# Principle Foundations of Ethereum

Alireza Rafiei

Coinbase, Inc.

October 15, 2020

# This Lecture

***First Part*** **:**
History and significance of blockchains

***Second Part*** **:**
Ethereum!

# Possible Historical Roots

- Applications (Digital Cash, Smart Contracts)
- Incentive compatible protocol design
- Consensus

# State Machine Replication

- State Machine := Set of States & Set of Inputs & A State transition function: (State, Input) $\rightarrow$(State)

# State Machine Replication

- State Machine := Set of States & Set of Inputs & A State transition function: (State, Input) $\rightarrow$(State)
- Replicated State Machines: State Machines that you can swap with eachother at any time

# State Machine Replication

- State Machine := Set of States & Set of Inputs & A State transition function: (State, Input) $\rightarrow$(State)
- Replicated State Machines: State Machines that you can swap with eachother at any time
- Consensus == Building a replicated state machine

# State Machine Replication

- State Machine := Set of States & Set of Inputs & A State transition function: (State, Input) $\rightarrow$(State)
- Replicated State Machines: State Machines that you can swap with eachother at any time
- Consensus == Building a replicated state machine
- Authenticated channels := Honest nodes will know which nodes sent a message

# State Machine Replication

- State Machine := Set of States & Set of Inputs & A State transition function: (State, Input) $\rightarrow$(State)
- Replicated State Machines: State Machines that you can swap with eachother at any time
- Consensus == Building a replicated state machine
- Authenticated channels := Honest nodes will know which nodes sent a message
- Maximum Delay $\Delta$

# Permissioned

- Number of nodes is common knowledge
- Nodes are always alive
- Authenticated, and the id of every node is common knowledge

# Permissionless

- Number of nodes is unknown.
- Churn is allowed.
- Unauthenticated.

# Results

- With classical permissioned consensus algorithms, consensus is possible in ***sync*** and ***partial sync***.

# Results

- With classical permissioned consensus algorithms, consensus is possible in ***sync*** and ***partial sync***.
- Consensus becomes impossible without authentication.

# Results

- With classical permissioned consensus algorithms, consensus is possible in ***sync*** and ***partial sync***.
- Consensus becomes impossible without authentication.
- Nakamoto Consensus is possible, and is permissionless.

# Nakamoto Blockchain

A Nakmoto Blockchain is a Blockchain that has Proof of Work + Longest chain.
Proof of Work is the main mechanism that provides Sybil resistance.

# Ethereum

Ethereum is a replicated state machine such that:

- Its set of states is composed of elements called World State.

# Ethereum

Ethereum is a replicated state machine such that:

- Its set of states is composed of elements called World State.
- Its set of inputs is composed of elements called Transactions.

# Ethereum

Ethereum is a replicated state machine such that:

- Its set of states is composed of elements called World State.
- Its set of inputs is composed of elements called Transactions.
- Its transition function is implemented as EVM.

# Ethereum

Ethereum is a replicated state machine such that:

- Its set of states is composed of elements called World State.
- Its set of inputs is composed of elements called Transactions.
- Its transition function is implemented as EVM.
- Implements a Nakmoto Blockchain, but also includes uncle blocks.

# Ethereum

Ethereum is a replicated state machine such that:

- Its set of states is composed of elements called World State.
- Its set of inputs is composed of elements called Transactions.
- Its transition function is implemented as EVM.
- Implements a Nakmoto Blockchain, but also includes uncle blocks.
- Each node agrees on the value that's returned from executing an arbitrary 'program'.

# Value

Ethereum has an intrinsic currency called Ether.
Fee schedule is denominated in Gas.

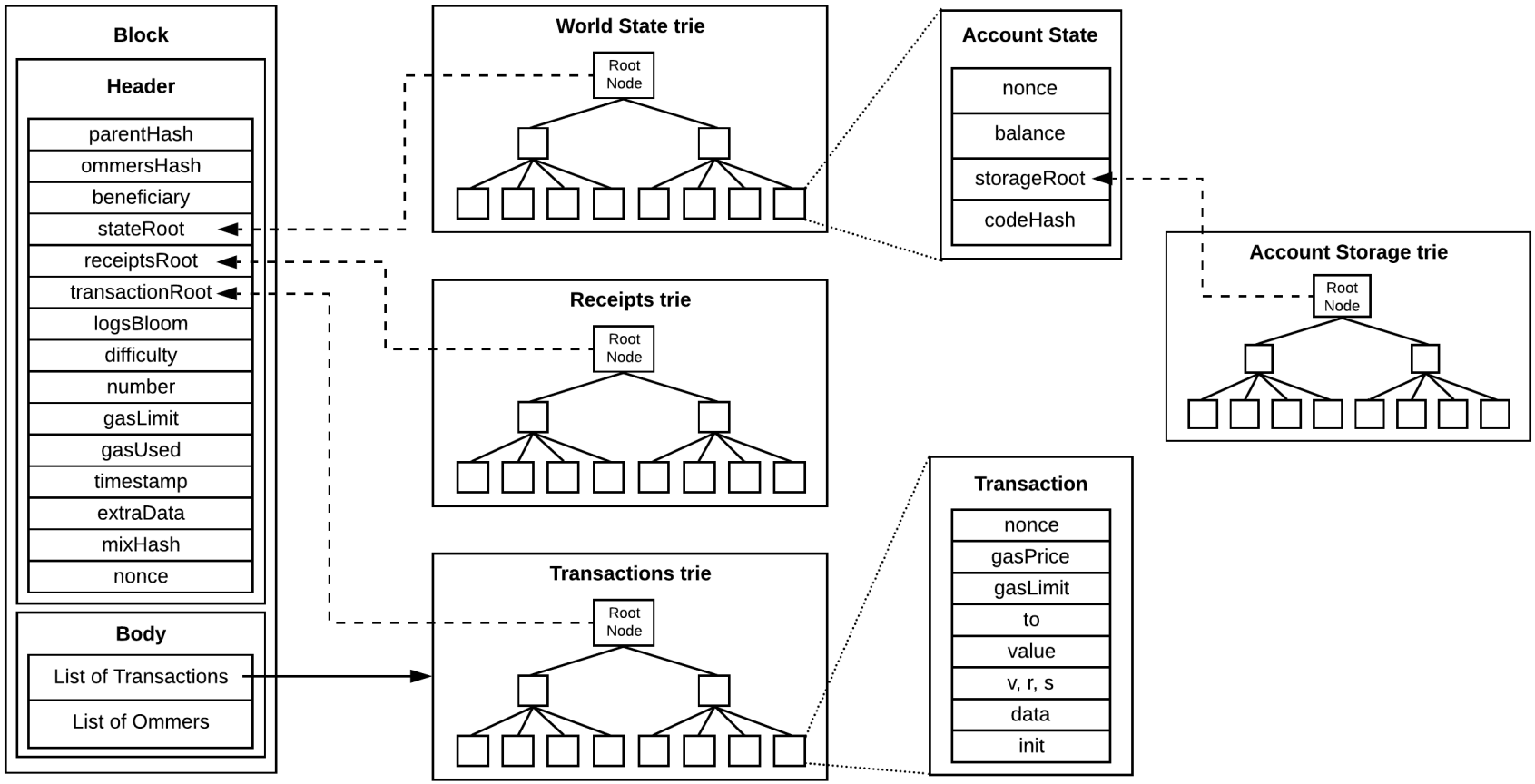
# RLP

The inputs and outputs of almost every mapping in Ethereum is serialized with RLP protocol: https://eth.wiki/fundamentals/rlp

- The string “dog” = [ 0x83, ‘d’, ‘o’, ‘g’ ]
- The list [ “cat”, “dog” ] = [ 0xc8, 0x83, ’c’, ’a’, ’t’, 0x83, ’d’, ’o’, ’g’ ]
- [ [], [[]], [ [], [[]] ] ] = [ 0xc7, 0xc0, 0xc1, 0xc0, 0xc3, 0xc0, 0xc1, 0xc0 ]

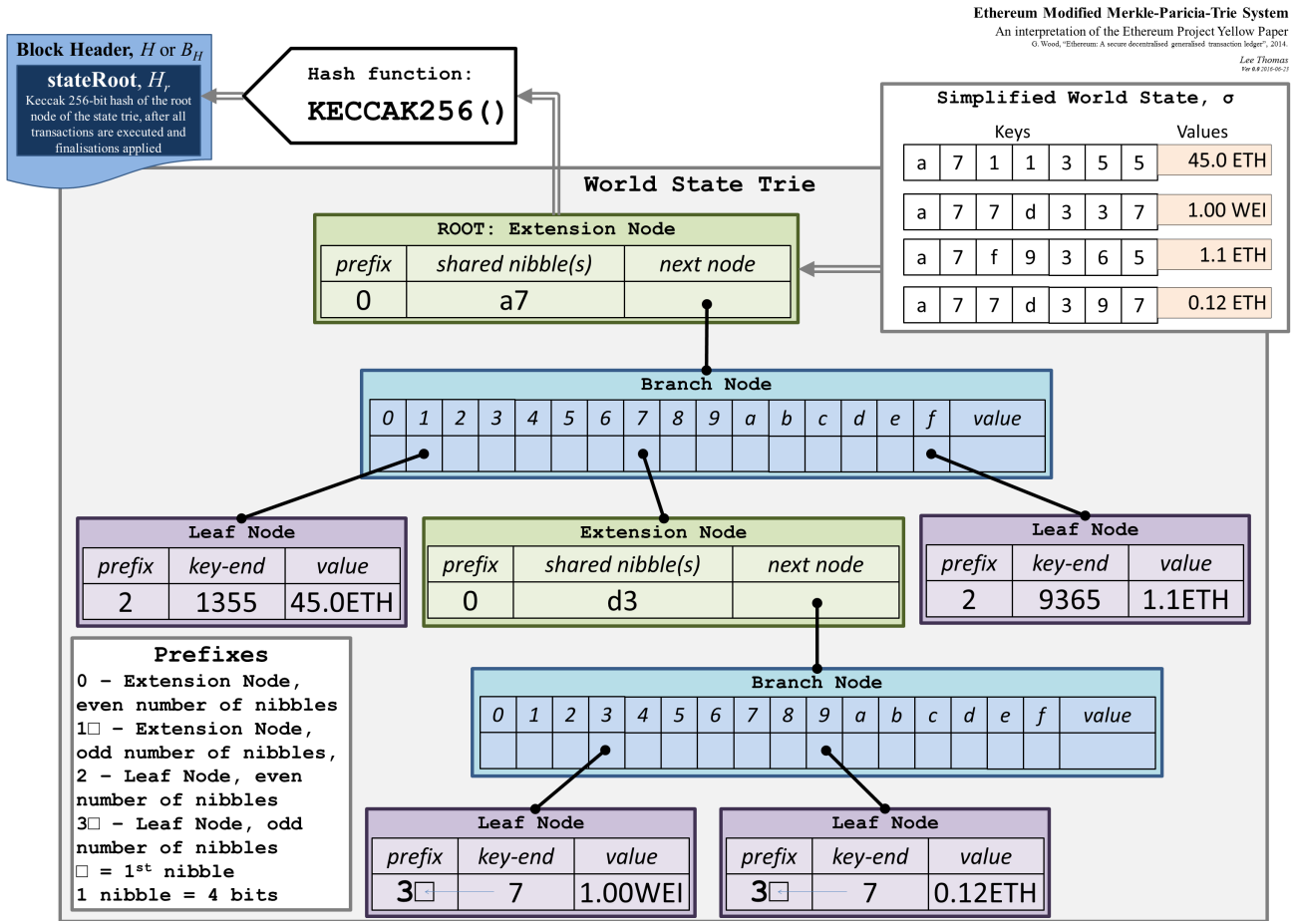
# Overview

https://www.lucassaldanha.com/ethereum-yellow-paper-walkthrough-2/



# World State

A mapping between addresses and account states, implemented in the form of a Merkle-Patricia Trie.



# Accounts

Account Types:

- ***Externally Owned***: Can use private key.
- ***Contract accounts***

Account State contains:

- ***Nonce*** **:** Number of (transactions sent | contracts created) by this account.
- ***Balance***
- ***Storage Root***
- ***codeHash***

# Transactions

- ***Nonce***: Number of transactions sent
- ***gasPrice***: Eth value of every unit of Gas.
- ***gasLimit***
- ***to***: (if for contract creation, nil)
- ***value***
- ***v***, ***r***, ***s***
- ***Init*** (if contract creation)
- ***data***

# Block

Block = Headers + A list of Ommer block headers + a List of transactions

The canonical difficulty of a block of header $H$ is defined as $D(H)$:

(41)
$$D(H) \equiv \begin{cases} D_0 & \text{if} \quad H_\mathrm{i} = 0 \\ \max\left(D_0, P(H)_{H_\mathrm{d}} + x \times \varsigma_2 + \epsilon\right) & \text{otherwise} \end{cases}$$

where:

(42)
$$D_0 \equiv 131072$$

(43)
$$x \equiv \left\lfloor \frac{P(H)_{H_\mathrm{d}}}{2048} \right\rfloor$$

(44)
$$\varsigma_2 \equiv \max\left(y - \left\lfloor \frac{H_\mathrm{s} - P(H)_{H_\mathrm{s}}}{9} \right\rfloor, -99\right)$$

$$y \equiv \begin{cases} 1 & \text{if} \|P(H)_\mathbf{U}\| = 0 \\ 2 & \text{otherwise} \end{cases}$$

(45)
$$\epsilon \equiv \left\lfloor 2^{\lfloor H'_\mathrm{i} \div 100000 \rfloor - 2} \right\rfloor$$

(46)
$$H'_\mathrm{i} \equiv \max(H_\mathrm{i} - 5000000, 0)$$

# Transaction flow

1. Increment Nonce.
2. Deduct max Gas put aside the intrinsic gas..
3. Execute
4. Refund the (remaining Gas) + (the Gas from freeing up storage / 2).
5. Pay the miner gas used plus intrinsic gas.