Ethereum

University of Athens
Christos Nasikas, Dionysis Zindros

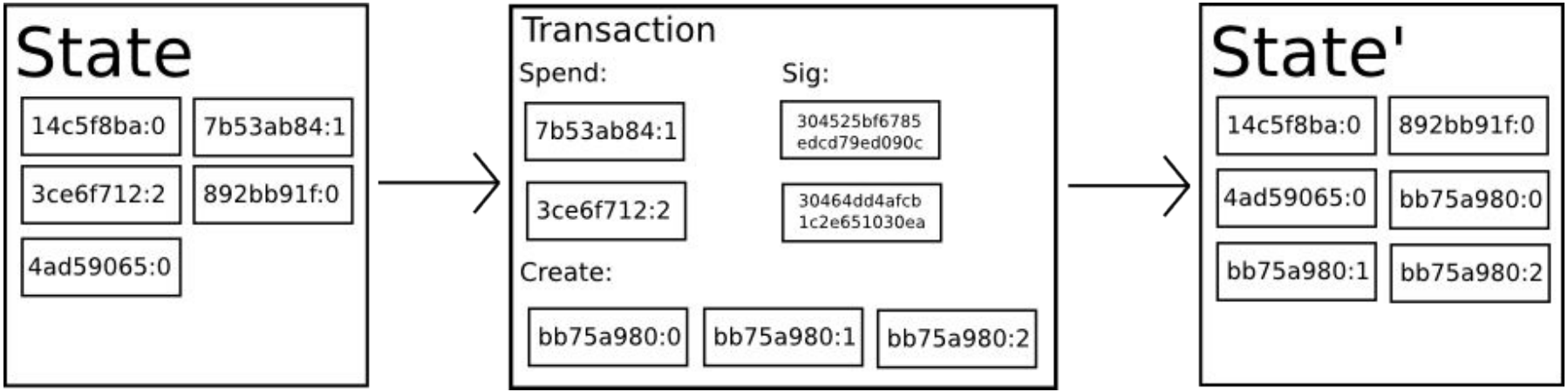
Overview

- Ethereum accounts
- Ethereum transactions
- Ethereum blockchain
- Solidity (programming language)

Extending Bitcoin functionality: adding new opcodes

- Distributed naming (Namecoin)
- Options, financial derivatives (OpenBazaar, MasterCoin)
- Prediction markets (Futurecoin)
- Open-ended, user-defined functionality?

Bitcoin as a state transition system



State = UTXO
Transaction is applied to state to give a new state

Ethereum: A universal RSM

- Transaction-based deterministic state machine
  - Global singleton state
  - A virtual machine that applies changes to global state
- A global decentralized computing infrastructure
- Anyone can create their own state transition functions

Ethereum: A universal RSM

- Stack-based bytecode language
- Turing-completeness
- Smart contracts
- Decentralized applications

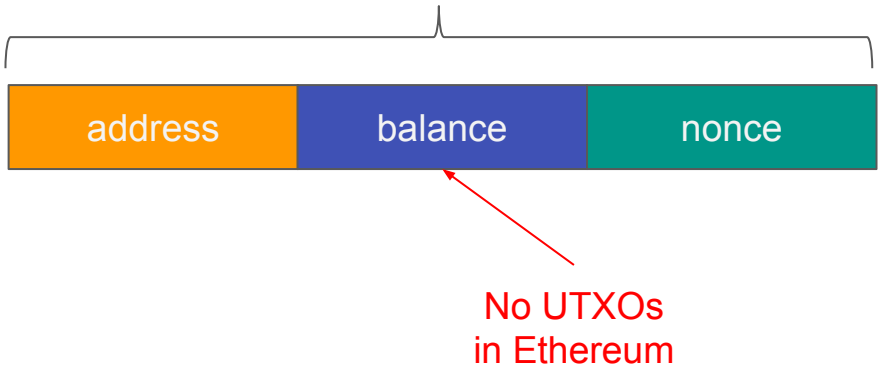
Same principles as Bitcoin

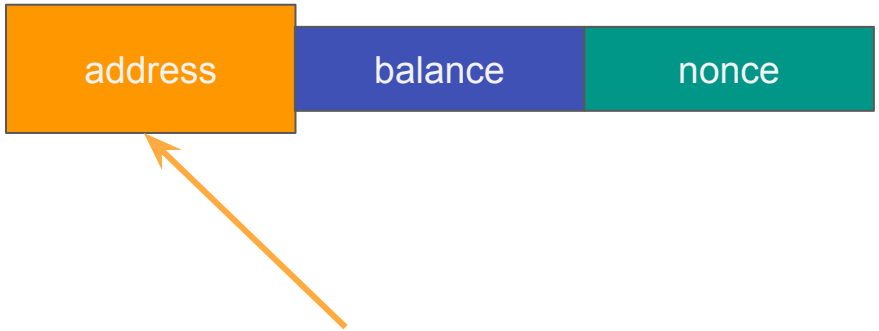
- **A peer-to-peer network:** connects the participants
- **A consensus algorithm**: Proof of Work (will move to PoS)
- **A digital currency:** ether
- **A global ledger**: the blockchain
  - Addresses: key pair
  - Wallets
  - Transactions: digital signatures
  - Blocks

Ethereum accounts

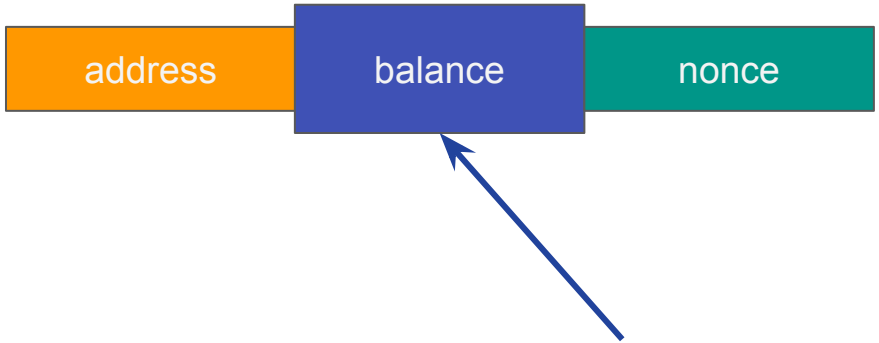
- Global state of Ethereum: **accounts**
- They **interact** to each other **through transactions** (messages)
- A **state associated** with it and a 20-byte **address** (160-bit identifier)

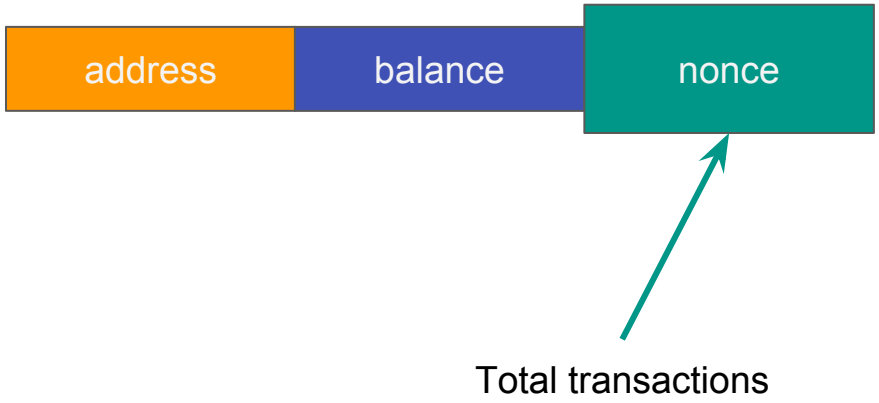
Ethereum account



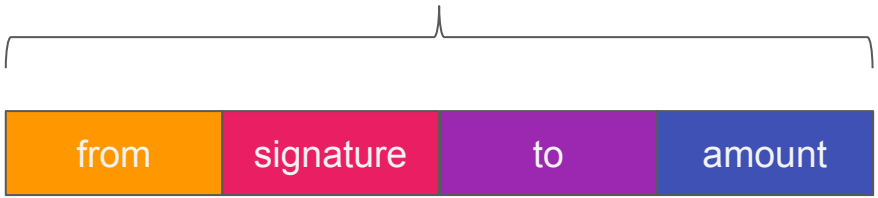


The **address** of the account

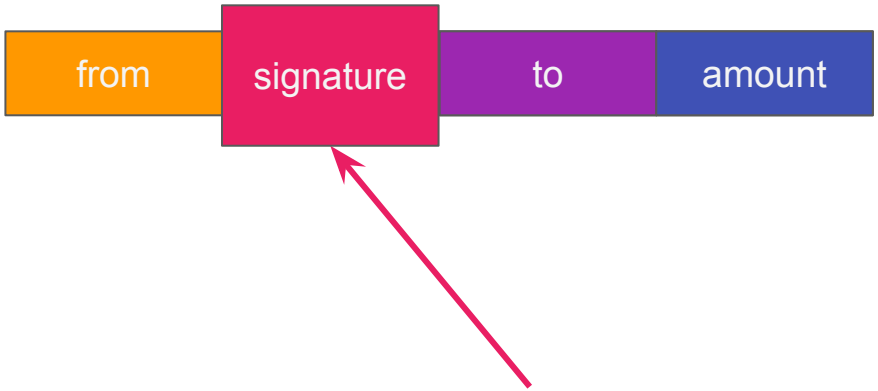

address
balance
nonce
The **balance** of the account


address
balance
nonce
Total transactions

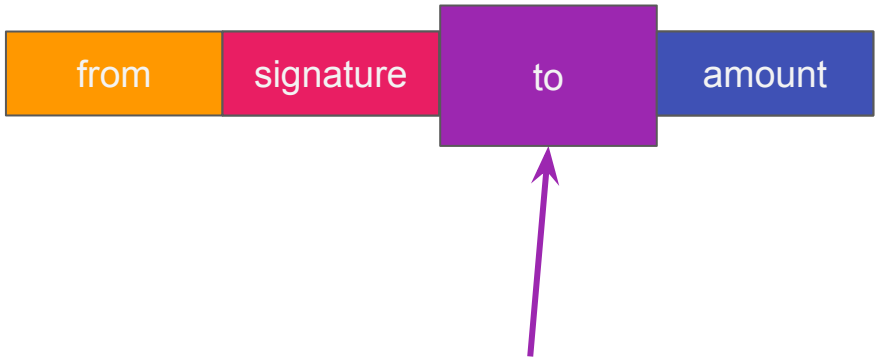
Ethereum transaction



The **sender** of the transaction

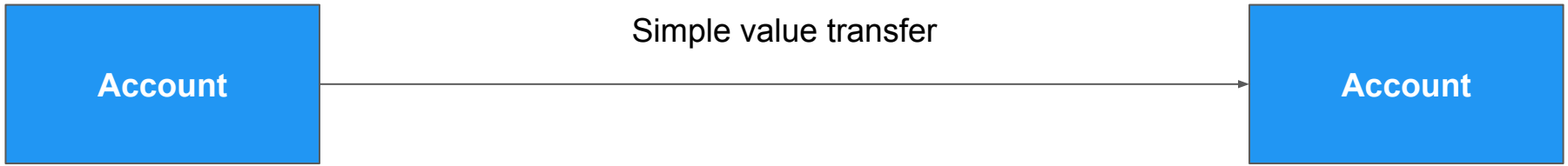


Digital signature on the **new transaction** created by **the sender's public key**



Receiver of the transaction

Amount transferred by transaction
Given in Wei


Account
Simple value transfer
Account

Two types of accounts

- Personal accounts (what we've seen)
- **Contract accounts**

Ethereum contract account

What is a smart contract?

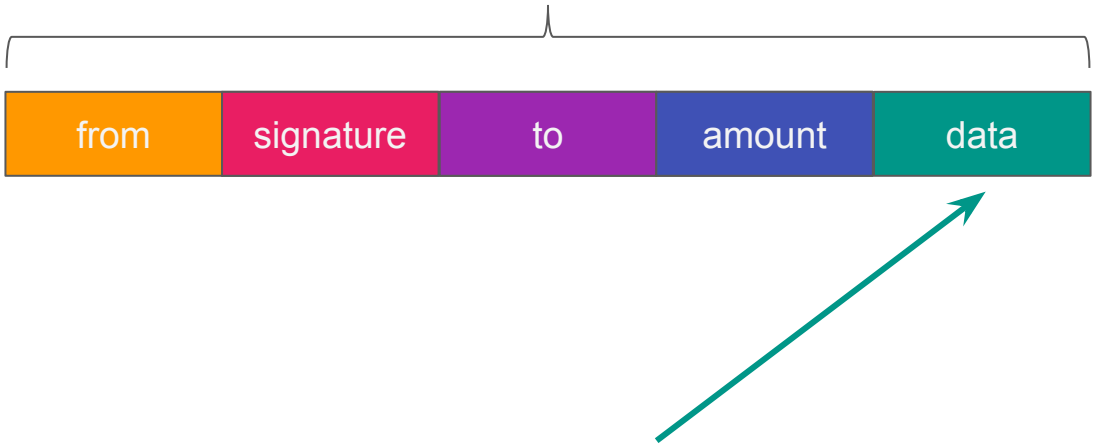
- Computer programs
- The code of a smart contract cannot change
- The outcome of a smart contract is the same for everyone
- Context: Internal storage, transaction context, most recent blocks
- Contract code is executed by all full nodes

```
contract Namespace {

    struct NameEntry {
        address owner;
        bytes32 value;
    }

    uint32 constant REGISTRATION_COST = 100;
    uint32 constant UPDATE_COST = 10;
    mapping(bytes32 => NameEntry) data;

    function nameNew(bytes32 hash){
        if (msg.value >= REGISTRATION_COST){
            data[hash].owner = msg.sender;
        }
    }

    function nameUpdate(bytes32 name, bytes32 newValue, address newOwner){
        bytes32 hash = sha3(name);
        if (data[hash].owner == msg.sender && msg.value >= UPDATE_COST){
            data[hash].value = newValue;
            if (newOwner != 0){
                data[hash].owner = newOwner;
            }
        }
    }

    function nameLookup(bytes32 name){
        return data[sha3(name)];
    }

}
```

Ethereum accounts

	Personal account	Contract account
address	H(pub_key)	H(creator, nonce)
code	∅	Code to be executed
storage	∅	Data of the contract
balance	ETH balance (in Wei)	
nonce	# transaction sent	

a transaction about a contract



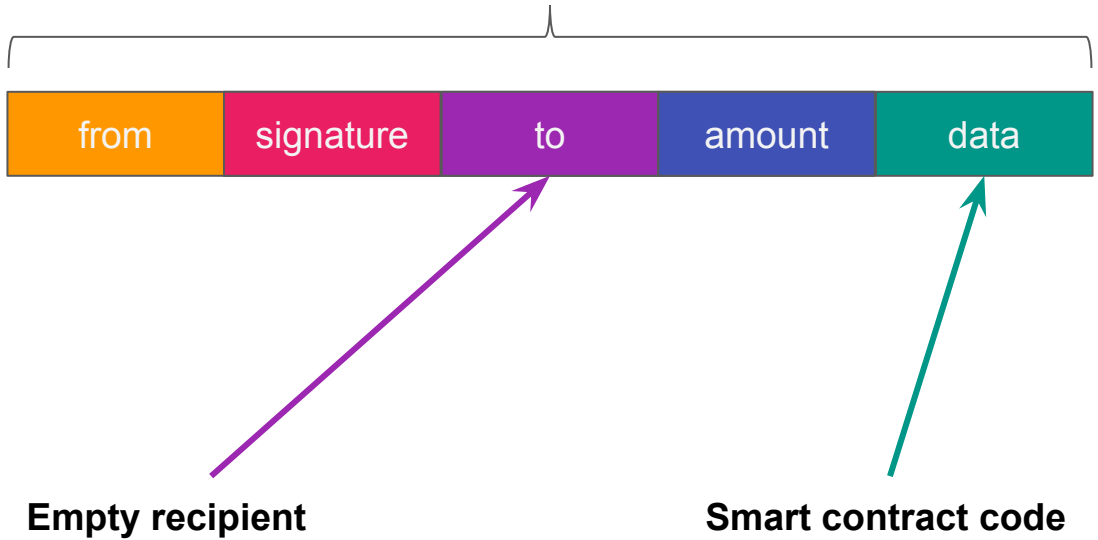
Transaction **about personal accounts**:
Field is unused

Transaction **about contracts**:
Will contain **data about the contract**

Smart contract lifecycle

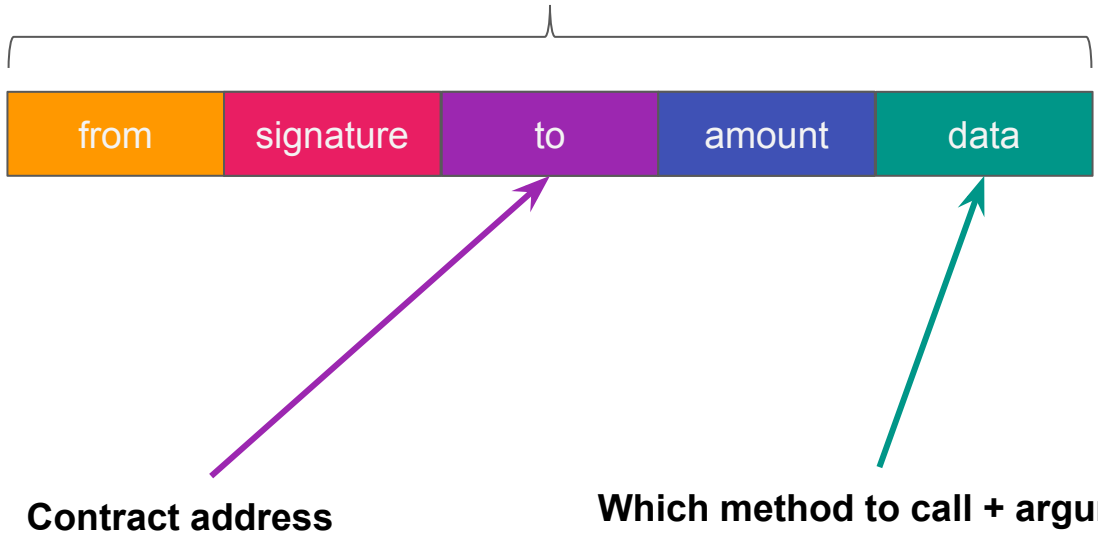

Create
Interact
Destroy

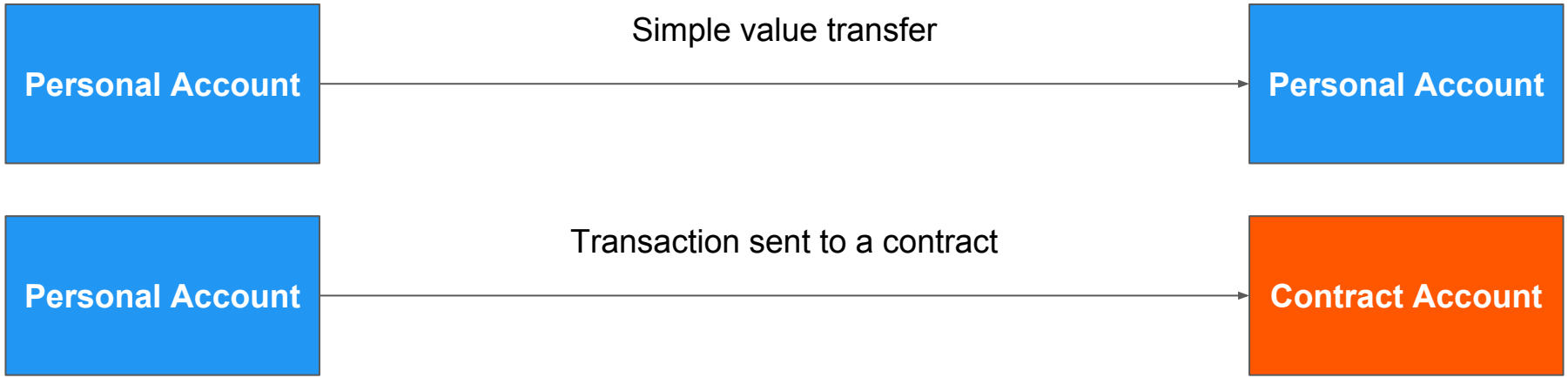
Transaction for contract creation




Create
Interact
Destroy

Transaction for contract interaction



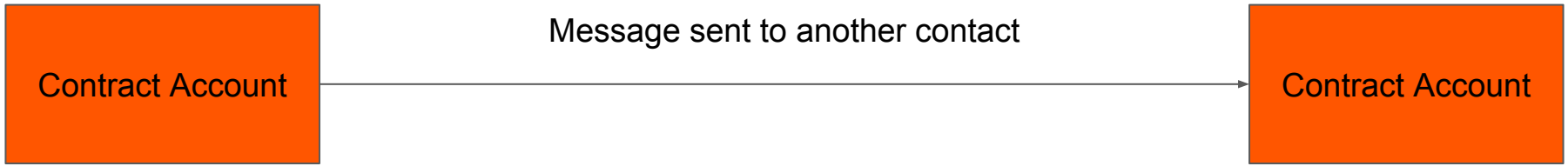

Personal Account
Simple value transfer
Personal Account
Personal Account
Transaction sent to a contract
Contract Account

Contract method call

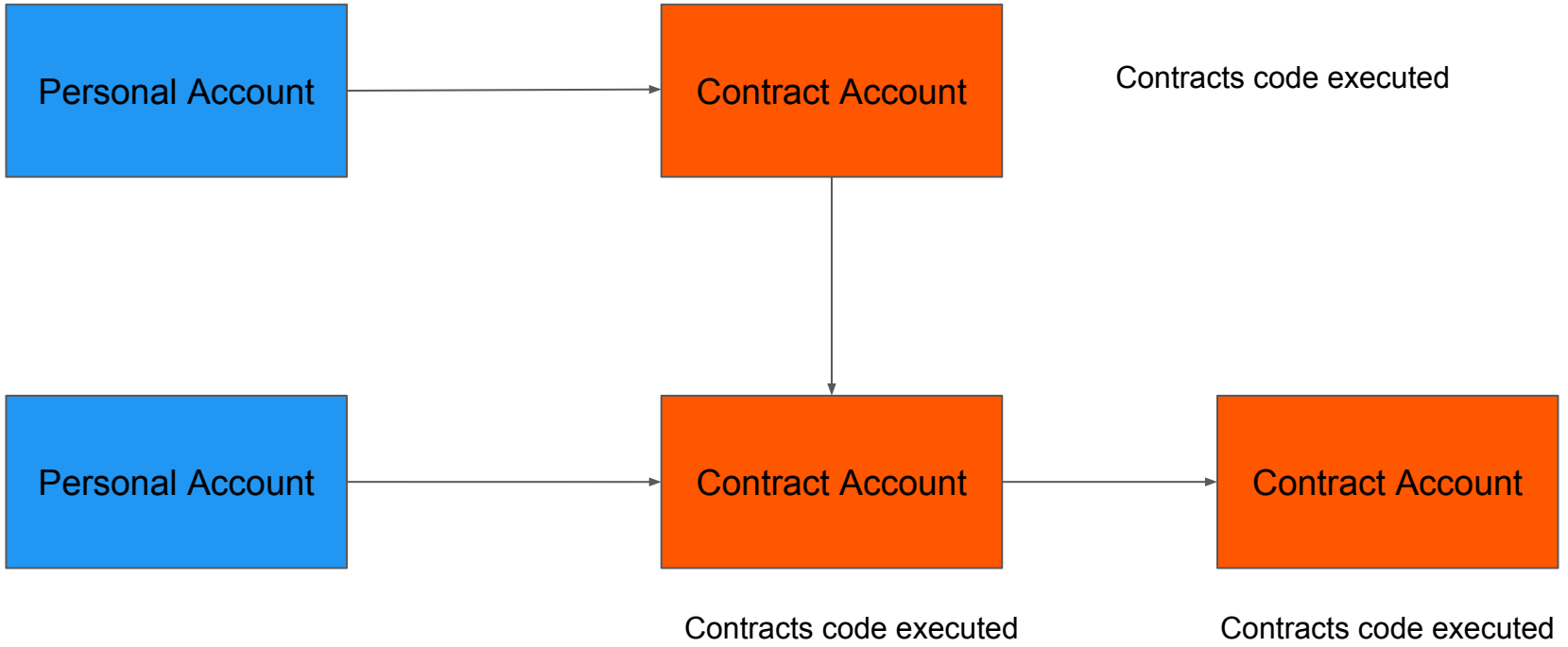
- When contract account is activated:
  a. Contract **code** runs
  b. It can read / write to **internal storage**
  c. It can **send other messages** or create **new contracts**
- Can’t initiate new transactions on their own
- Can only fire transactions in response to other transactions received

Messages

- Like a **transaction** except it is **produced by a contract**
- Virtual objects
- Exist **only** in the **Ethereum execution environment**
- A message leads to the recipient account running its code
- **Contracts** can have **relationships** with **other contracts**


Contract Account
Message sent to another contact
Contract Account

Transactions & messages

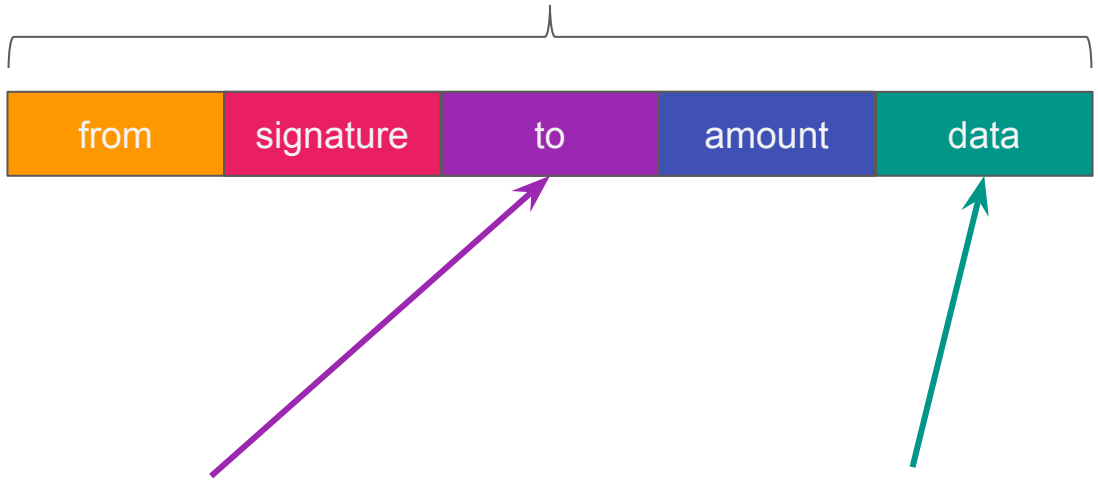


Types of transactions

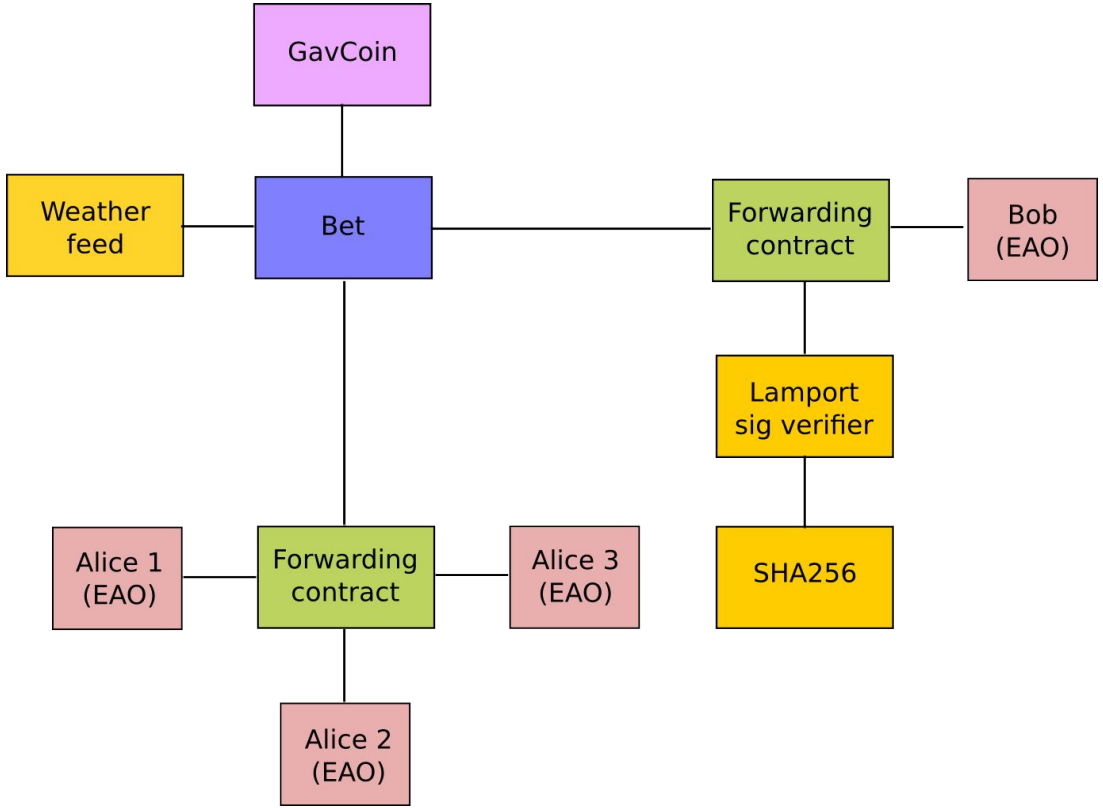
	create	send	call
from	creator	sender	caller
signature	sig	sig	sig
to	∅	receiver	contract
amount	ETH	ETH	ETH
data	code	∅	f, args


Create
Interact
Destroy

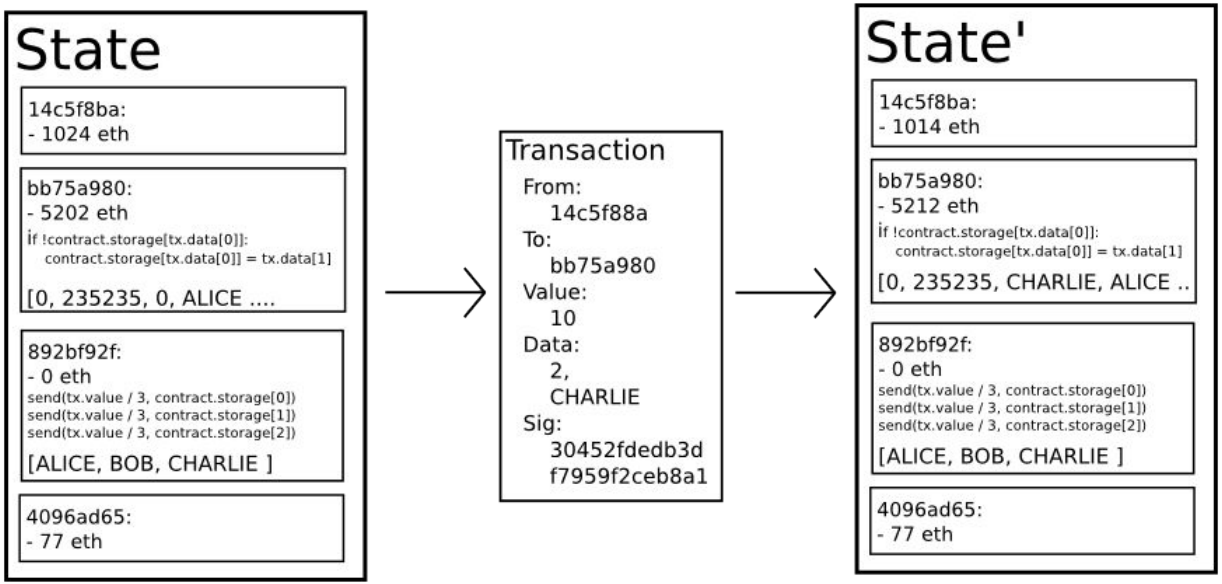
a transaction for contract destruction

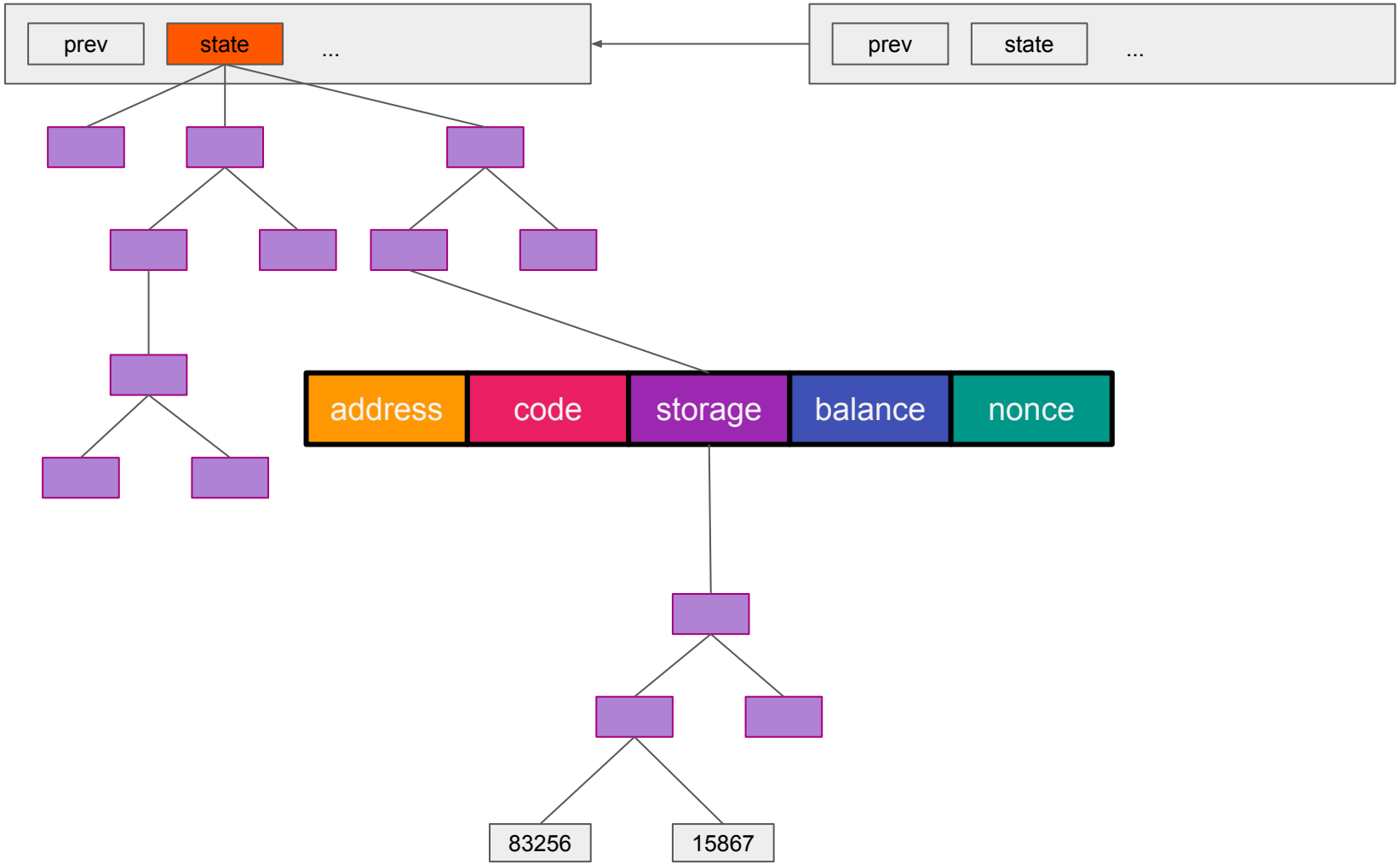


Example of contract and account interaction

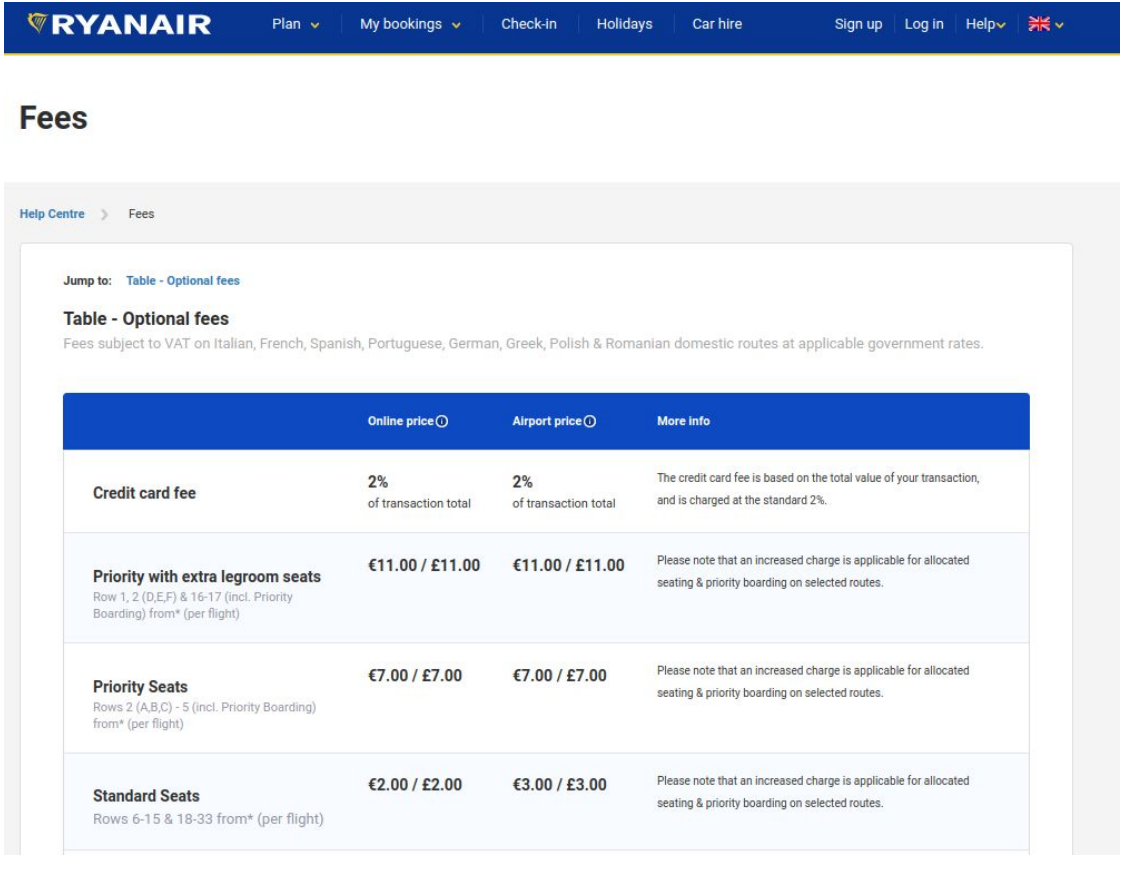


Ethereum state machine




prev
state
...
prev
state
...
address
code
storage
balance
nonce
83256
15867

“Ethereum is Ryanair”: pay to board, then keep paying



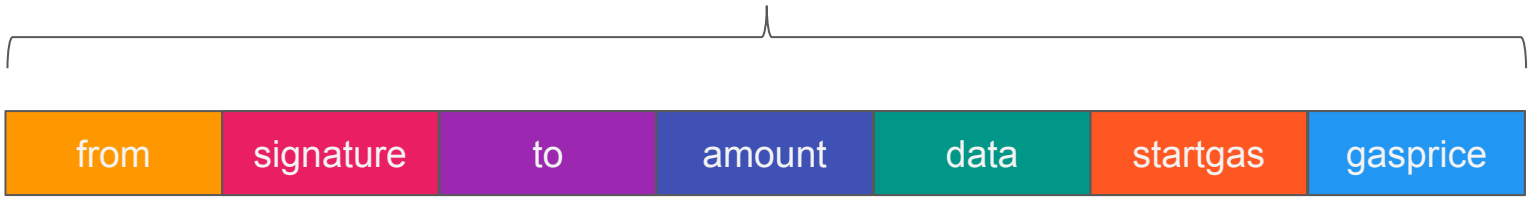
Gas: a necessary evil

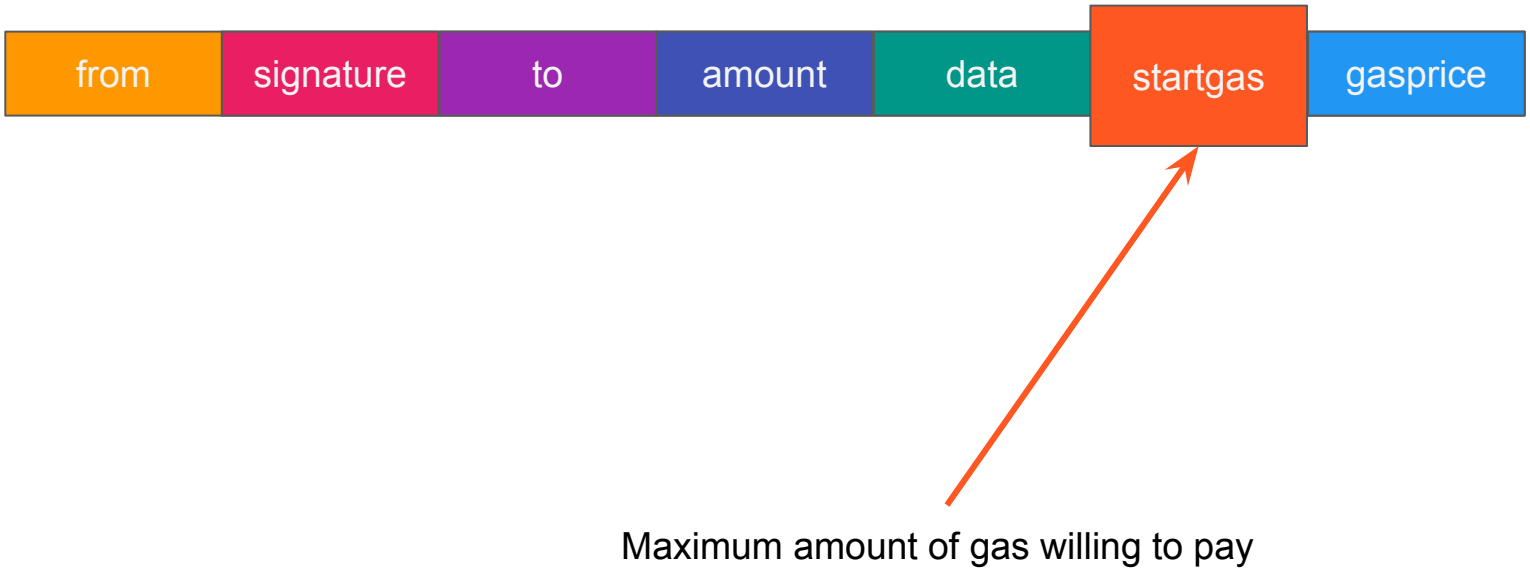
- Every node on the network:
  - evaluate all **transactions**
  - store all **state**
- Halting problem

Gas: a necessary evil

- Every **computation step** has a **fee**
- Is **paid** in **gas**
- **Gas** is the **unit** used to **measure computations**

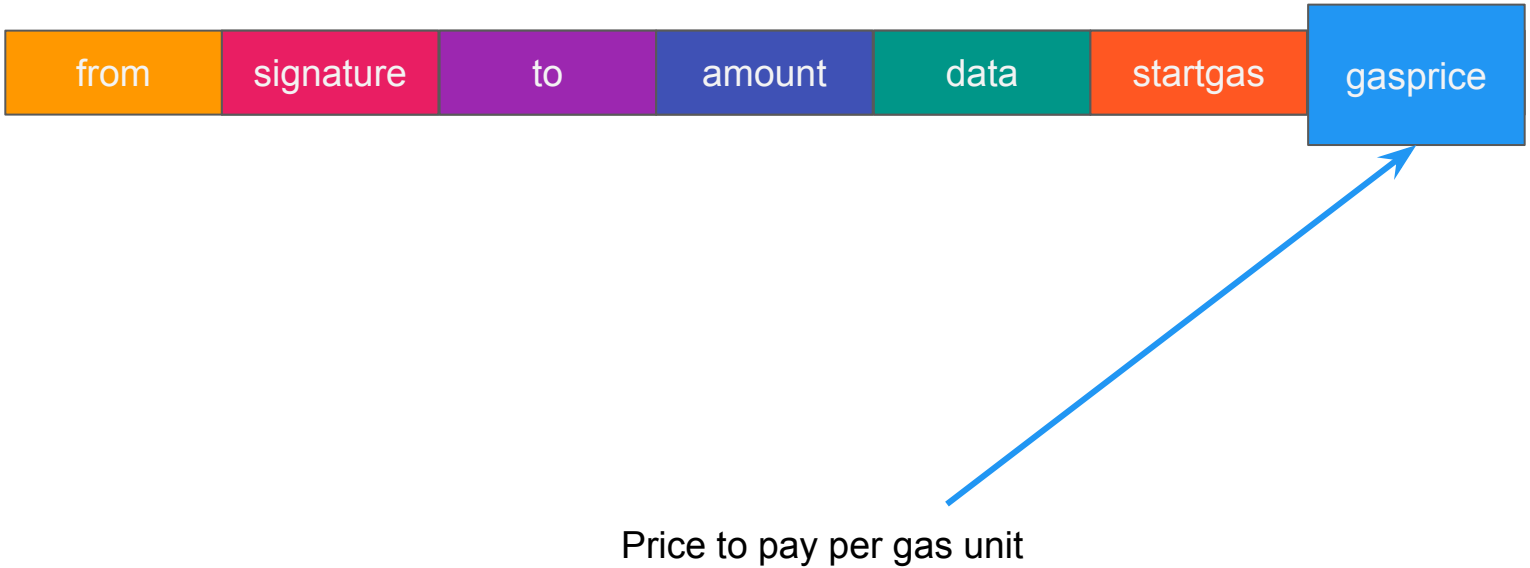
Ethereum transaction




from
signature
to
amount
data
startgas
gasprice
Maximum amount of gas willing to pay

Gas Limit

- All **unused gas** is **refunded** at the end of a transactio
- **Out of gas** transaction are **not refundable**


from
signature
to
amount
data
startgas
gasprice
Price to pay per gas unit

Gas Price

- Measured in **gwei** (1 × 10^9 Wei)
- Determines how **quickly** a transaction will be **mined**

Transaction Fees

Gas costs

Operation	Gas	Description
ADD/SUB	3	Arithmetic operation
MUL/DIV	5	Arithmetic operation
ADDMOD/MULMOD	8	Arithmetic operation
AND/OR/XOR	3	Bitwise logic operation
LT/GT/SLT/SGT/EQ	3	Comparison operation
POP	2	Stack operation
PUSH/DUP/SWAP	3	Stack operation
MLOAD/MSTORE	3	Memory operation

Gas costs

Operation	Gas	Description
JUMP	8	Unconditional jump
JUMPI	10	Conditional jump
SLOAD	200	Storage operation
SSTORE	5.000 / 20.000	Storage operation
BALANCE	400	Get balance of an account
CREATE	32.000	Create a new account using CREATE
CALL	25.000	Create a new account using CALL

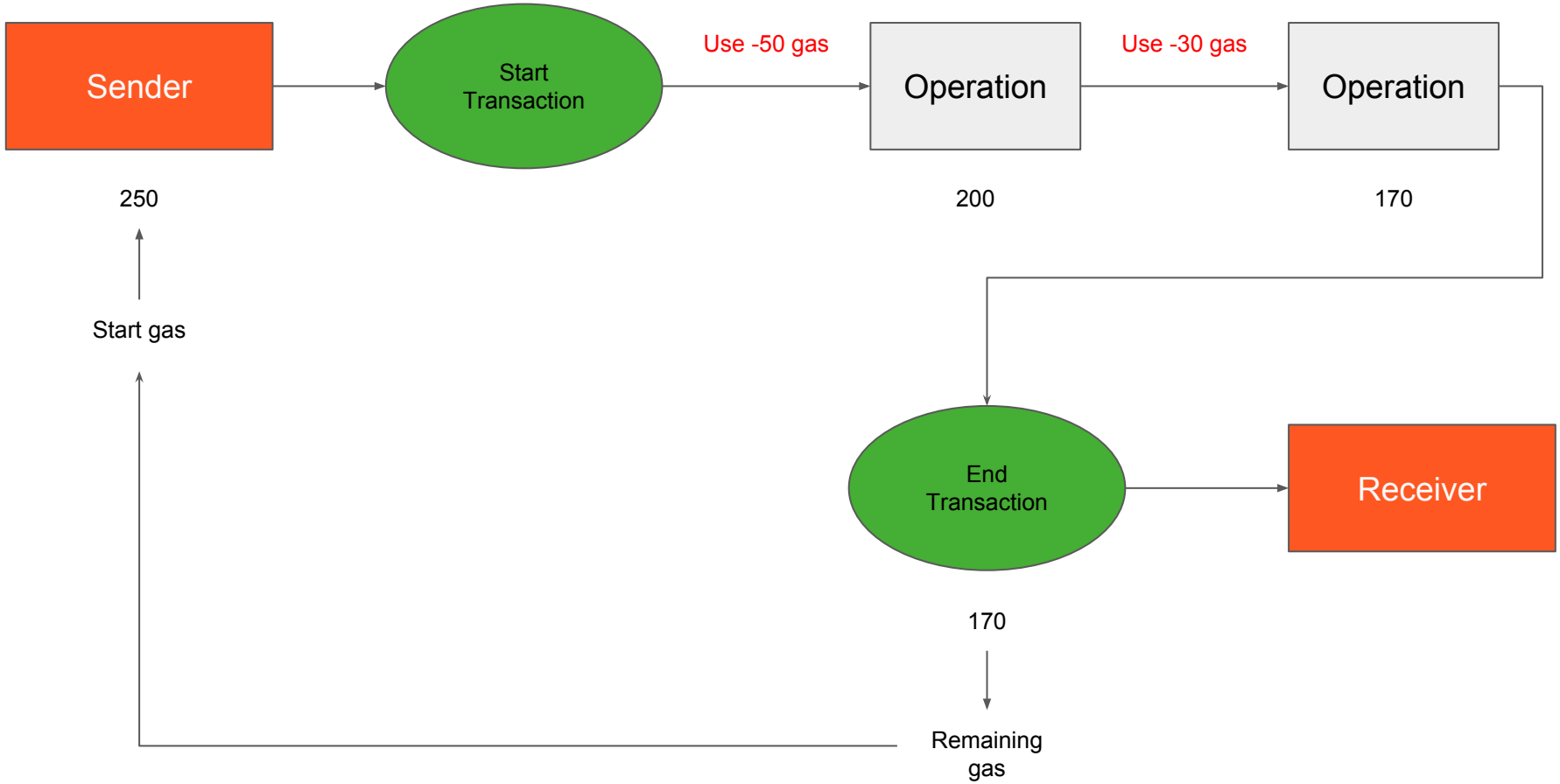
Storage in Ethereum

ETH Price: $966.33 (Feb 17, 2018) - Gas Price: 3 Gwei

Size	Gas	Cost
32 bytes	20.000	$0,058
1KB	724.664	$2.104
1MB	697.325.562	$2,025.03
10MB	~7.000.000.000	~$20,328
100MB	~70.000.000.000	~$203,280
1GB	~700.000.000.000	~$2,032,800

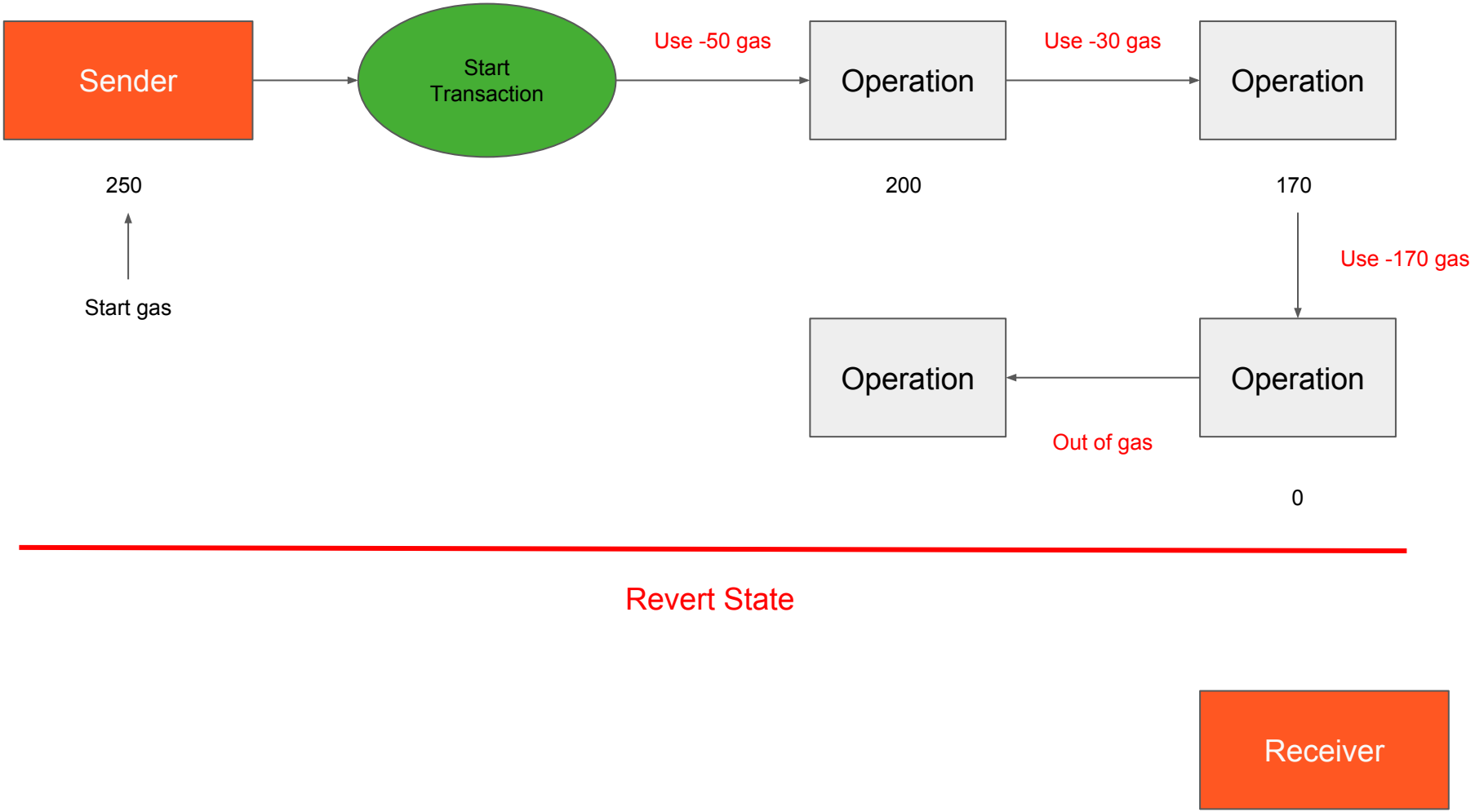
Computation steps

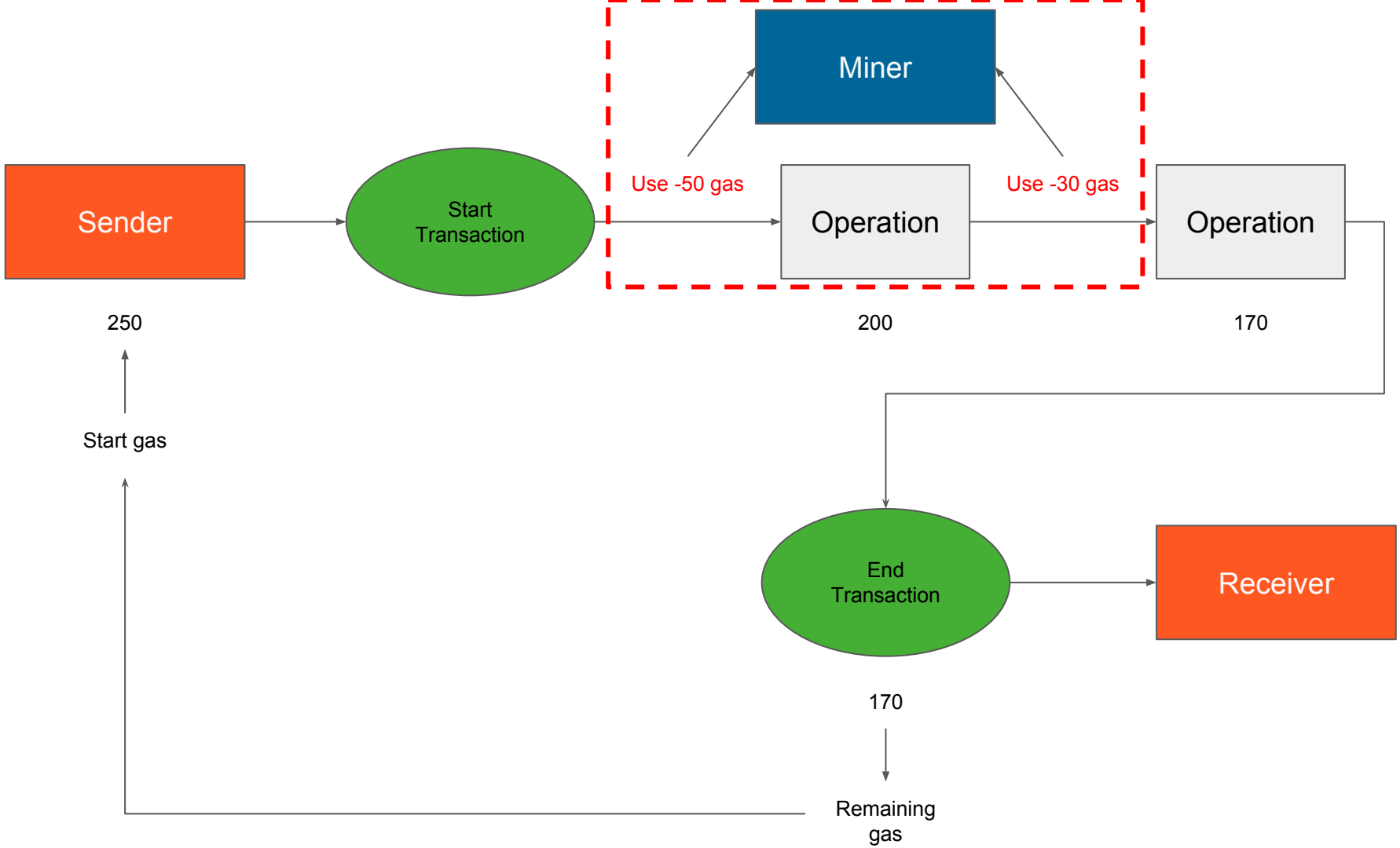
1. If **gas_limit** * **gas_price** > **balance** then **halt**
2. **Deduct** gas_limit * gas_price from **balance**
3. Set gas = gas_limit
4. **Run code** deducting from gas
5. After termination **return remaining gas** to **balance**


Sender
Start Transaction
Use -50 gas
Operation
Use -30 gas
Operation
250
200
170
Start gas
End Transaction
Receiver
170
Remaining gas

Out of gas exceptions

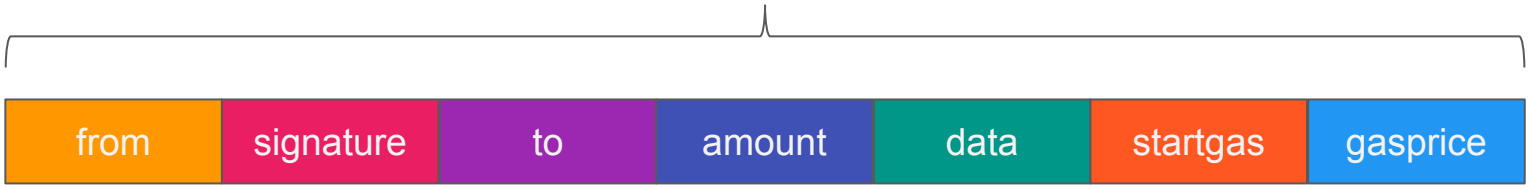
- State **reverts** to **previous state**
- gas_limit * gas_price is **still deducted** from **balance**


Sender
Start Transaction
Use -50 gas
Operation
Use -30 gas
Operation
250
200
170
Start gas
Use -170 gas
Operation
Operation
Out of gas
0
Revert State
Receiver


Miner
Sender
Start Transaction
Use -50 gas
Operation
Use -30 gas
Operation
250
200
170
Start gas
End Transaction
Receiver
170
Remaining gas

Account

Transaction



Ethereum Virtual Machine

- Series of **bytecode** instructions (EVM code)
- Each **bytecode** represents an **operation** (opcode)
- A quasi **Turing complete** machine
- **Stack-based** architecture (1024-depth)
- **32-byte** words (256-bit words)
- **Crypto** primitives

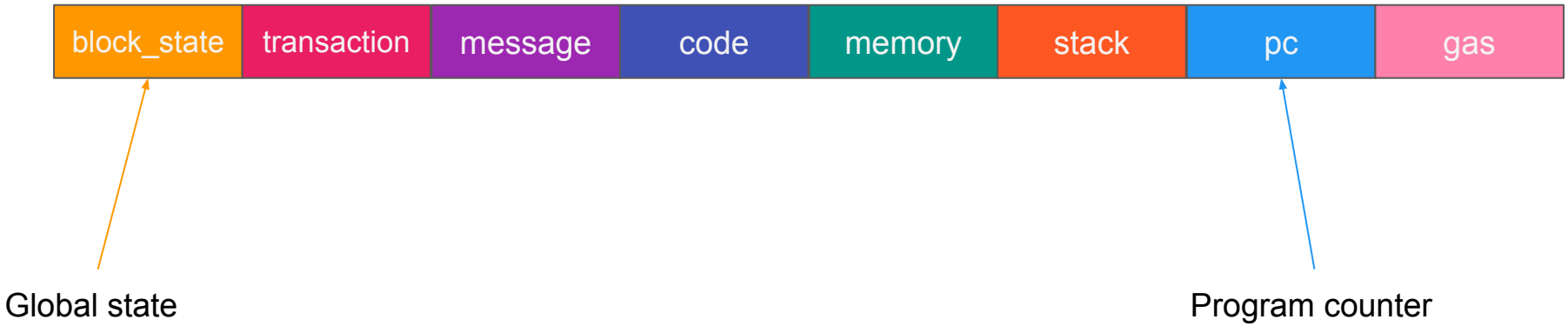
EVM bytecode

```
PUSH1 0
CALLDATALOAD
SLOAD
NOT
PUSH1 9
JUMPI
STOP
JUMPDEST
PUSH1 32
CALLDATALOAD
PUSH1 0
CALLDATALOAD
SSTORE
```

EVM: contract execution

- Three types of storage:
  - **Stack**
  - **Memory** (expandable byte array)
  - **Storage** (key/value store)
- All memory is **zero-initialized**
- Access: **value**, **sender**, **data**, **gas** limit and **block header** data (depth, timestamp, miner, hash)

EVM: computational state



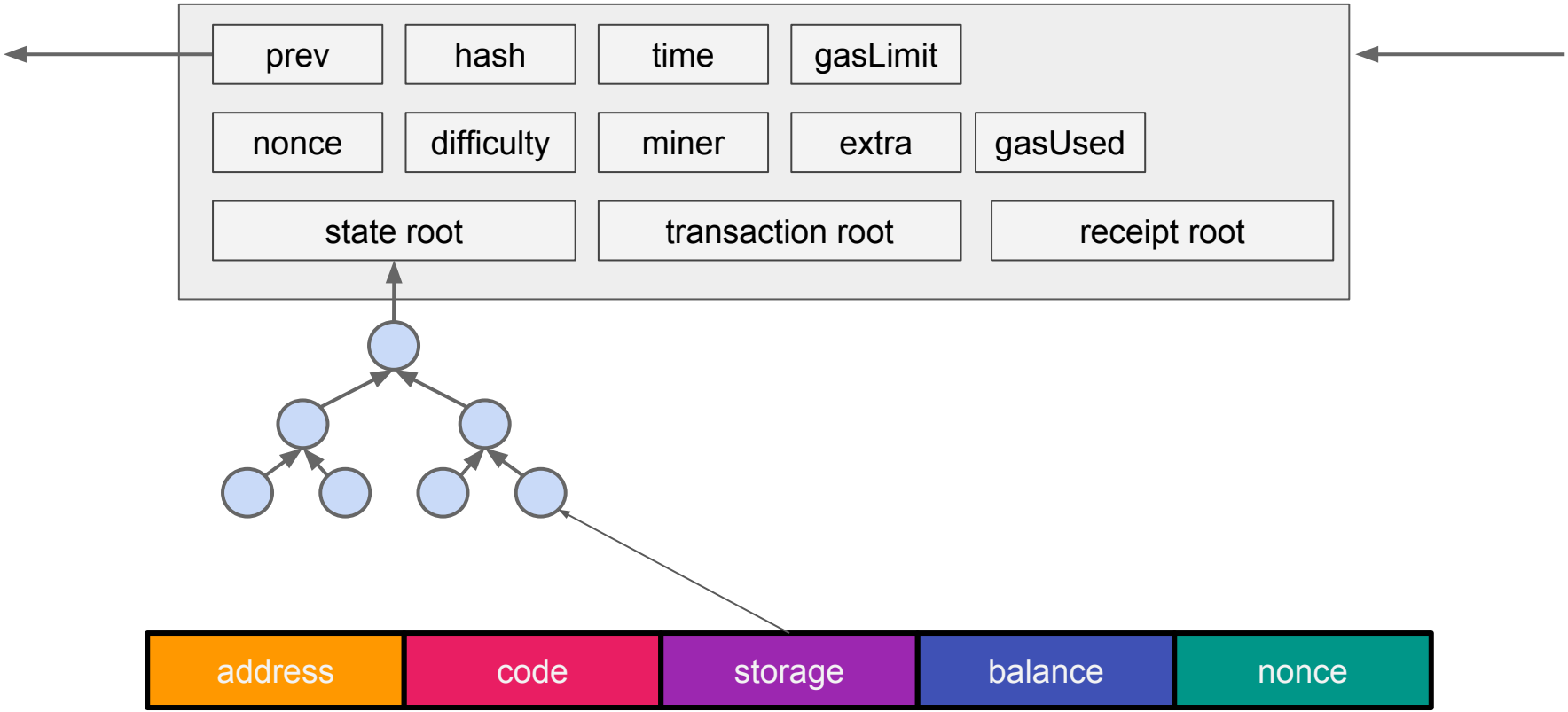
Ethereum Mining

- **Similar** to **Bitcoin**
- **Blocks** contain: **transaction** list and most **recent state**
- Block **time**: ~12 - 15 **seconds**
- **Proof-of-work**: Ethash (designed to be **memory-hard**)
- Casper: Future transition to **proof-of-stake**
- **Winner** of the block: **3 ETH**

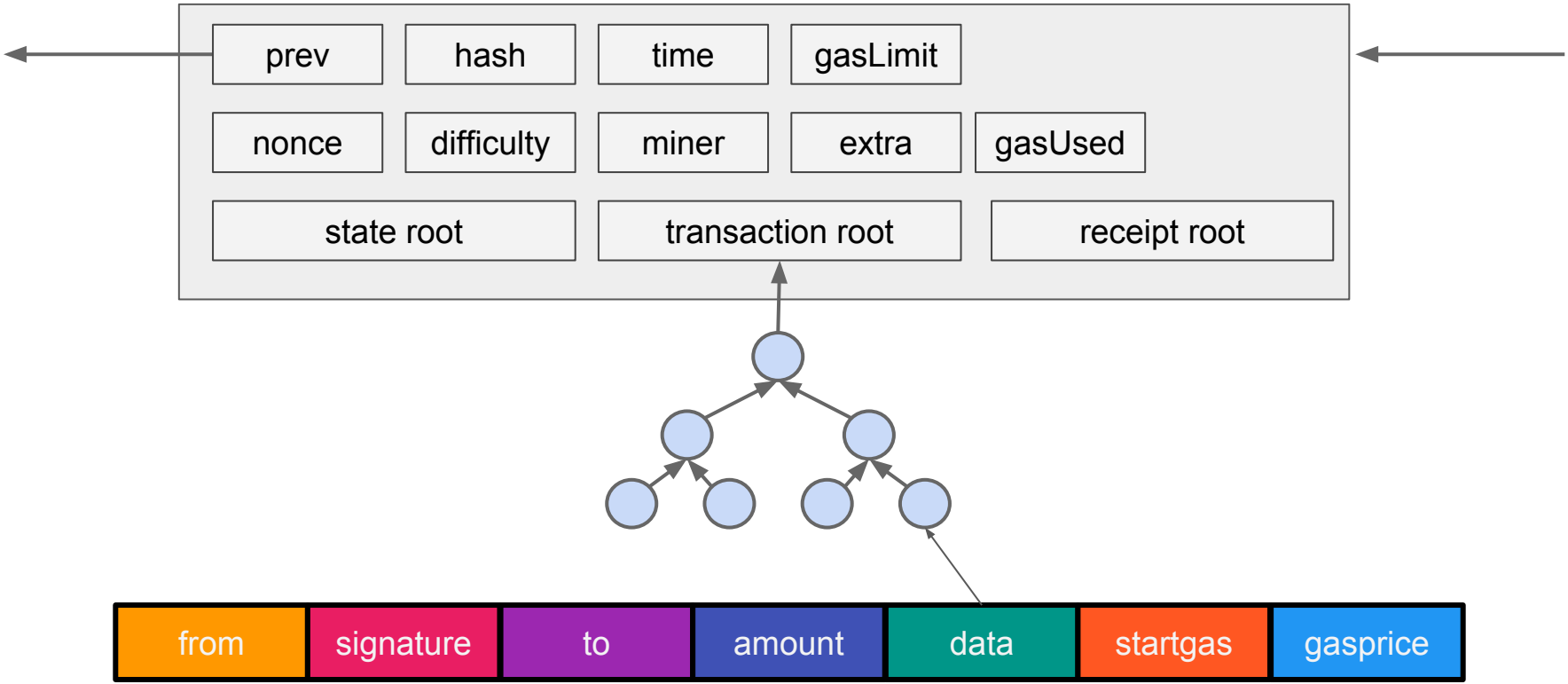
Ethereum Mining

- Uses a variant of **GHOST** (Greedy Heaviest Observed Subtree) protocol to **reward stale blocks**
- The GHOST protocol rule **picks the chain** that has had the **most computation** done upon it
- Planned hard forks: Next one at 2018 (Metropolis)

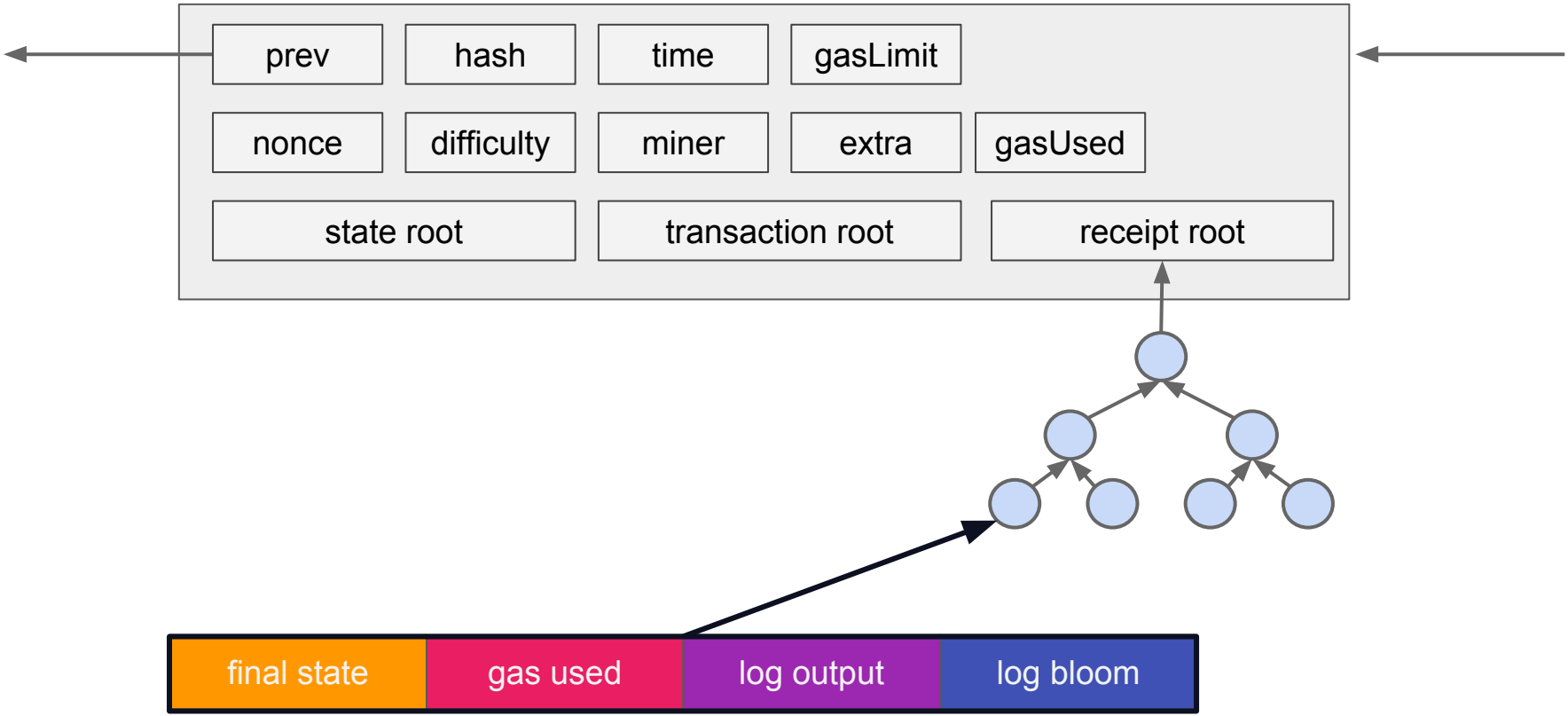
Ethereum block

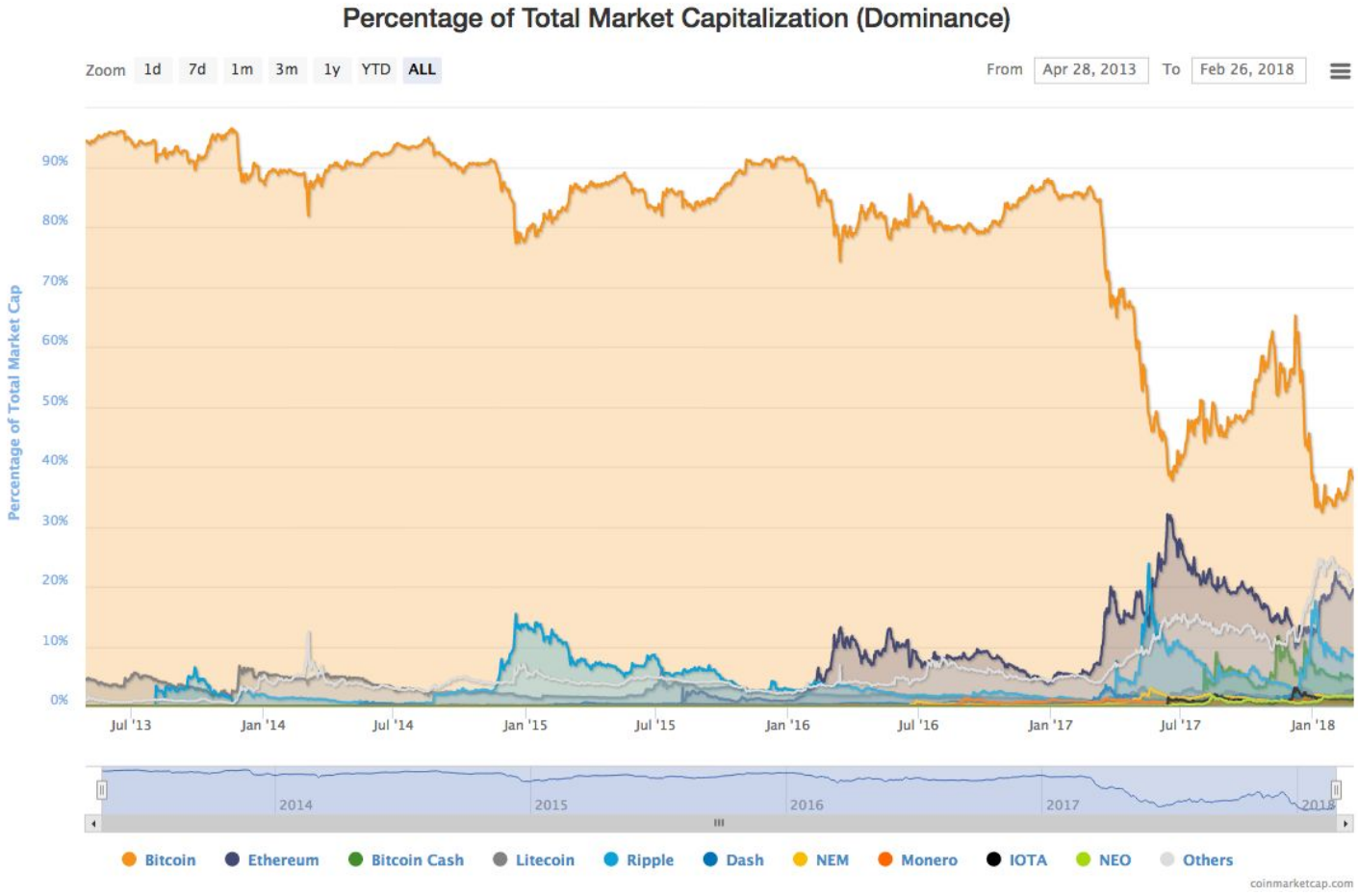


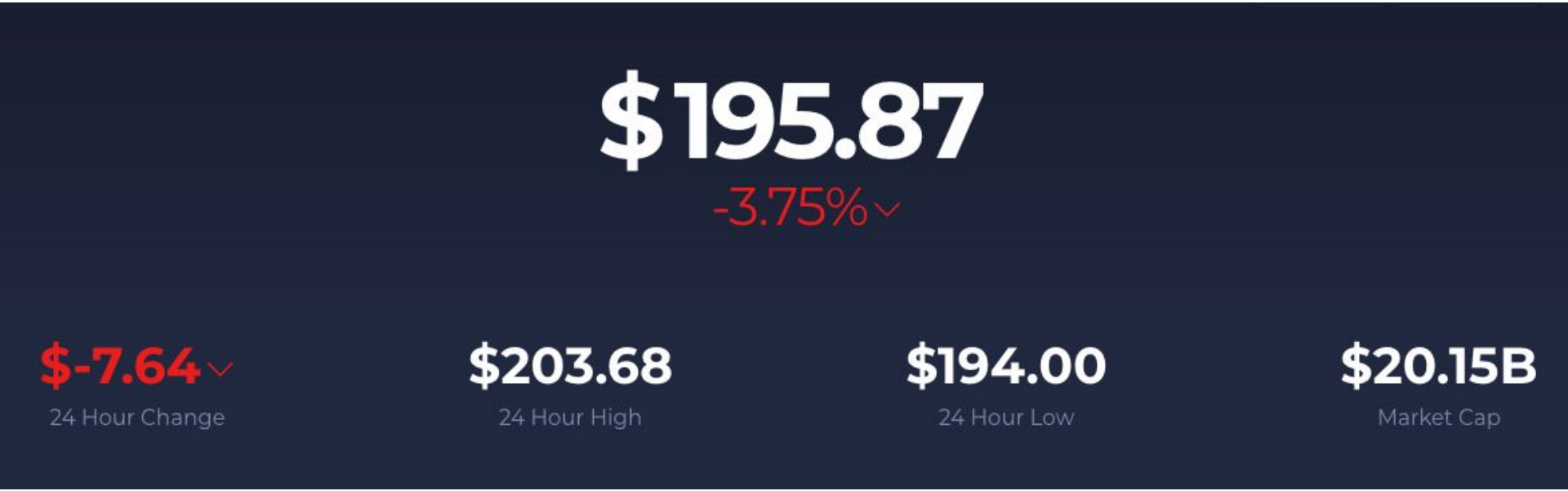
Ethereum block



Ethereum block




Percentage of Total Market Capitalization (Dominance)
Zoom 1d 7d 1m 3m 1y YTD ALL
From Apr 28, 2013 To Feb 26, 2018
Percentage of Total Market Cap
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17
Jan '18
2014
2015
2016
2017
2018
Bitcoin
Ethereum
Bitcoin Cash
Litecoin
Ripple
Dash
NEM
Monero
IOTA
NEO
Others
coinmarketcap.com

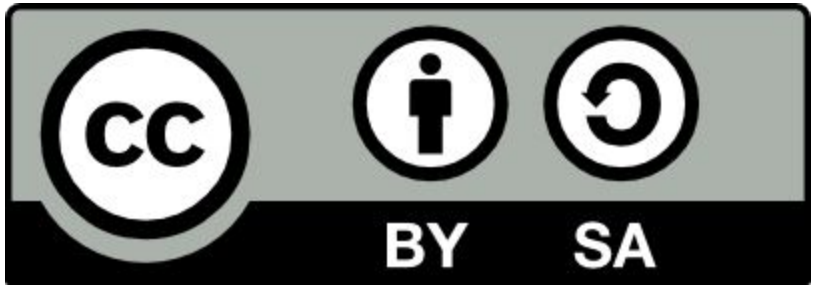


30 October 2018


ETH/USD - MARKET AVERAGE PRICE
ETH/USD: 18.57
Sunday, Mar 5, 2017
May '17
Jun '17
Jul '17
Aug '17
Sep '17
Oct '17
Nov '17
Dec '17
Jan '18
Feb '18
1250
1000
750
500
250
0
-250
Linear
Log
EthereumPrice.org


ETH/USD - MARKET AVERAGE PRICE
ETH/USD: 1 385.06
Sunday, Jan 14, 2018
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17
Sep '17
Oct '17
Nov '17
Dec '17
1250
1000
750
500
250
0
-250
Linear
Log

Thank You


BY
SA