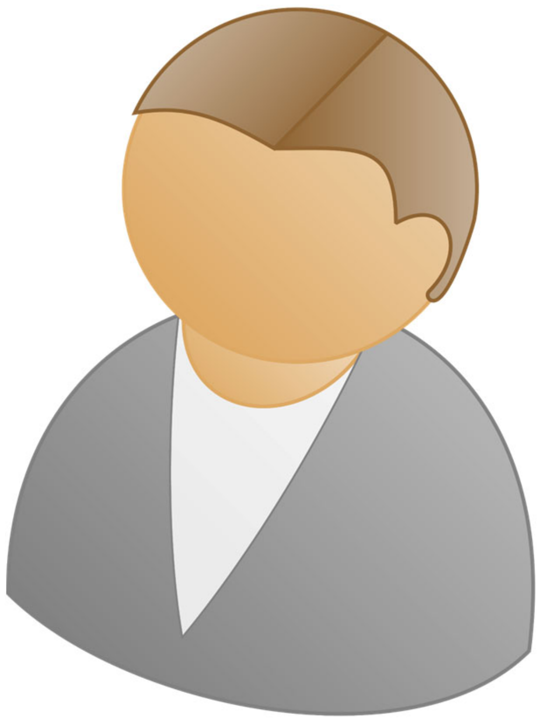


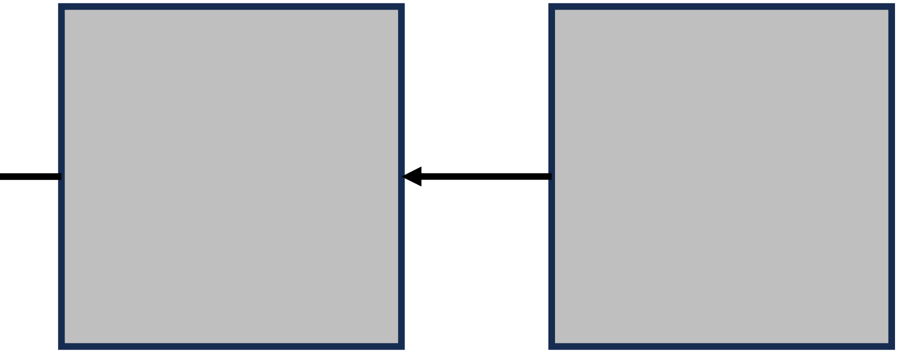
Miner





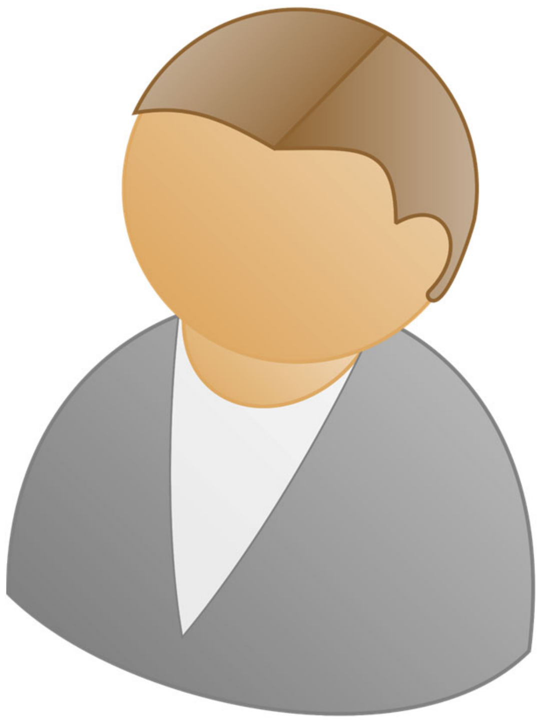
Miner

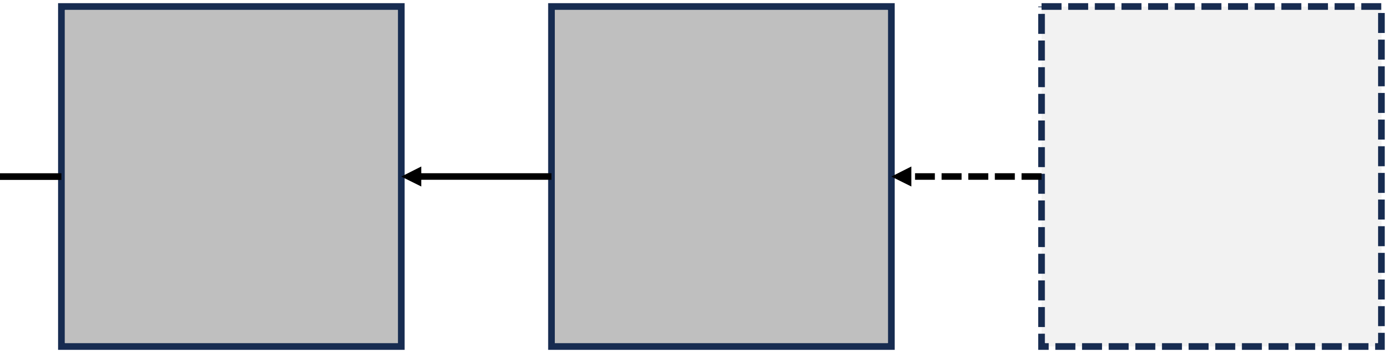




p_x: proportion of mining power

Miner

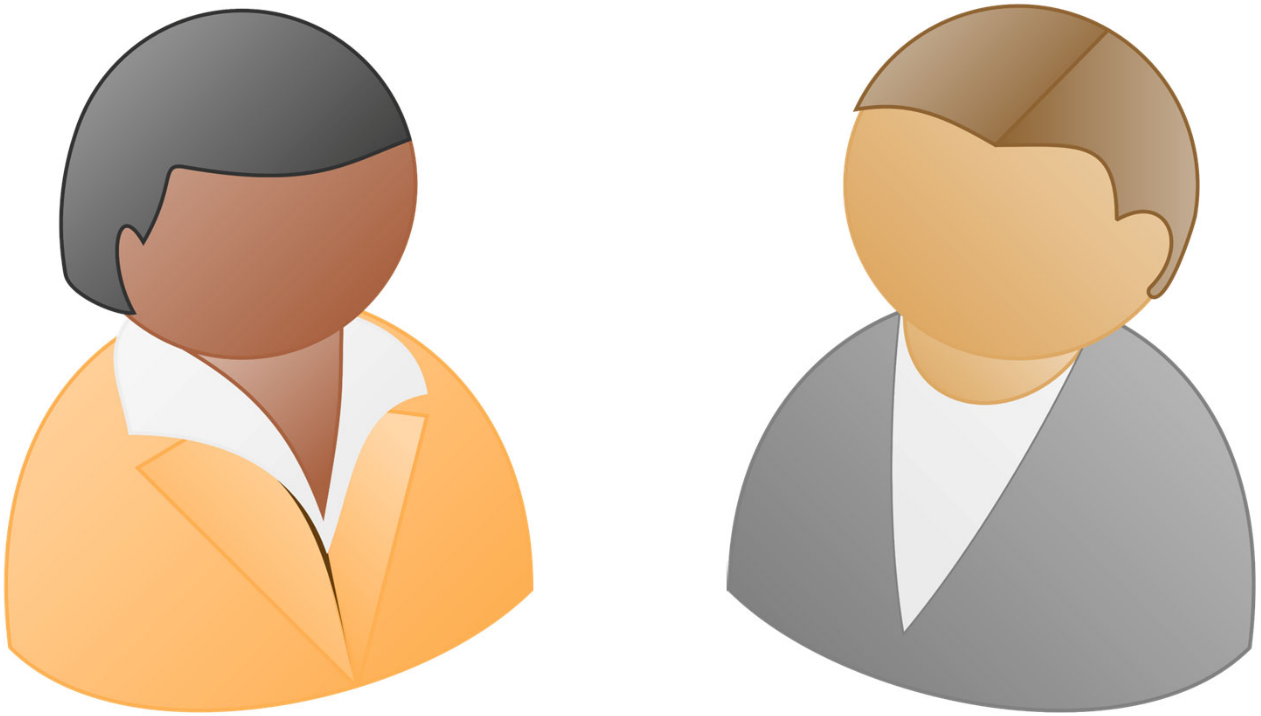




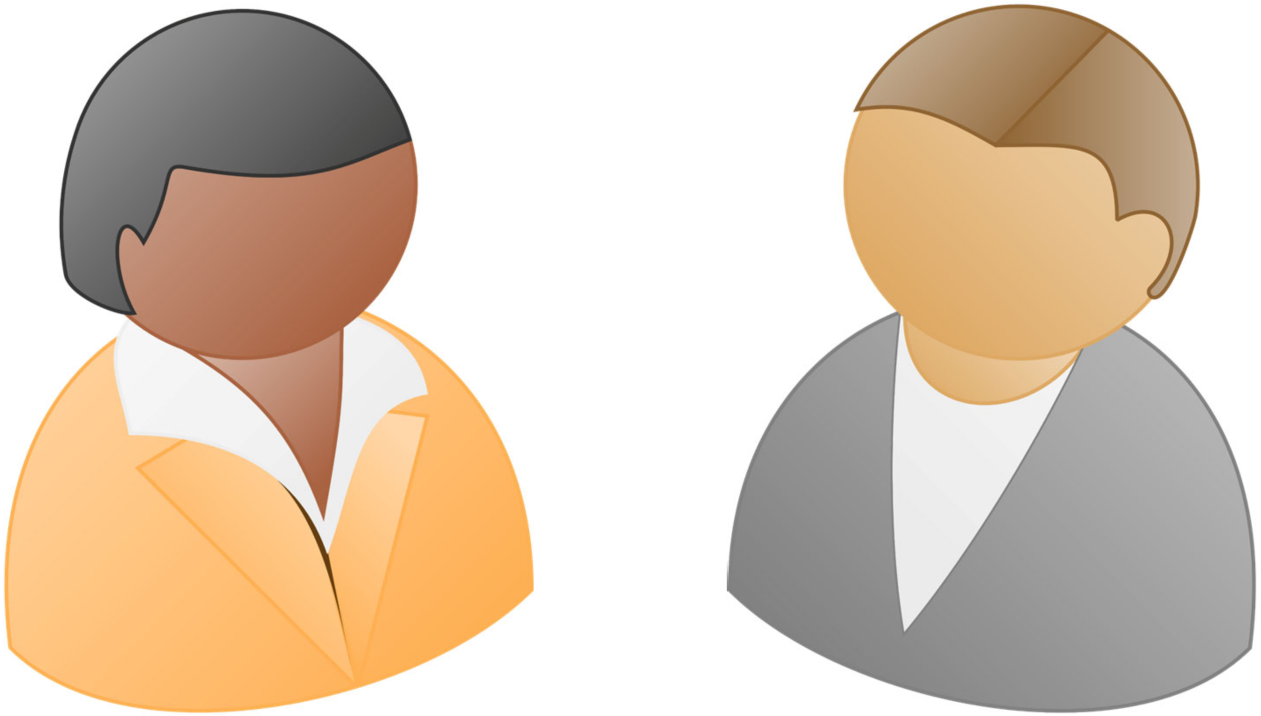
p_x: proportion of mining power

chosen with propbability p_x to mine the next block

Buyer-seller interaction

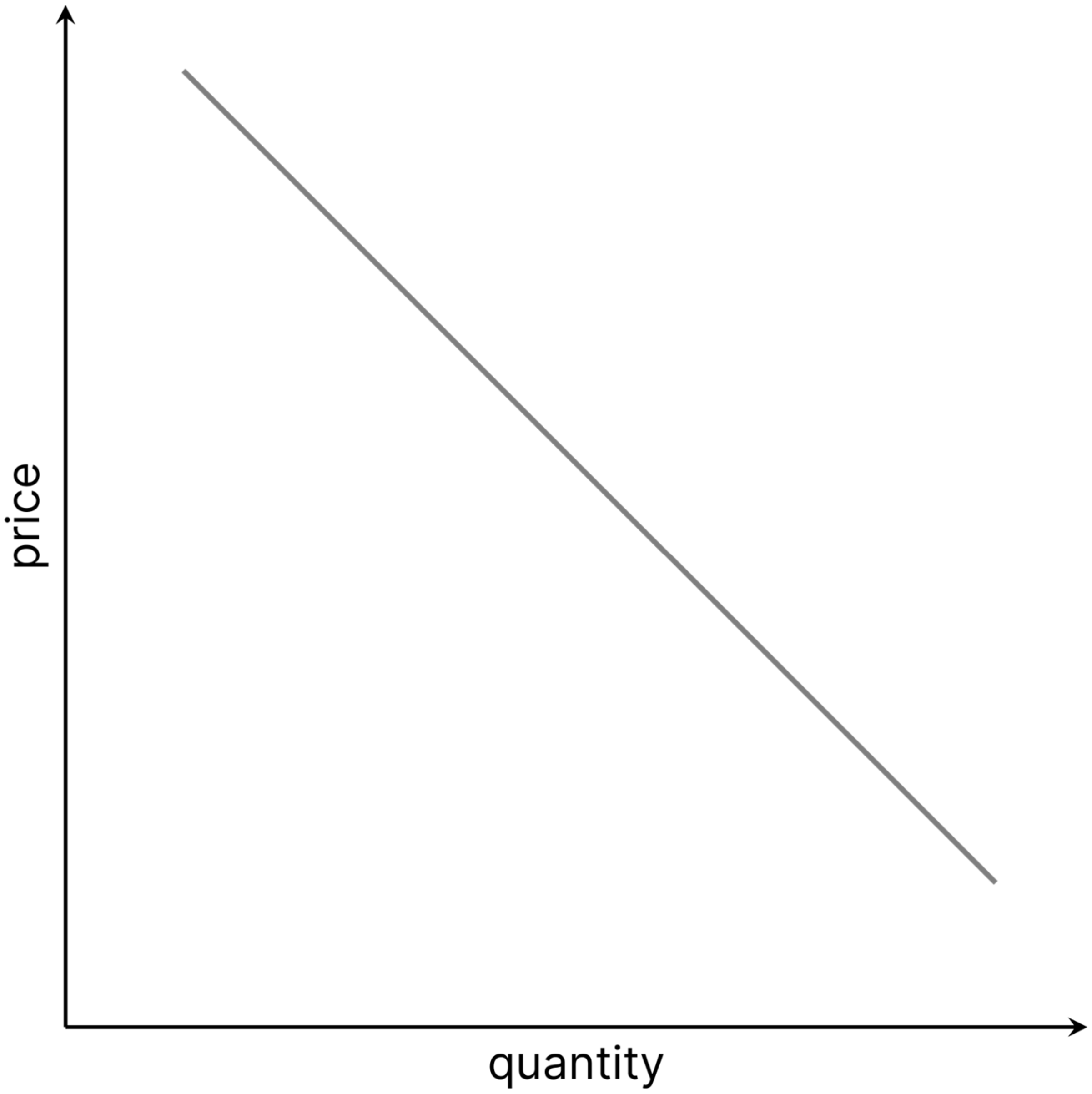


Buyer-seller interaction



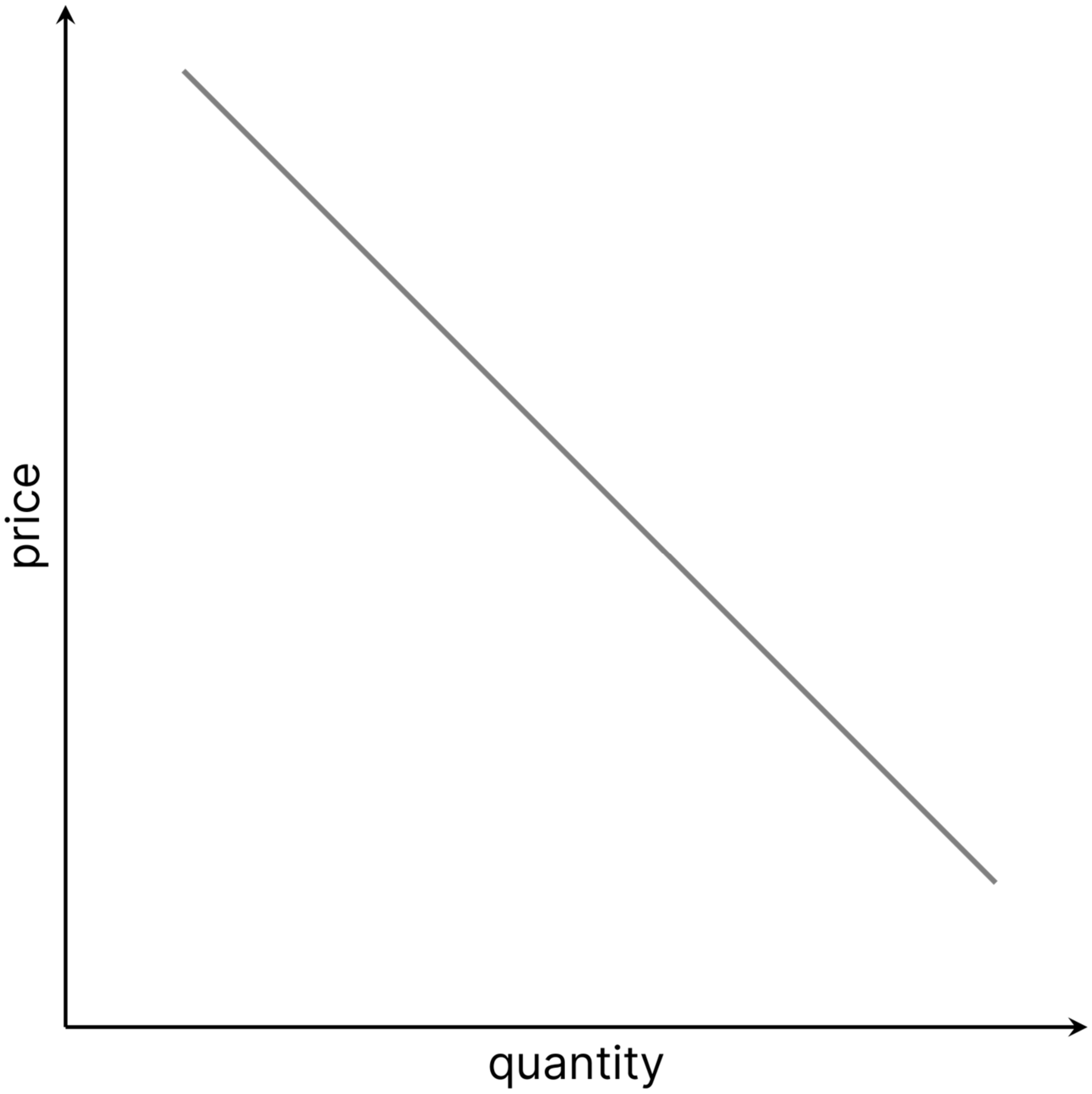
users collaborate with miners if it benefits them both

Steady state



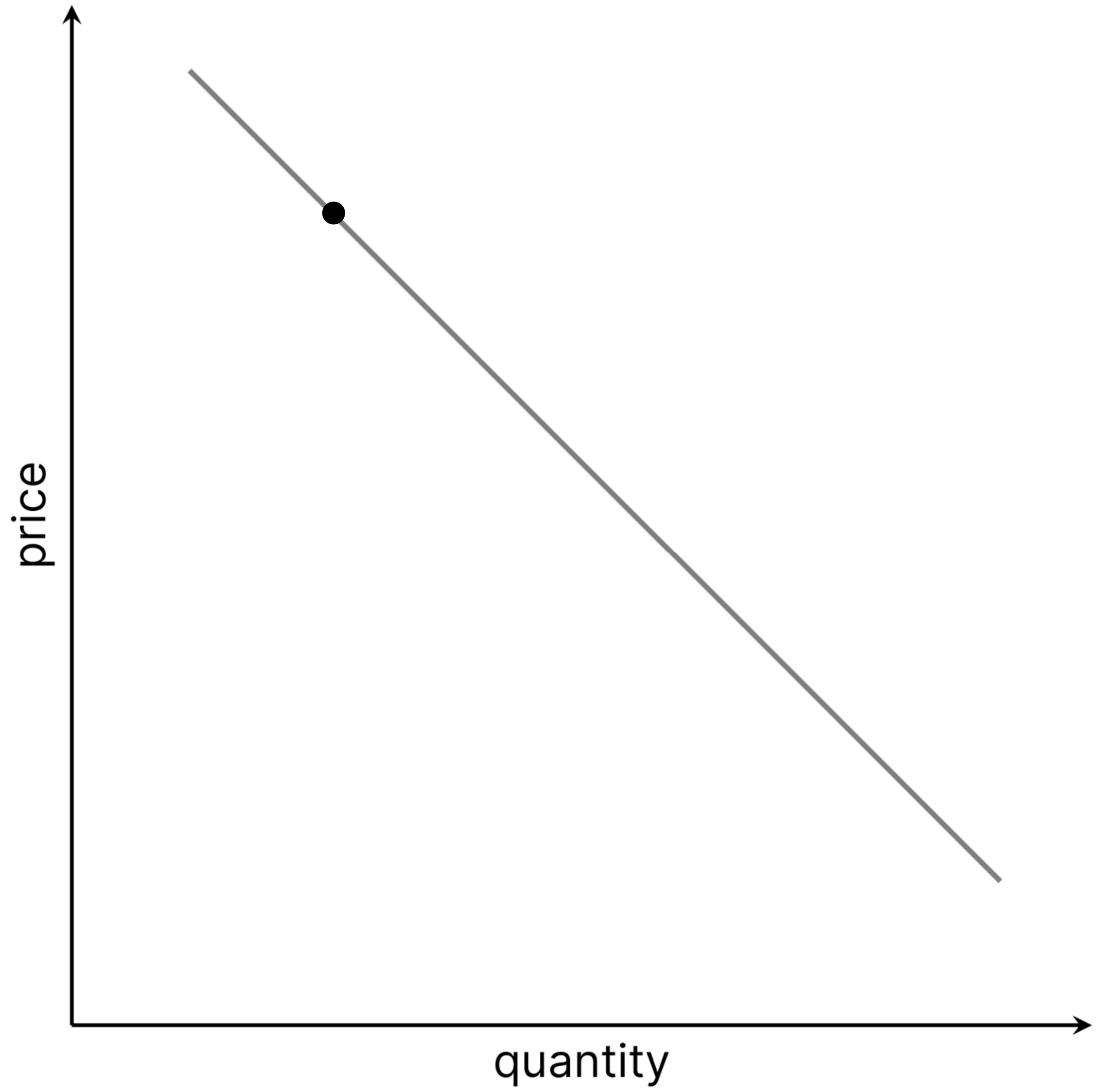
Steady state

only assumption on demand curve is that it is a decreasing function



Steady state

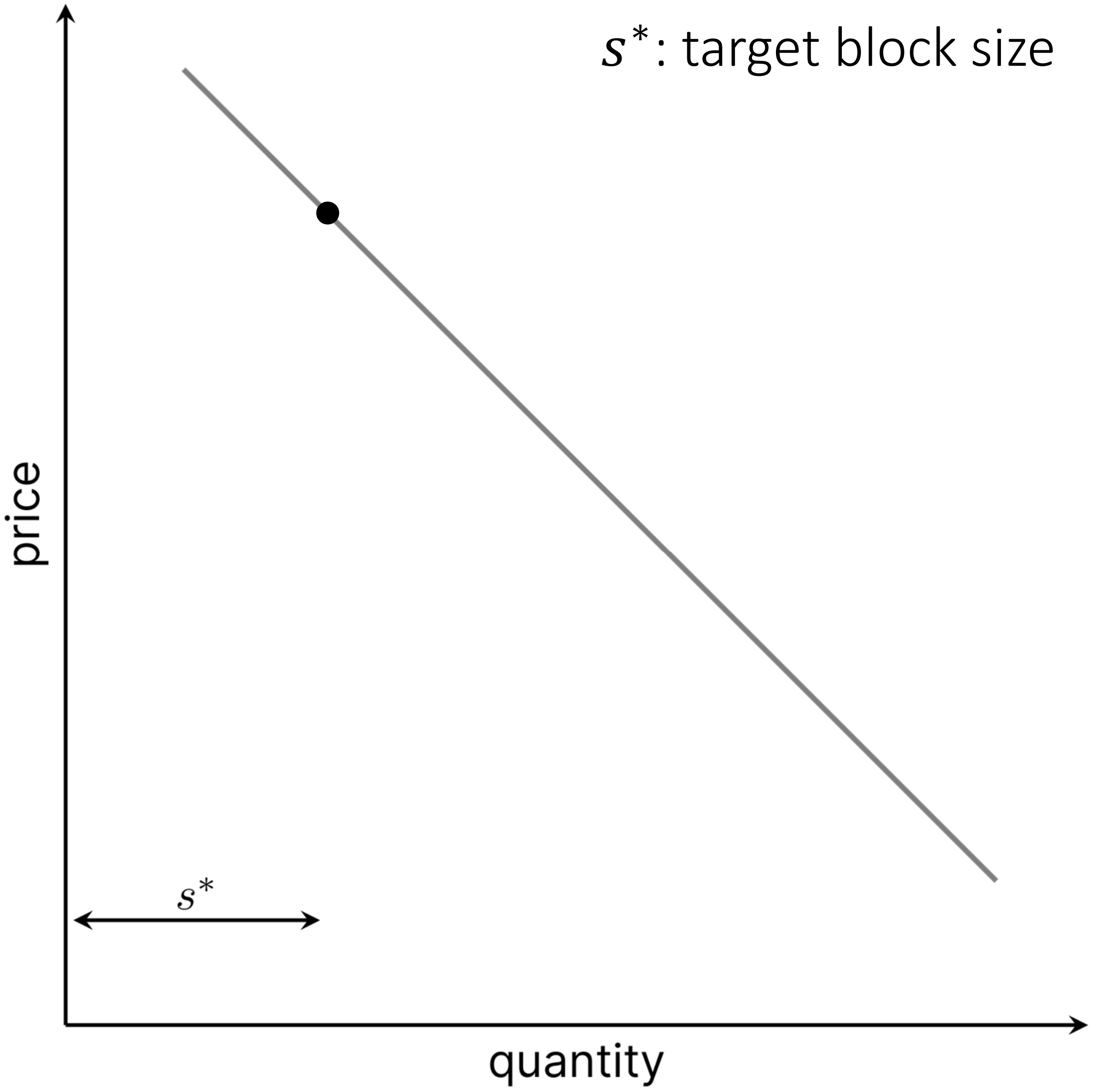
only assumption on demand curve
is that it is a decreasing function



Steady state

only assumption on demand curve
is that it is a decreasing function

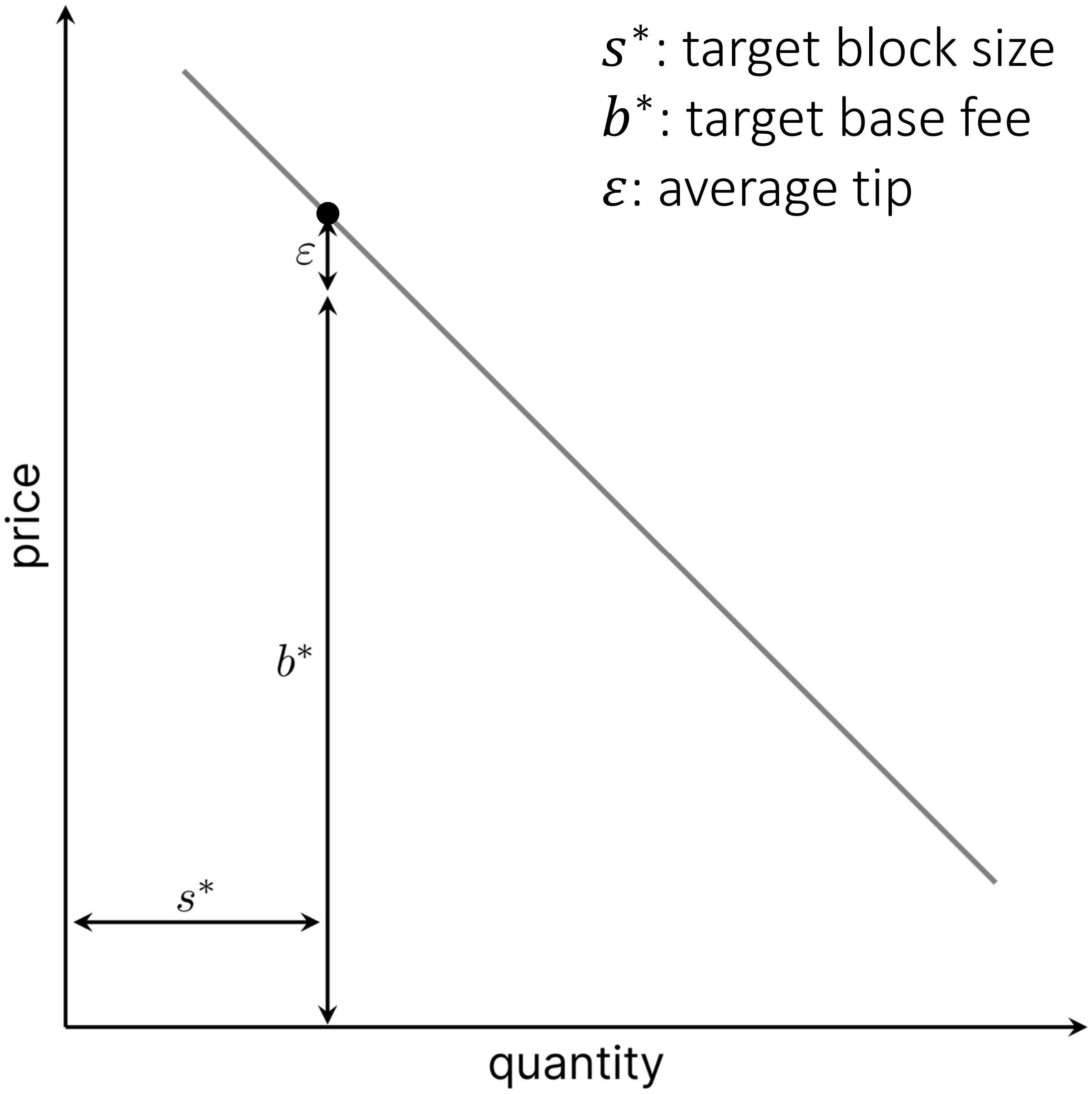
s^*: target block size



Steady state

only assumption on demand curve is that it is a decreasing function

$b^* + \varepsilon$: transaction fee



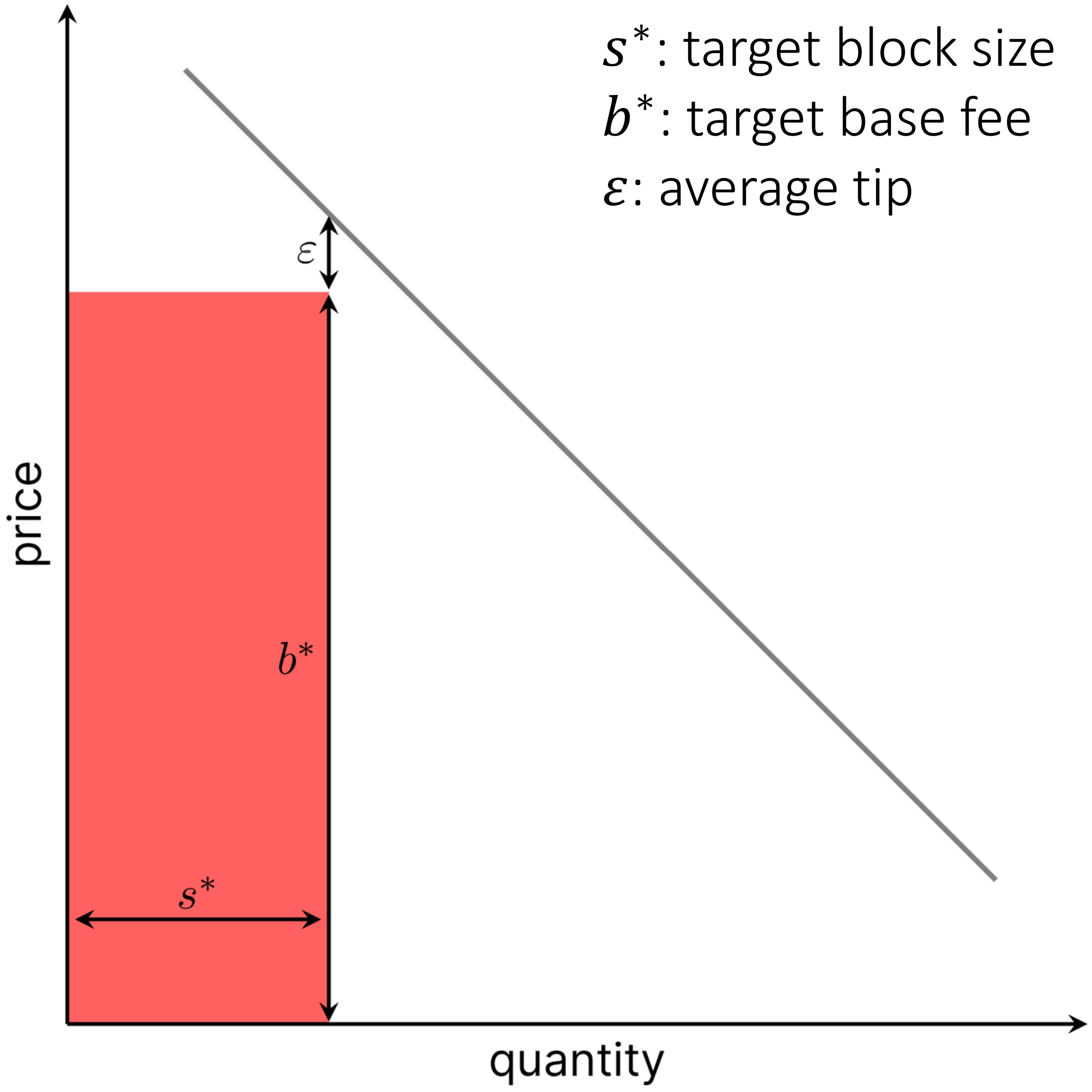
s^*: target block size
b^*: target base fee
ε: average tip

Steady state

only assumption on demand curve is that it is a decreasing function

$b^* + \varepsilon$: transaction fee

$b^* \cdot s^*$: burned



s^*: target block size
b^*: target base fee
ε: average tip

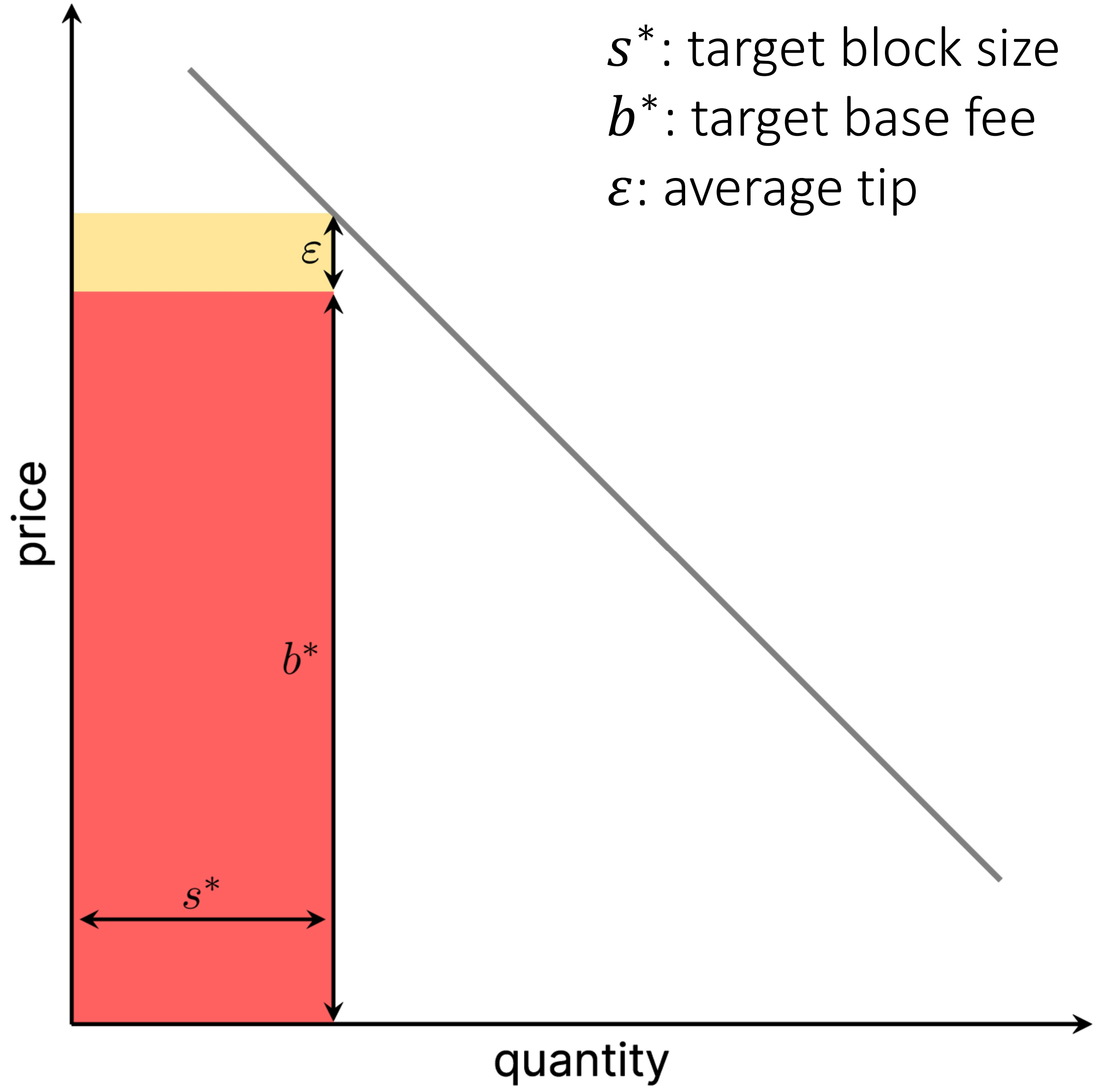
Steady state

only assumption on demand curve is that it is a decreasing function

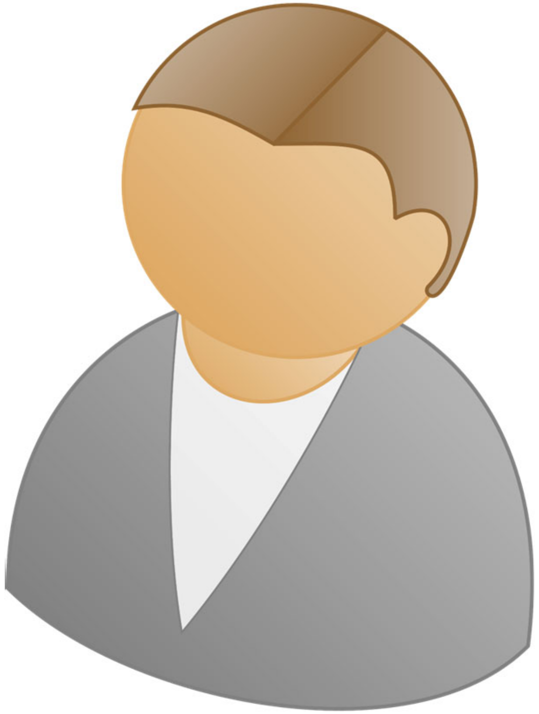
$b^* + \varepsilon$: transaction fee

$b^* \cdot s^*$: burned

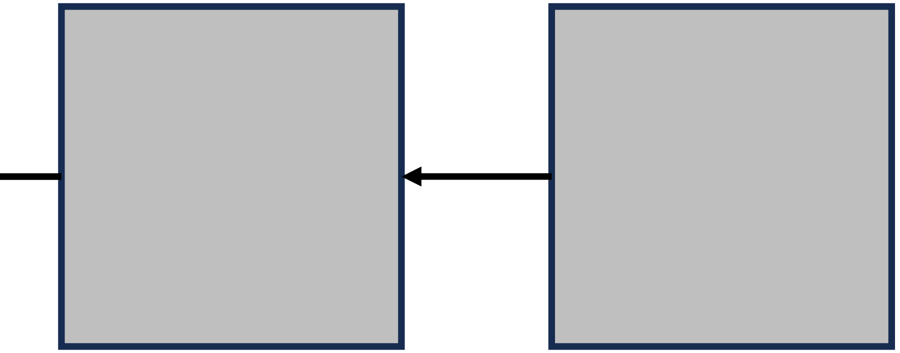
$\varepsilon \cdot s^*$: received by miner



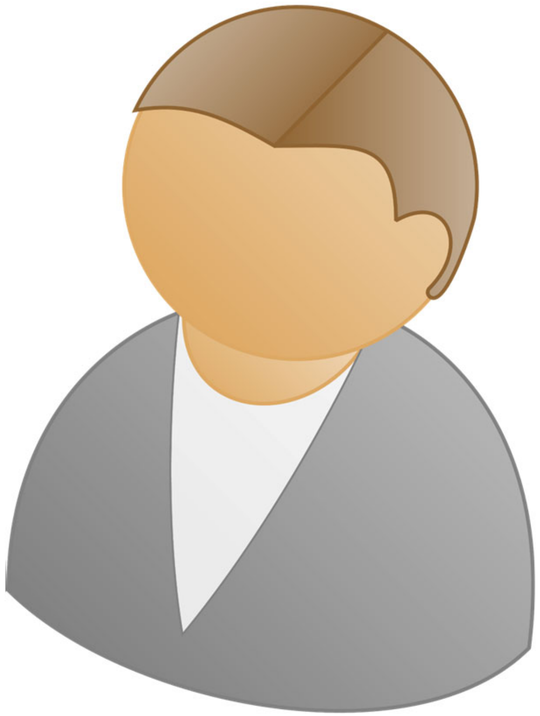
Honest strategy in steady state

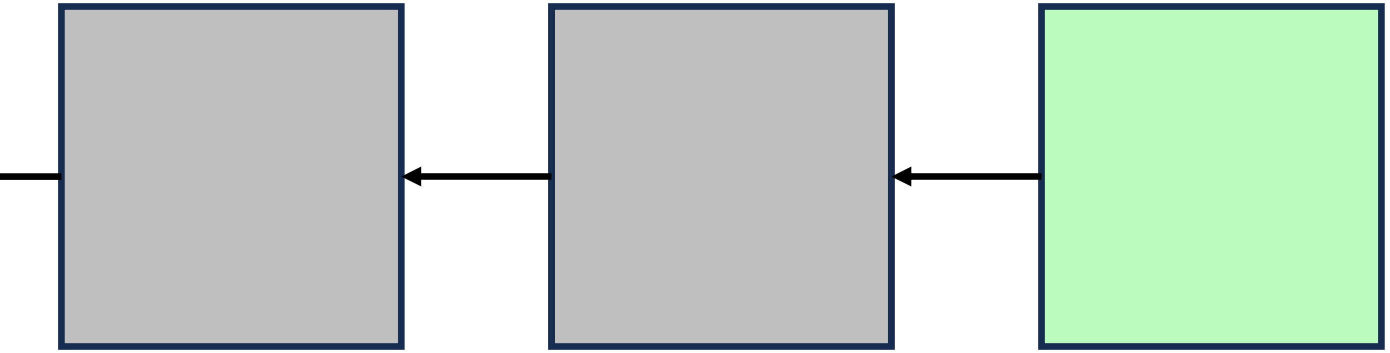


p_x: proportion of mining power

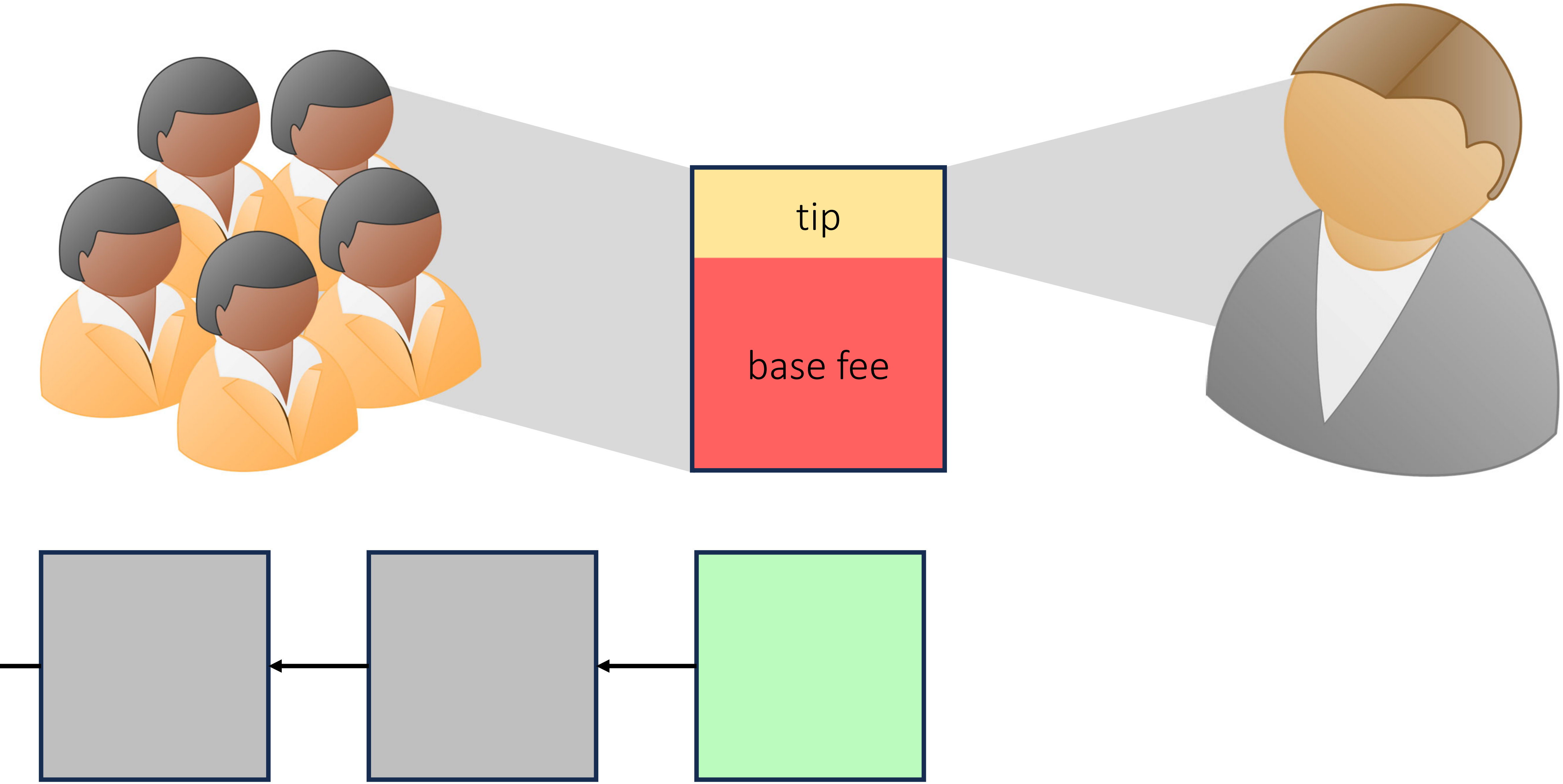


Honest strategy in steady state



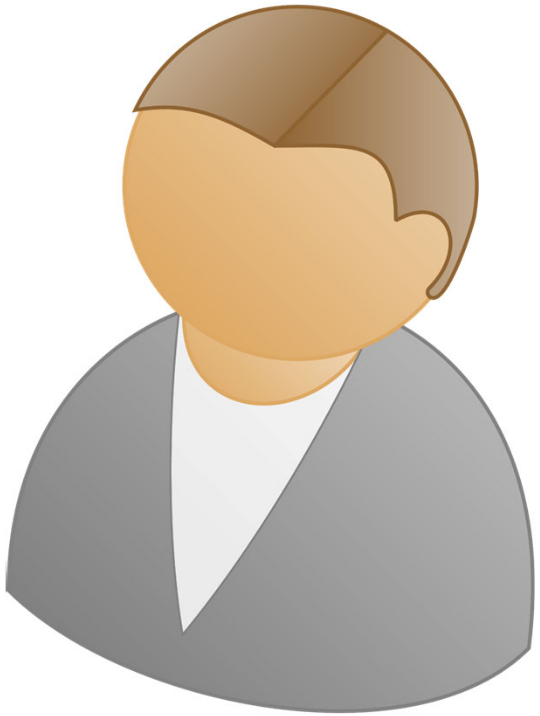


Honest strategy in steady state

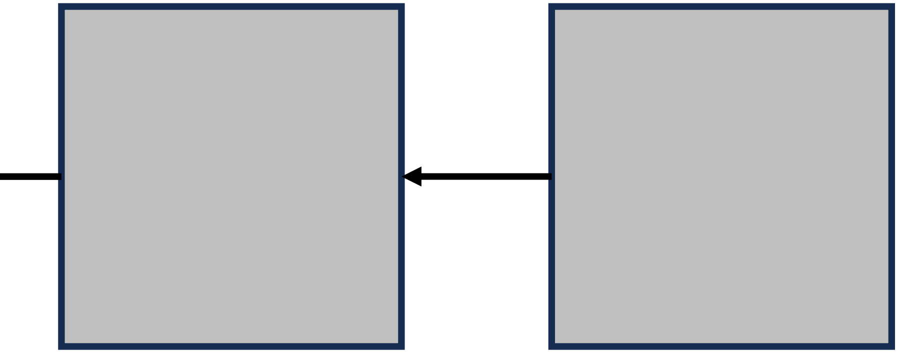


A Miner’s Deviation from the Honest Strategy

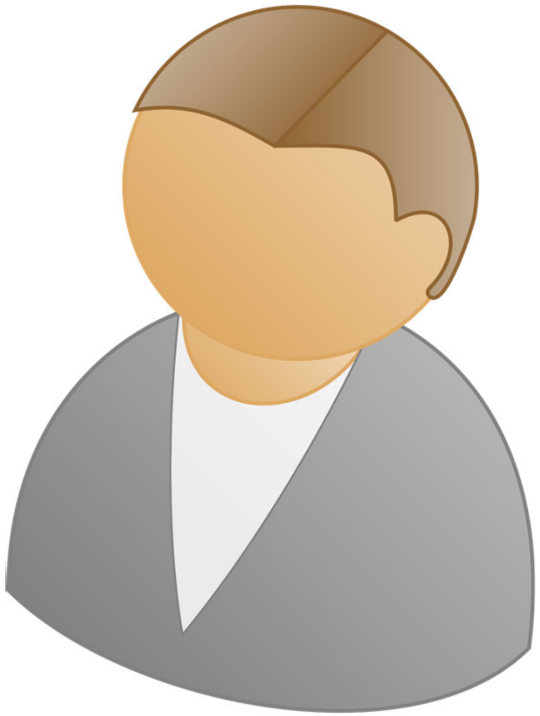
Deviation from honest strategy

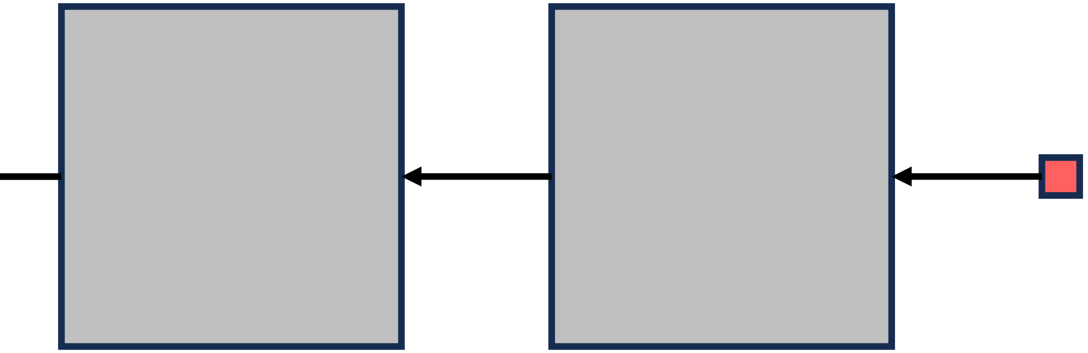


p_x: proportion of mining power

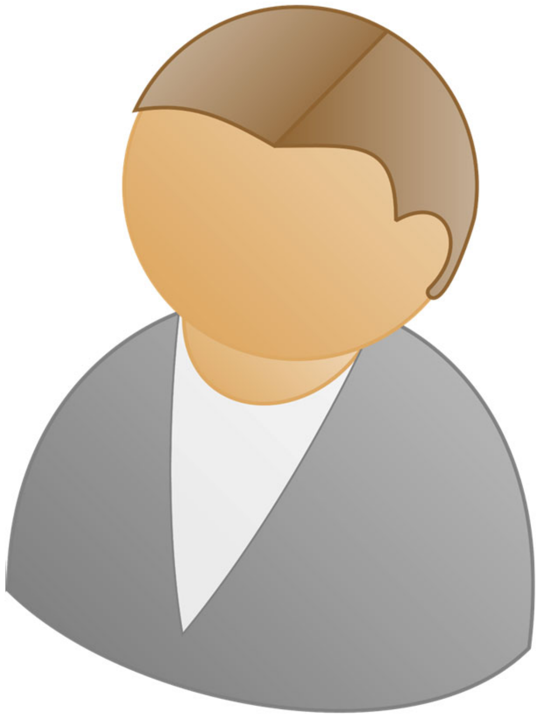


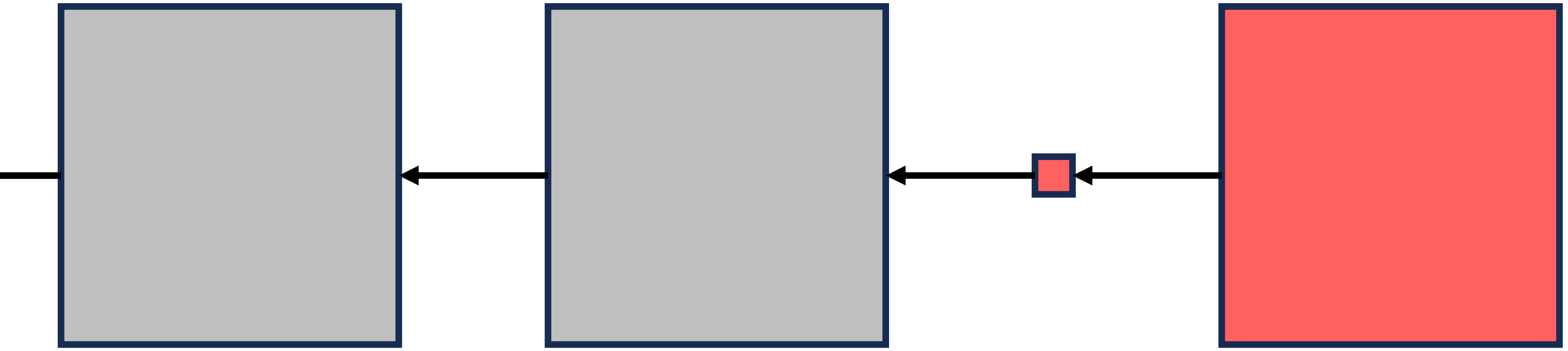
Deviation from honest strategy



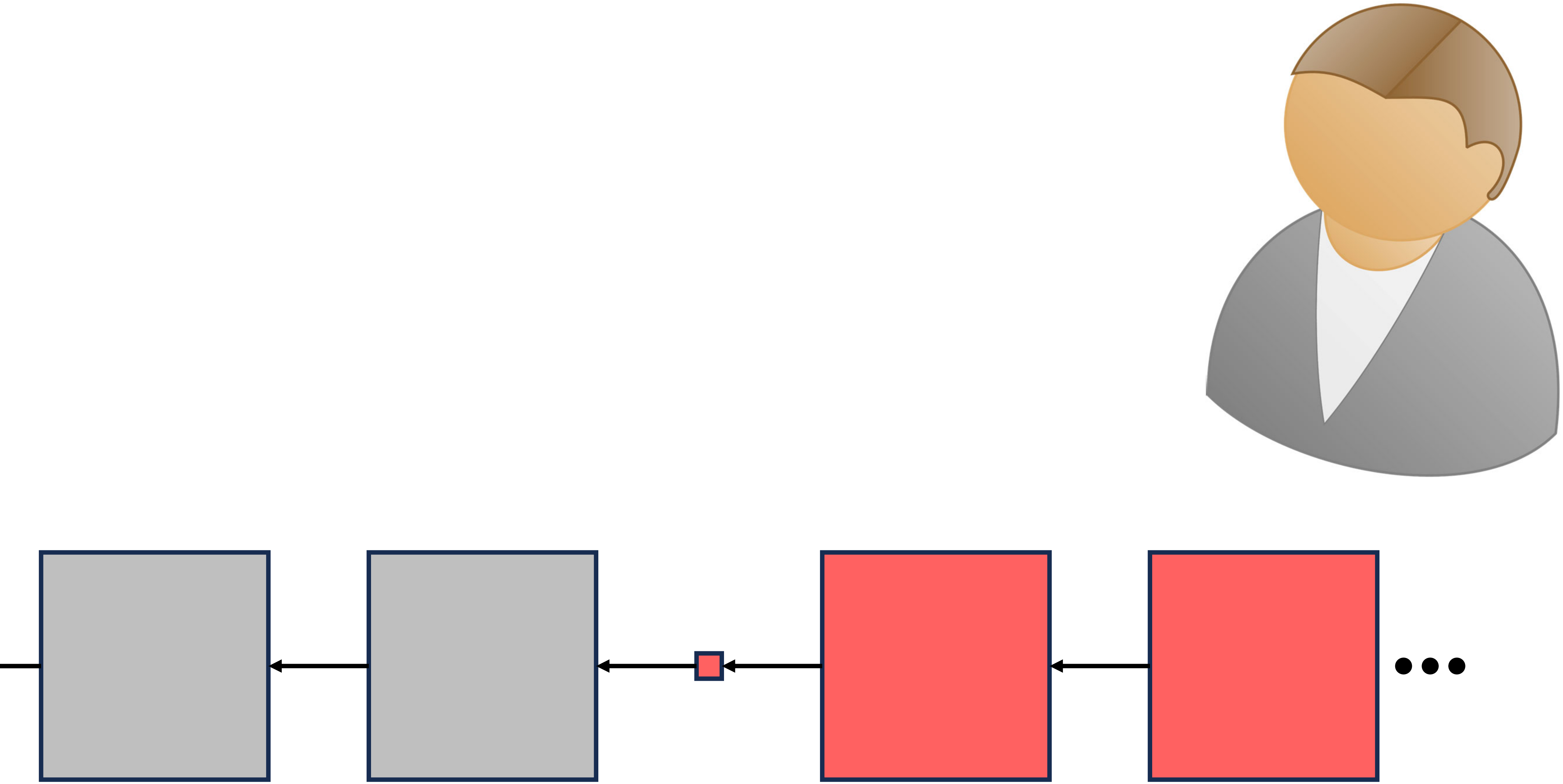


Deviation from honest strategy

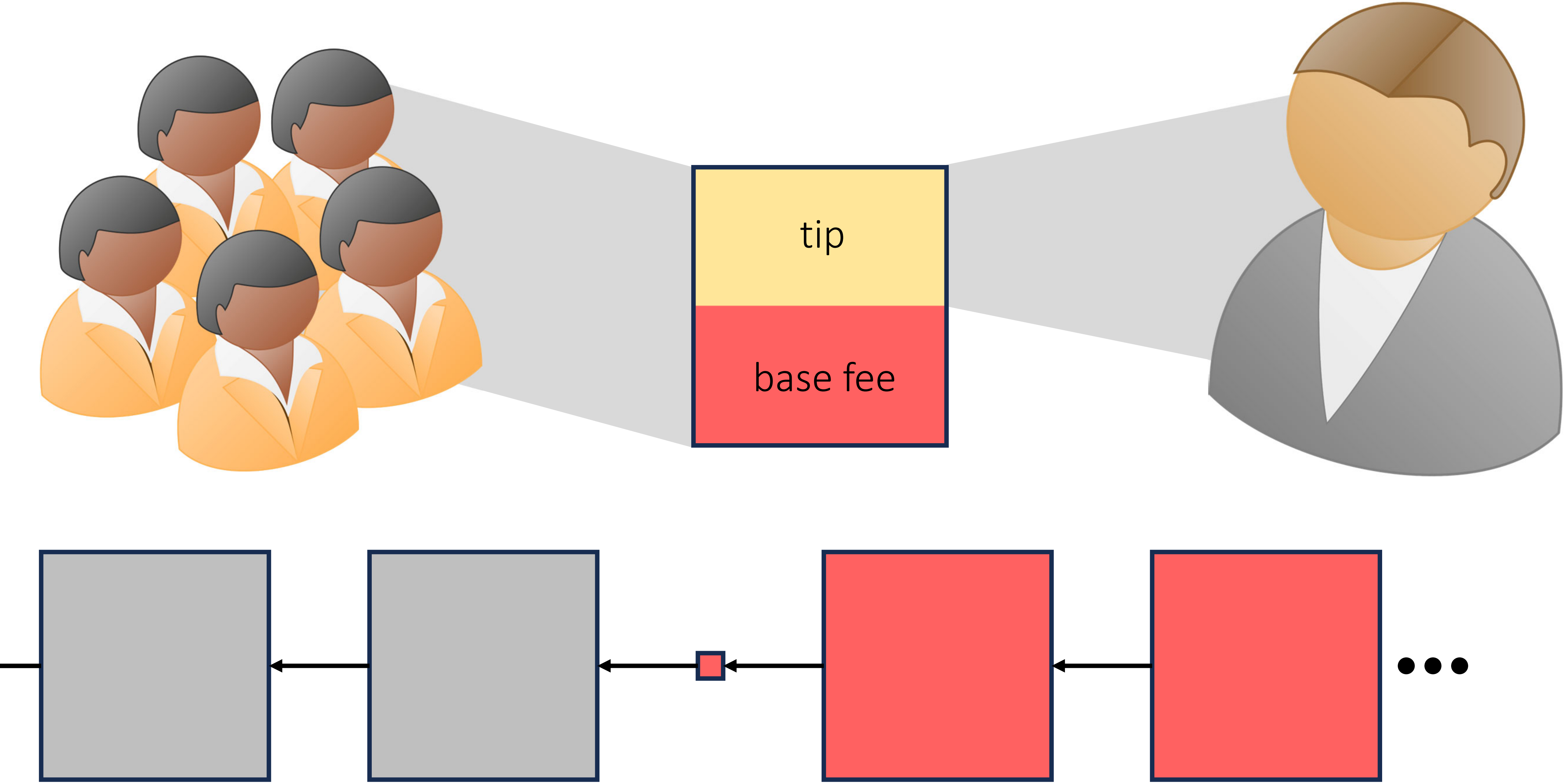




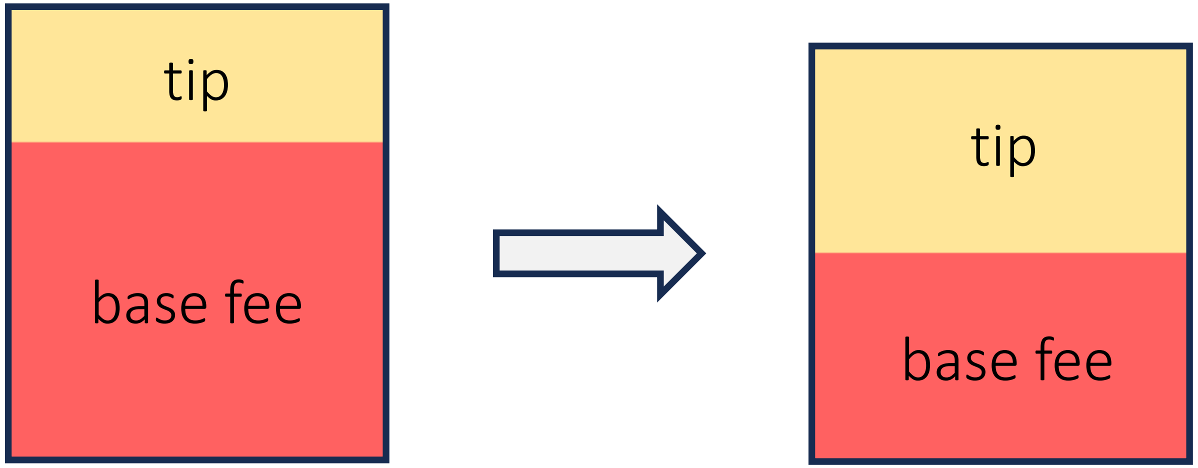
Deviation from honest strategy



Deviation from honest strategy

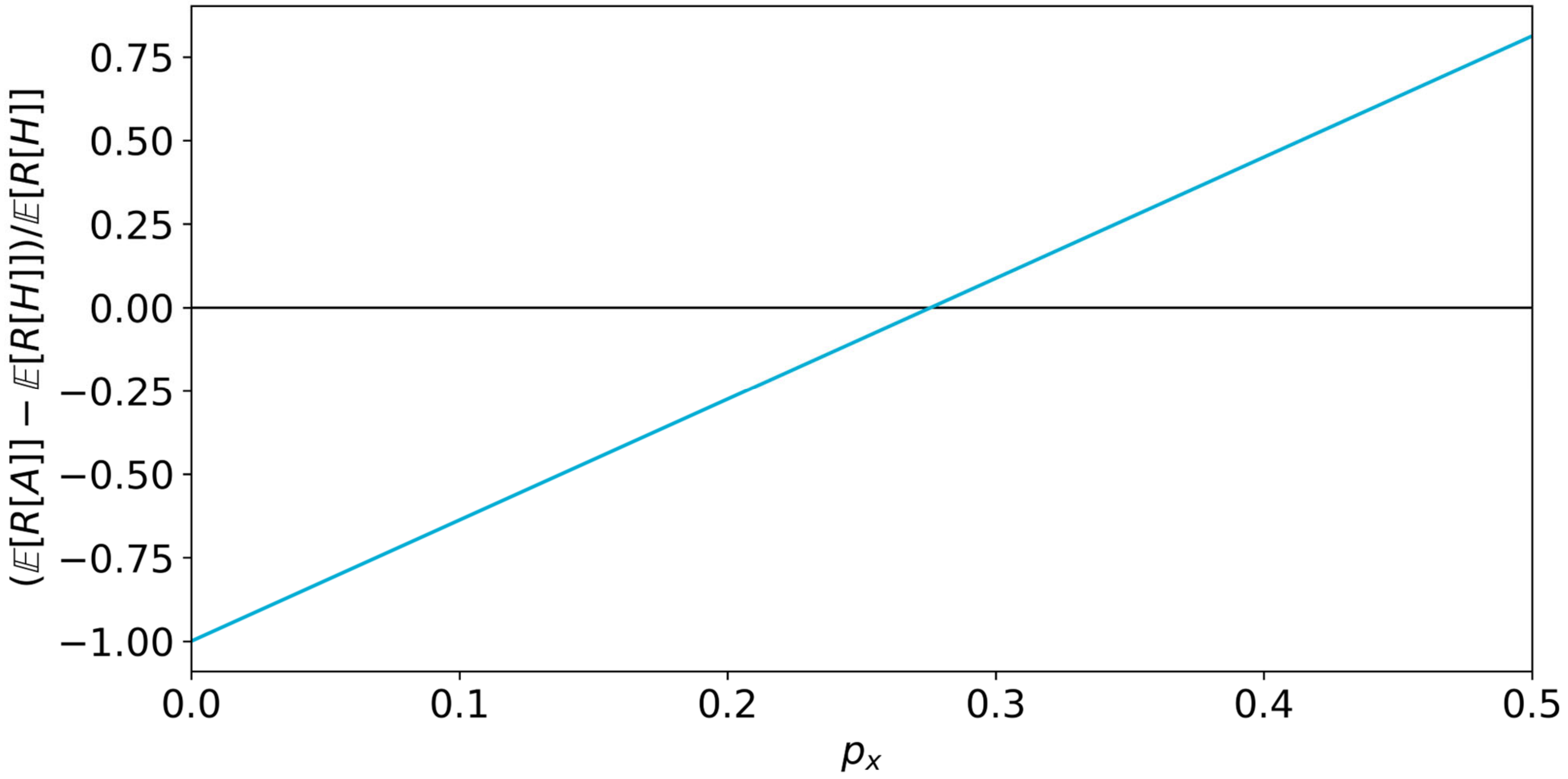


Profitability of deviation



users and miners profit from collaboration

Profitability of deviation

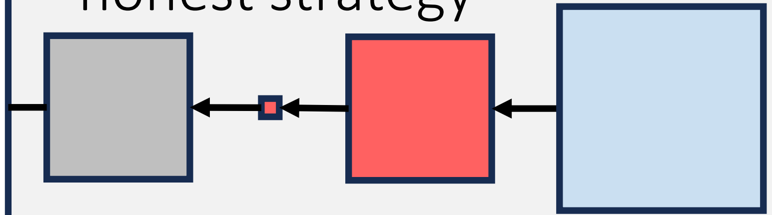


Effects on other miners

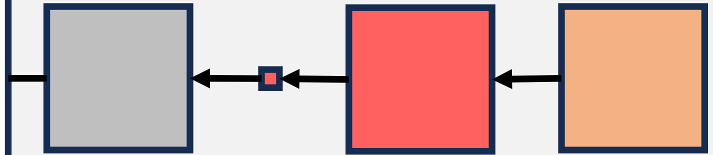
Effects on other miners

Joining the attack

honest strategy



deviation from honest strategy

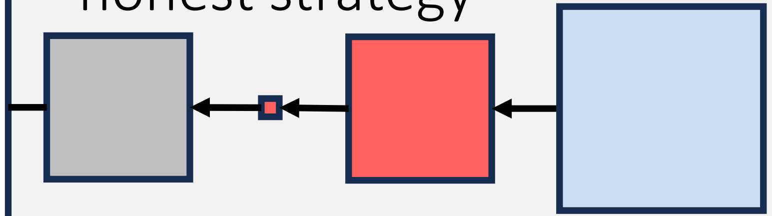


it can be rational for a smaller miner to join the attack it observes

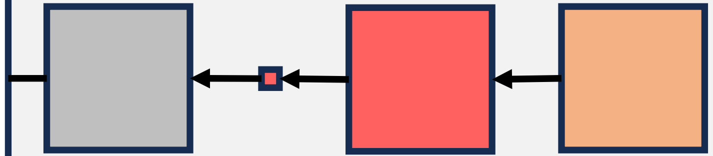
Effects on other miners

Joining the attack

honest strategy



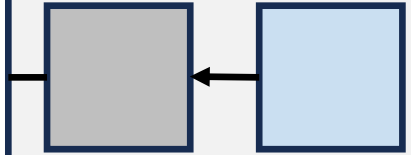
deviation from honest strategy



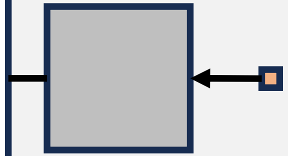
it can be rational for a smaller miner to join the attack it observes

Starting the attack

honest strategy



deviation from honest strategy



it can be rational for a smaller miner to start the attack it know is coming

Mitigating the Problem

Mitigation

decrease adjustment parameter

Mitigation

decrease adjustment parameter

reacts to slowly too changes in demand

Mitigation

decrease adjustment parameter

reacts to slowly too changes in demand

instead of burning base fee,
divert base fee to a special pool

Mitigation

decrease adjustment parameter

reacts to slowly too
changes in demand

instead of burning base fee,
divert base fee to a special pool

does not tackle the issue

Mitigation

decrease adjustment parameter

reacts to slowly too changes in demand

instead of burning base fee, divert base fee to a special pool

does not tackle the issue

use average of W previous block sizes instead of only previous block

Mitigation

decrease adjustment parameter

reacts to slowly too changes in demand

instead of burning base fee, divert base fee to a special pool

does not tackle the issue

use average of W previous block sizes instead of only previous block

exacerbates problem

Mitigation

decrease adjustment parameter

reacts to slowly too changes in demand

instead of burning base fee, divert base fee to a special pool

does not tackle the issue

use average of W previous block sizes instead of only previous block

exacerbates problem

use a geometric sequence as weights to average the history of block sizes

Mitigation

decrease adjustment parameter

reacts to slowly too changes in demand

instead of burning base fee, divert base fee to a special pool

does not tackle the issue

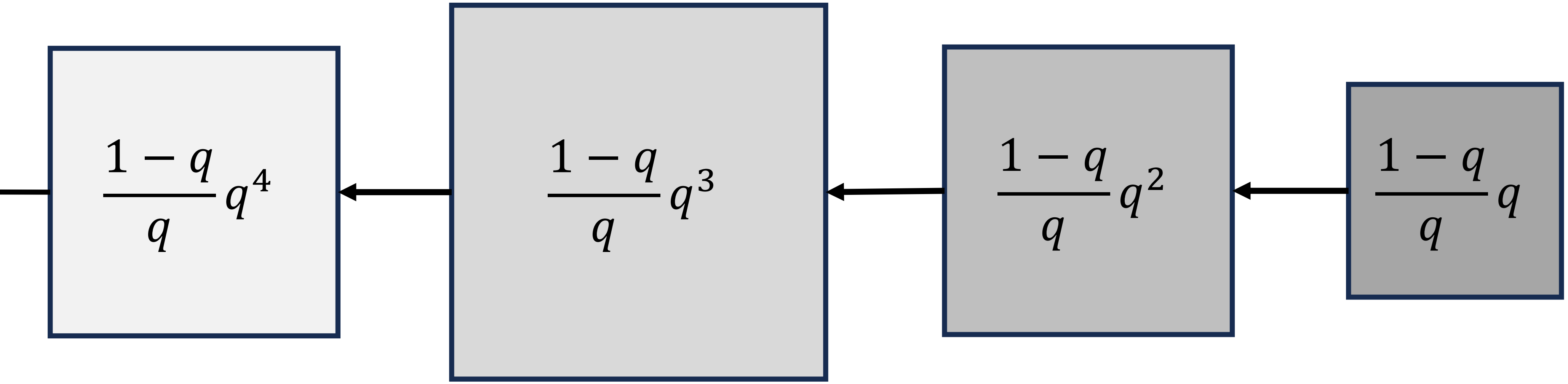
use average of W previous block sizes instead of only previous block

exacerbates problem

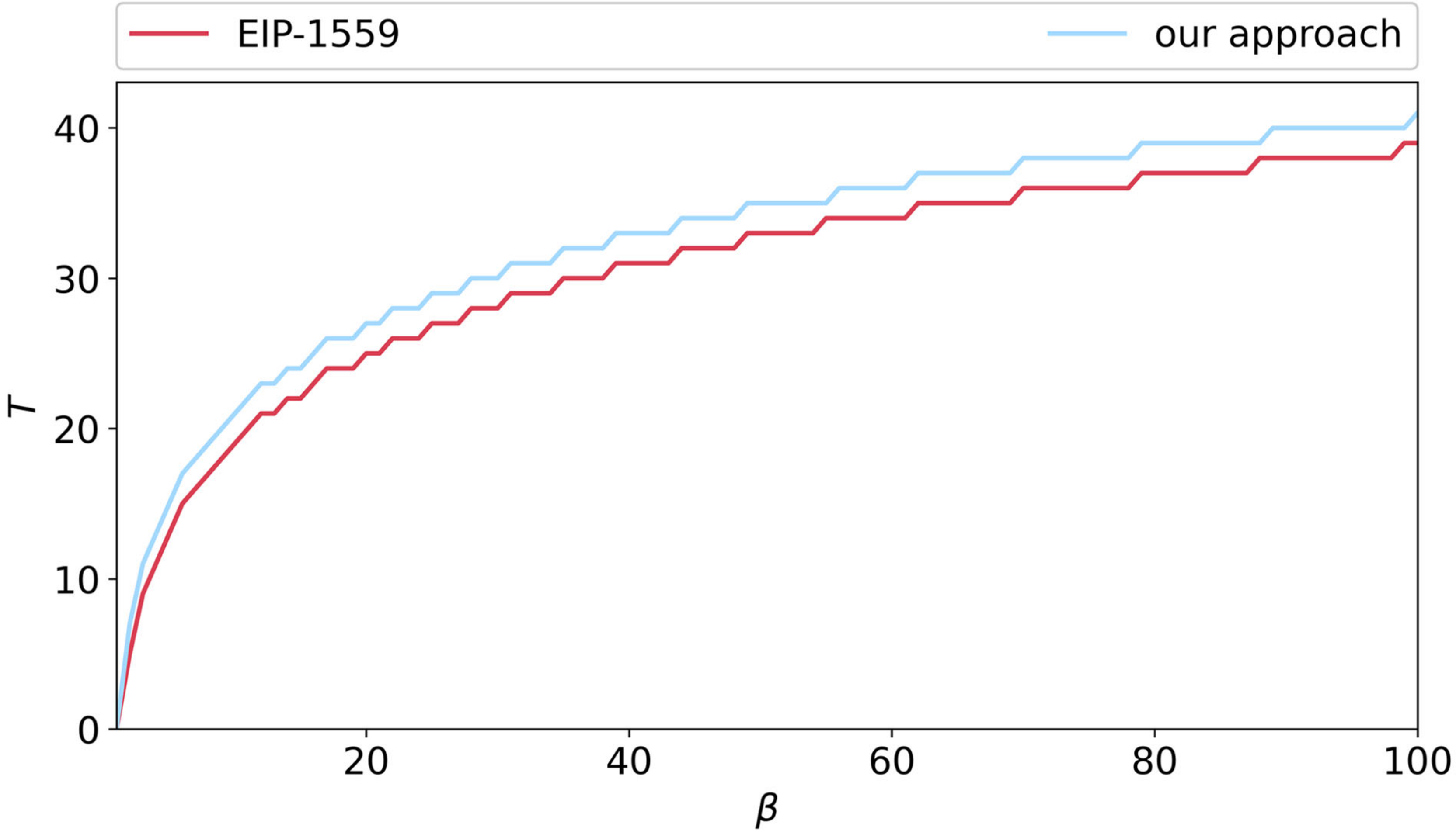
use a geometric sequence as weights to average the history of block sizes

our approach

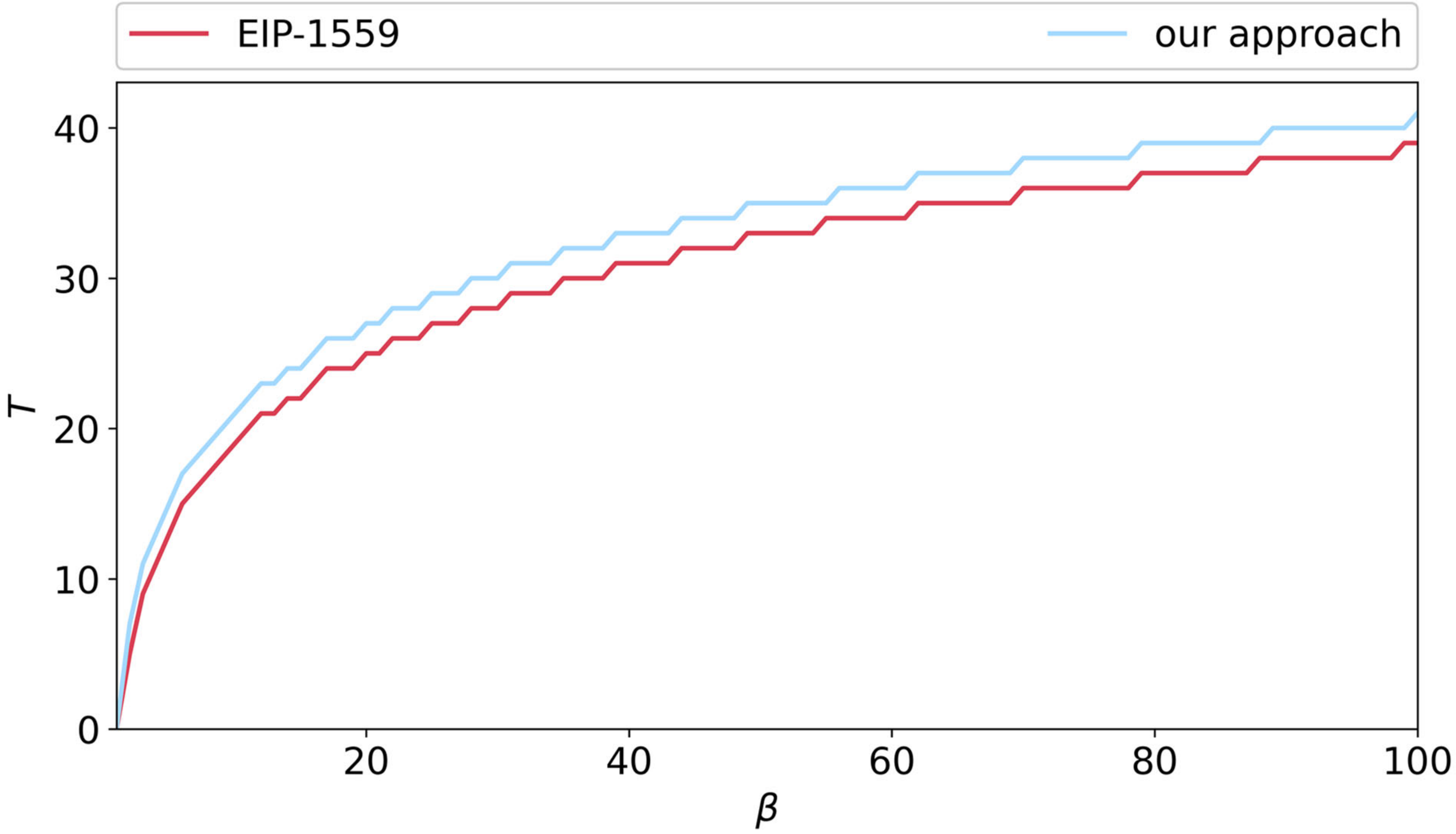
Mitigation



Mitigation

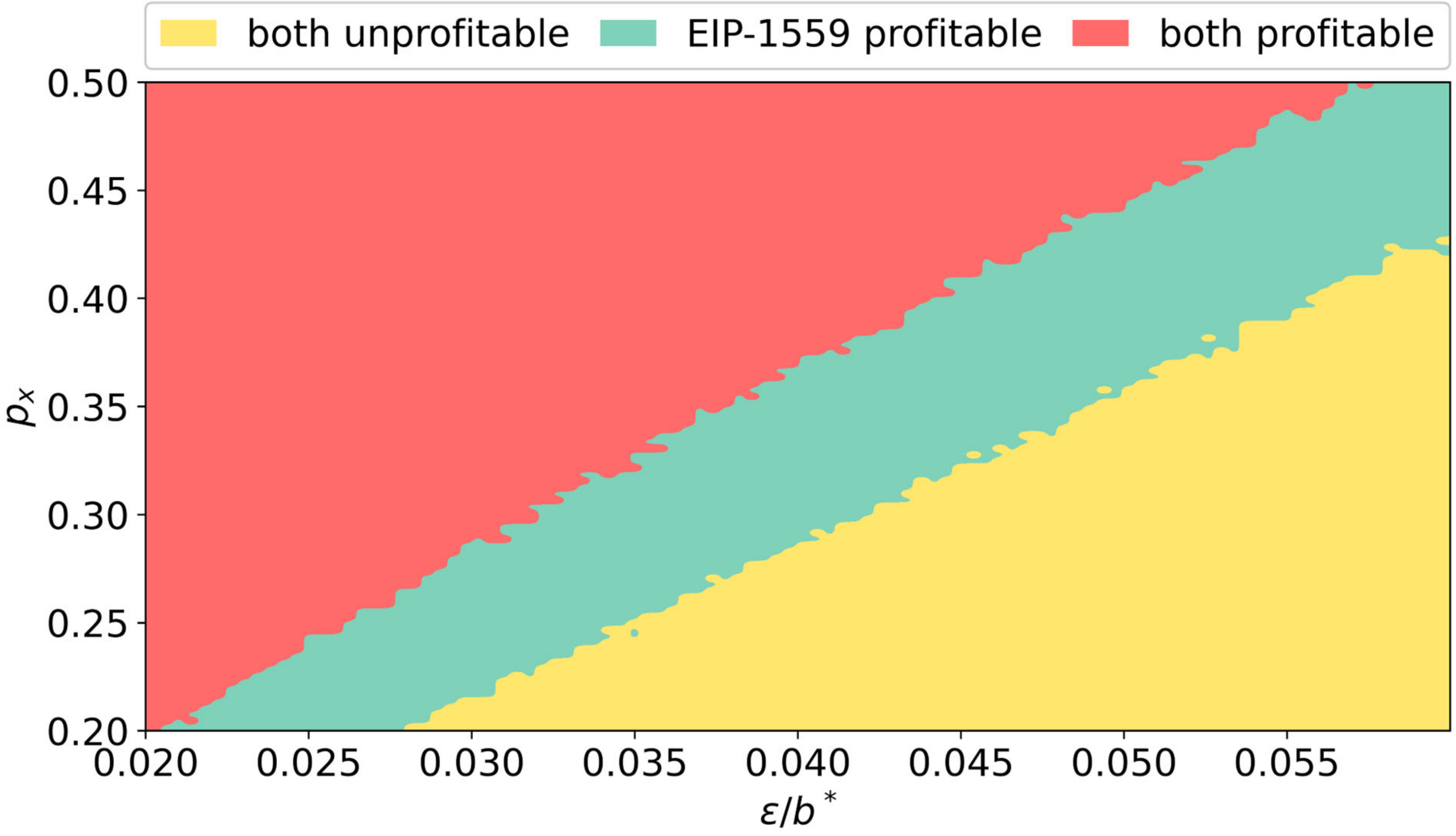


Mitigation



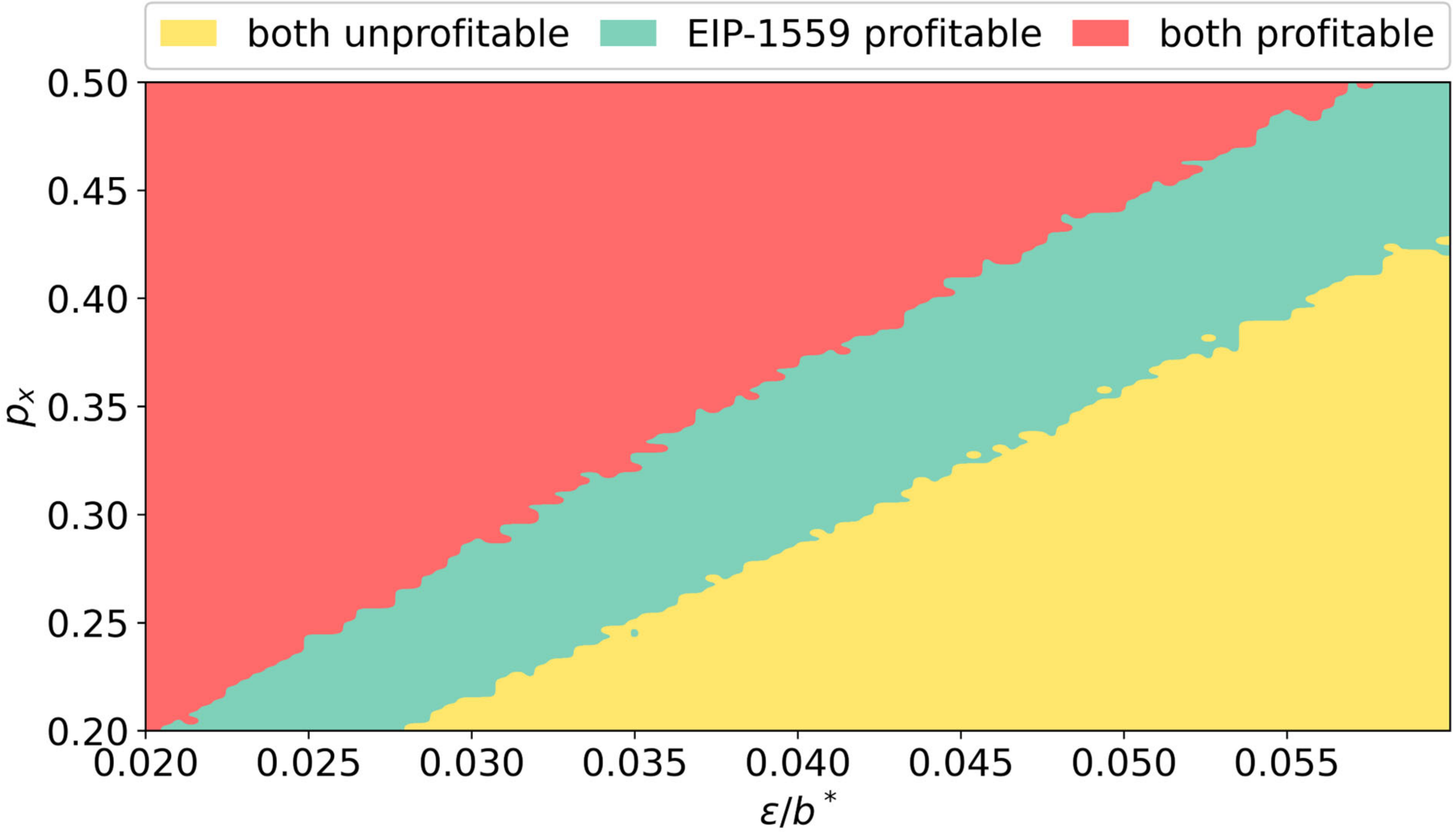
our proposed mitigation adjusts to new demand almost as quickly as EIP-1559

Mitigation



both unprofitable
EIP-1559 profitable
both profitable
0.50
0.45
0.40
0.35
0.30
0.25
0.20
p_x
0.020
0.025
0.030
0.035
0.040
0.045
0.050
0.055
ε/b^*

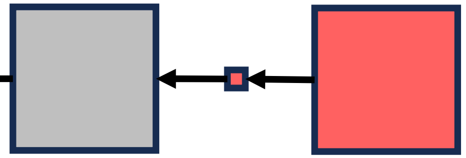
Mitigation



our proposed mitigation prevents the attack in a significant part of the parameter space

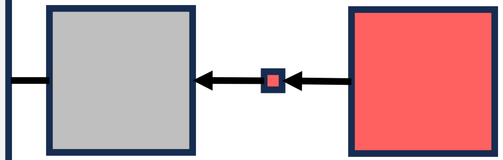
Conclusion

it can be rational to deviate from the honest strategy under conservative assumptions

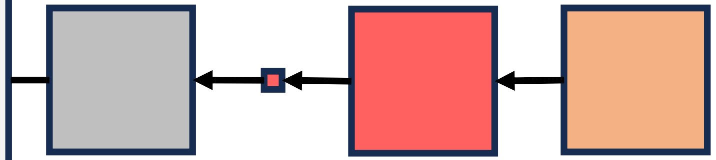


Conclusion

it can be rational to deviate from the honest strategy under conservative assumptions

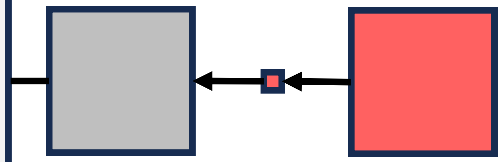


without assuming collaboration, it can be rational for smaller miners to join or even start an attack

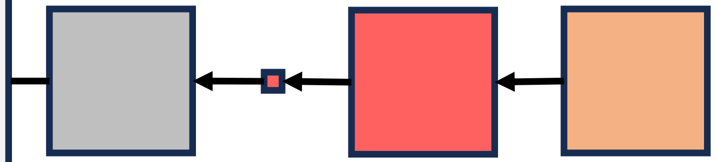


Conclusion

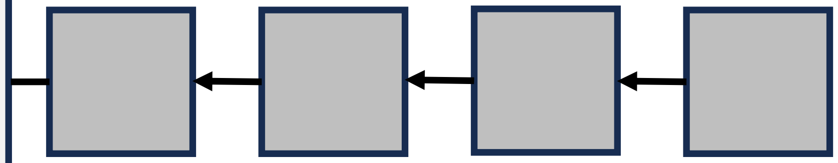
it can be rational to deviate from the honest strategy under conservative assumptions



without assuming collaboration, it can be rational for smaller miners to join or even start an attack

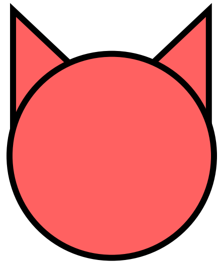


we proposed mitigation reduces the profitability and often even prevents the attack altogether



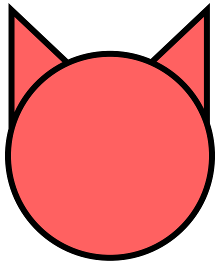
Open problems

finding the optimal attack



Open problems

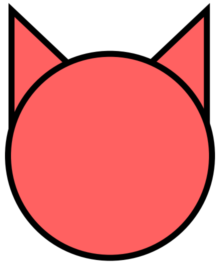
finding the optimal attack



in-depth analysis of proposed mitigation

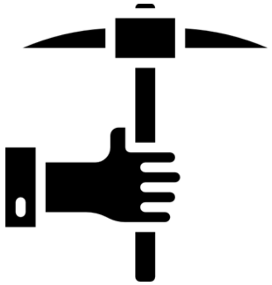
Open problems

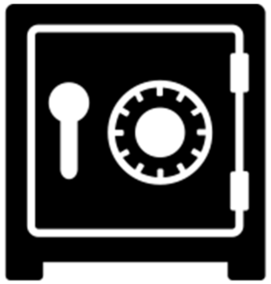
finding the optimal attack



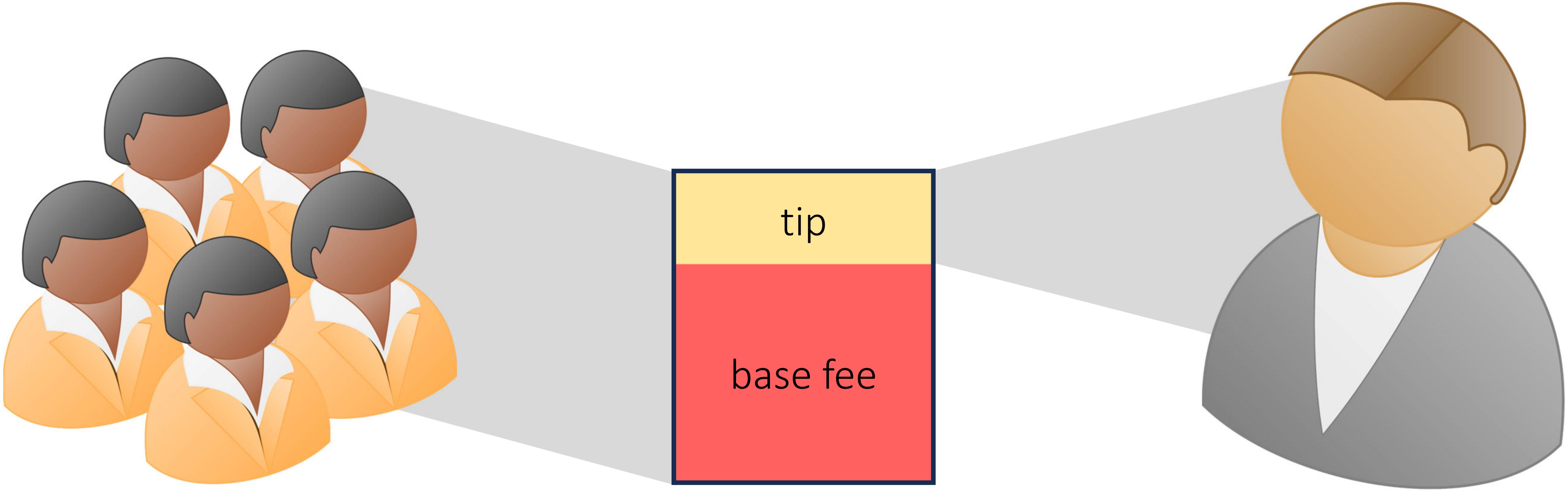
in-depth analysis of proposed mitigation

differences between proof-of-work
and proof-of-stake





Base Fee Manipulation In Ethereum's EIP-1559 Transaction Fee Mechanism



hlioba@ethz.ch

@liobaheimbach