NETHERMIND

From wallet to chain

A bridge of two worlds on an Ethereum transaction

Michał Zając
Nethermind

How Ethereum can accommodate institutional clients?

Accountability
Who is responsible for adding blocks to the chain?
Who is responsible for censoring transactions?

How Ethereum can accommodate institutional clients?

Accountability
Who is responsible for adding blocks to the chain?
Who is responsible for censoring transactions?

Integrity
How finality of blocks is reached and how robust Ethereum finality is?

How Ethereum can accommodate institutional clients?

Accountability
Who is responsible for adding blocks to the chain?
Who is responsible for censoring transactions?

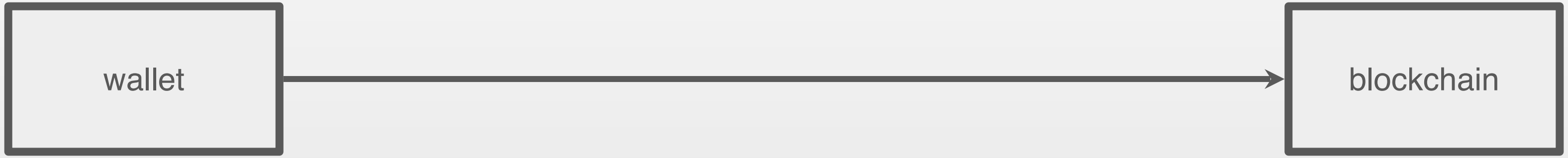
Integrity
How finality of blocks is reached and how robust Ethereum finality is?

Auditability
How traceable are Ethereum transactions?
Can we combine transaction privacy with auditability?

Ethereum transaction lifecycle – an overview

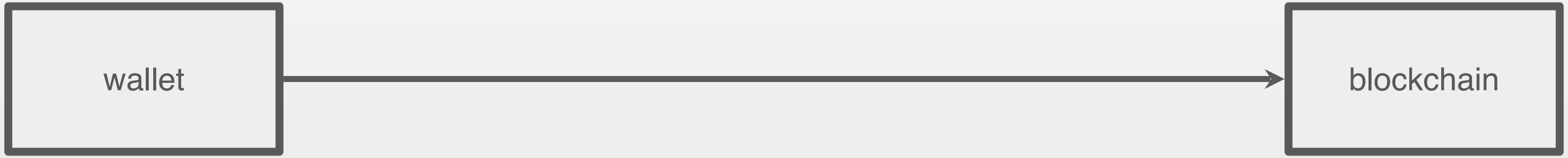
wallet
blockchain

Ethereum transaction lifecycle – an overview



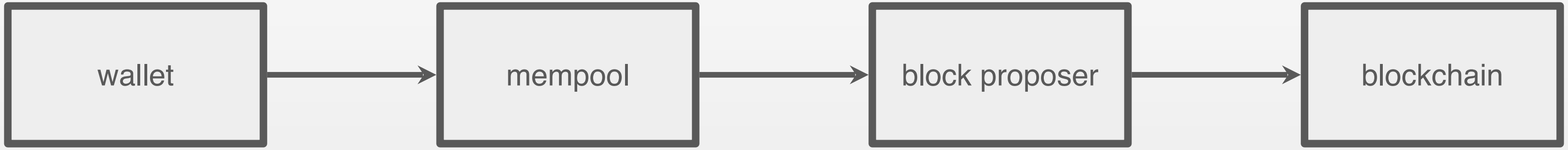
Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Exchange 1 ETH to USDC
Fee: 100 gwei

Ethereum transaction lifecycle – an overview



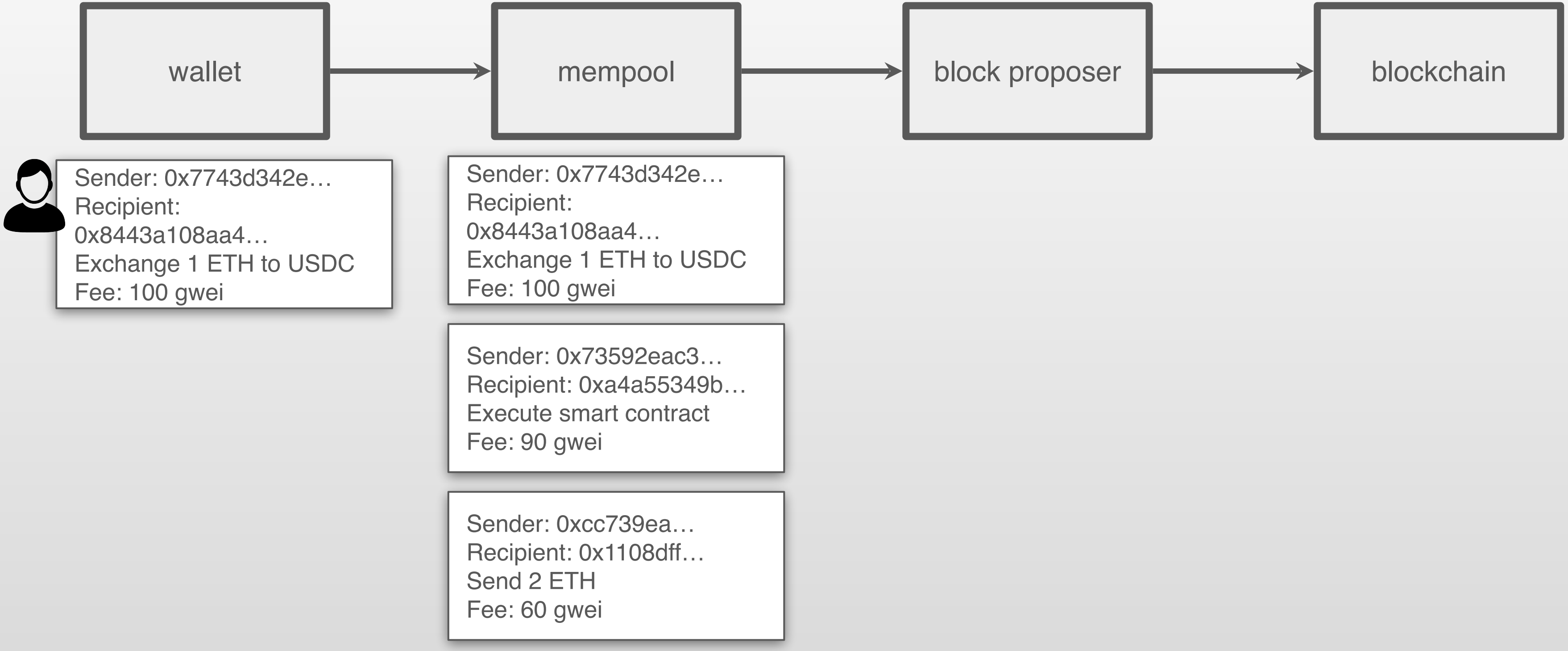
Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Exchange 1 ETH to USDC
Fee: 100 gwei

Ethereum transaction lifecycle – an overview



Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Ethereum transaction lifecycle – an overview



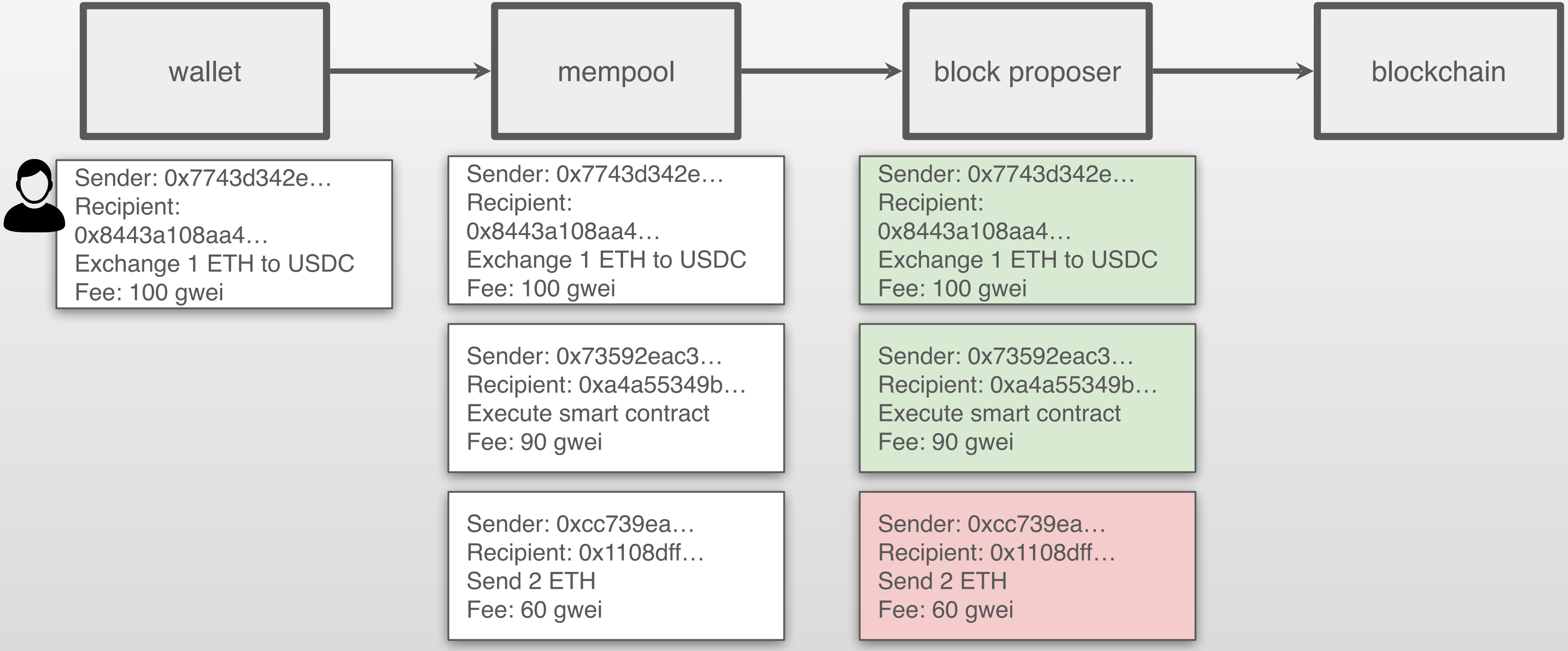
Sender: 0x7743d342e…
Recipient: 0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x7743d342e…
Recipient: 0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Ethereum transaction lifecycle – an overview



wallet

mempool

block proposer

blockchain

Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

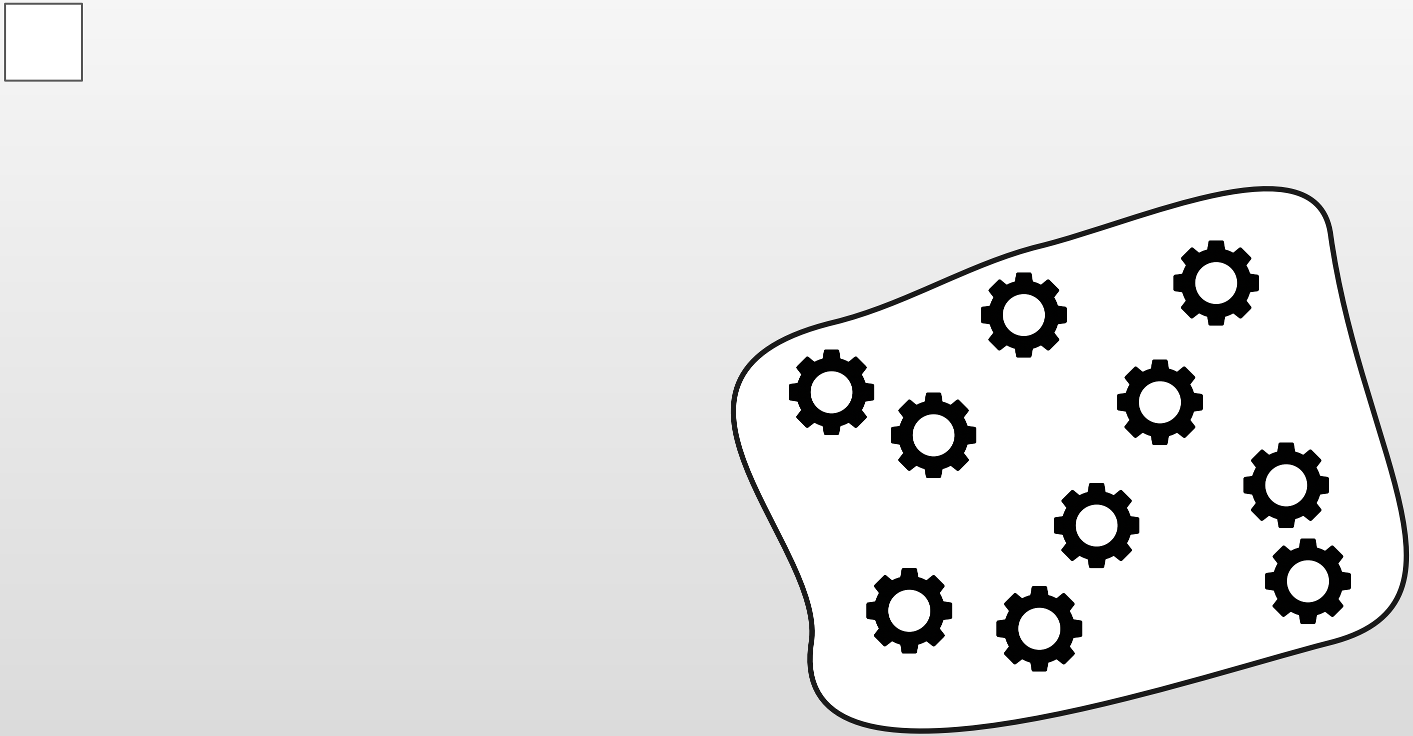
Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

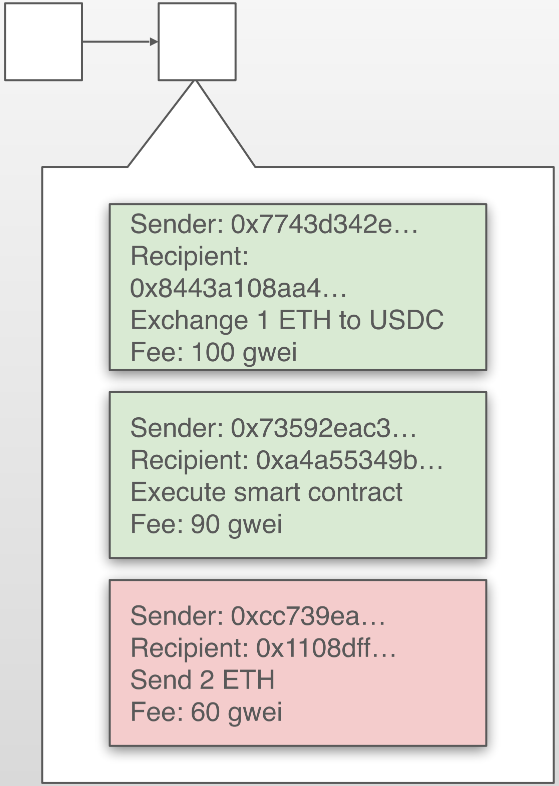
Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Ethereum transaction lifecycle – an overview



Ethereum transaction lifecycle – an overview

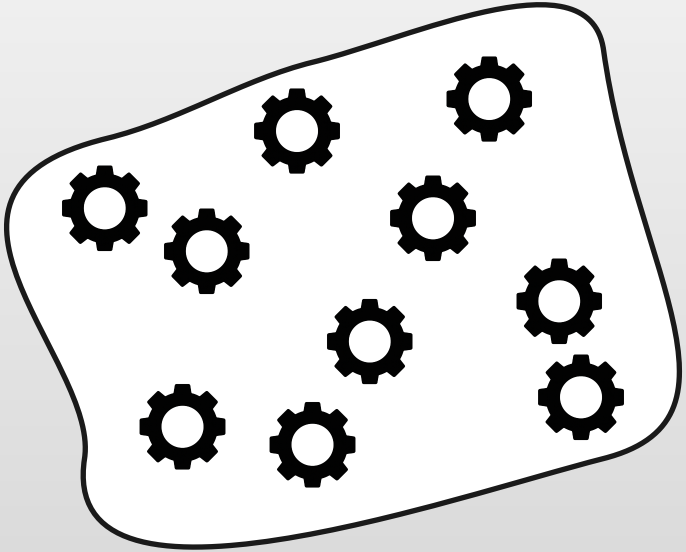


Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

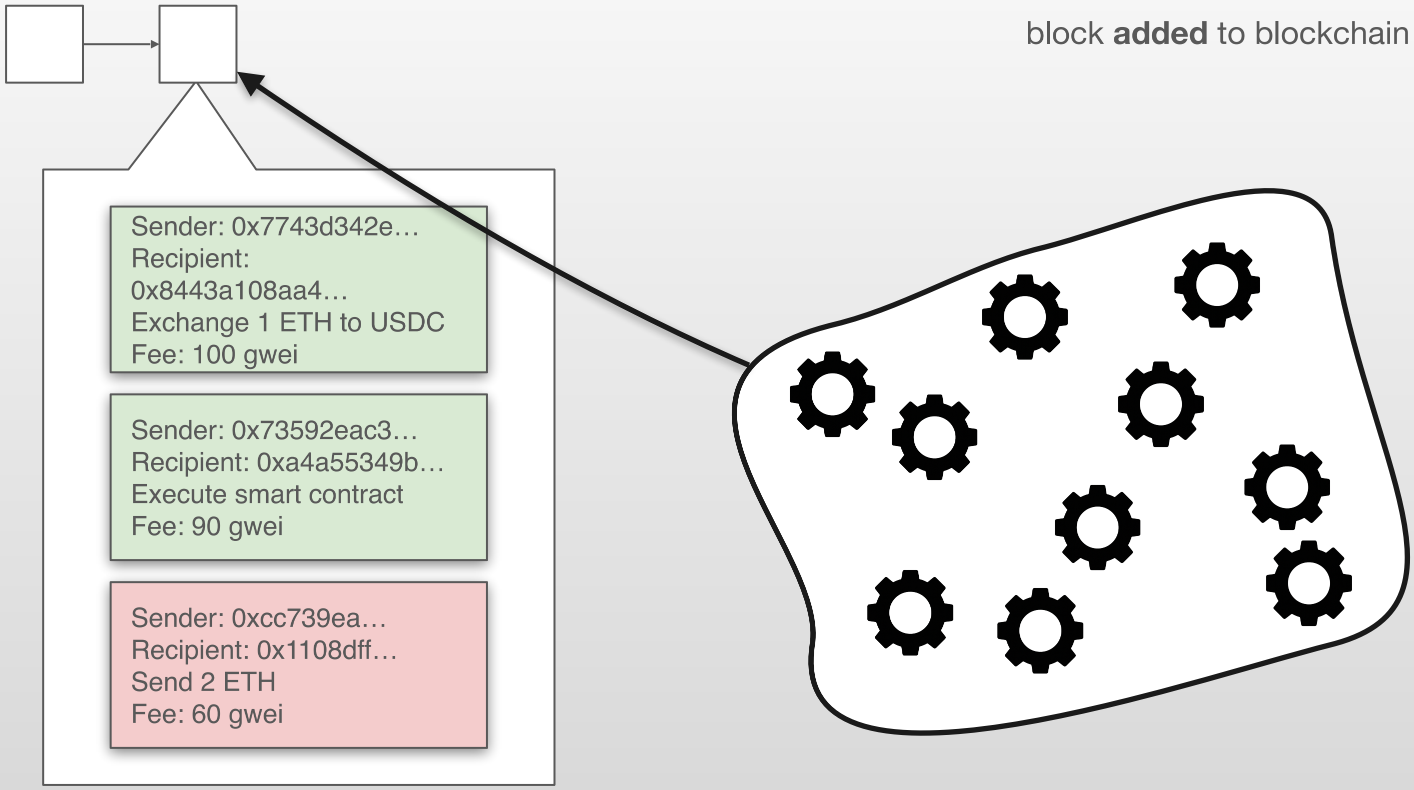
Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

block **added** to blockchain



Ethereum transaction lifecycle – an overview



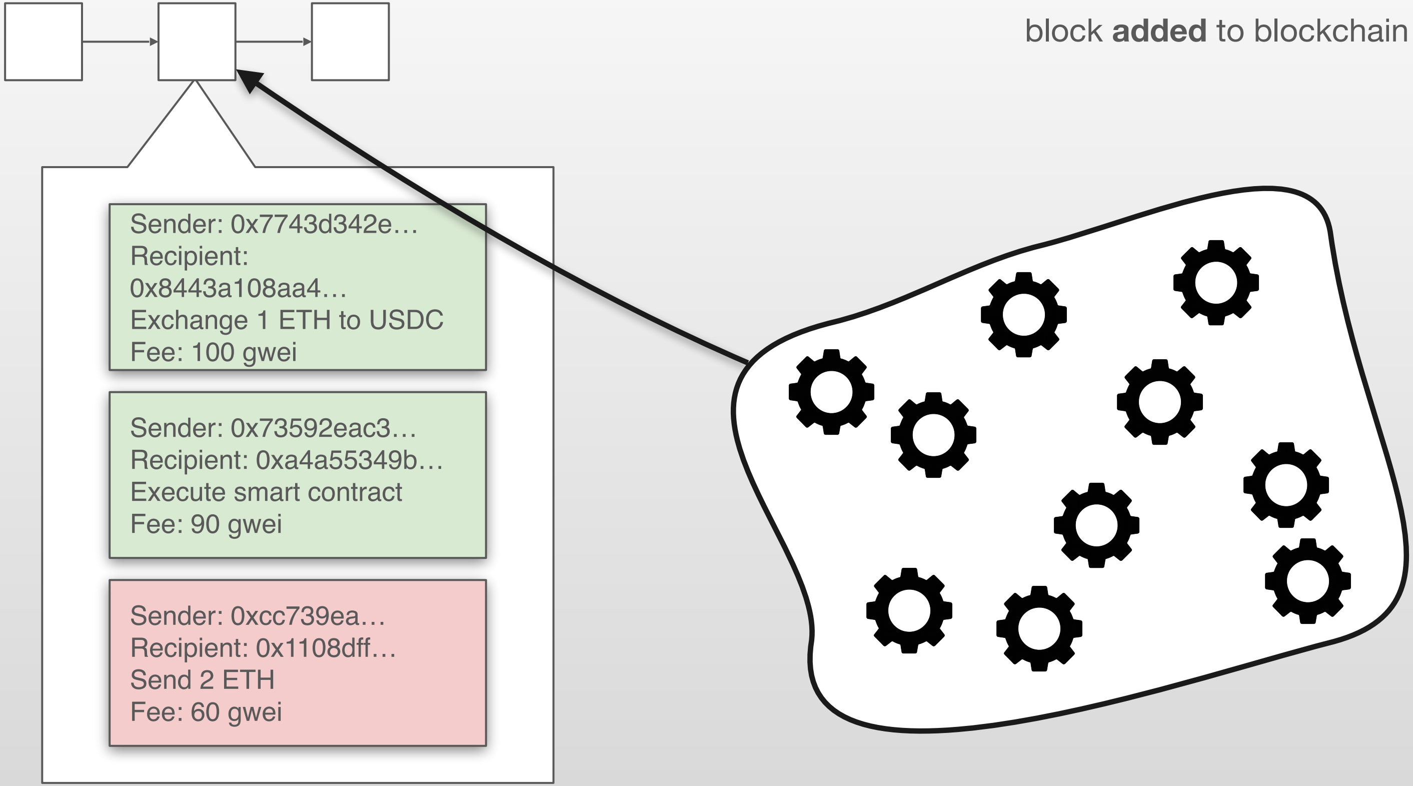
block **added** to blockchain

Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Ethereum transaction lifecycle – an overview



block **added** to blockchain

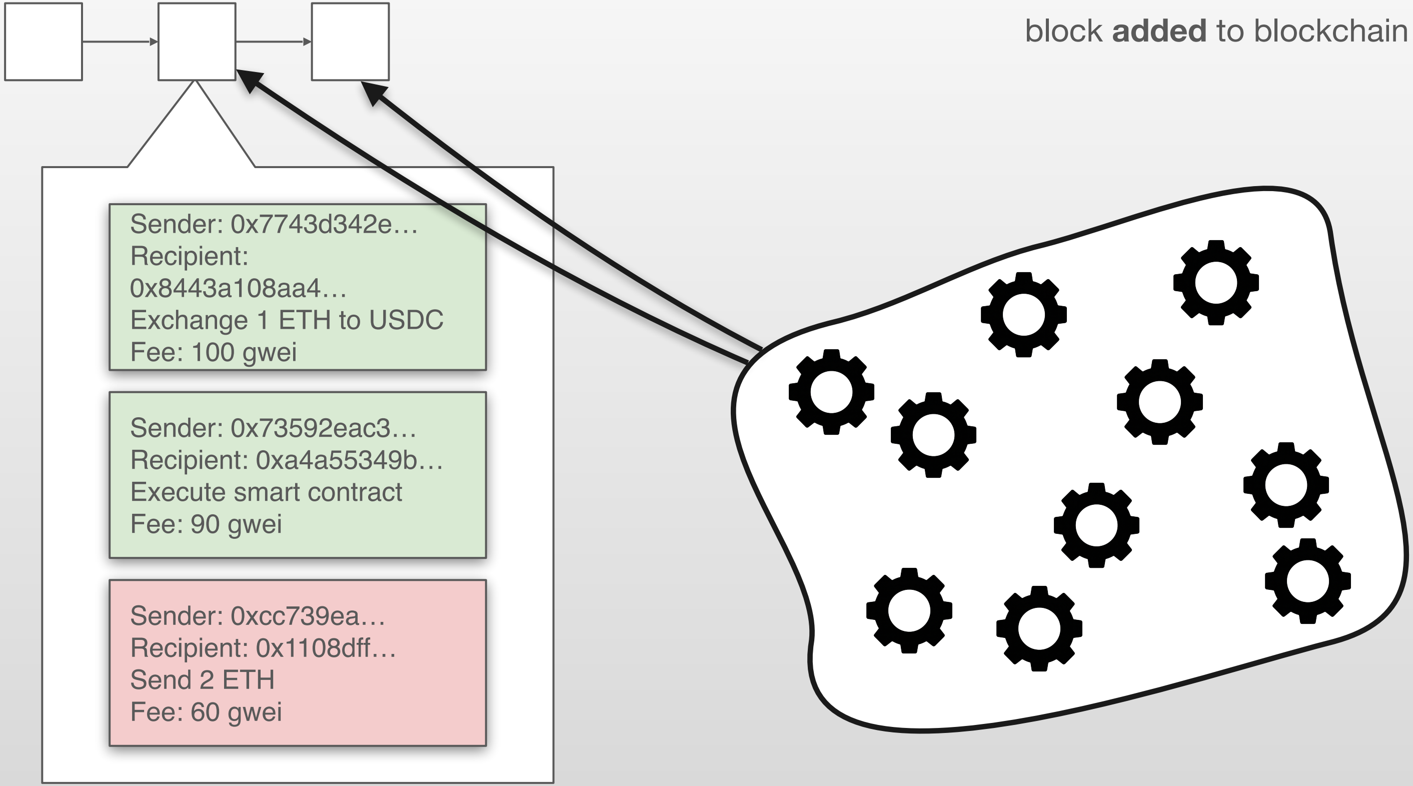
Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Ethereum transaction lifecycle – an overview

block **added** to blockchain

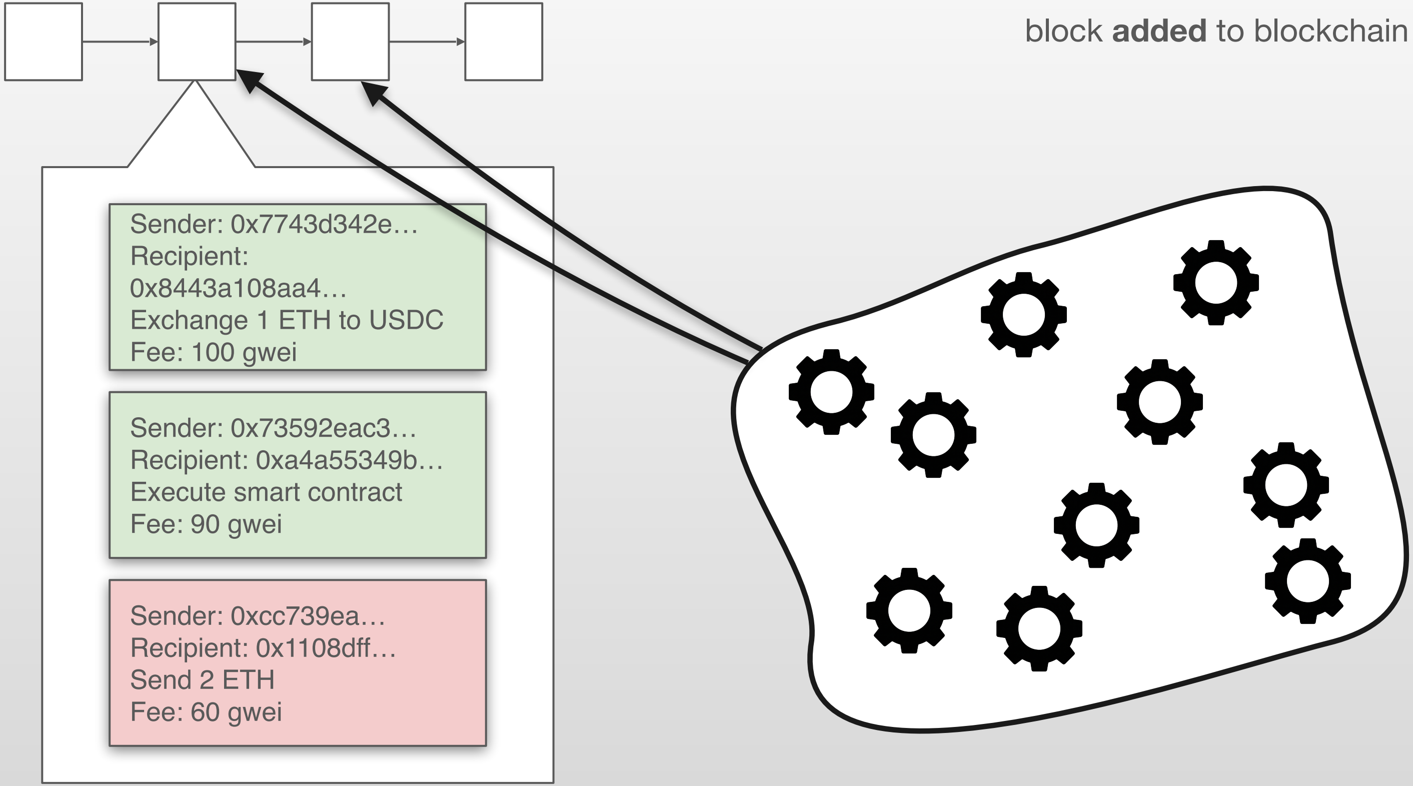


Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Ethereum transaction lifecycle – an overview



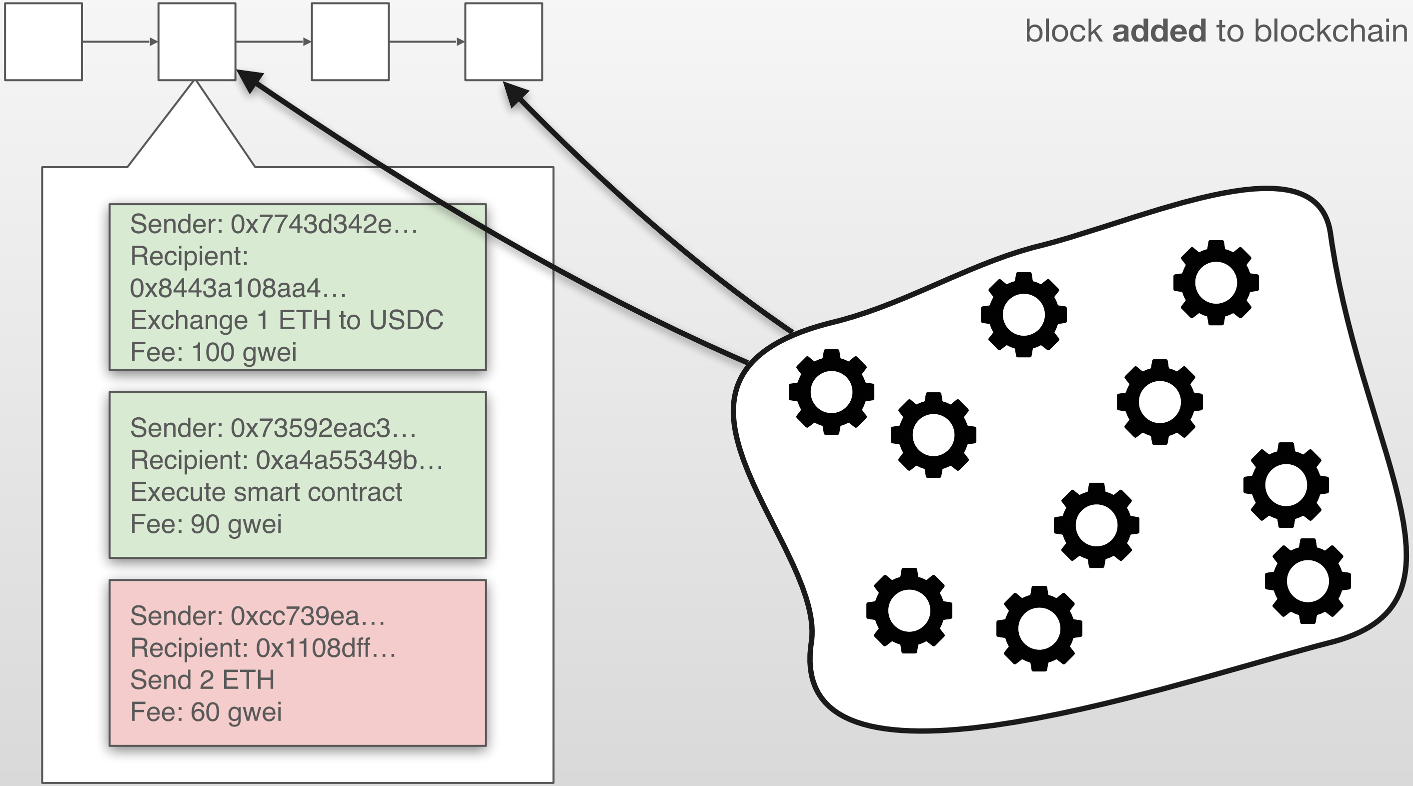
Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

block **added** to blockchain

Ethereum transaction lifecycle – an overview



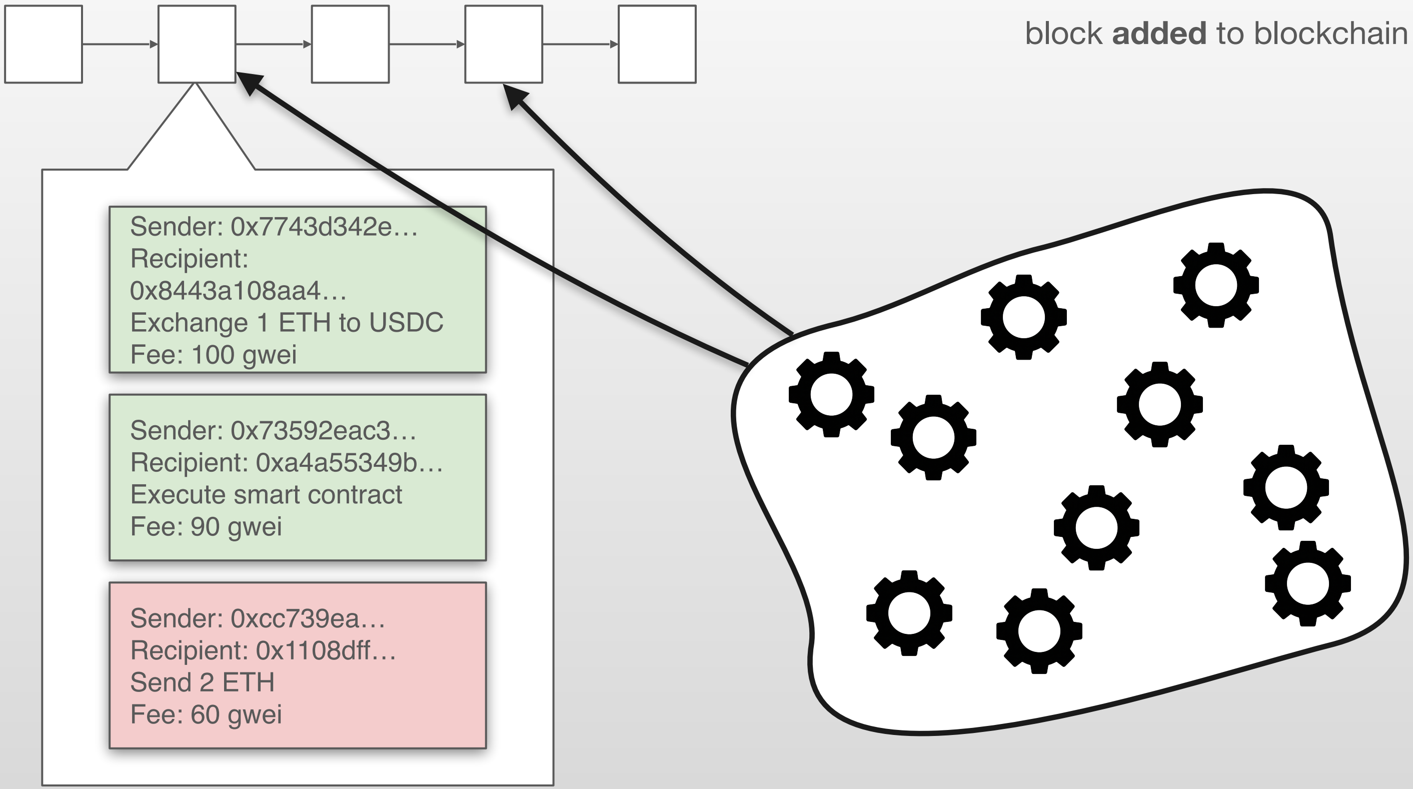
Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

block **added** to blockchain

Ethereum transaction lifecycle – an overview



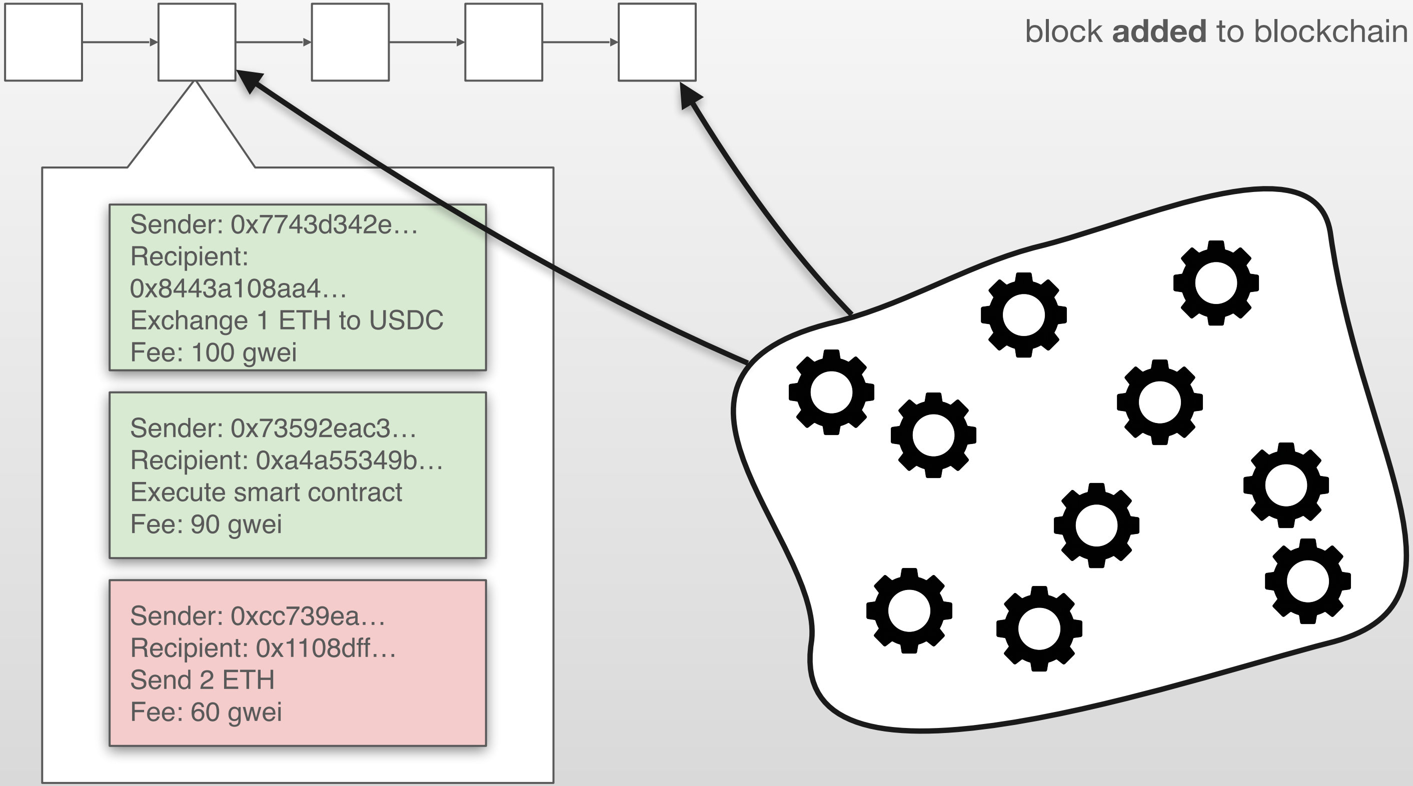
block **added** to blockchain

Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Ethereum transaction lifecycle – an overview



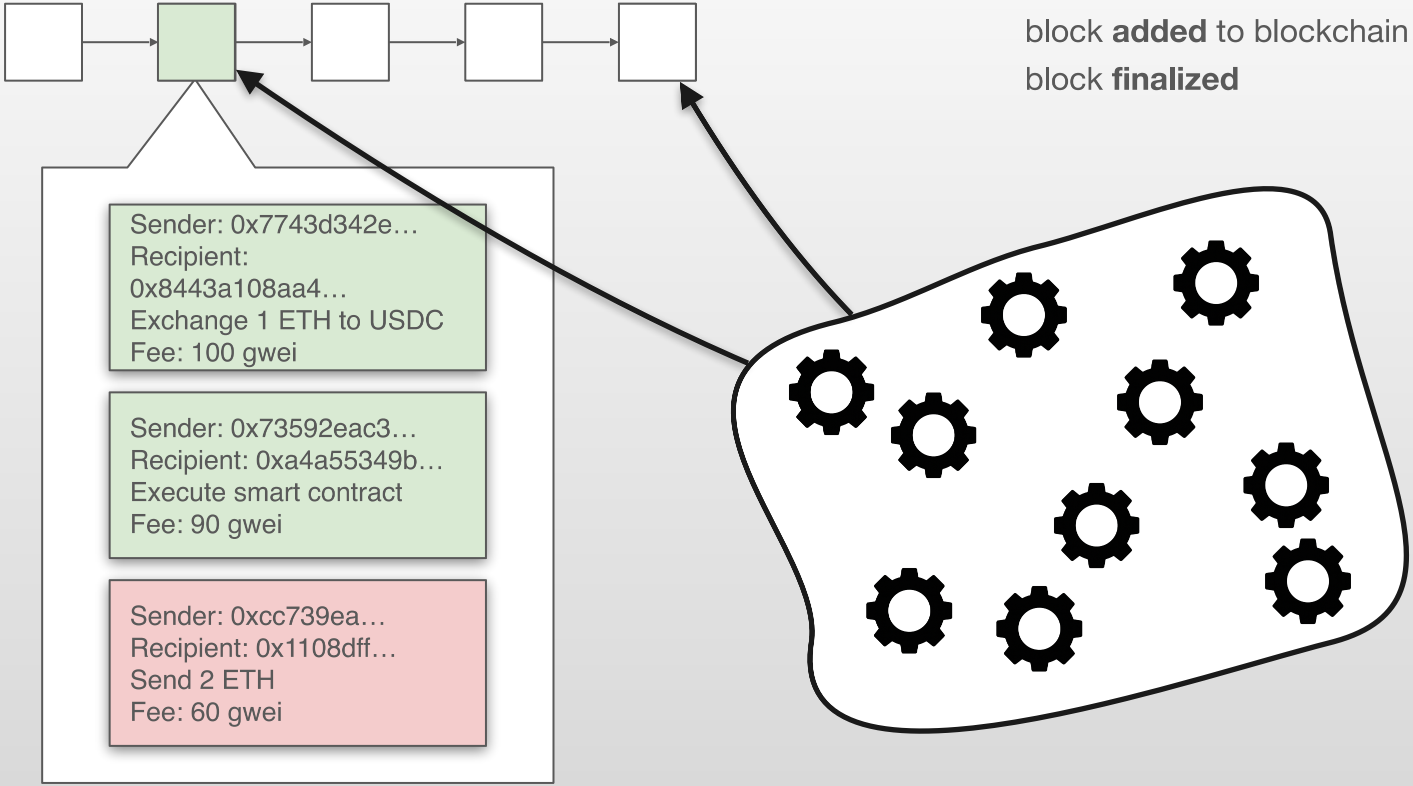
block **added** to blockchain

Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

Ethereum transaction lifecycle – an overview



Sender: 0x7743d342e…
Recipient:
0x8443a108aa4…
Exchange 1 ETH to USDC
Fee: 100 gwei

Sender: 0x73592eac3…
Recipient: 0xa4a55349b…
Execute smart contract
Fee: 90 gwei

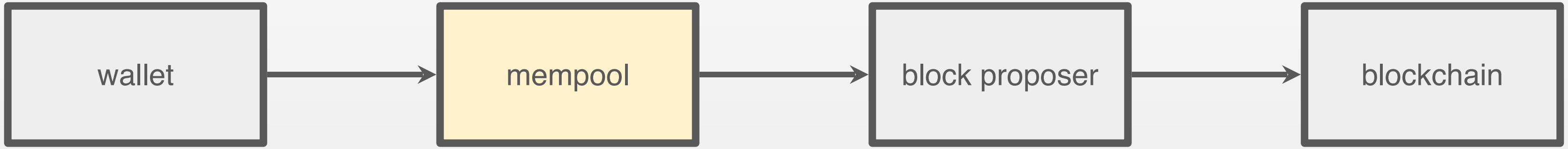
Sender: 0xcc739ea…
Recipient: 0x1108dff…
Send 2 ETH
Fee: 60 gwei

block **added** to blockchain

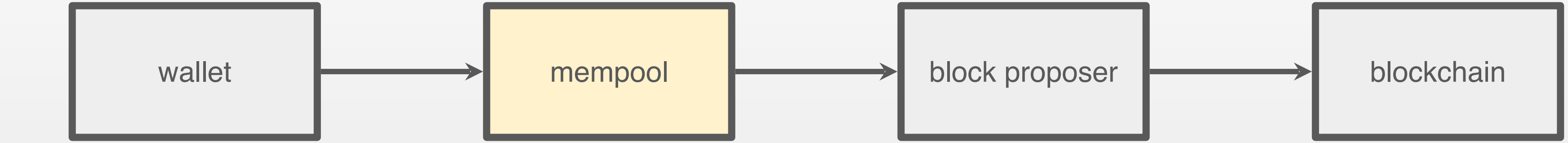
block **finalized**

Accountability

In the mempool

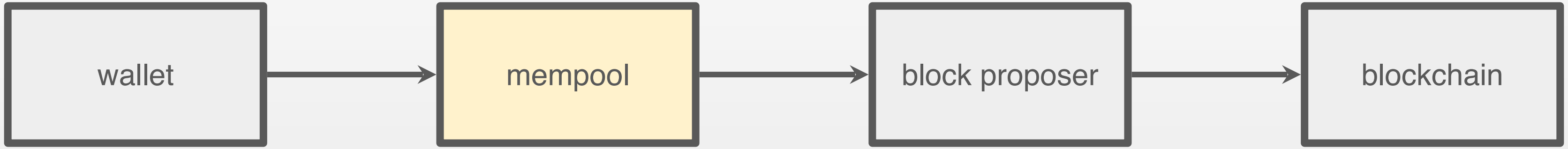


In the mempool



Sender: 0x234aae…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 120 gwei

In the mempool

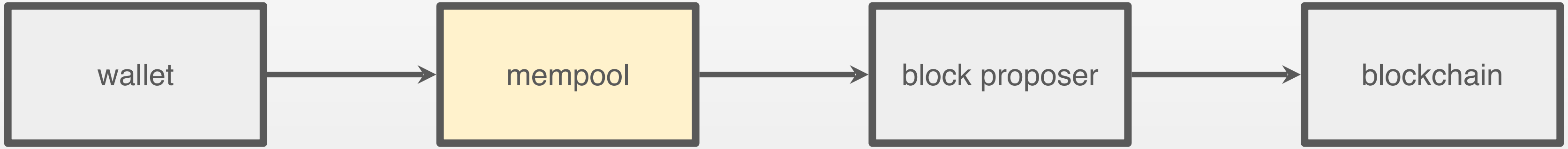


wallet → mempool → block proposer → blockchain

Sender: 0x234aae…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 120 gwei

Sender: 0x0934aad…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 140 gwei

In the mempool

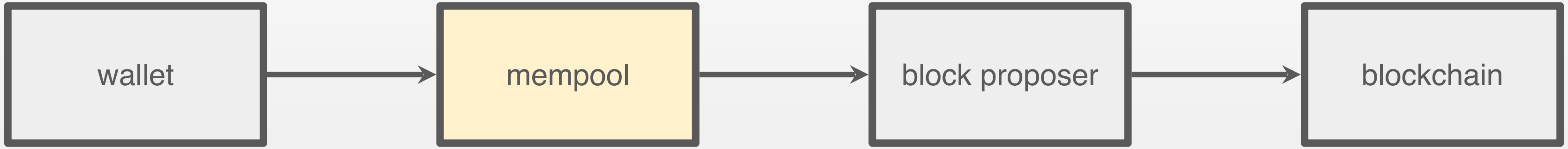


Sender: 0x234aae…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 120 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x0934aad…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 140 gwei

In the mempool



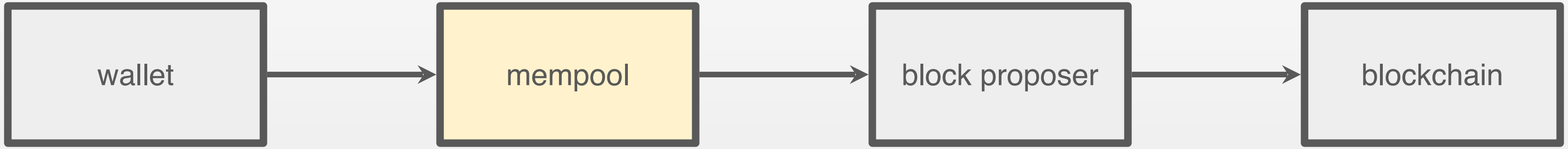
Sender: 0x234aae…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 120 gwei

Sender: 0x0934aad…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 140 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

In the mempool



Sender: 0x234aae…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 120 gwei

Sender: 0x0934aad…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 140 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

What is the power of a person who decides what and in what order ends up in a block?

In the mempool - Maximal Extractable Value (MEV)

Frontrunning: putting a transaction **before** the user's transaction

Sender: 0x234aae…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 120 gwei

In the mempool - Maximal Extractable Value (MEV)

Frontrunning: putting a transaction **before** the user’s transaction

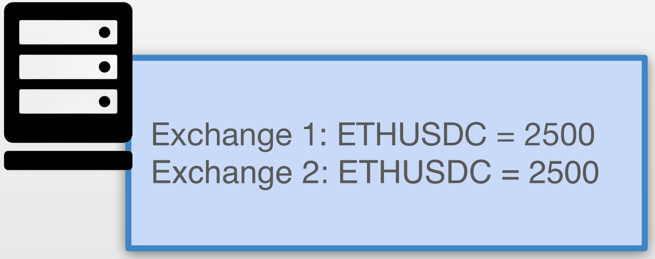
Sender: 0x234aae…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 120 gwei

Sender: 0x0934aad…
Recipient: 0x108eead4…
Amount 3ETH
Buy NFT
Fee: 140 gwei

“Same” transactions - one pays more fees
Guess which will be included first?

In the mempool - Maximal Extractable Value (MEV)

Backrunning: putting a transaction **after** the user's transaction



Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

In the mempool - Maximal Extractable Value (MEV)

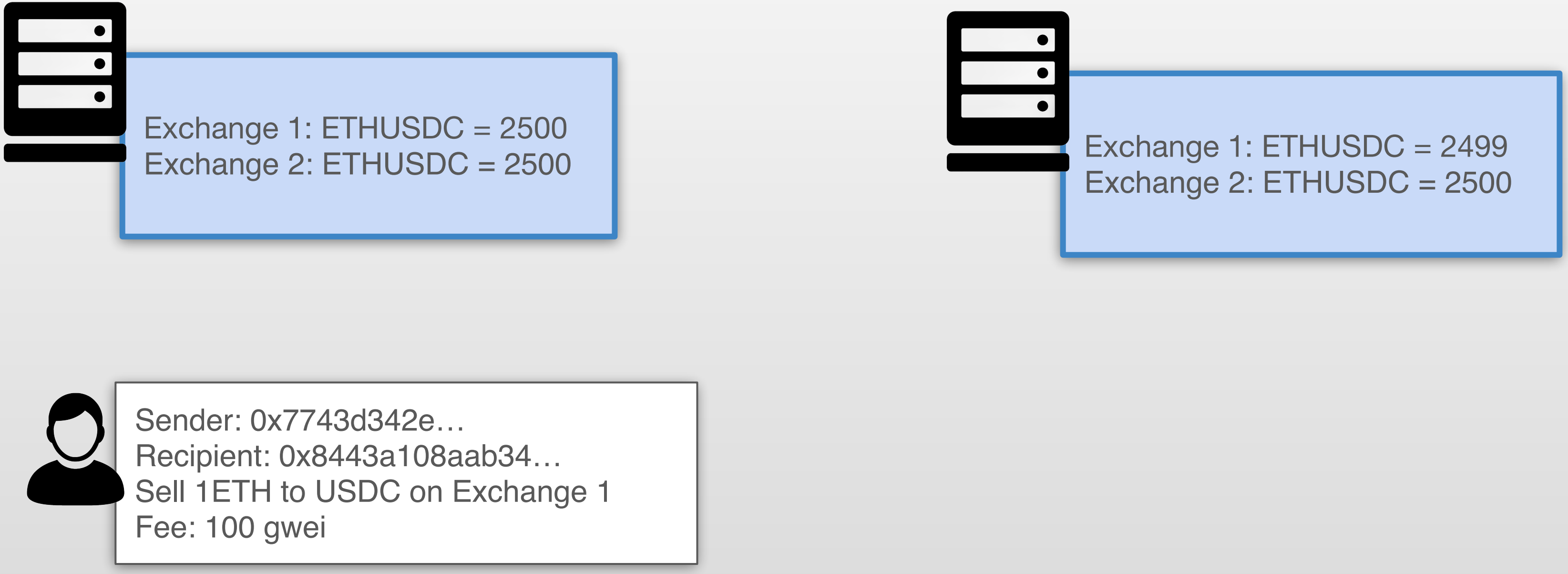
Backrunning: putting a transaction **after** the user’s transaction

Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

In the mempool - Maximal Extractable Value (MEV)

Backrunning: putting a transaction **after** the user’s transaction



Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

Exchange 1: ETHUSDC = 2499
Exchange 2: ETHUSDC = 2500

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

In the mempool - Maximal Extractable Value (MEV)

Backrunning: putting a transaction **after** the user's transaction

Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

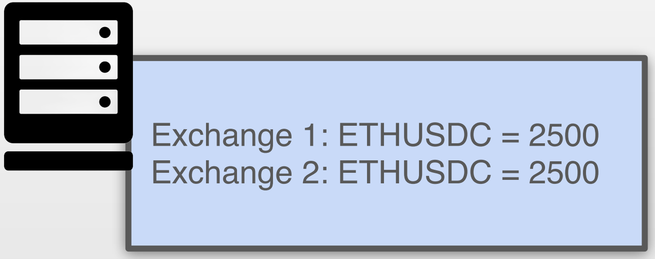
Exchange 1: ETHUSDC = 2499
Exchange 2: ETHUSDC = 2500

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Sender: 0x0934aad…
Recipient: 0x108eead4…
Sell 2499USDC for 1ETH on Exchange 1
Buy 1ETH for 2500USDC on Exchange 2
Fee: 100 gwei

In the mempool - Maximal Extractable Value (MEV)

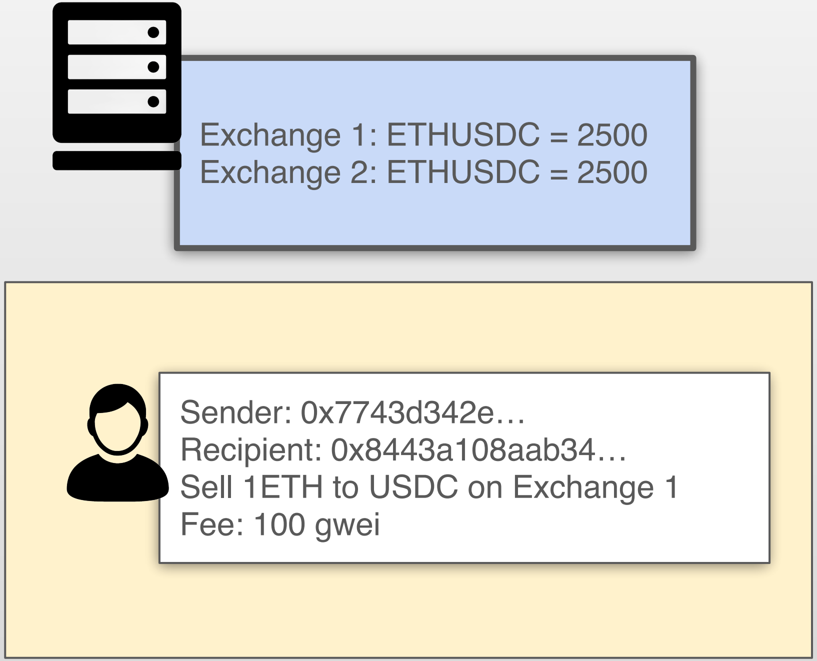
Sandwiching: putting transactions **before** and **after** the user’s transaction



Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

In the mempool - Maximal Extractable Value (MEV)

Sandwiching: putting transactions **before** and **after** the user’s transaction

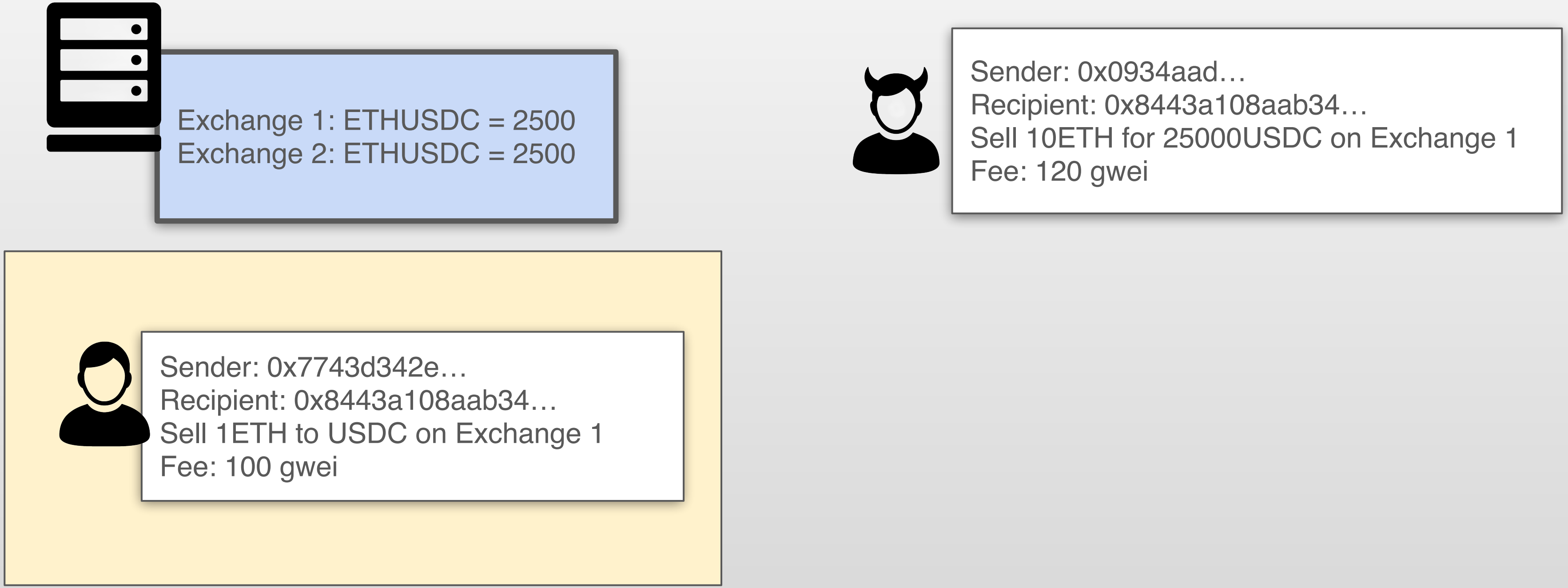


Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

In the mempool - Maximal Extractable Value (MEV)

Sandwiching: putting transactions **before** and **after** the user’s transaction



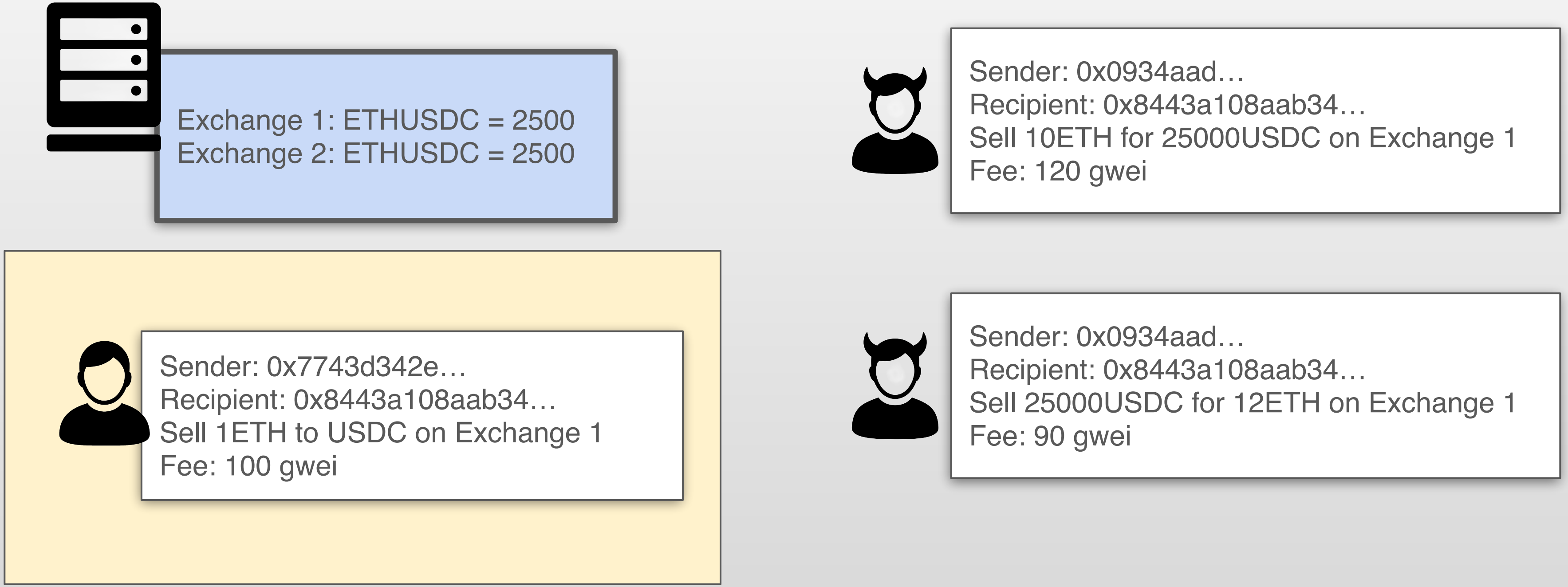
Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

In the mempool - Maximal Extractable Value (MEV)

Sandwiching: putting transactions **before** and **after** the user's transaction



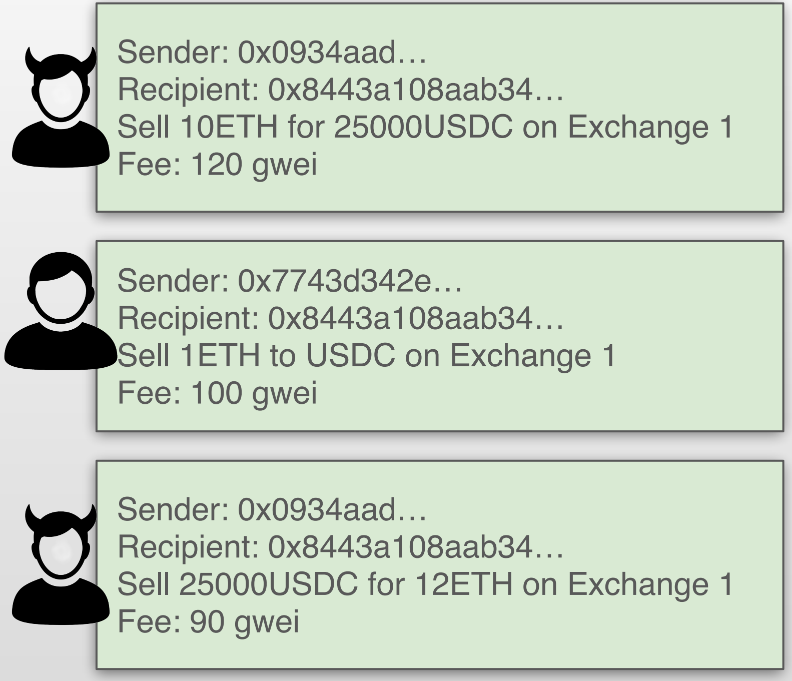
Exchange 1: ETHUSDC = 2500
Exchange 2: ETHUSDC = 2500

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 25000USDC for 12ETH on Exchange 1
Fee: 90 gwei

Sandwiching. In a block



Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 25000USDC for 12ETH on Exchange 1
Fee: 90 gwei

Sandwiching. In a block

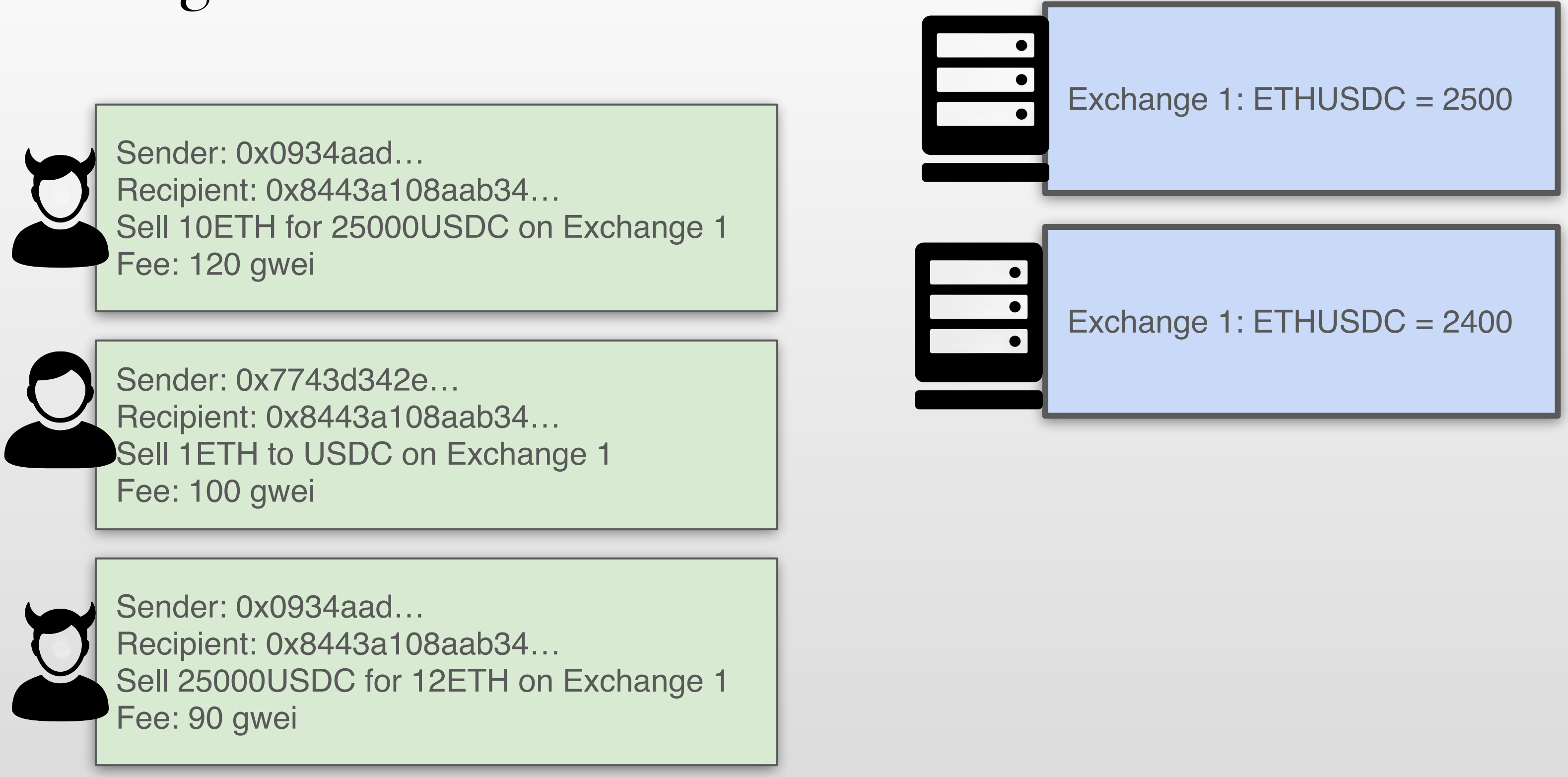
Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 25000USDC for 12ETH on Exchange 1
Fee: 90 gwei

Exchange 1: ETHUSDC = 2500

Sandwiching. In a block



Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

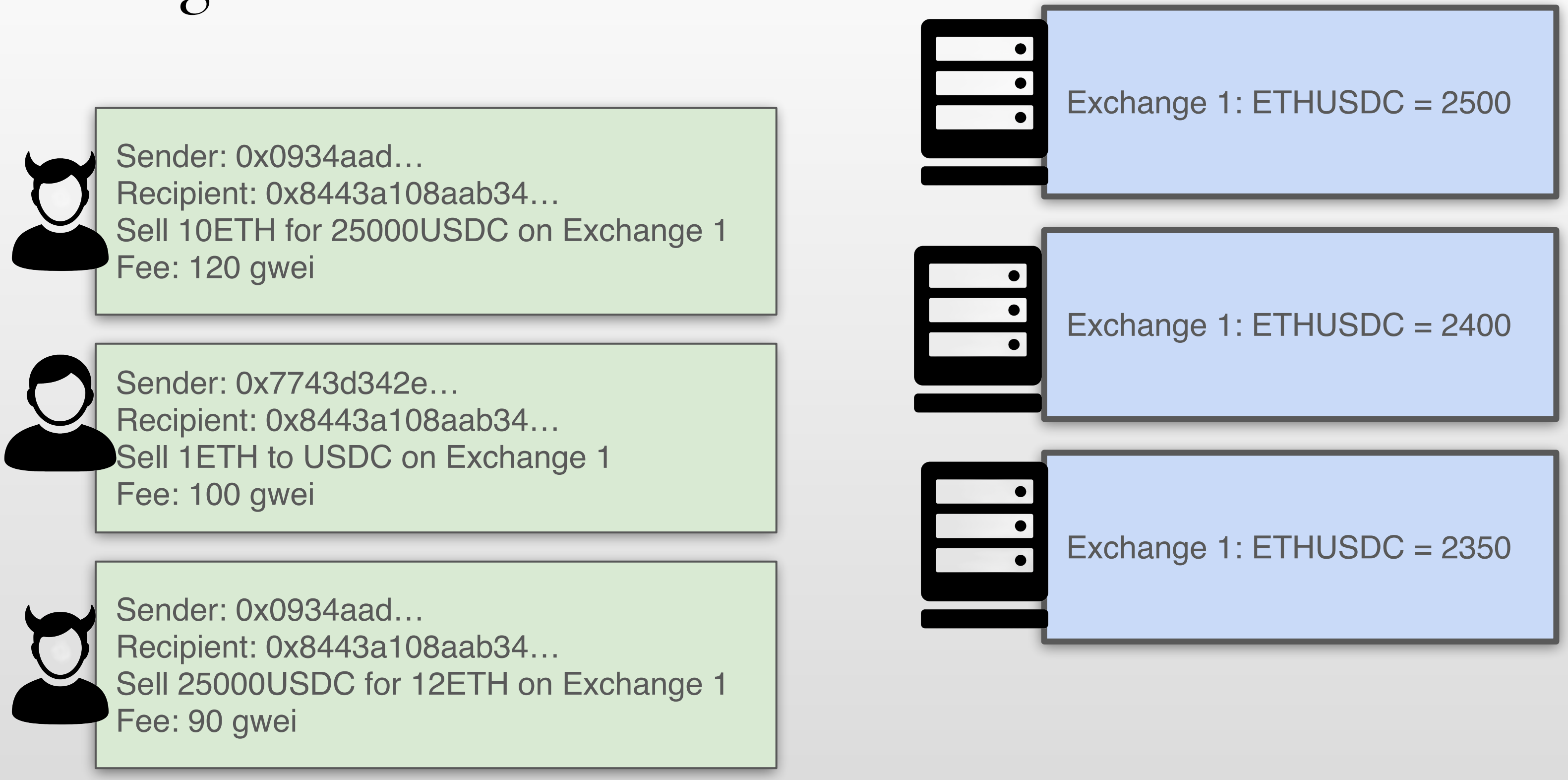
Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 25000USDC for 12ETH on Exchange 1
Fee: 90 gwei

Exchange 1: ETHUSDC = 2500

Exchange 1: ETHUSDC = 2400

Sandwiching. In a block



Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Exchange 1: ETHUSDC = 2500

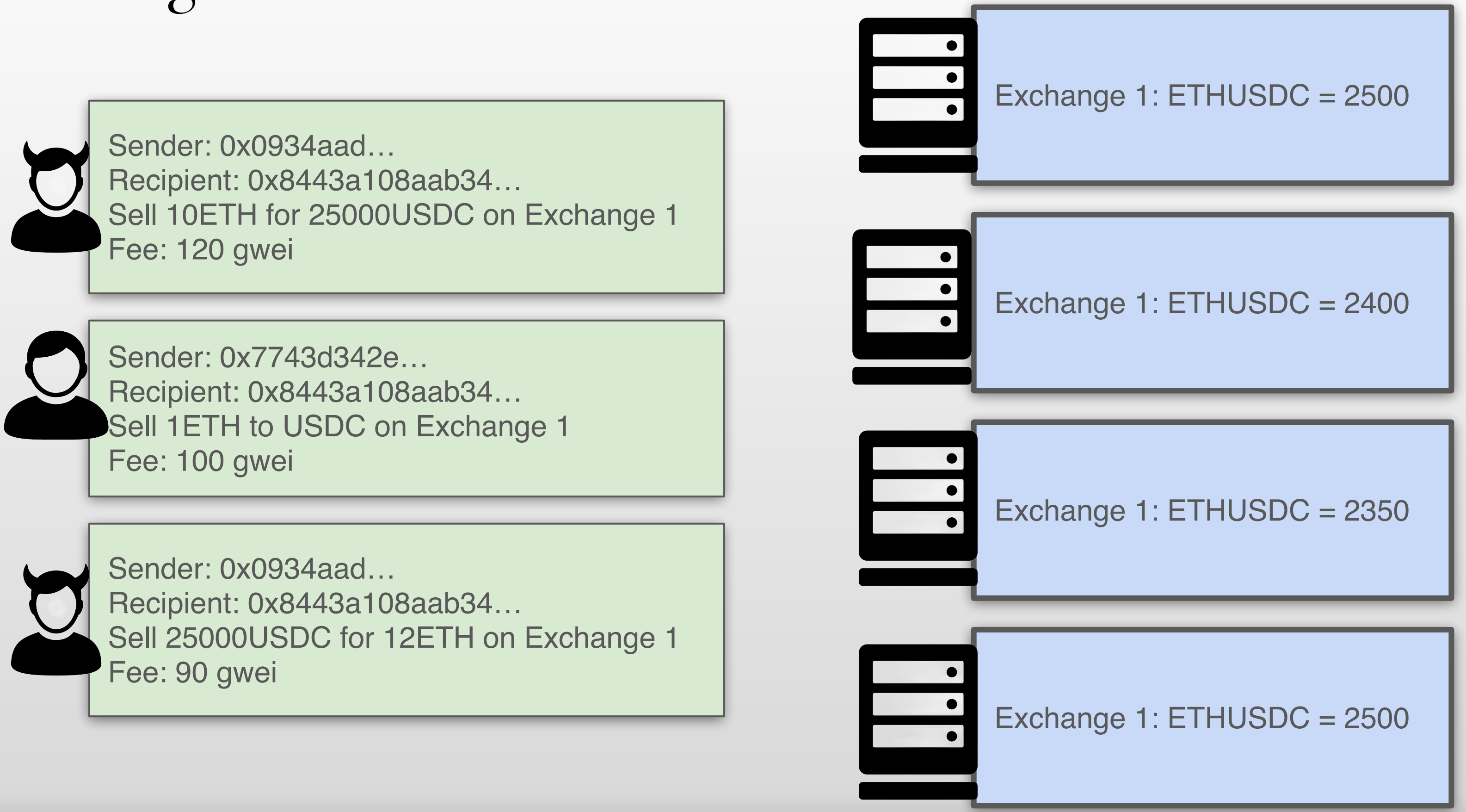
Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Exchange 1: ETHUSDC = 2400

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 25000USDC for 12ETH on Exchange 1
Fee: 90 gwei

Exchange 1: ETHUSDC = 2350

Sandwiching. In a block



Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 10ETH for 25000USDC on Exchange 1
Fee: 120 gwei

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Sender: 0x0934aad…
Recipient: 0x8443a108aab34…
Sell 25000USDC for 12ETH on Exchange 1
Fee: 90 gwei

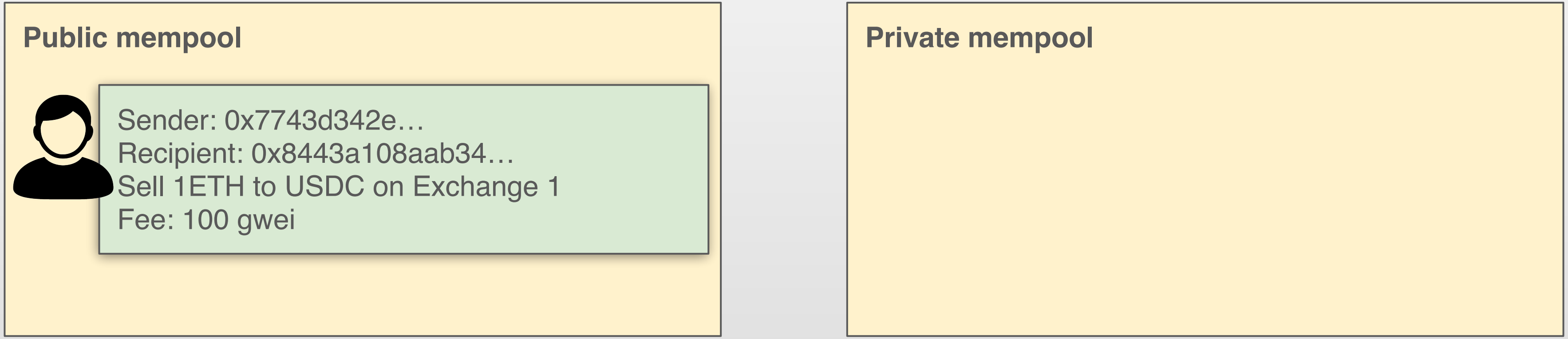
Exchange 1: ETHUSDC = 2500

Exchange 1: ETHUSDC = 2400

Exchange 1: ETHUSDC = 2350

Exchange 1: ETHUSDC = 2500

Private orderflow for mitigating MEV

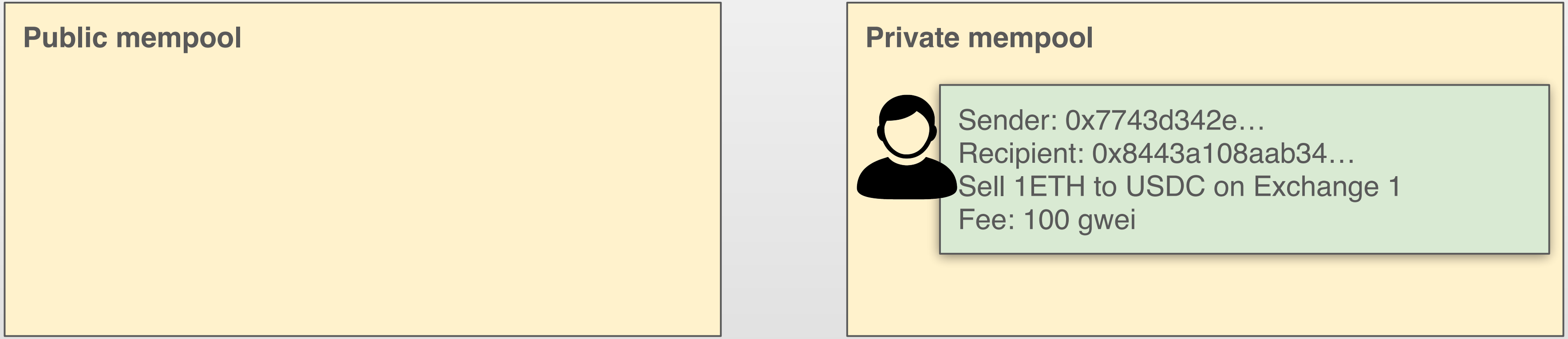


Public mempool

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Private mempool

Private orderflow for mitigating MEV

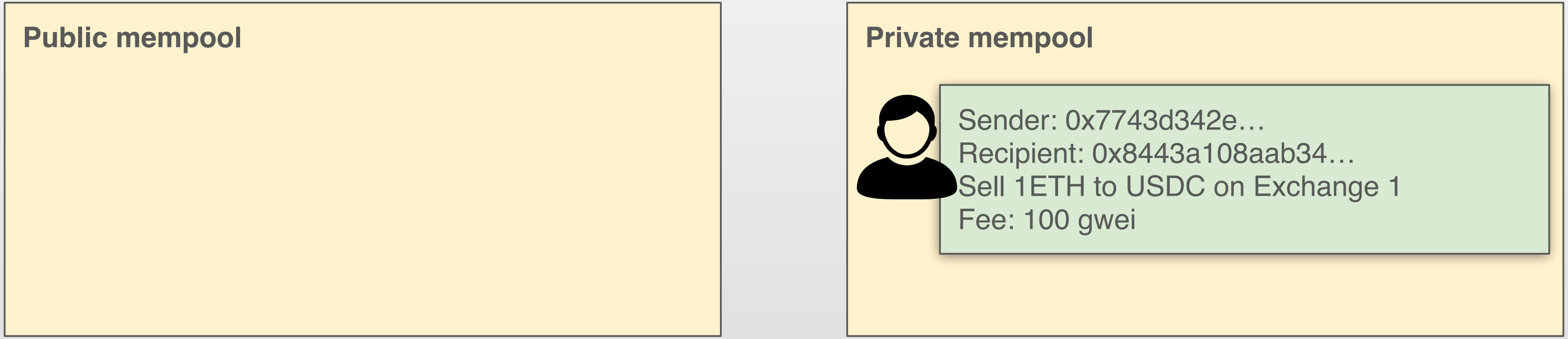


Public mempool

Private mempool

Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Private orderflow for mitigating MEV



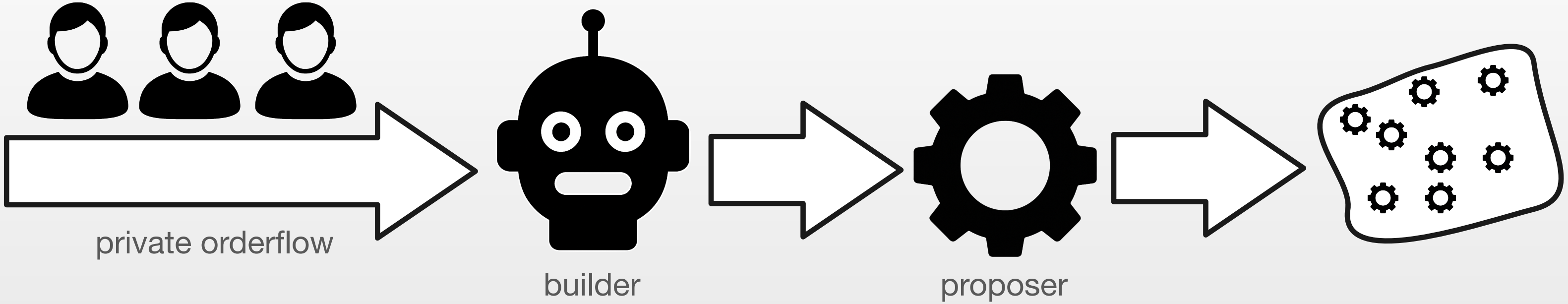
Public mempool

Private mempool

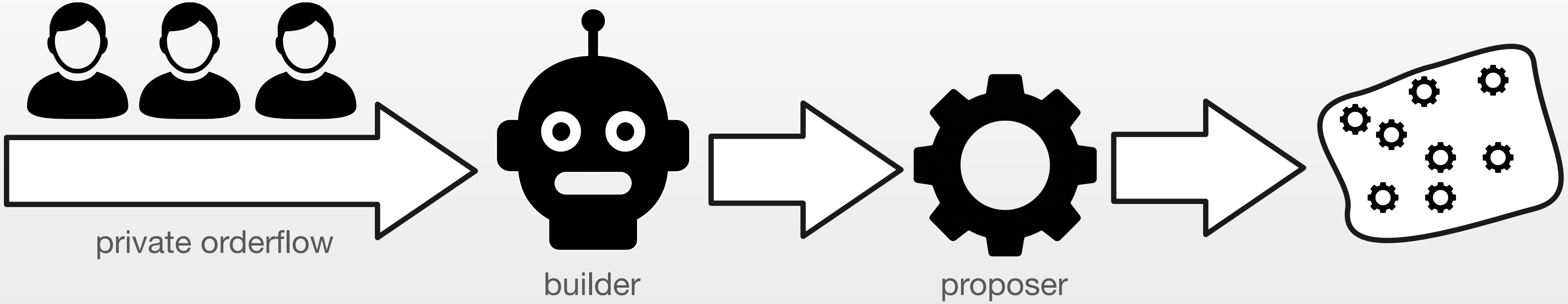
Sender: 0x7743d342e…
Recipient: 0x8443a108aab34…
Sell 1ETH to USDC on Exchange 1
Fee: 100 gwei

Whose private mempool it is?

Private orderflow. Builders



Private orderflow. Builders

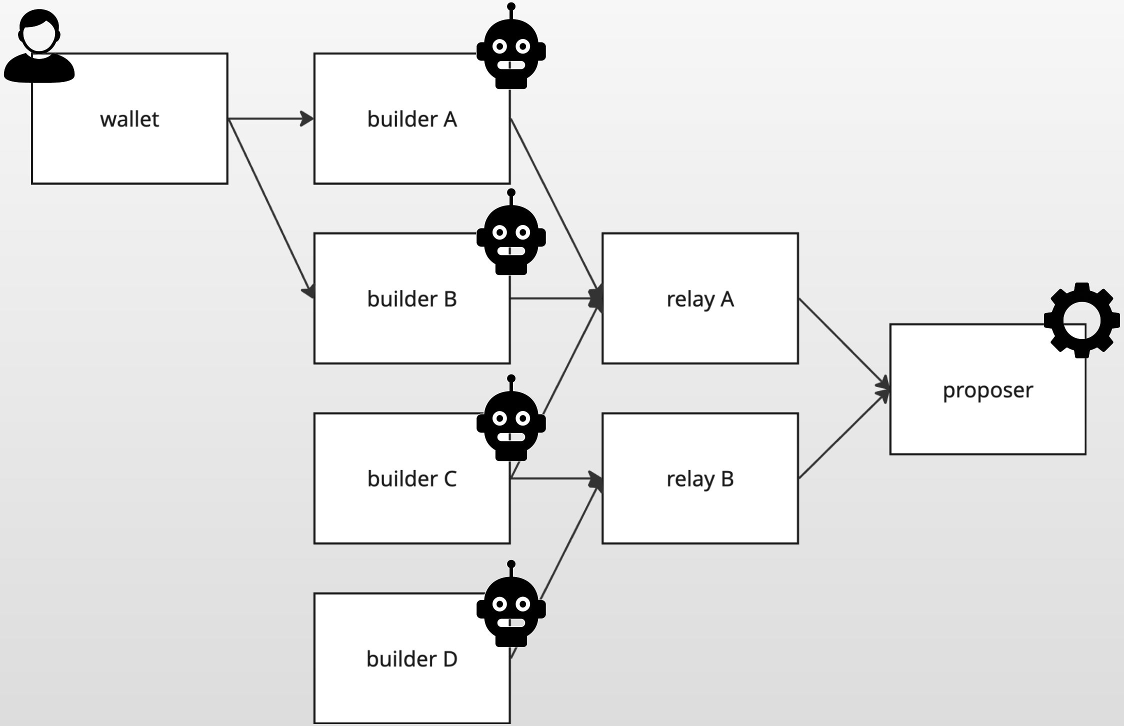


Build blocks for proposers

Specialized entities that make blocks as profitable as possible

Handful of actors (vs 1’000’000 of validators)

Proposer-builder separation



1. Builders compete with each other.
2. Relays are trusted by both the proposer and builders
3. Builders try to build the most profitable block
4. They compete in an auction. The bids are collected by the relay.
5. The highest bid wins.
6. The relayer sends the block header to the proposer, who signs it
7. The relayer reveals the block to the proposer who propagates it

Accountability in PBS

Collaborating with compliant builders
Institutions can collaborate with selected builders who follow particular AML, KYC practices, so institutional transactions are not processed with transactions of unknown origin

Censorship and delays
Institutions can have SLA-s with builders that specify how their transactions should be processed.
If something goes wrong, institutions know who is responsible for the issue.

Integrity

Ethereum finality

“51% attack”

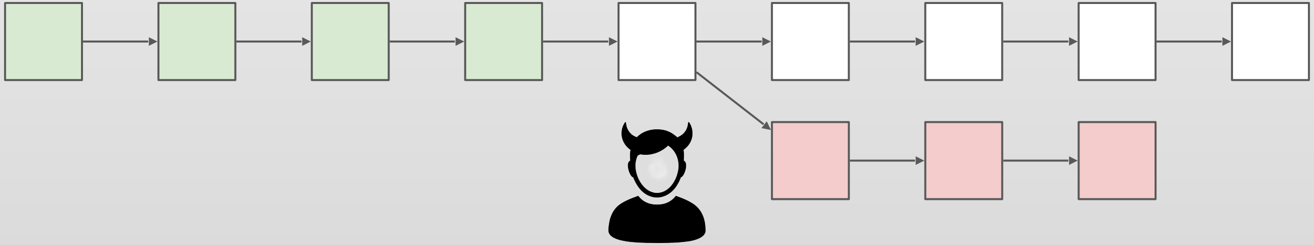
Malicious majority of nodes re-write the history and efficiently fork the chain

Forking

Bug in a node software or network issues make the chain split

Finality delay

Malicious users might be incentivized to delay finality to achieve financial gains



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees randomly with each epoch

Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks

Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks

Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

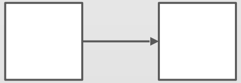
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can
propose only 1
block per slot

Validators cannot
vote on conflicting
blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

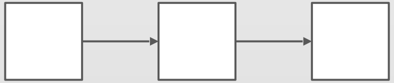
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can
propose only 1
block per slot

Validators cannot
vote on conflicting
blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

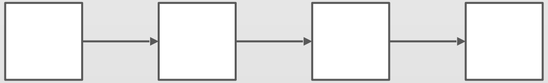
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

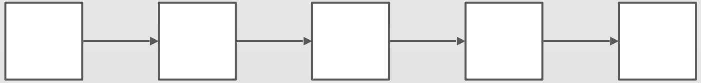
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees randomly with each epoch

Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

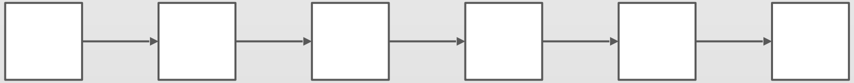
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can
propose only 1
block per slot

Validators cannot
vote on conflicting
blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

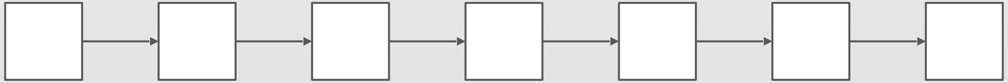
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

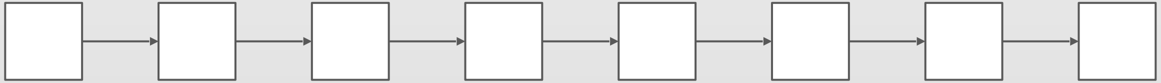
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can
propose only 1
block per slot

Validators cannot
vote on conflicting
blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

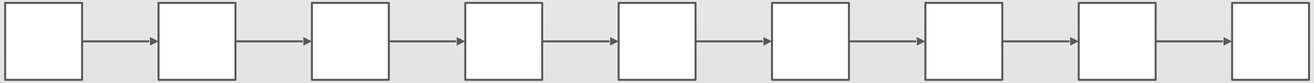
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can
propose only 1
block per slot

Validators cannot
vote on conflicting
blocks



Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

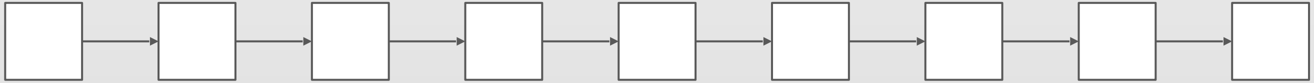
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees randomly with each epoch

Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks



A block that gets votes from ⅔ of validators is **finalized**

Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

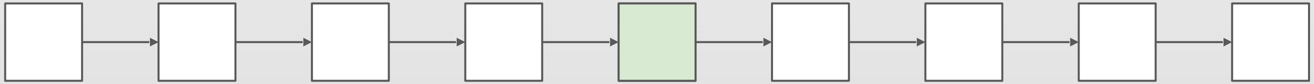
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

Proposers can
propose only 1
block per slot

Validators cannot
vote on conflicting
blocks



A block that gets votes from ⅔ of validators is **finalized**

Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

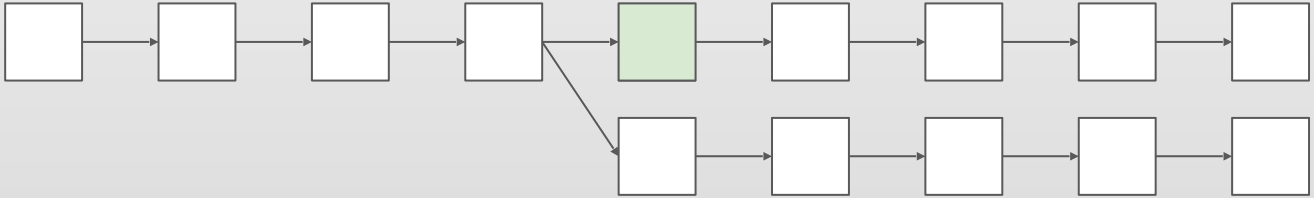
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees randomly with each epoch

Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks



A block that gets votes from ⅔ of validators is **finalized**

Proof of stake

Slots
Place for a block
New slot every **12s**

Epoch
32 slots
(12.8 minutes)

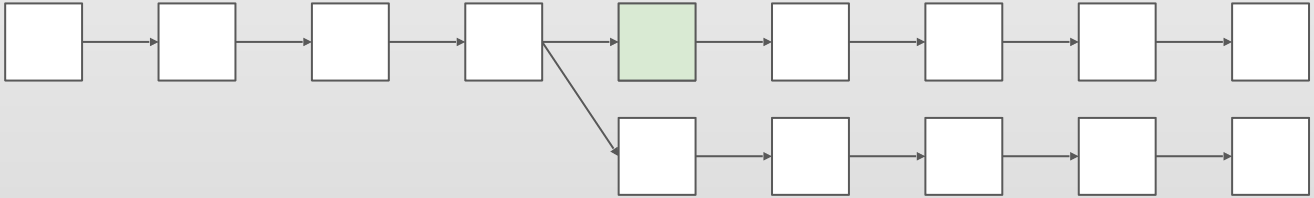
Nodes
32ETH deposited

Proposers
Picked randomly
One for each slot

Validators
Divided into committees
randomly with each epoch

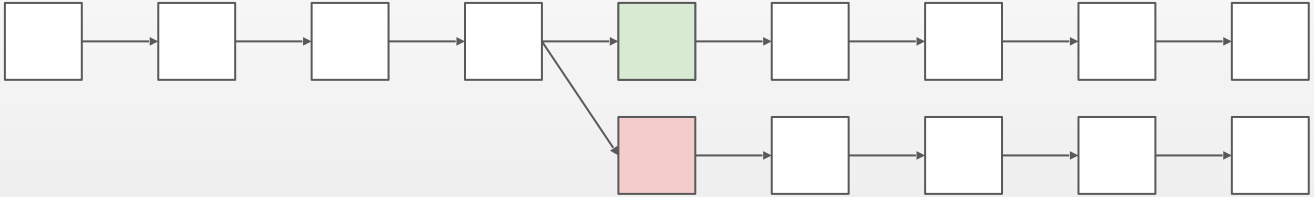
Proposers can propose only 1 block per slot

Validators cannot vote on conflicting blocks



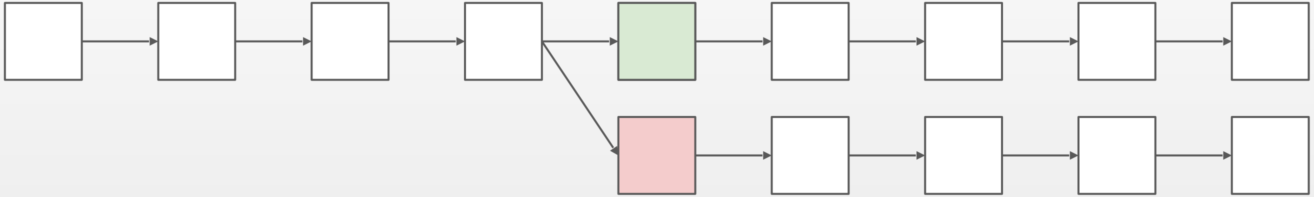
A block that gets votes from ⅔ of validators is **finalized**
(validators who votes in both chains are slashed)

Economic finality brings blockchain integrity

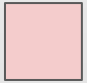


A block that gets votes from ⅔ of validators is **finalized**
(validators who votes in both chains are slashed)

Economic finality brings blockchain integrity



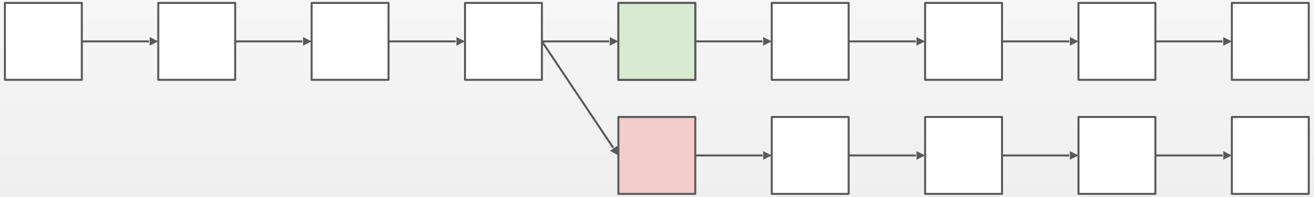
A block that gets votes from ⅔ of validators is **finalized**
(validators who votes in both chains are slashed)



Cost of finalizing a malicious block

- Upper chain confirmed by ⅔ of validators
- Lower chain needs to be confirmed by at least ⅔ of validators
- Upper and lower chains have at least ⅓ validators in common – these will be slashed
- ⅓ * 1’000’000 * 32 ETH > 10.5M ETH > $26B

Economic finality brings blockchain integrity



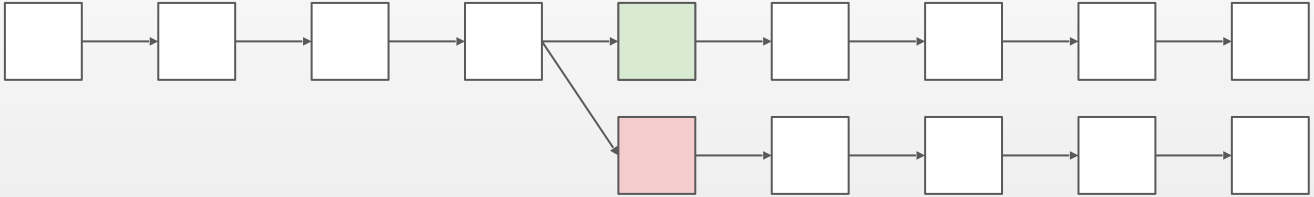
A block that gets votes from ⅔ of validators is **finalized**
(validators who votes in both chains are slashed)

Cost of finalizing a malicious block 🟥

- Upper chain confirmed by ⅔ of validators
- Lower chain needs to be confirmed by at least ⅔ of validators
- Upper and lower chains have at least ⅓ validators in common – these will be slashed
- ⅓ * 1’000’000 * 32 ETH > 10.5M ETH > $26B

✚

Economic finality brings blockchain integrity



A block that gets votes from ⅔ of validators is **finalized**
(validators who votes in both chains are slashed)

Cost of finalizing a malicious block 🟥

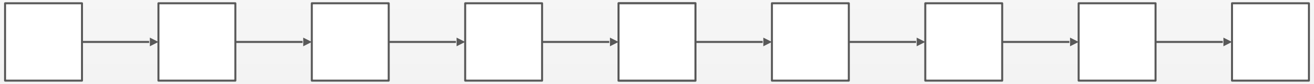
- Upper chain confirmed by ⅔ of validators
- Lower chain needs to be confirmed by at least ⅔ of validators
- Upper and lower chains have at least ⅓ validators in common – these will be slashed
- ⅓ * 1’000’000 * 32 ETH > 10.5M ETH > $26B

+

Social consensus may decide to abandon malicious fork

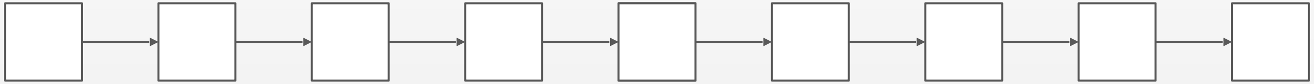
Auditability

Auditability with privacy



Everything is in the blocks

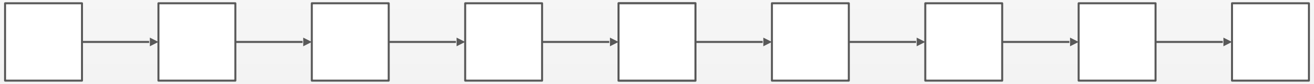
Auditability with privacy



Everything is in the blocks

… with privacy

Auditability with privacy

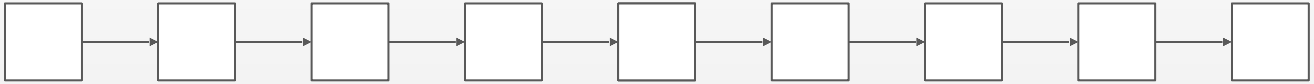


Everything is in the blocks

… with privacy

Zero-knowledge technology allows institutions to trade privately without revealing the transaction sender, recipient, amount or asset type

Auditability with privacy



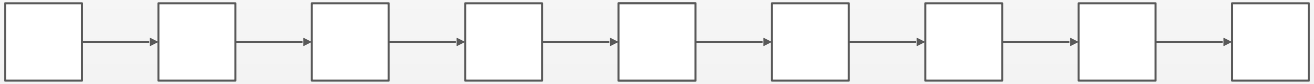
Everything is in the blocks

… with privacy

Zero-knowledge technology allows institutions to trade privately without revealing the transaction sender, recipient, amount or asset type

zcash

Auditability with privacy



Everything is in the blocks

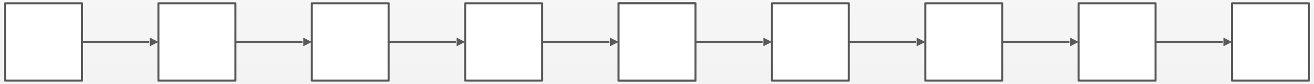
… with privacy

Zero-knowledge technology allows institutions to trade privately without revealing the transaction sender, recipient, amount or asset type

zcash

privacy pools

Auditability with privacy



Everything is in the blocks

… with privacy

Zero-knowledge technology allows institutions to trade privately without revealing the transaction sender, recipient, amount or asset type

zcash

privacy pools

Zero-knowledge allows to privately check

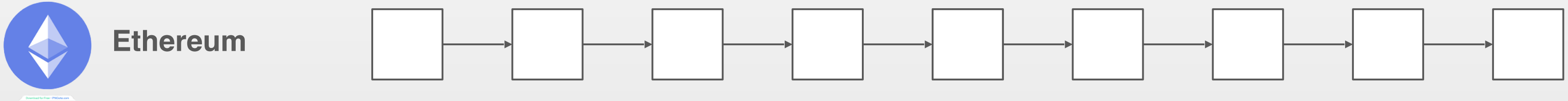
- That the transaction was compliant with a set of predefined rules
- That none of the transaction parties were blacklisted

It is also possible to de-anonymize and audit trades when a party is audited.

Between public and private chains

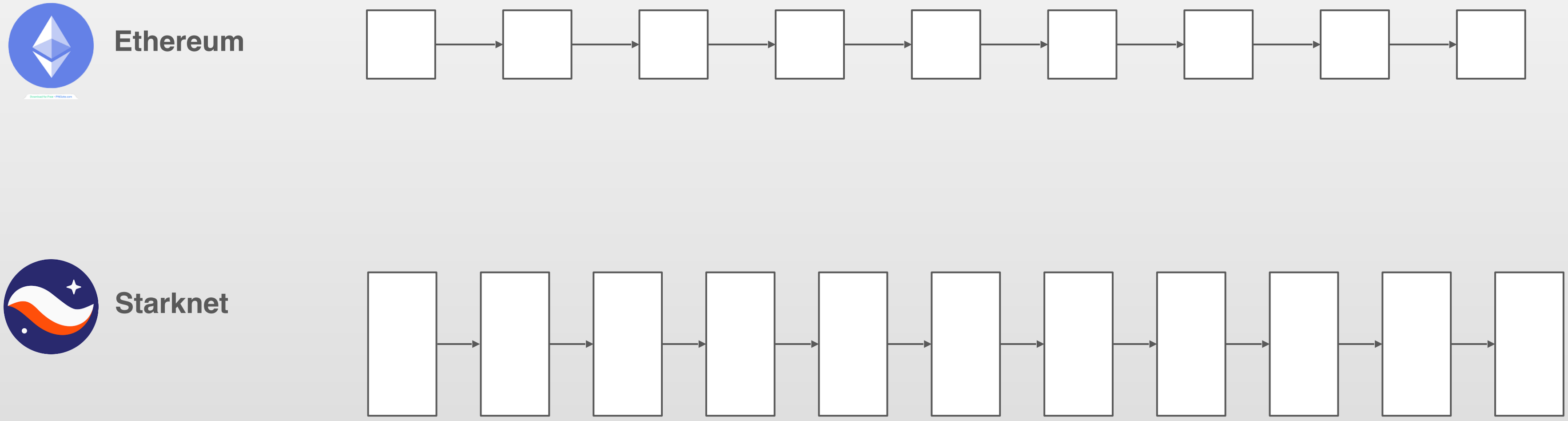
Scaling Ethereum throughput - Rollups

Subchains which inherit security from Ethereum



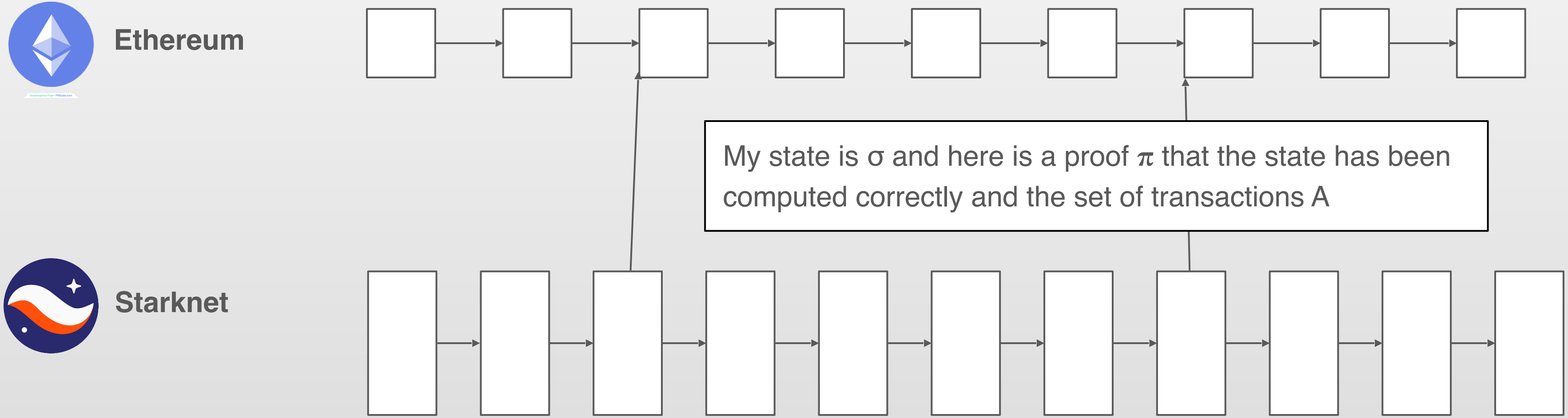
Scaling Ethereum throughput - Rollups

Subchains which inherit security from Ethereum



Scaling Ethereum throughput - Rollups

Subchains which inherit security from Ethereum

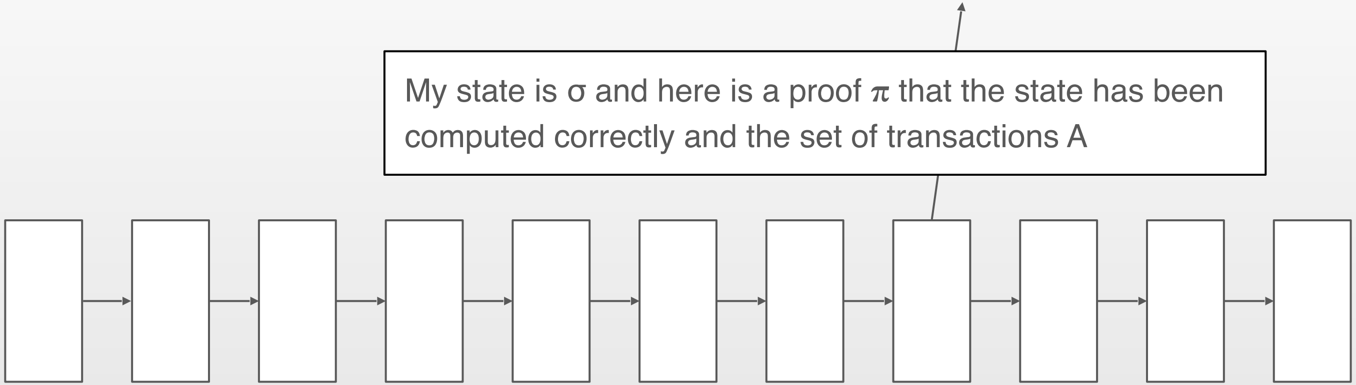


Ethereum

My state is σ and here is a proof π that the state has been computed correctly and the set of transactions A

Starknet

Public-permissioned chains – a middleground



My state is σ and here is a proof π that the state has been computed correctly and the set of transactions A

Rollups allow institutions to

- Maintain **access to the assets** traded and stored on Ethereum
- **Control who they are trading with** with great granularity: e.g. only KYCed, AML-compliant parties could be allowed to the rollup

Key takeaways

Key takeaways

- Institutions can ensure accountability and compliance of block production by utilizing **Proposer-Builder Separation** tools

Key takeaways

- Institutions can ensure accountability and compliance of block production by utilizing **Proposer-Builder Separation** tools
- Integrity of Ethereum transactions is protected by its proof of stake mechanism that makes **forking finalized blocks economically infeasible**

NETHERMIND

Key takeaways

- Institutions can ensure accountability and compliance of block production by utilizing **Proposer-Builder Separation** tools
- Integrity of Ethereum transactions is protected by its proof of stake mechanism that makes **forking finalized blocks economically infeasible**
- **Auditability** of transactions can be achieved along with **transaction privacy** thanks to the zero-knowledge technology.

Key takeaways

- Institutions can ensure accountability and compliance of block production by utilizing **Proposer-Builder Separation** tools
- Integrity of Ethereum transactions is protected by its proof of stake mechanism that makes **forking finalized blocks economically infeasible**
- **Auditability** of transactions can be achieved along with **transaction privacy** thanks to the zero-knowledge technology.
- **Bespoke institutional rollups** allow institutions to maintain better control over their public blockchain activity and still benefit from **network effects**.

Whitepaper

From Wallet to Chain.

A Bridge of Two Worlds on an Ethereum Transaction

Nethermind & Deutsche Bank

May 2025

thank you