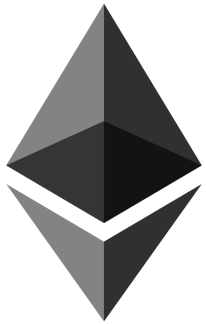


以太坊硬分叉与下一代共识算法

熊伟伦

2017/11/22

区块链沙龙

以太坊是什么

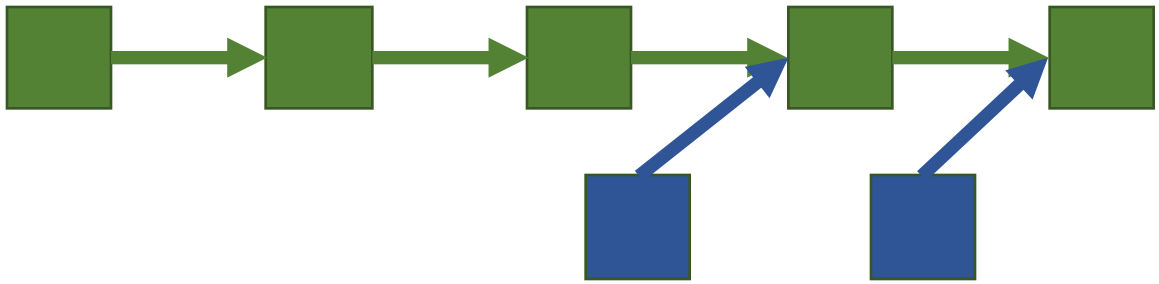
- 英文全称 Ethereum

- Ether: 以太，亚里士多德哲学假设的五大元素之一，光和波的传播介质，无处不在
- -eum: 拉丁语中表示科学名词的后缀构词

- Vitalik Buterin 在2013年写下《以太坊白皮书》
- 目标：构建去中心化的 **程序**

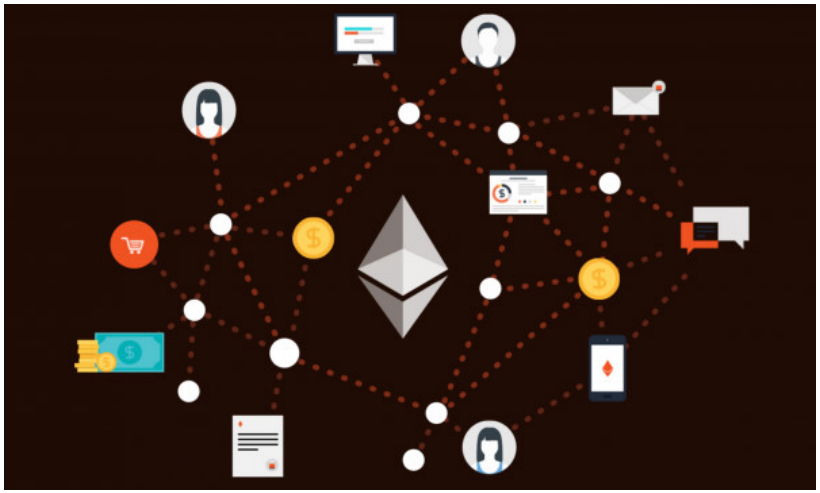
以太坊的亮点

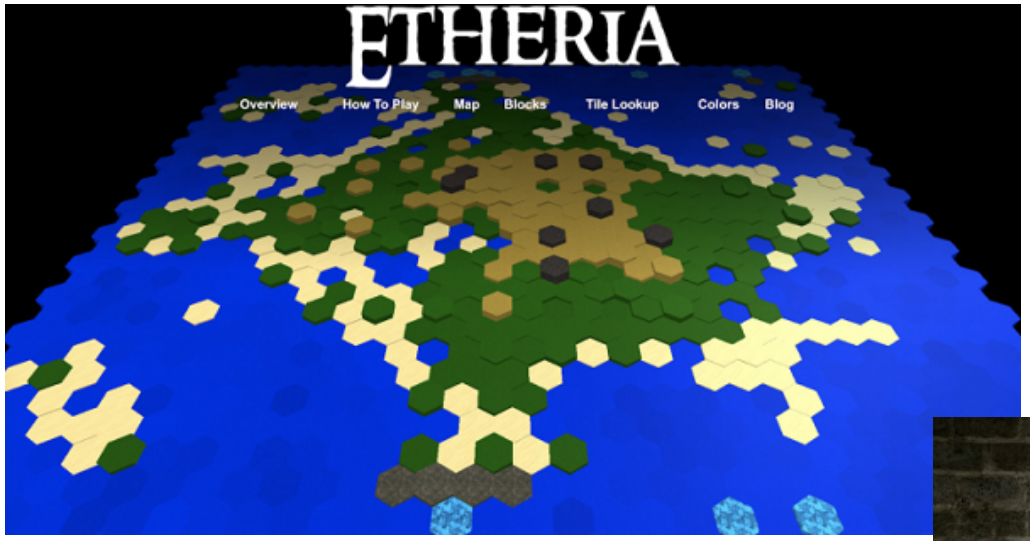
- 以太币
  - 以太坊的代币，由 ICO 阶段和挖矿产生
- 以太虚拟机 (Ethereum Virtual Machine)
  - 执行图灵完备的指令集，以太坊节点就是虚拟机
- 智能合约 (Smart Contract)
  - EVM指令集编写的程序，根据程序大小，支付以太币让其他虚拟机执行。可以认为以太坊是一台巨型分布式共用电脑。
- 叔块 (Uncle Block)
  - 被最长链引用的非主块



DApp

- 去中心化应用
  Decentralized Application
- 以太坊的正菜
- 运行在以太坊网络中的以太虚拟机的 App



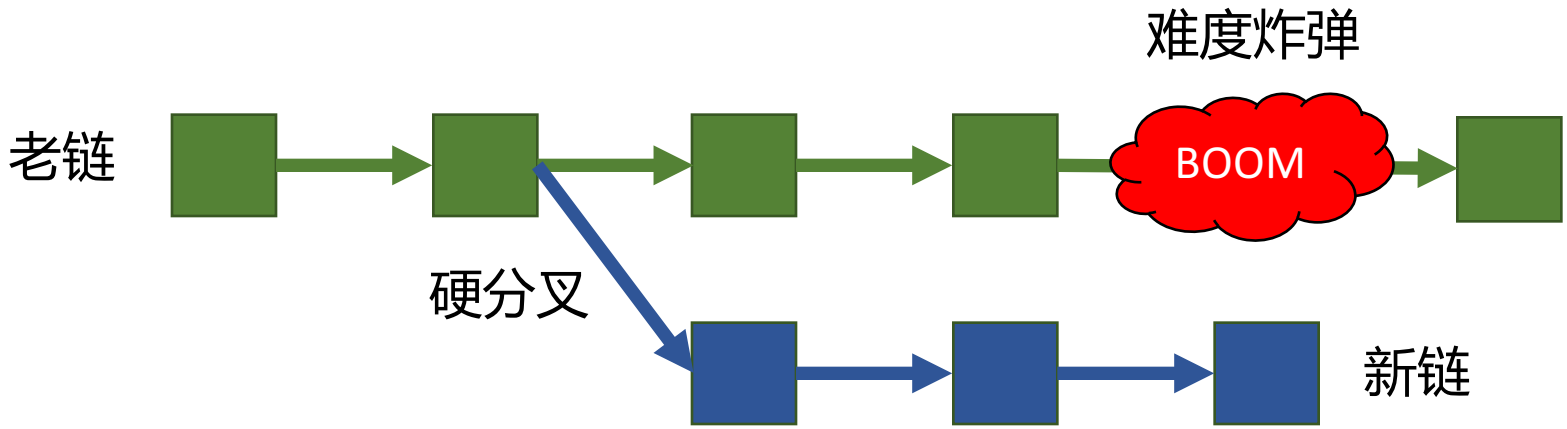


Etheria
以太坊网络中的 MineCraft

Ampliative Art
艺术作品展示与打赏

Eth-Tweet
区中心化社交平台

硬分叉



以太坊基金会

- 以太坊社区的中心
- 开发、运营、推广

- 硬分叉能够达成共识的关键

- DevCon
  2014 ~ 2017
  以太坊开发者大会

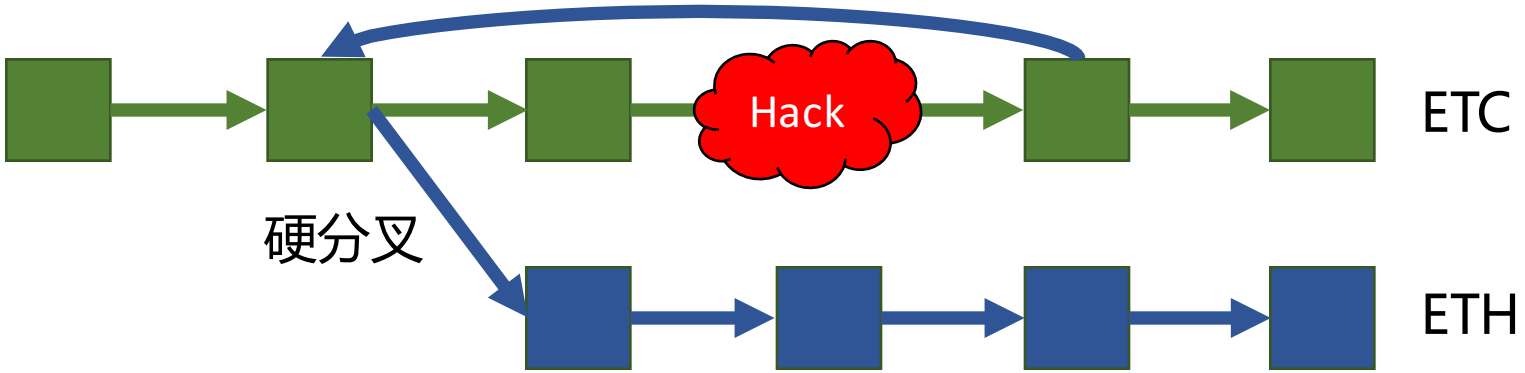
以太坊发展历程

- 2015年5月 Olympic 主网上线
- 2015年7月 Frontier 版本
- 2016年3月 Homestead 版本
- 2016年6月 由于骇客时间被迫硬分叉 !
- 2017年10月 Metropolis vByzantium 版本
- 计划中 Metropolis vConstantinople 版本
- 最终计划 Serenity (Proof-of-Stake)

以太币 ETH ETC

- DApp The DAO “去中心化的组织”
  由于智能合约漏洞导致以太币被盗取
  价值 1.5 亿美元的 360 万以太币

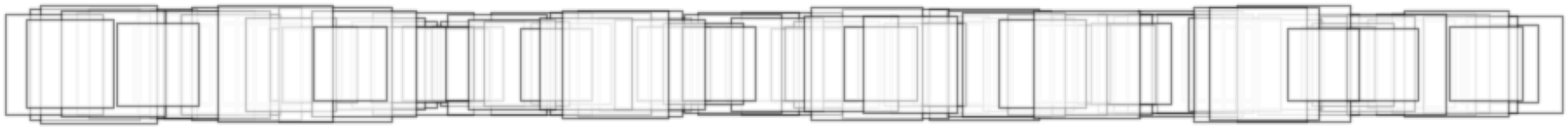
- 以太坊基金会修复了漏洞相关的 EVM op
  并进行硬回滚



Casper 共识算法

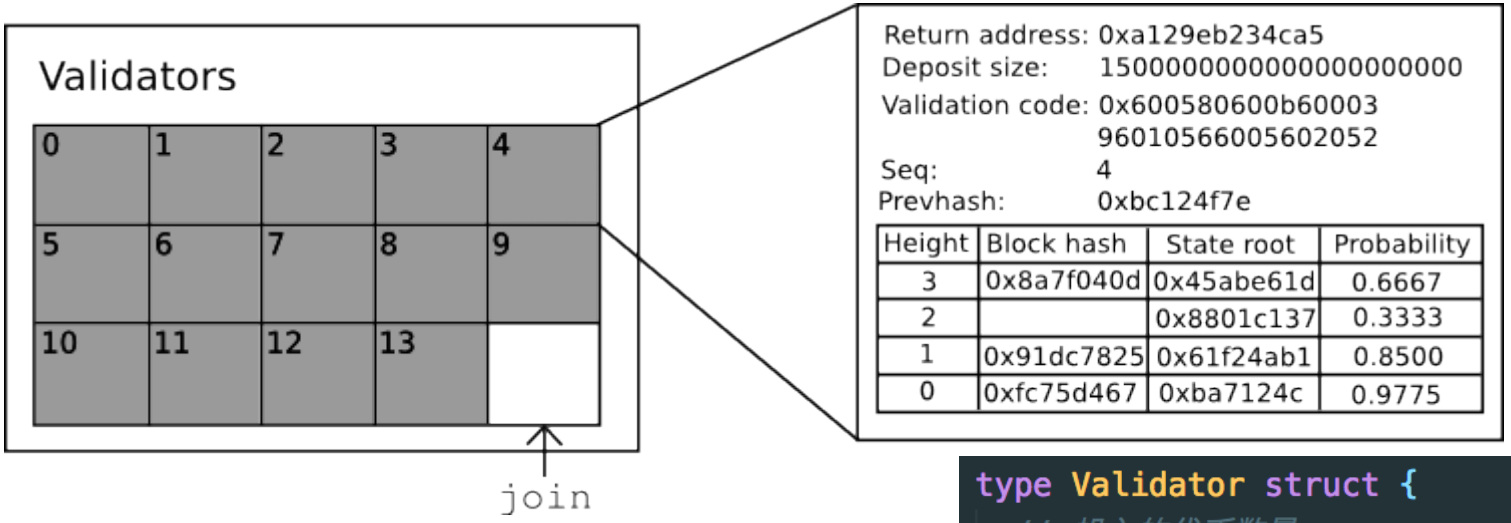
- 以太坊最终阶段 Serenity 的共识算法
- 通用去中心化计算 分布式系统

- Vitalik 提出，众多开发者和数学家进行证明



- PoW (Proof-of-Work)
- PoS (Proof-of-Stake)

Casper 智能合约



投注，加入，取款，获取共识，惩罚

以美国大选为例

```
// validators 见证人池
validators []contracts.Validator
```

```
type Validator struct {
  // 投入的代币数量
  Deposit *big.Rat
  // validator 加入的 dynasty
  Dynasty_start uint64
  // validator 退出的 dynasty
  Dynasty_end uint64
  // validator 的签名地址
  Addr string
  // 收回代币的地址
  Withdrawal_addr string
  // 该 validator 提交的上一个时间戳
  Prev_commit_epoch uint64
}
```

Casper in DevCon3

10:20 am - 10:45 am

Intro to Casper Implementation

Breakout Hall

Chang-Wu Chen

More info

1:00 pm - 1:20 pm

Verifying Casper

Main Hall

Yoichi Hirai

More info

2:35 pm - 3:00 pm

Casper the Friendly GHOST: A correct-by-construction blockchain

Main Hall

Vlad Zamfir

More info

3:30 pm - 4:00 pm

Panel: Casper and Consensus

Main Hall

Elaine Shi

Emin Gun Sirer

Peter Czaban

Vlad Zamfir

Vitalik Buterin

More info

Casper 资源

- https://github.com/ethereum/simplecasper
- https://github.com/ethereum/casper
- https://github.com/ethereum/cbc-casper
- 以太坊紫皮书
- https://www.youtube.com/channel/UCNOfzGXD_C9YMYmnefmPH0g

谢谢

本幻灯片下载: https://github.com/Azard/talks