Blockchain and Digital Currencies

Lecture 7

PHBS 2024 M3

Ethereum Overview

- Account based ledger
- Mining algorithms
- Smart contract

不同的记账系统
不同的挖矿算法

Agenda

- Ethereum Overview
- Modified Merkle Patricia Tree (MMPT)

Motivation

- Bitcoin blockchain aims to facilitate the transfer of bitcoins
- What else can be done?
  - Transfer of other coins or even fiat currencies?
- How to motivate miners to keep mining (providing services)?
  - Instead of voluntary service fees, make it mandatory

Changes

- UTXO seems cumbersome and Bitcoin scripts only support limited functions and computation
- Introducing accounts to keep track of balance
  - The balance of all accounts needs to be saved into ledger
- The whole network becomes a distributed state machine and the block chain keeps track of the changes of states
  - Each full node (miner) keeps a snapshot/copy of the state machine

Ethereum

- Ethereum is a decentralized platform designed to run smart contracts
  - Smart contracts are executable codes
  - Distributed computer to execute executable codes
  - Account-based blockchain
  - Transactions ←→ state transition function
  - Blocks ←→ snapshots of state machines
- Ethereum has a native asset called ether
  - Basis of values in the Ethereum ecosystem

Smart Contract

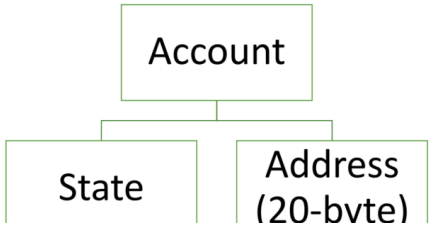
- Unlike an ordinary contracts, written or spoken agreement , which is intended to be enforceable by law

  智能合约就是一些可执行代码

- A smart contract is some executable code that facilitates, verifies, or enforces the negotiation or execution of a digital agreement
  - Example: an execution of an expired option contract
  - Storage place? Execution environment?

Account

- Similar to daily common practice in banks



Bitcoin:

Bob owns private keys to set of UTXOs

Easy to make transactions and prevent double spending

5 BTC ⇒ Bob

3 BTC ⇒ Bob

2 BTC ⇒ Bob

分布式的就需要循环所有的 Blocks 来得到 Bob 的情况

Ethereum:

Alice owns private keys to an account

address: "0xfa38b..."

balance: 10 ETH

code: c := a + b

160 bits (or 40 Hex code)

Space-efficient to update balances instead of storing UTXOs

Easier to look up balance and transfer between accounts when programming

Account Security Issues – Nonce

☑ What is this about? What is the usage?

- No need to worry about double spending
  - Sender broadcasts multiple different transactions using the same account
- Replay attack becomes a problem
  - Receiver broadcasts the same transaction to the network

Tx: A transfer x to B
nonce = 15
signed by A

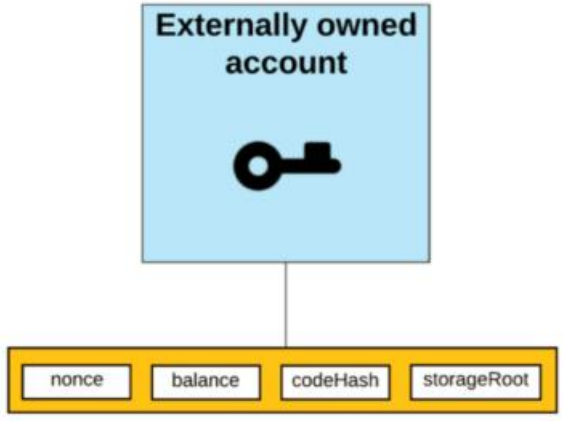
Tx: A transfer x to B
nonce = 16
signed by A

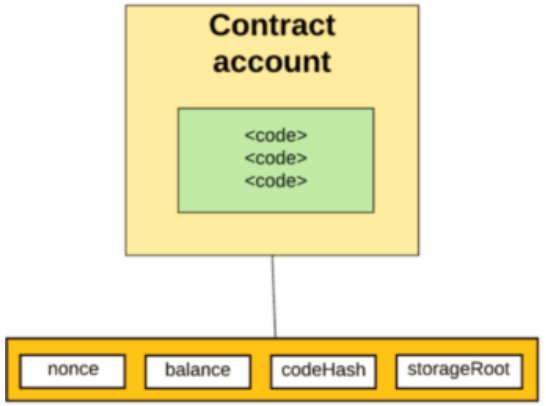
加一个 sequence number 来判断后面广播的交易是否被使用过

Account Types

Smart Account 不能随意向外转钱

- Externally owned account and Contract account





storage 里面存的就是当前的各类账户信息

Protected by signature of users;
Balance indicates the wealth;
Nonce is used for sequence #;
Can initiate a transfer or trigger contract account to run code

Including code and storage;
Anyone can create; Publicly accessible and anyone can call;
Also uses nonce to keep track of sequence #;
CANNOT start a transfer

用 ATM 就可以理解，ATM 是不能自己交易的，只有获得签名后才能交易

Account Fields

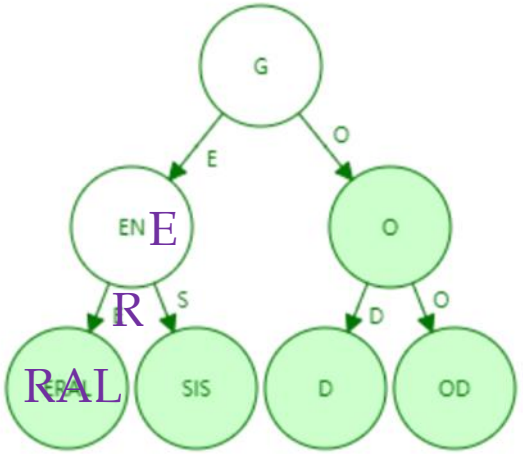
- nonce: # transactions sent/ # contracts created
- balance: # Wei owned (1 ether=10^18Wei)
  - http://www.weidai.com
  - 1 BTC = 10^8 Satoshi
- storageRoot: Hash of the root node of a Merkle Patricia tree. The tree is empty by default.
- codeHash: Hash of empty string / Hash of the EVM (Ethereum Virtual Machine) code of this account

Warning!!

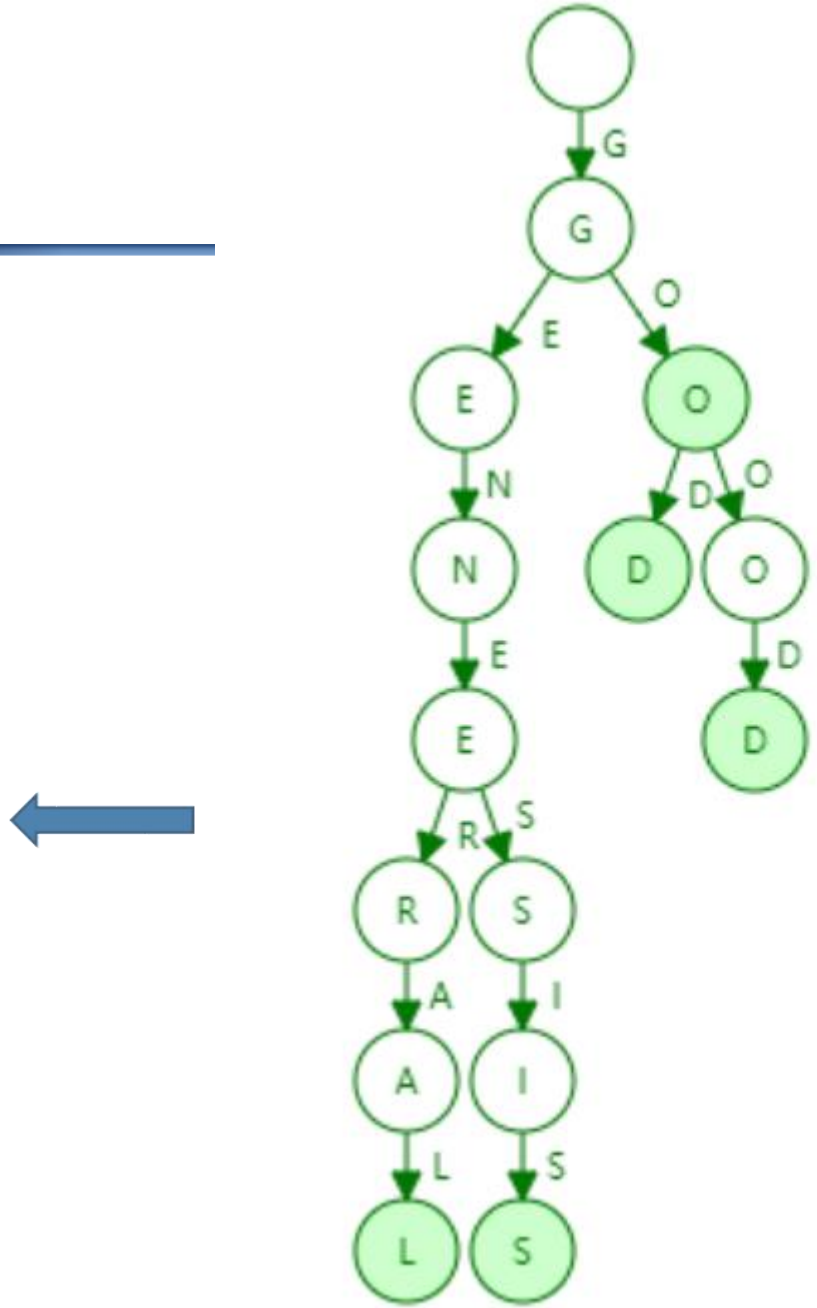
☑ What is this about? What is the usage?

- Merkle Patricia tree
  - A data structure for storing key/value pairs in a cryptographically authenticated manner.
  - The tree root is a hash of all key/values in the structure, where updates/deletions are fast.

Trie Example



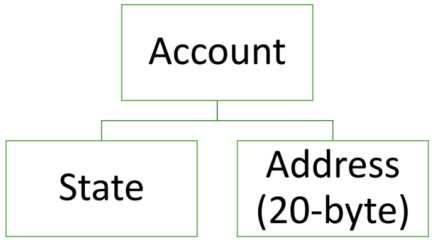
General
Genesis
Go
God
Good



General
Genesis
Go
God
Good

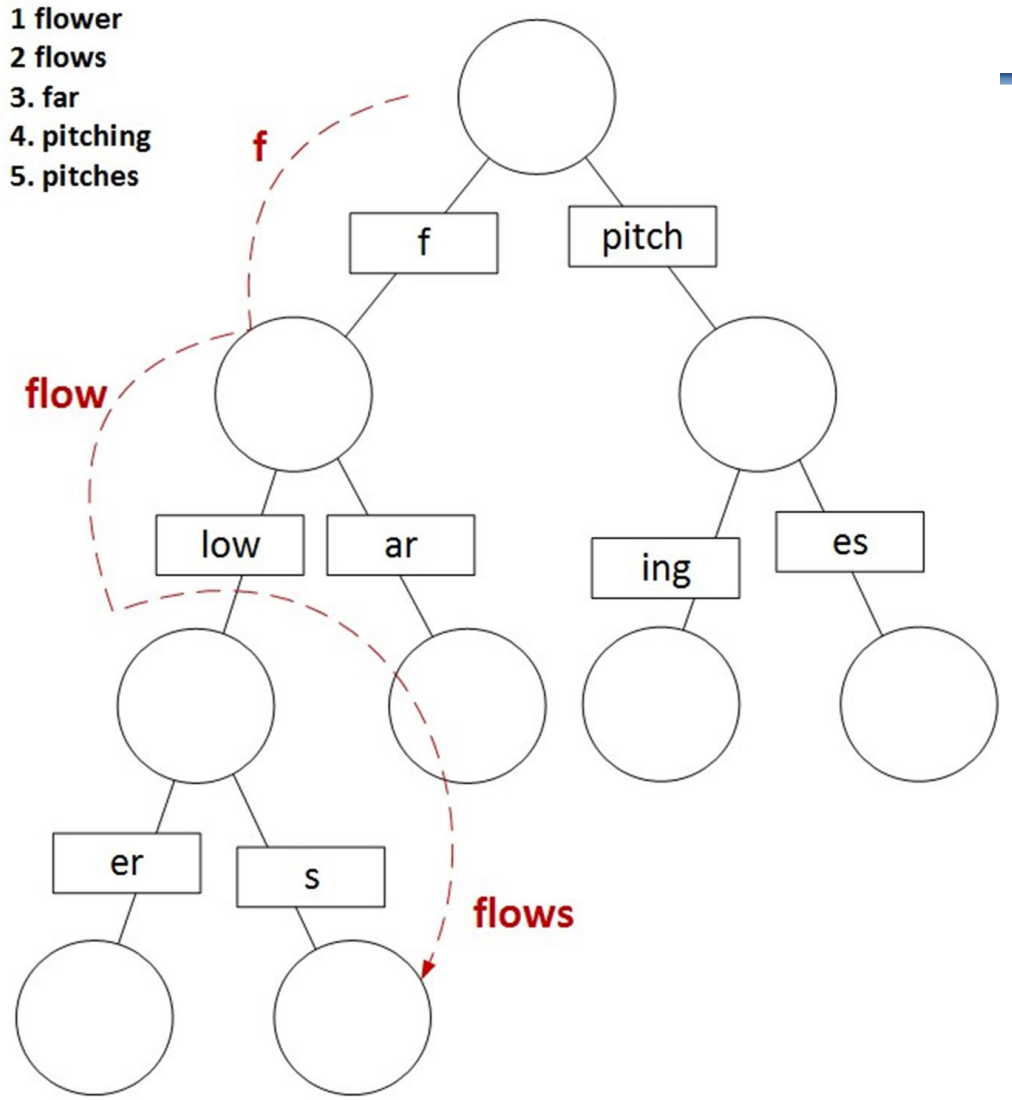
Patricia Trie Example

From Trie:字典树



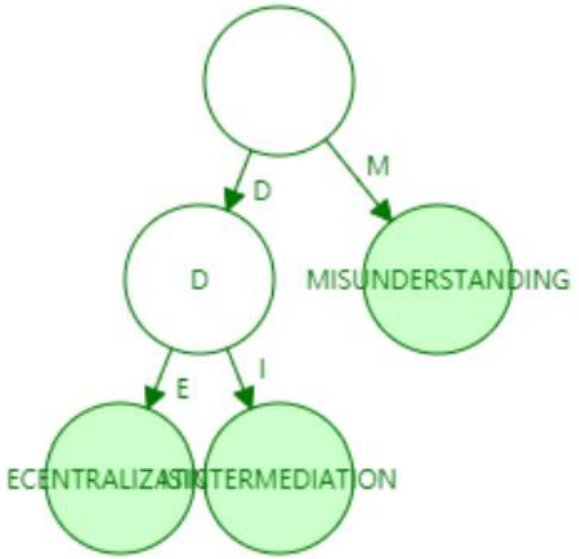
160 bits (or 40 Hex code)

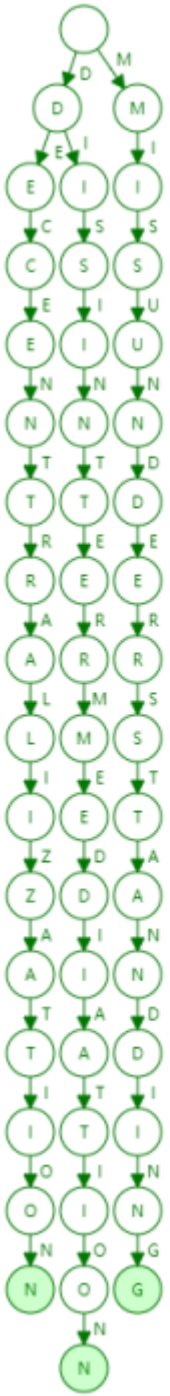
查很简单，但是改很困难



Extreme Patricia Trie Example

The more spread the key values,
the more compressed the Patricia Trie.





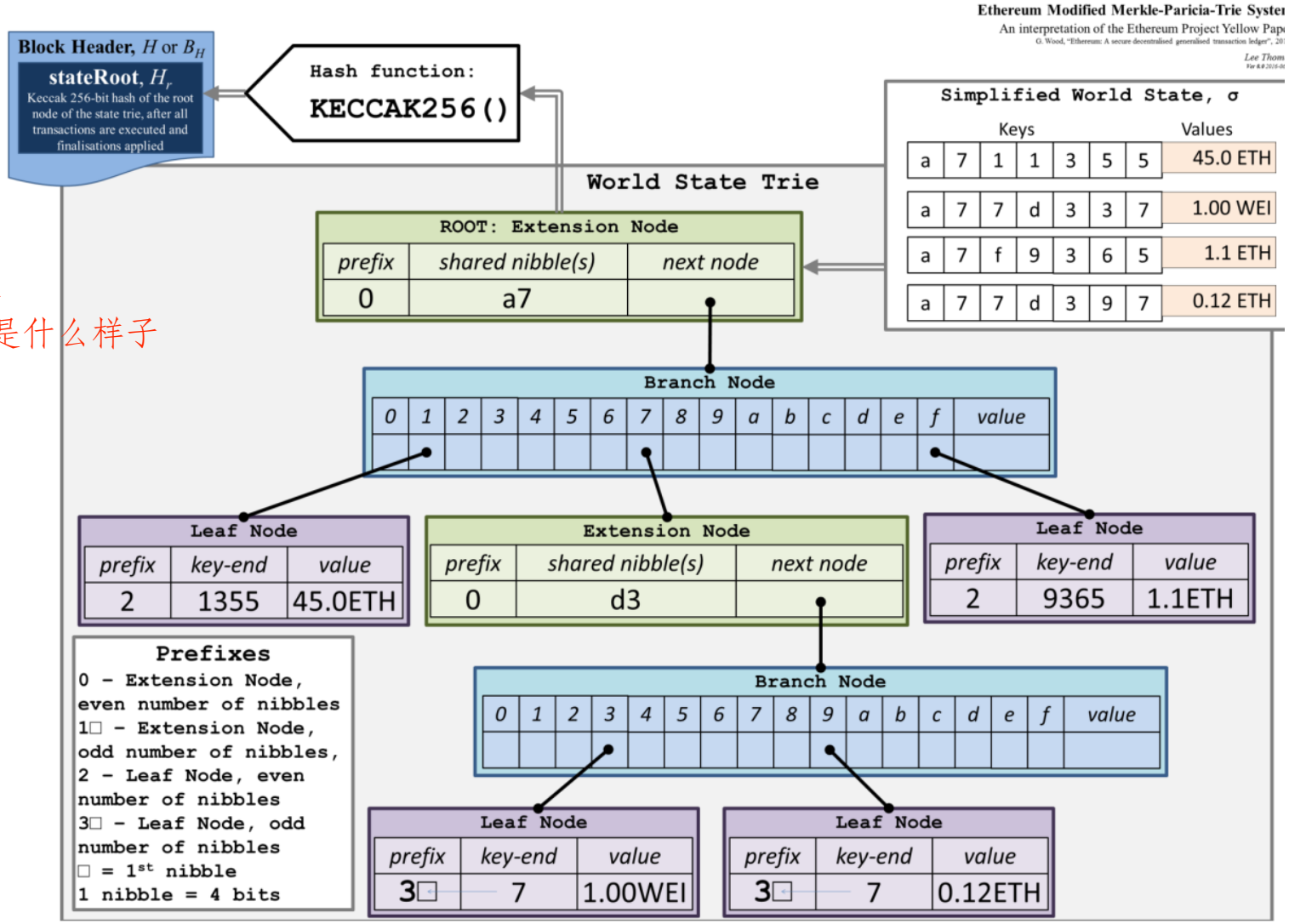
Misunderstanding
Decentralization
Disintermediation

Motivation for Merkle Patricia Trie (Tree)

- Why do we need Merkle Patricia tree?
  - Why Merkle tree for BTC blockchain is sufficient?
  - What will be included in Merkle Patricia tree?
  - The states of all accounts
- What are the benefits?
  - Temper resistant
  - Existence and non-existence proof

Modified Merkle Patricia Tree (MMPT)

经典的一个例子
存储 ETH 的树是什么样子



MMPT in Different Blocks