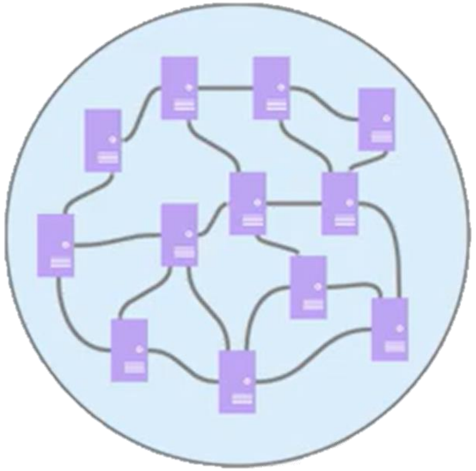
Ethereum: a Secure Decentralised Generalised Transaction Ledger

Dr. Gavin Wood

Founder, Ethereum & Ethcore

What is Ethereum?

- A new way to create and transfer values
- Decentralized computer network
- Using smart contract



Smart Contract

Motivation

Facilitate transactions between consenting individuals who would otherwise have no means to trust one another.

- Geographical separation
- Interfacing difficulty
- Expense
- Uncertainty
- Corruption of existing legal systems

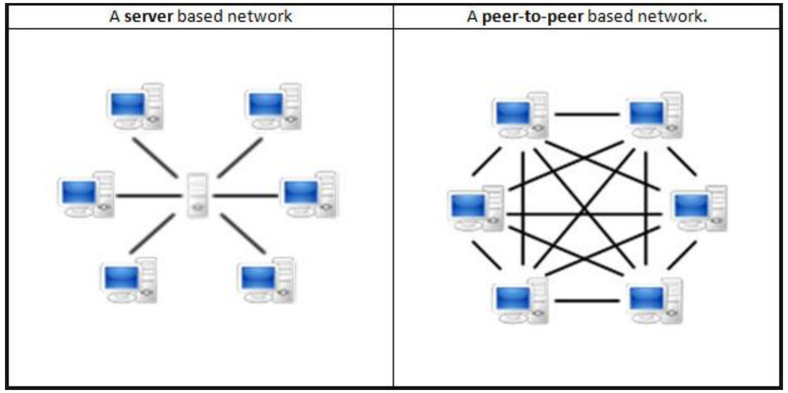
Goal

Provide a system such that users can be guaranteed that no matter with which other individuals, systems or organizations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about.

Decentralized System

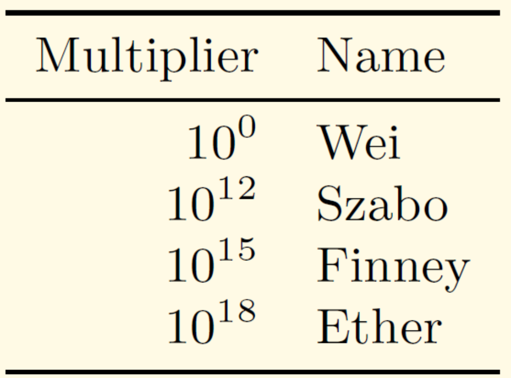
- The network is decentralized.

- Blockchains are peer-to-peer networks.

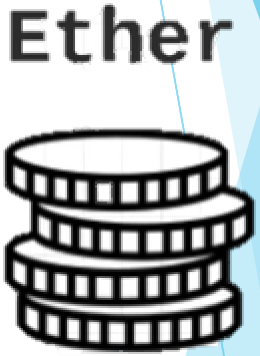


Value

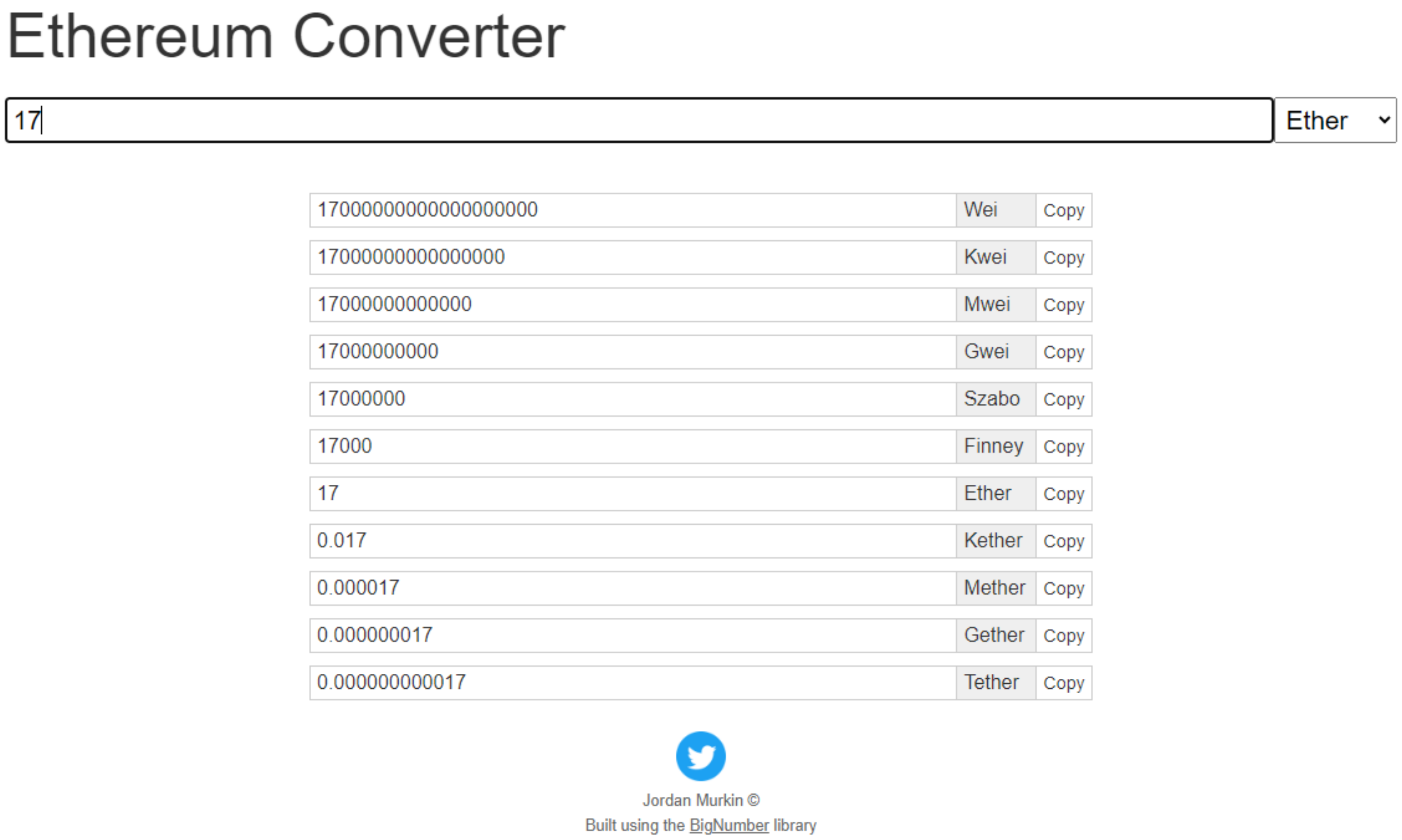
Ethereum has an intrinsic currency, Ether, known also as ETH and sometimes referred to by the Old English *Đ*.



Multiplier	Name
10^{0}	Wei
10^{12}	Szabo
10^{15}	Finney
10^{18}	Ether



Value

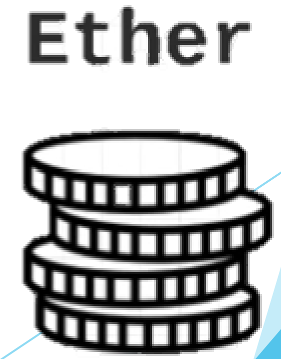


Ethereum Converter

17 | Ether

17000000000000000000	Wei	Copy
17000000000000000	Kwei	Copy
17000000000000	Mwei	Copy
17000000000	Gwei	Copy
17000000	Szabo	Copy
17000	Finney	Copy
17	Ether	Copy
0.017	Kether	Copy
0.000017	Mether	Copy
0.000000017	Gether	Copy
0.000000000017	Tether	Copy

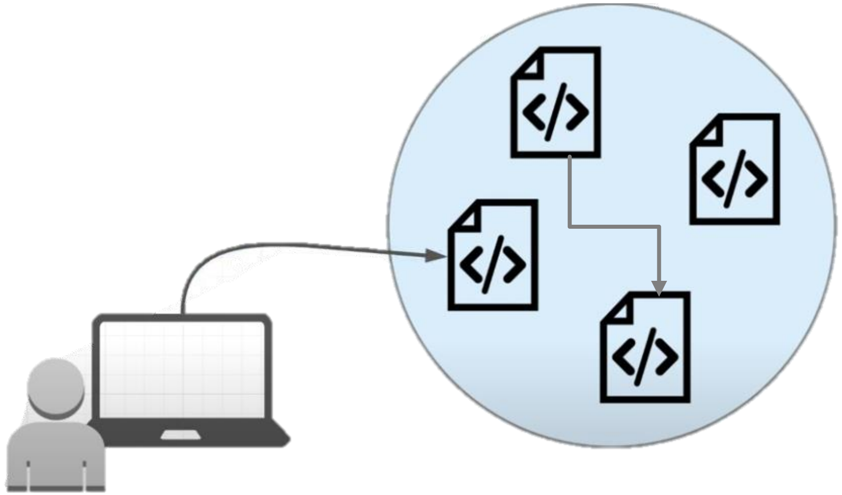
Jordan Murkin ©
Built using the BigNumber library



Account

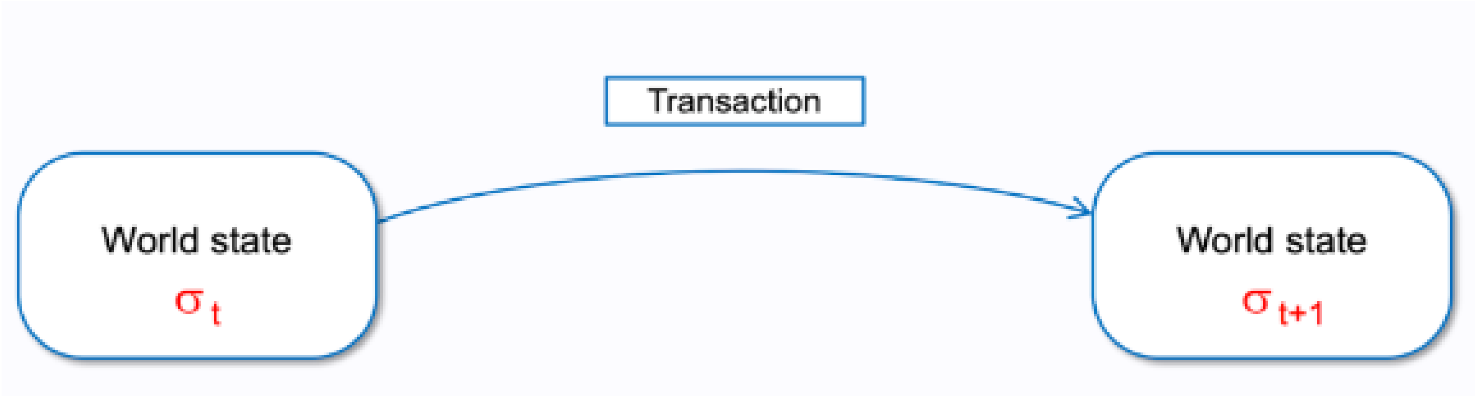
There are two types of accounts:

- Externally Owned Accounts (EOAs)
- Contract accounts



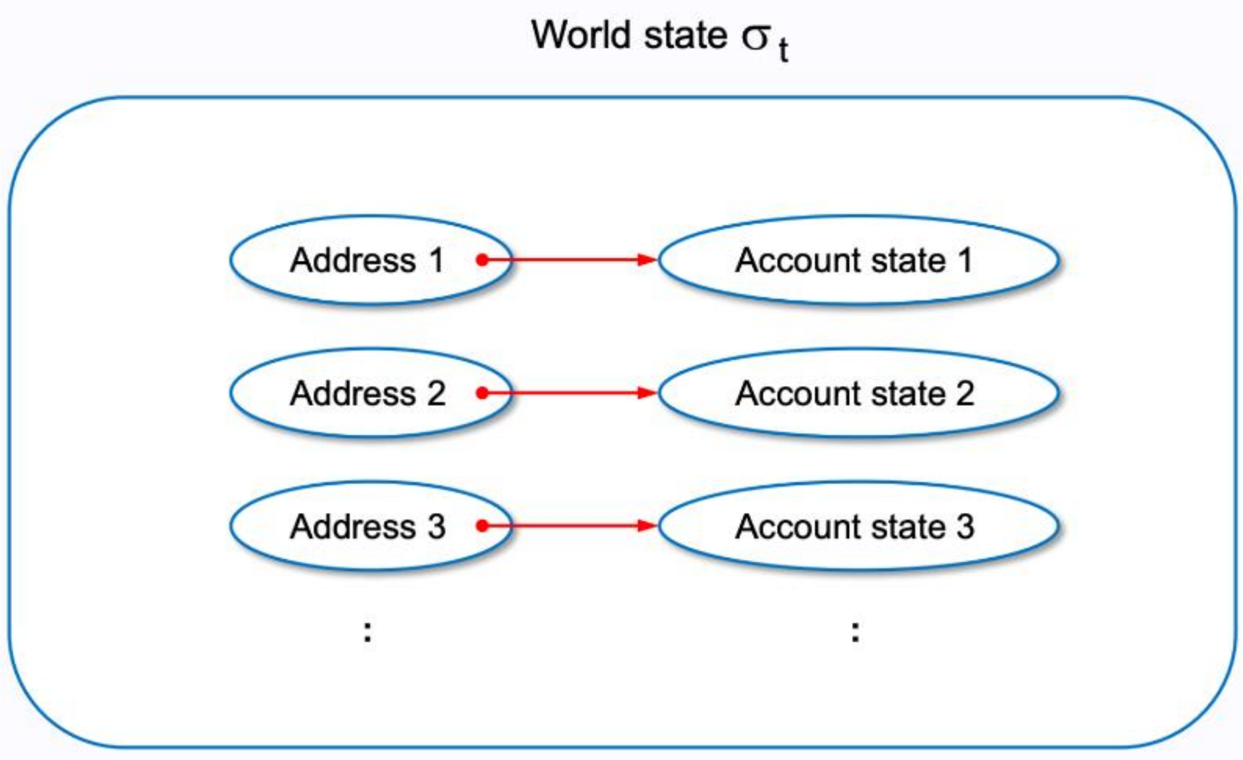
World State

- Transaction-based state machine: $\boldsymbol{\sigma}_{t+1} \equiv \Upsilon(\boldsymbol{\sigma}_t, T)$



World State

- The world state is a mapping between addresses (accounts) and account states.



World state σ_t

Address 1 → Account state 1

Address 2 → Account state 2

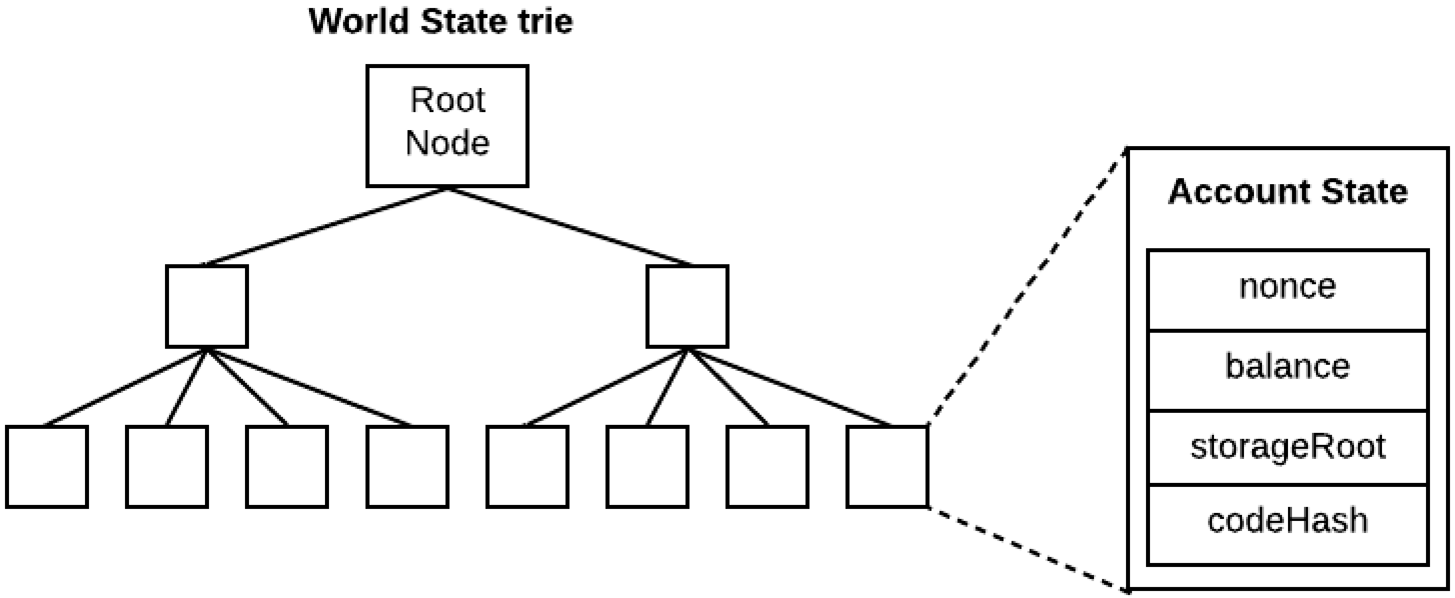
Address 3 → Account state 3

:

:

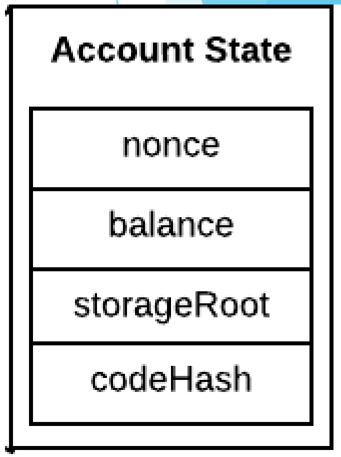
World State

- The implementation will maintain this mapping in a modified Merkle Patricia tree.



Account State

- **nonce** – Number of transactions sent from this address.
- **balance** – Total Ether (in Wei) owned by this account.
- **storageRoot** – Hash of the root node of the account storage trie.
- **codeHash** - For contract accounts, the hash of the EVM code of this account. For EOAs, this will be empty.



Account State

nonce

balance

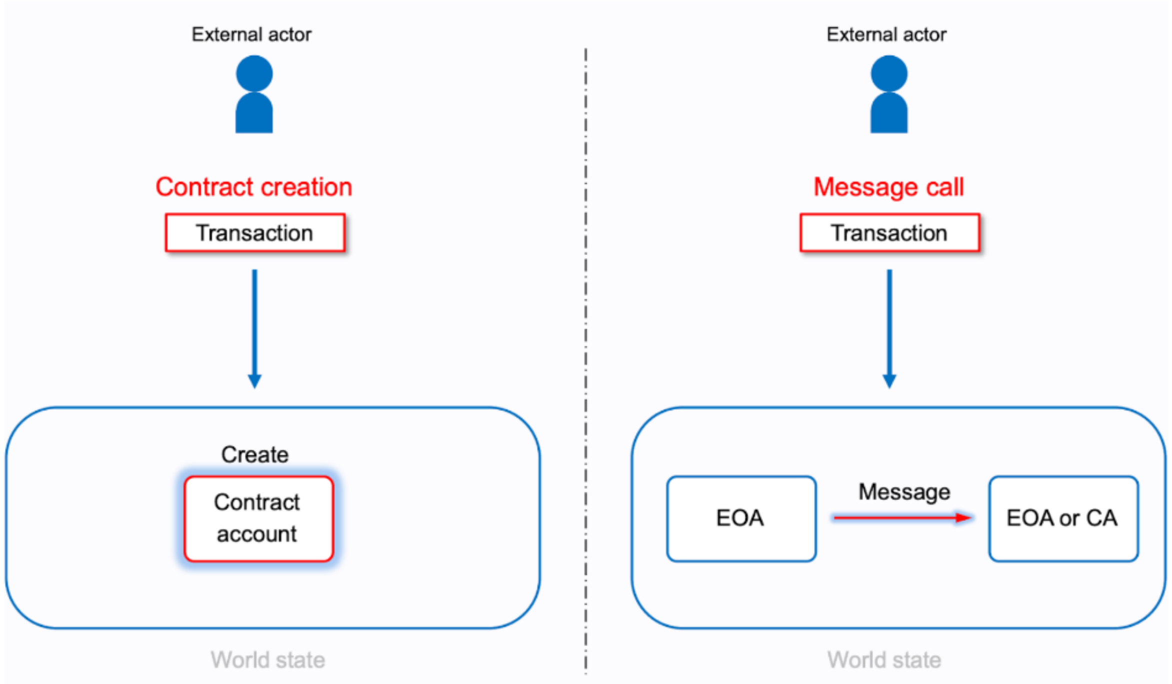
storageRoot

codeHash

Transaction

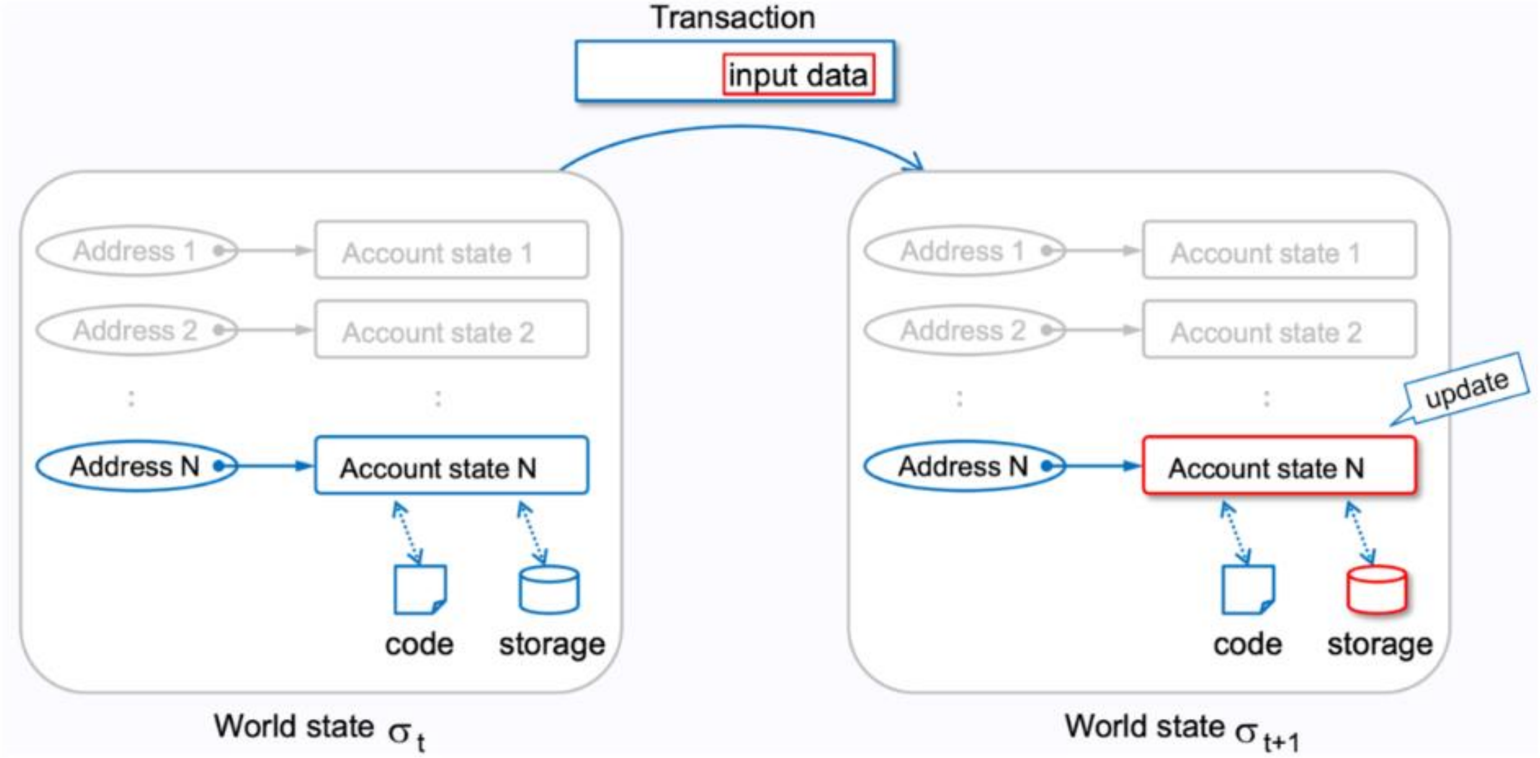
A single cryptographically signed instruction constructed to transfer value.

- **Massage call**
- **Contract creation**



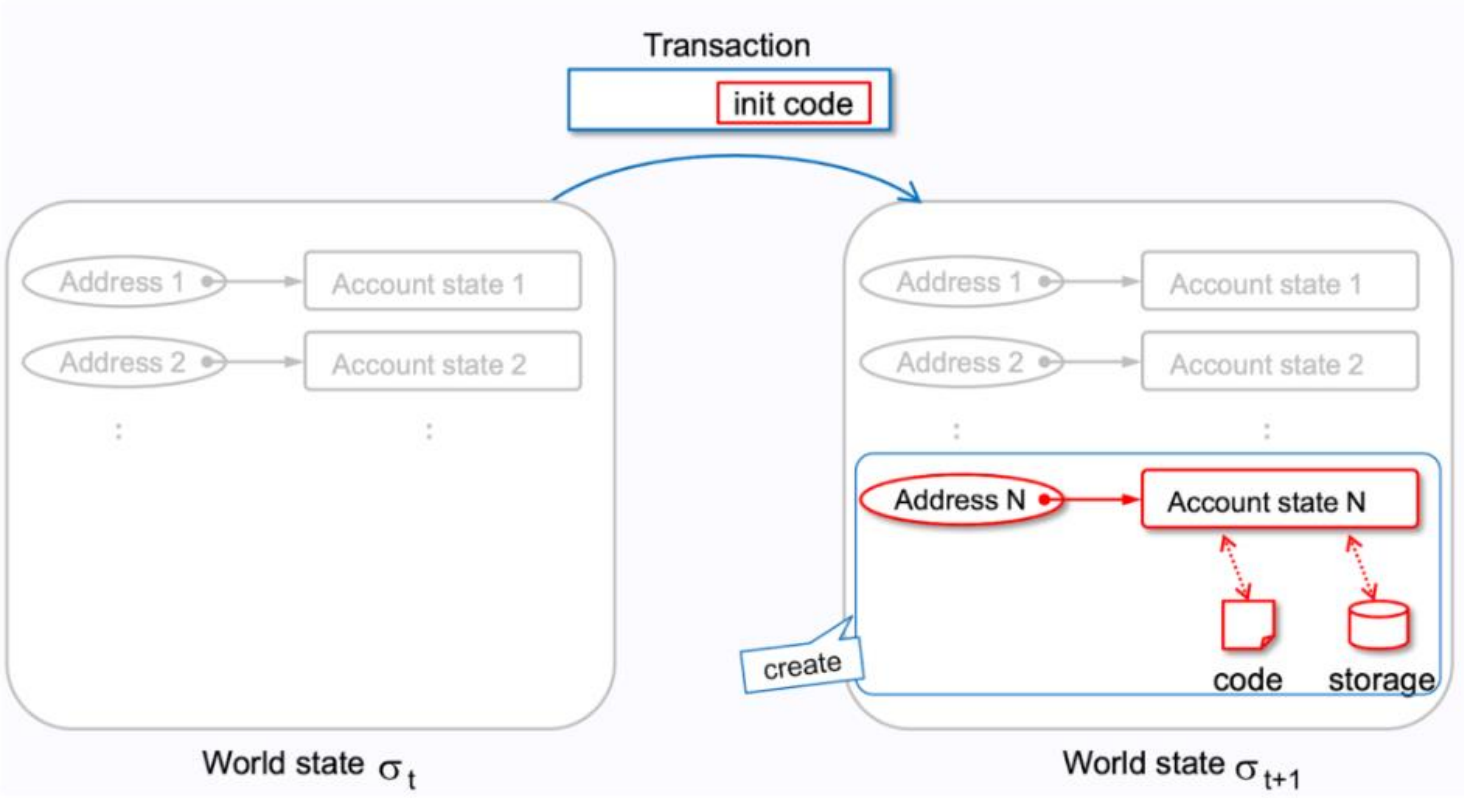
Transaction

Massage call - *updates* an existing entry in the Ethereum world state.

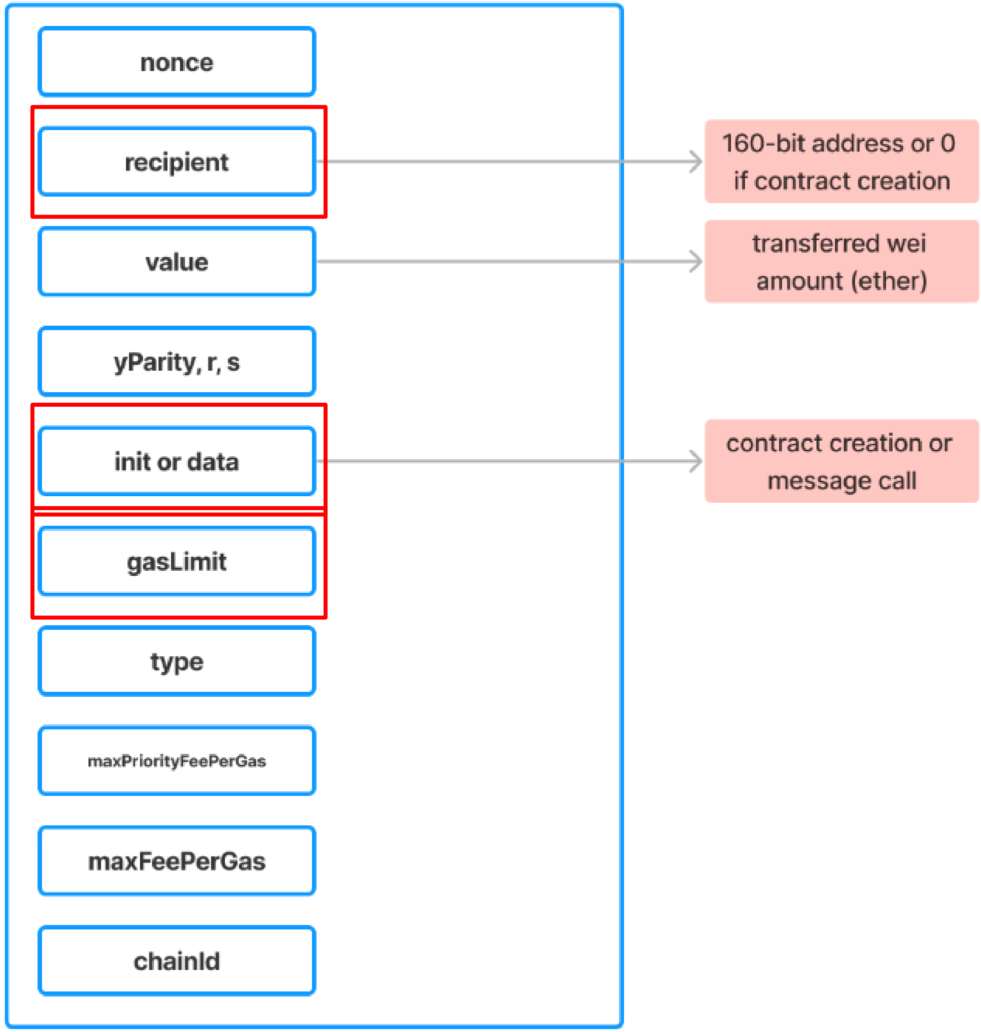


Transaction

Contract creation - *deploys* a new smart contract

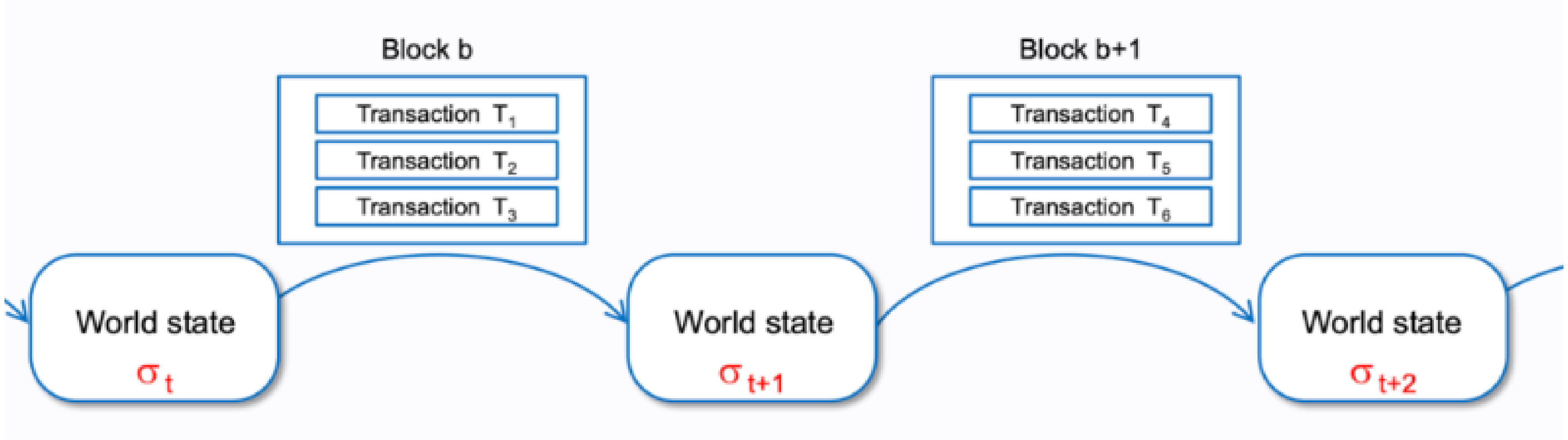


Transaction

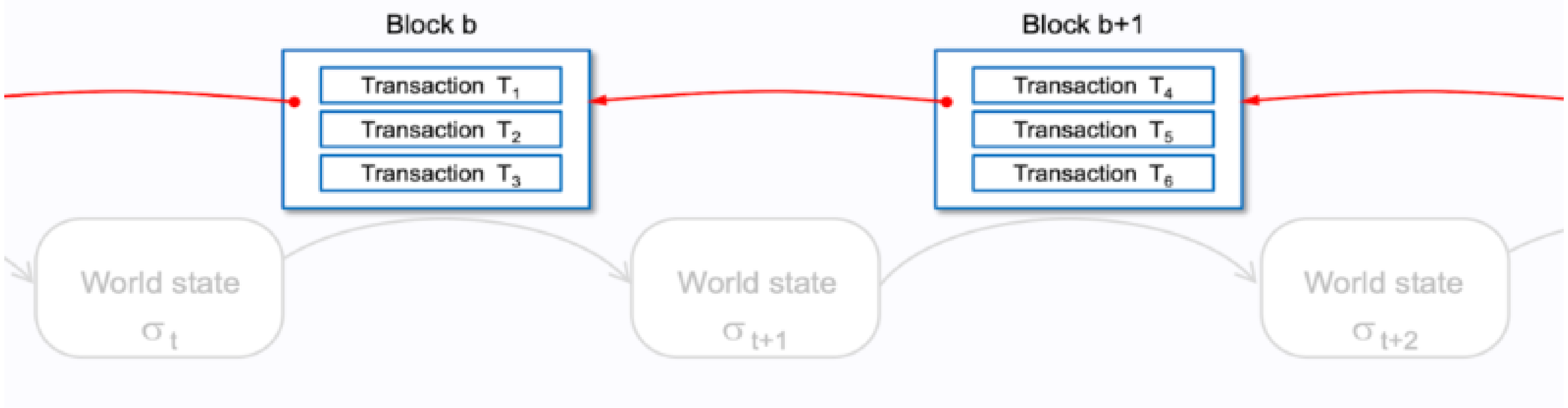

nonce
recipient
value
yParity, r, s
init or data
gasLimit
type
maxPriorityFeePerGas
maxFeePerGas
chainId
160-bit address or 0 if contract creation
transferred wei amount (ether)
contract creation or message call

Transactions

- **Transactions** are collected into blocks

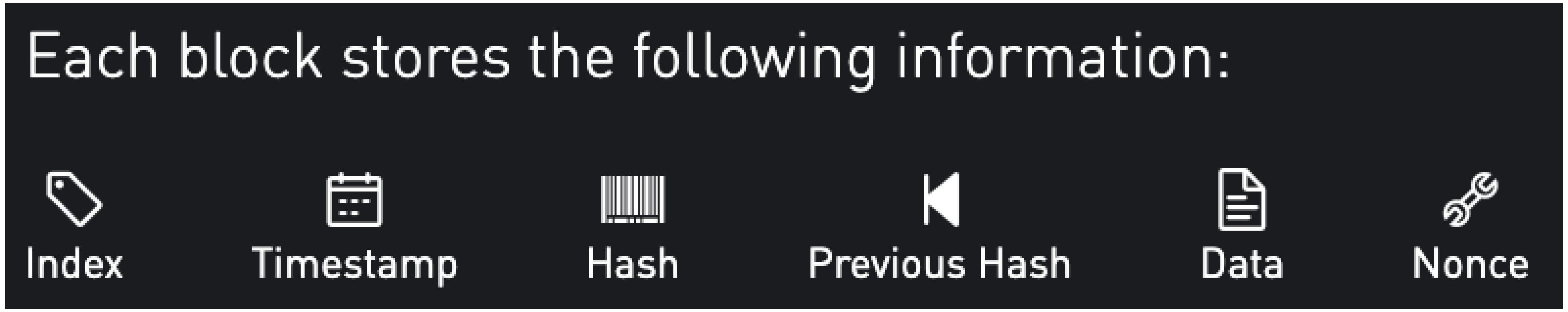


Chain of Blocks - A Blockchain

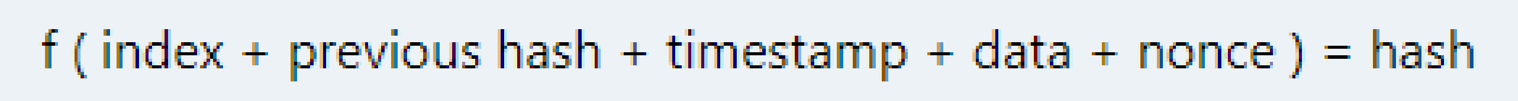


Blockchain demo

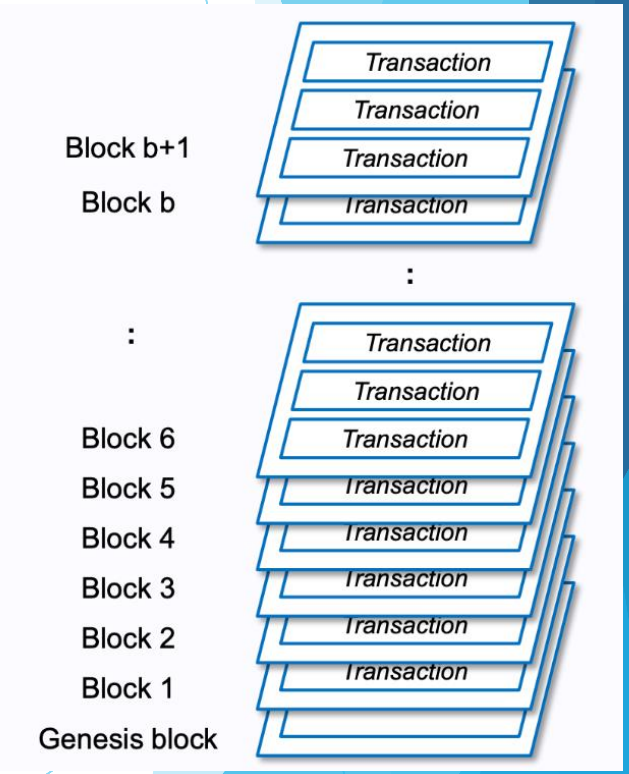
- A **blockchain** has a list of blocks. It starts with a single block, called the **genesis block**.


Each block stores the following information:

Index Timestamp Hash Previous Hash Data Nonce


f (index + previous hash + timestamp + data + nonce) = hash

[redacted]



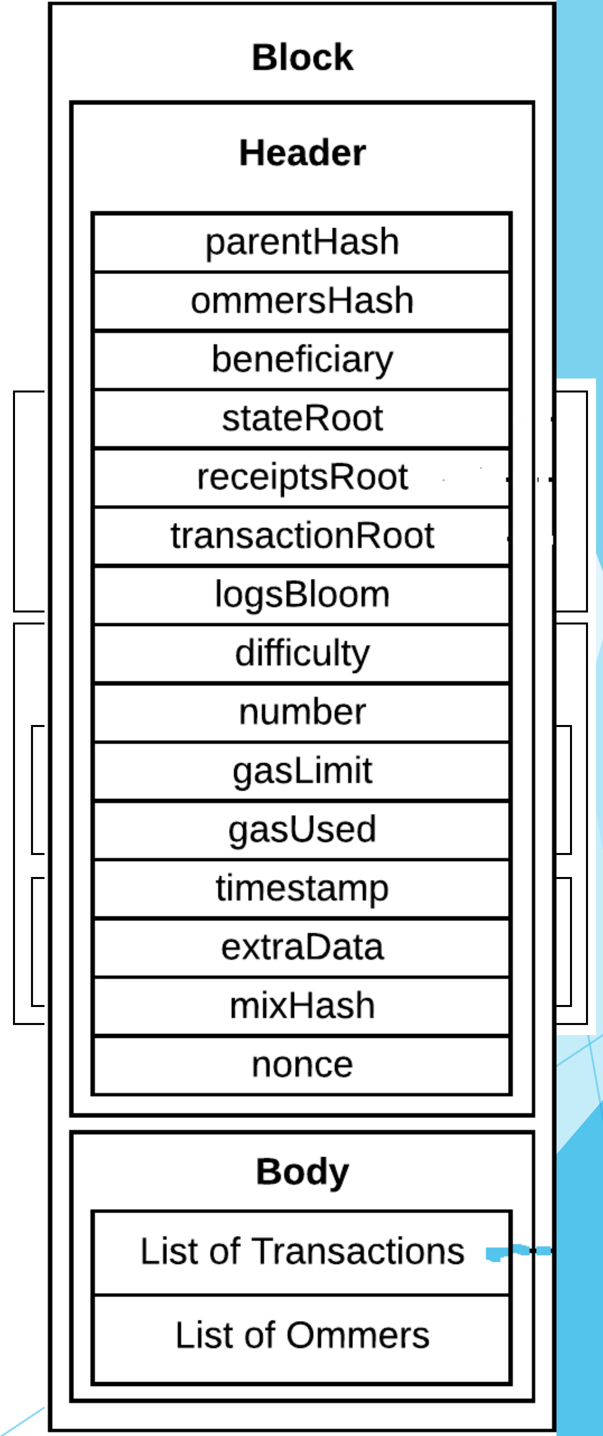
https://.io/blockchaindemo

Block

The block is divided into two parts

- The **block header** is a collection of relevant pieces of information.
- the **block body** contains a list of transactions that have been included in this block, and a list of uncle (ommer) block headers

$$B \equiv (B_H, B_\mathrm{T}, B_\mathrm{U})$$



Block

Header

parentHash
ommersHash
beneficiary
stateRoot
receiptsRoot
transactionRoot
logsBloom
difficulty
number
gasLimit
gasUsed
timestamp
extraData
mixHash
nonce

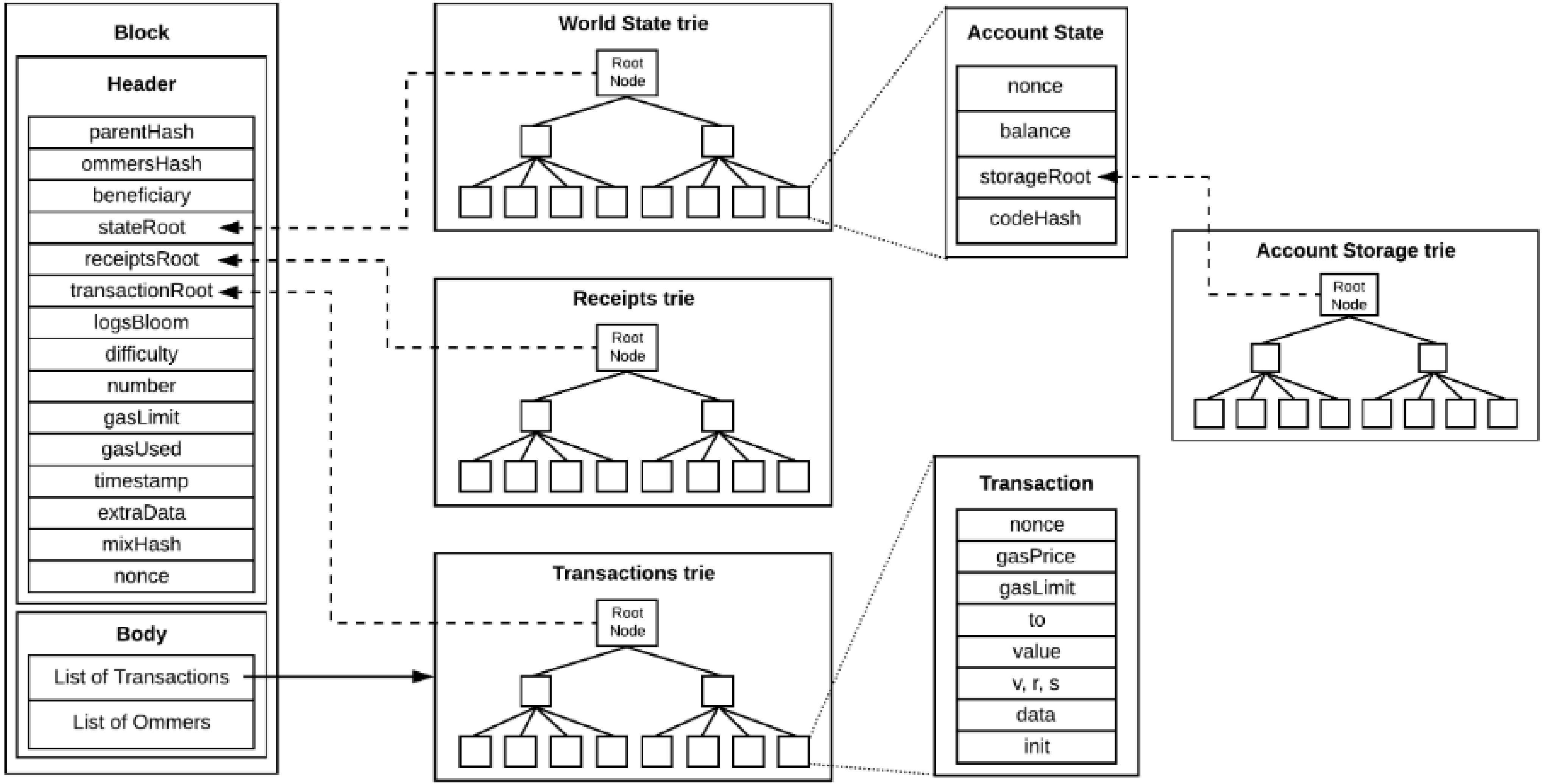
Body

List of Transactions
List of Ommers

Transaction Receipt

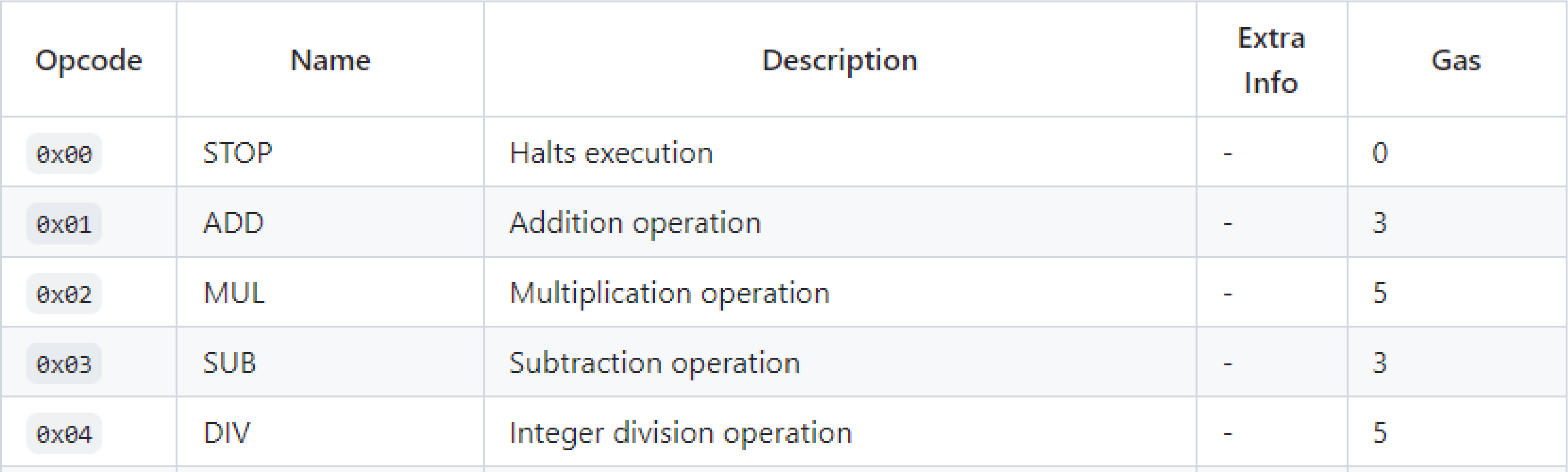
Every time a transaction is executed, Ethereum generates a transaction receipt that contains information about the transaction execution.

Objects covered



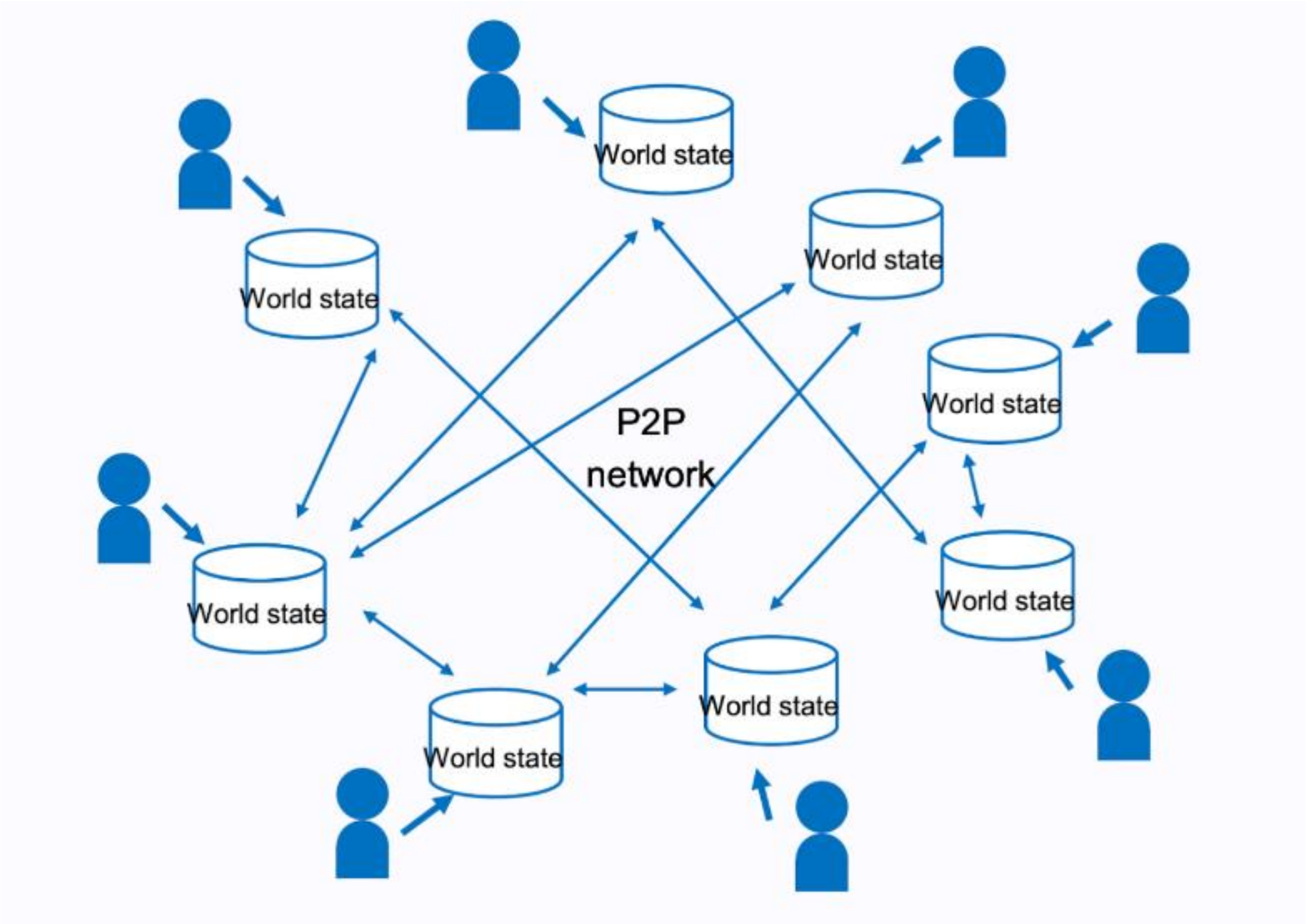
Gas & Payment

- All programmable computation in Ethereum is subject to fees
- The fee schedule is specified in units of *gas*.



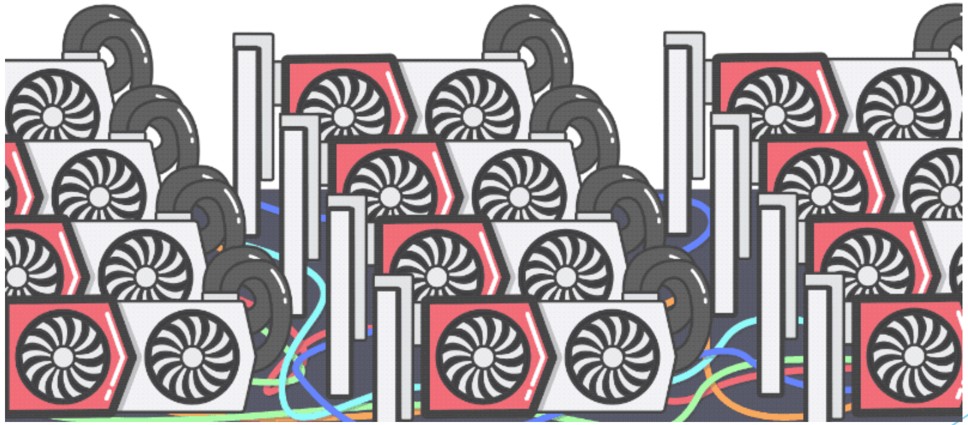
Opcode	Name	Description	Extra Info	Gas
`0x00`	STOP	Halts execution	-	0
`0x01`	ADD	Addition operation	-	3
`0x02`	MUL	Multiplication operation	-	5
`0x03`	SUB	Subtraction operation	-	3
`0x04`	DIV	Integer division operation	-	5

Fees


World state
World state
World state
World state
P2P
network
World state
World state
World state
World state

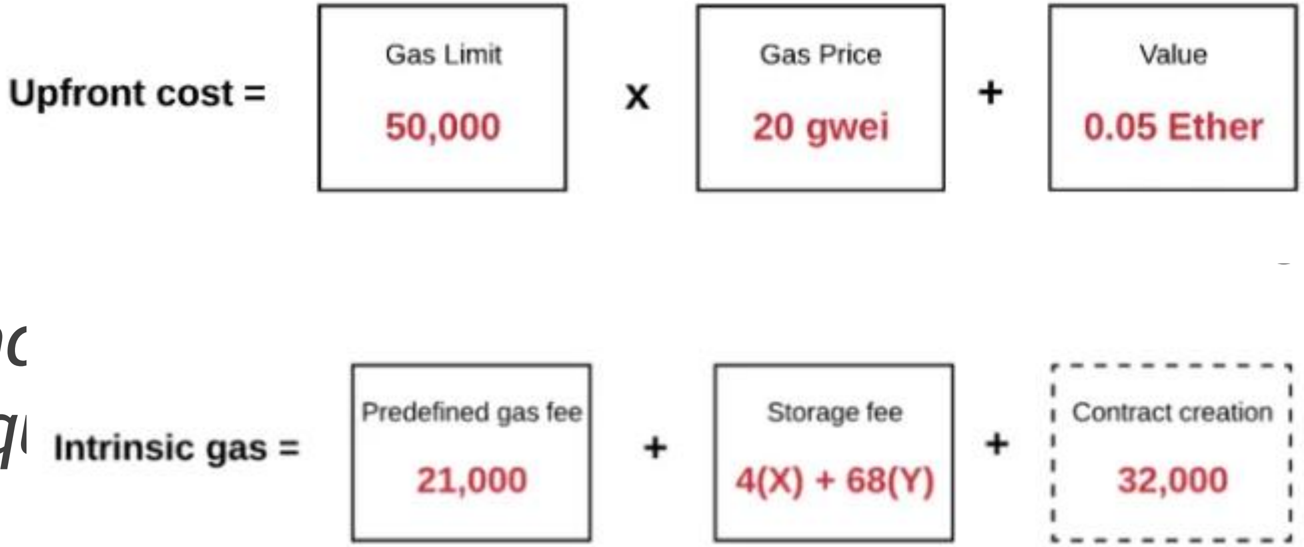
Proof of Work

- Proof-of-work is the consensus mechanism that allows decentralized networks like Ethereum to come to a consensus.
- The consensus mechanism ends up providing security to a blockchain network just because it demands that everyone follow the consensus rules if they want to participate!



Transaction Execution

- *Well-formed RLP*
- *Valid s*
- *Valid n*
- *The ga ... s*
- *The senc ... ne cost req*



Upfront cost = Gas Limit 50,000 x Gas Price 20 gwei + Value 0.05 Ether

Intrinsic gas = Predefined gas fee 21,000 + Storage fee 4(X) + 68(Y) + Contract creation 32,000

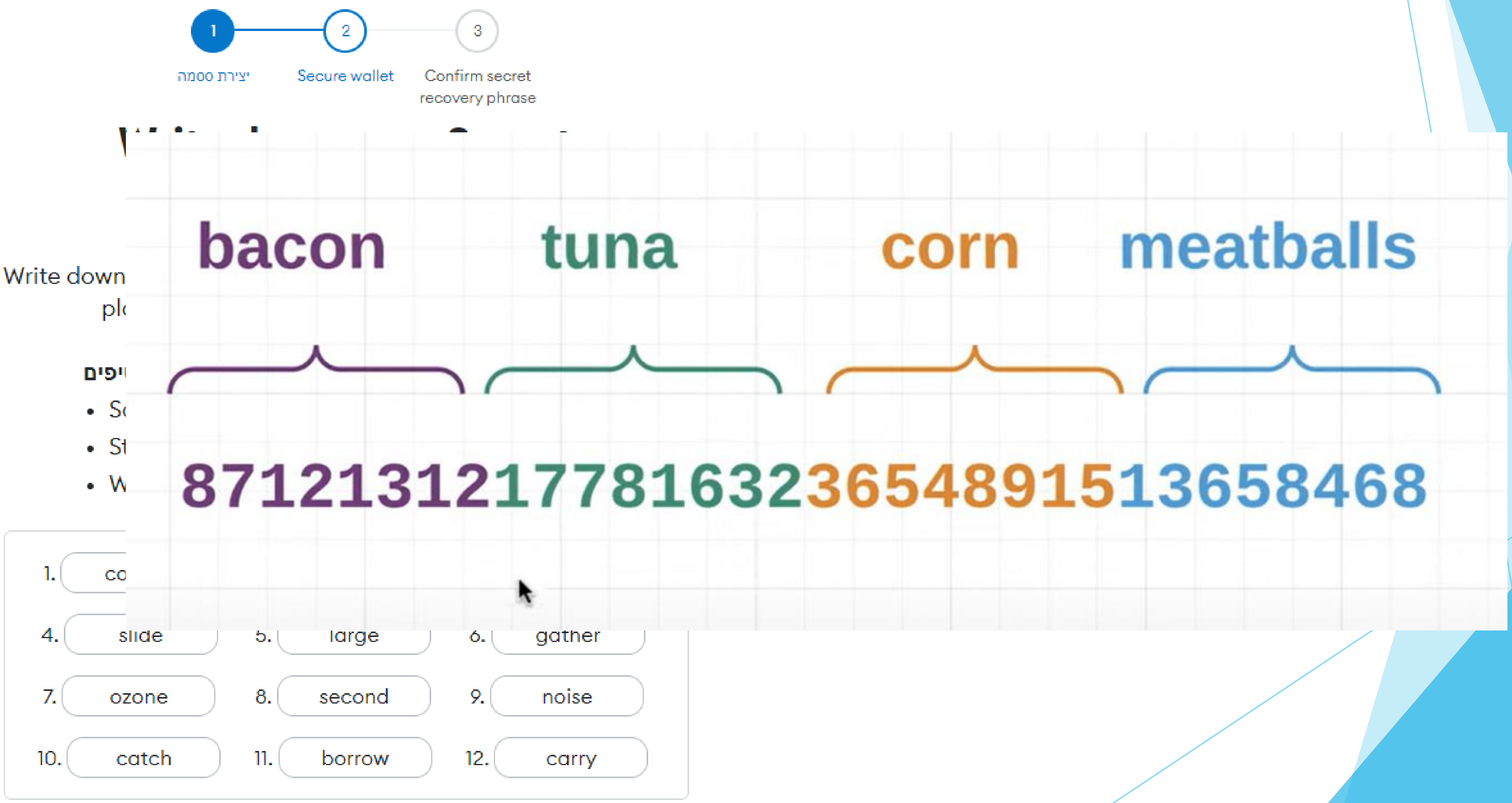
Block Finalisation

- Validate ommers
- Validate transactions
- Apply rewards
- Verify state and nonce

Conclusion

- Decentralized system
- Guarantee contract outcome
- Provide security to the network
- The system structure
- The way Ethereum work

Open METAMASK Account



1 יצירת סממה

2 Secure wallet

3 Confirm secret recovery phrase

Write down
pl

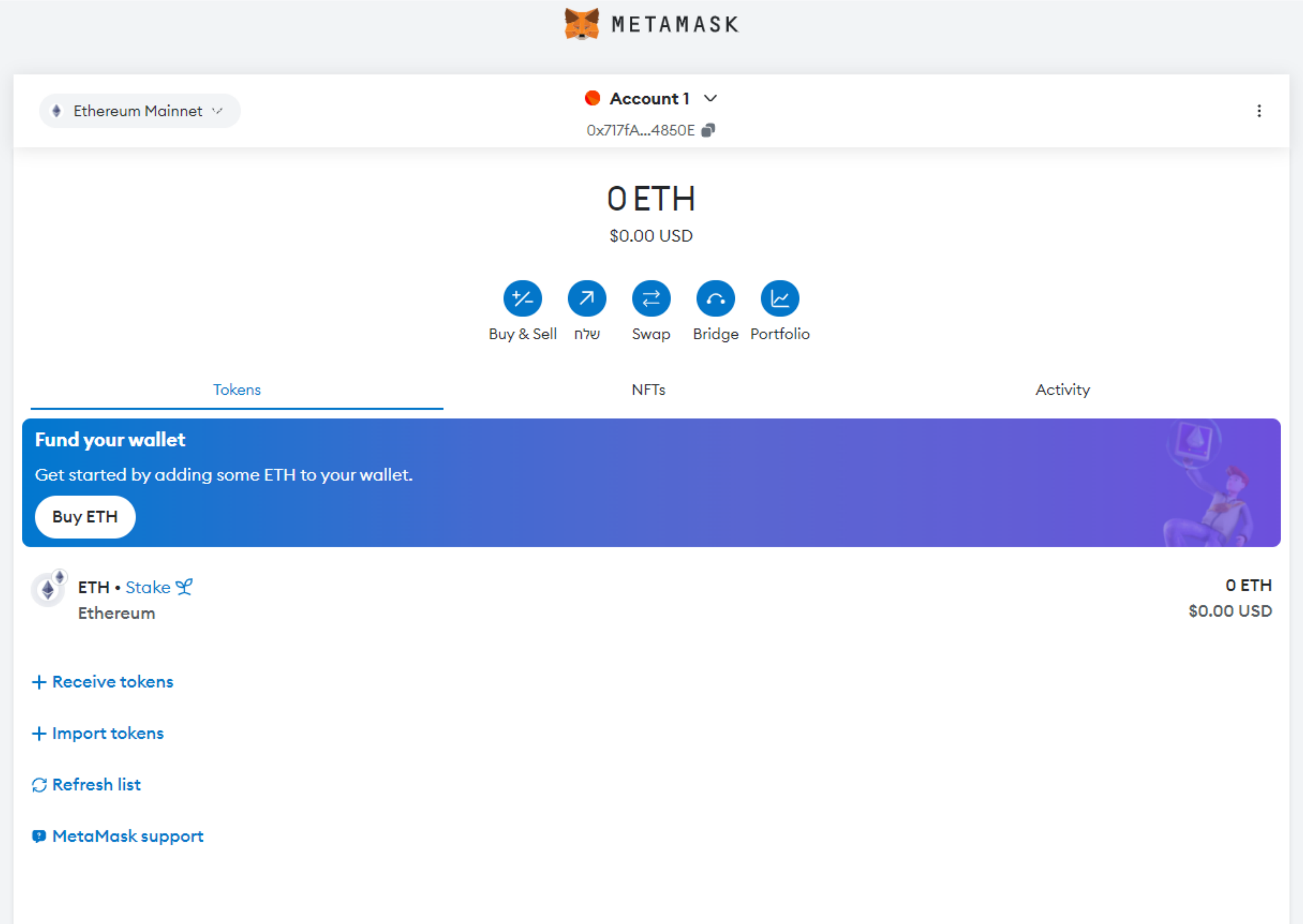
יפים
- S
- St
- W

bacon tuna corn meatballs

87121312177816323654891513658468

1. co
4. slide
5. large
6. gather
7. ozone
8. second
9. noise
10. catch
11. borrow
12. carry

Open METAMASK Account



METAMASK

Ethereum Mainnet

Account 1

0x717fA...4850E

0 ETH

$0.00 USD

Fund your wallet

Get started by adding some ETH to your wallet.

ETH • Stake 0 ETH

Ethereum $0.00 USD