



ethereum

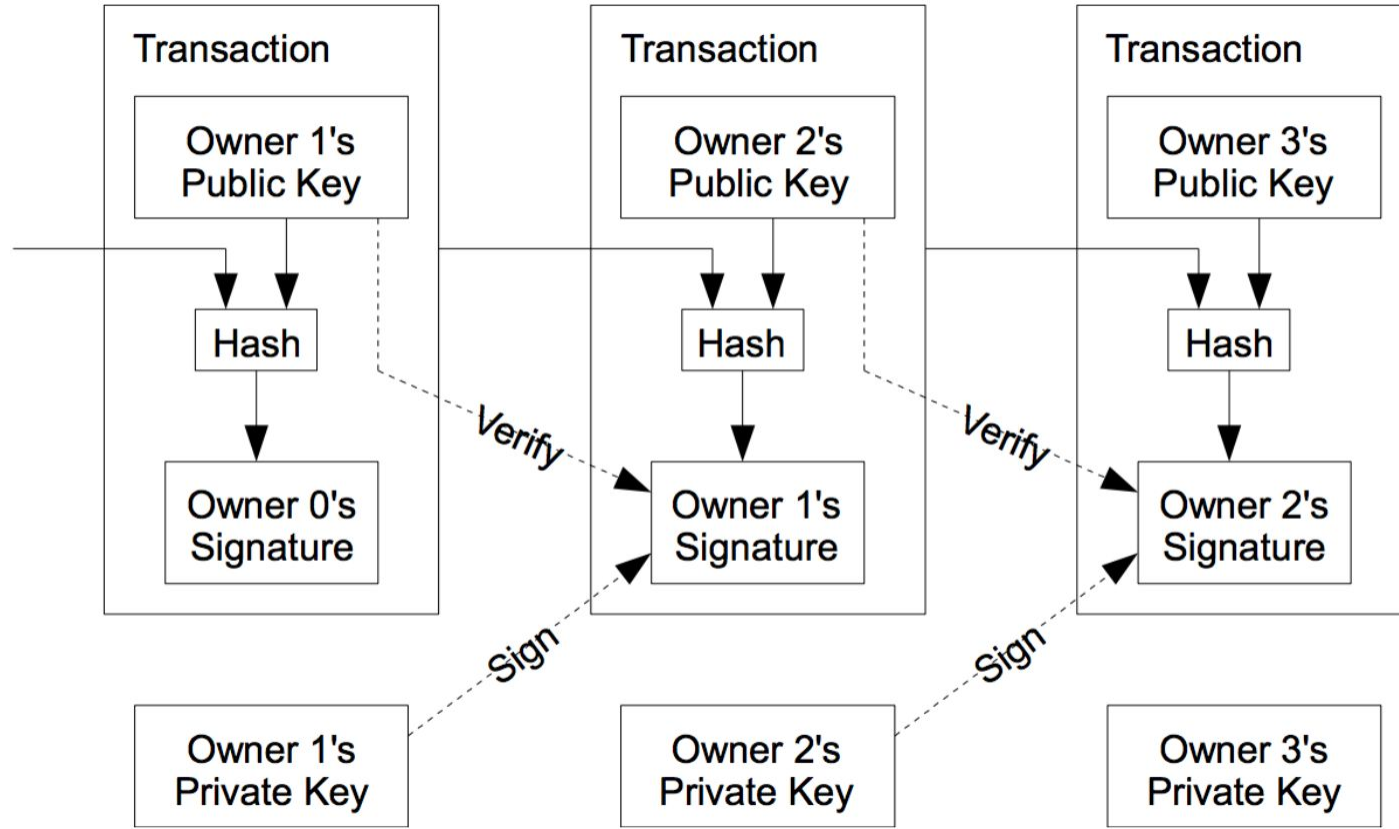
Туктаров Ренат
МГТУ им. Н. Э. Баумана



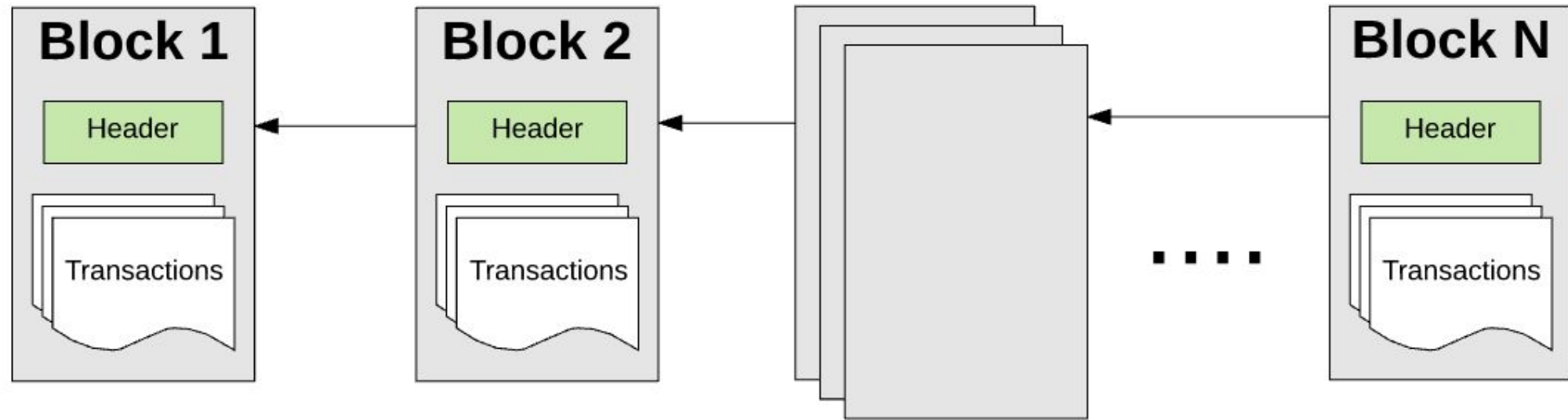
Ethereum

- cryptographically secure transactional singleton machine with shared-state

Blockchain

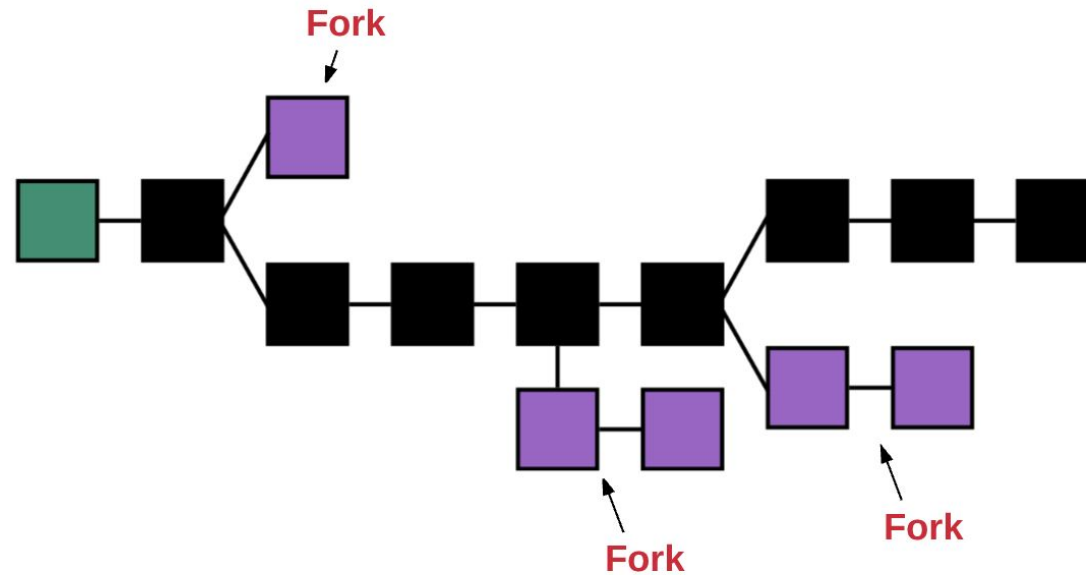


Blockchain

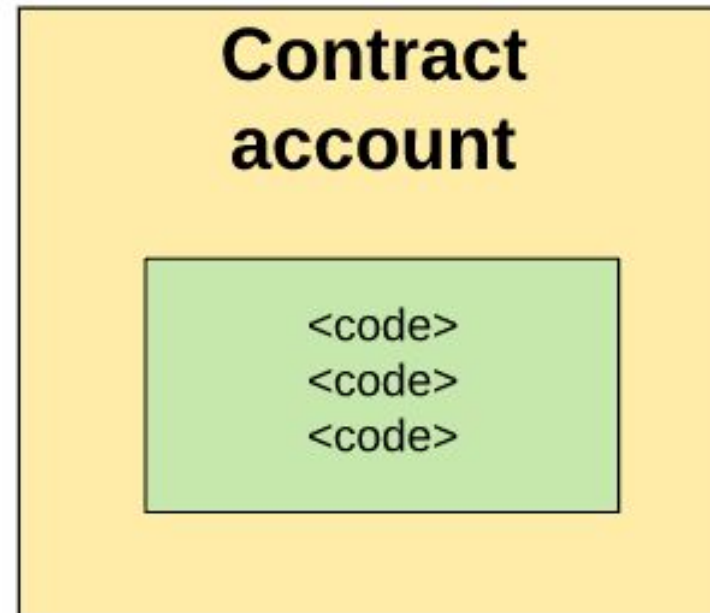


Blockchain – разрешение конфликтов

GHOST – Greedy Heaviest Observed SubTree



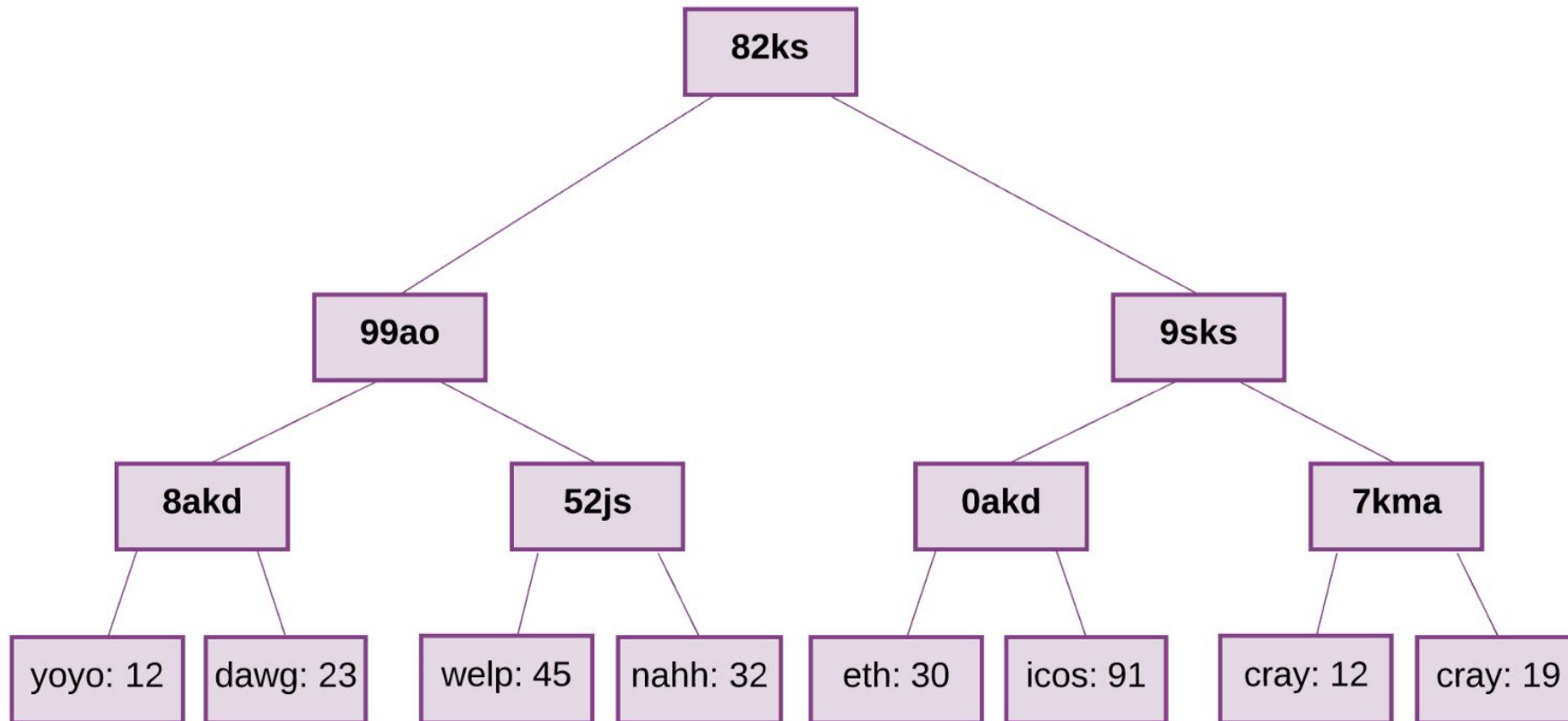
Ethereum – учетные записи



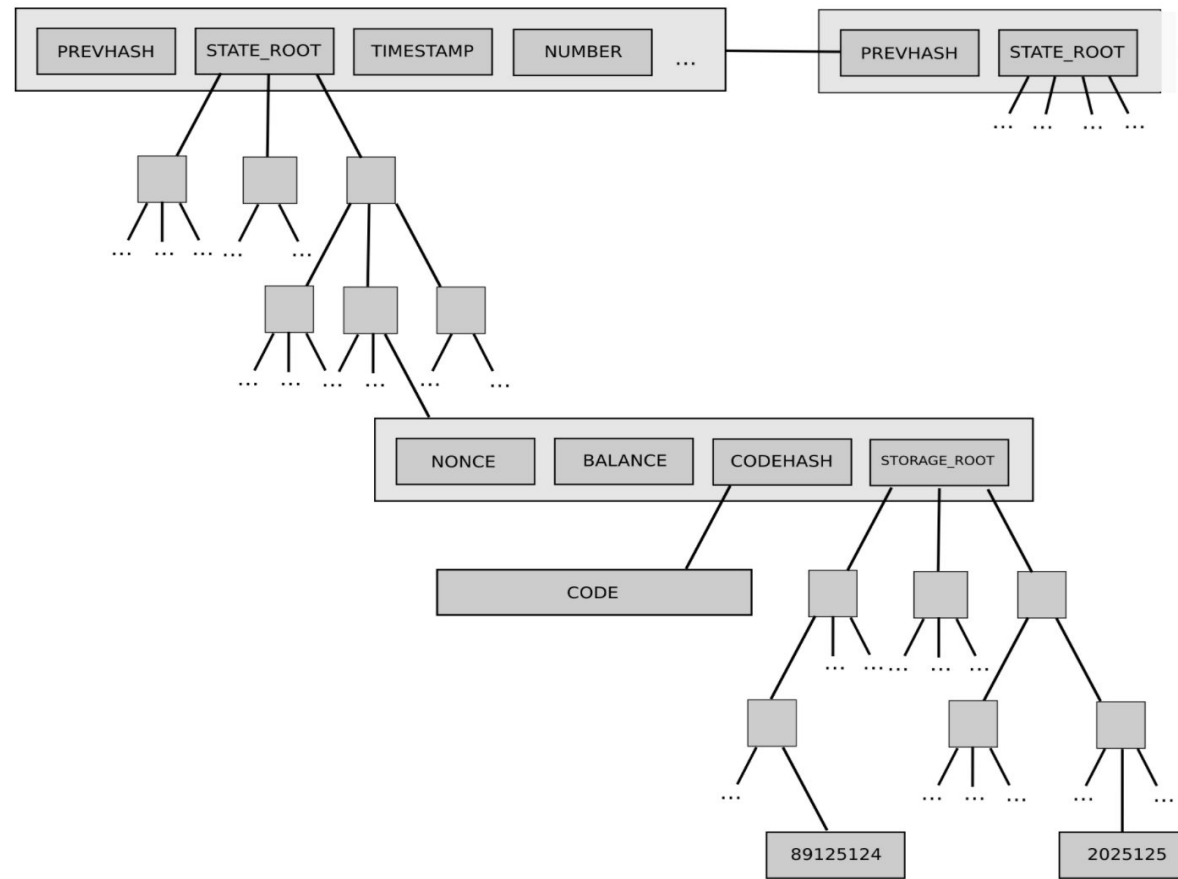
Ethereum – СОСТОЯНИЕ

- Mapping Account address -> Account state

Ethereum – состояние (merkle tree)

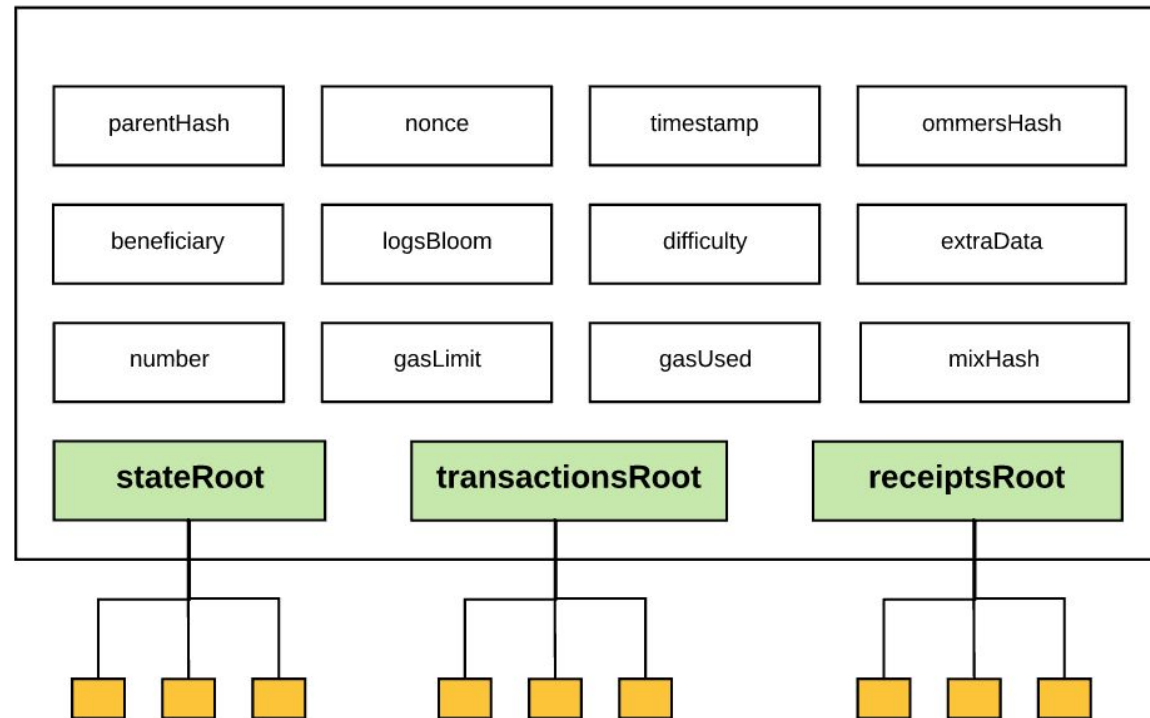


Ethereum – СОСТОЯНИЕ



Ethereum – структура блока

Block header

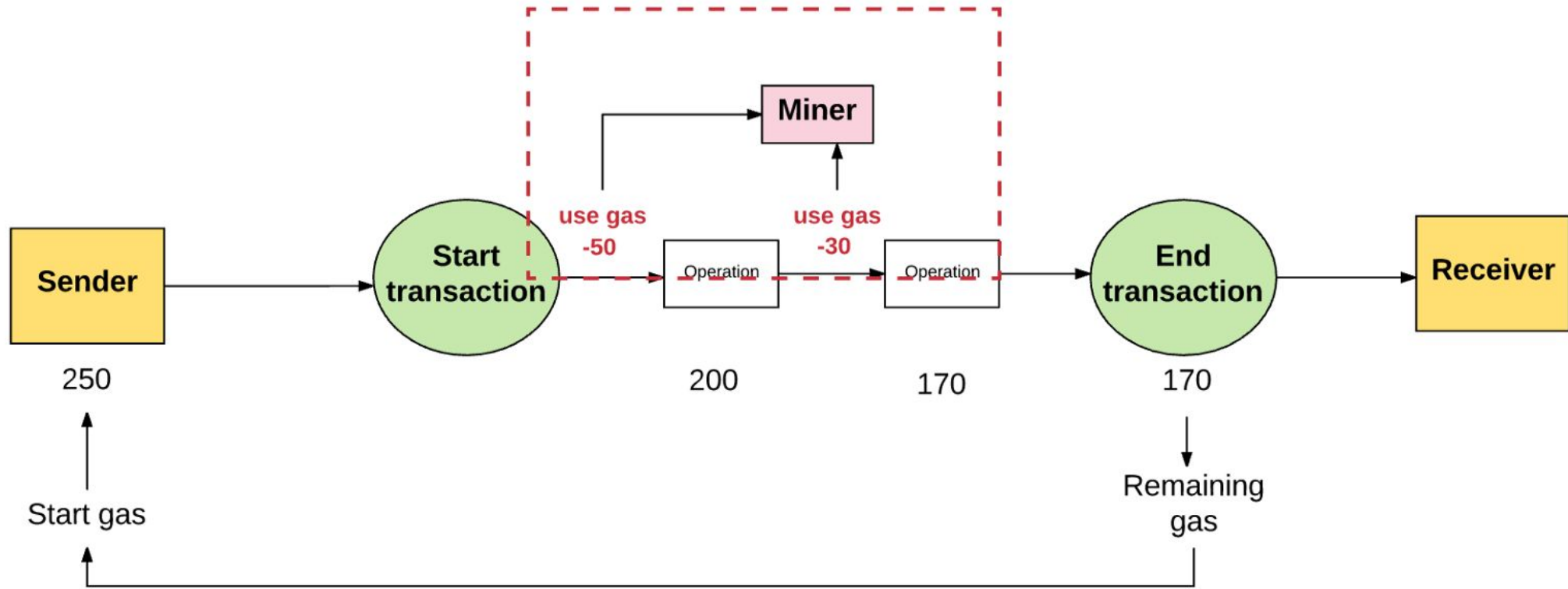


Ethereum – газ

- 1 Ether = 1e18 Wei = 1e9 gwei
- Вознаграждение майнеров
- Оплата места на диске

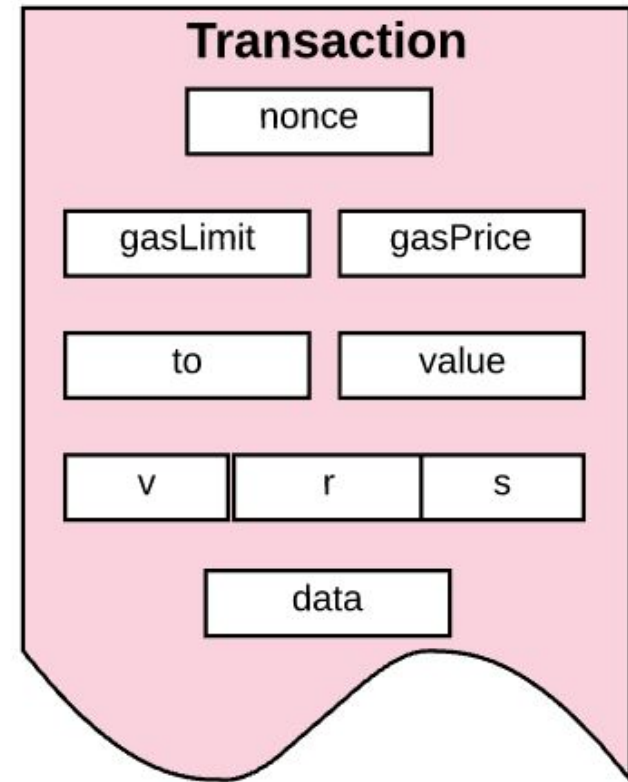
Gas Limit 50,000	x	Gas Price 20 gwei	=	Max transaction fee 0.001 Ether
----------------------------	----------	-----------------------------	----------	---

Ethereum – газ



Ethereum – транзакции

- gasLimit, gasPrice
- to, value
- init



Ethereum – ВЫПОЛНЕНИЕ ТРАНЗАКЦИИ

- Recursively Length Prefixed
- Valid signature
- Gas limit \geq intrinsic gas limit
 - $21000 + 4 * \text{null-bytes} + 68 * \text{non-null-bytes} + 32000$ (if contract creating transaction)
- Transaction substate (refund balance, logs, self-destruct set)

Спасибо за
внимание