从远到近认识区块链（二）初窥以太坊

高昊烨 2022-09-23

什么是以太坊?

一台世界级单体计算机。

关键词：*开源、内建经济、高可用、可审计、透明、中立、消除审查、减少第三方介入...*

来自比特币

我们已经了解比特币，以太坊与其同时作为公共区块链技术的代表，均具备几个基本特征：

1. P2P网络
2. 共识算法
3. 密码学
4. 数字货币

不同之处在于：

1. 以太坊的核心不在于提供数字货币，货币的存在仅服务于使用以太坊计算的开销计算
2. 提供无限复杂（图灵完备）代码的执行能力

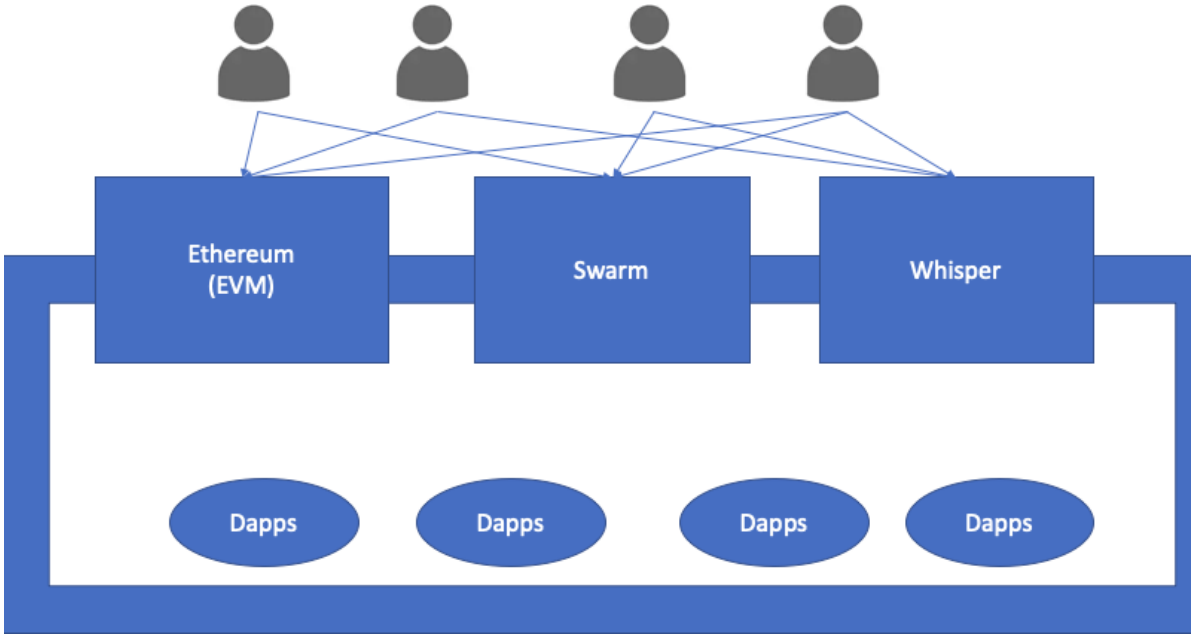
从分布式账本到分布式状态机

web3.0

三大基石：

1. 以太坊：共识&计算
2. Whisper：通信
3. Swarm：存储

以太坊P2P网络架构



web3.0以太坊抽象

DApp

去中心化应用，即在以太坊上构建的应用，基本要素：

1. 智能合约（solidity）
2. web前端（web3.js库）

通过以太坊学习区块链

区块链涉及到的知识范围广，难以上手，通过学习以太坊原理、使用以太坊搭建应用，可以在层层渐进中逐步发掘区块链。

从钱包了解以太坊

什么是钱包?

管理钱，根本上是**私钥管理**和**广播交易**信息数据包的工具（一种远程调用以太坊客户端，全功能客户端功能的子集）。

以太币基本单位是wei，一个以太币等于10^18wei（1 ether = 10^18 wei）

密码学基础

1. 非对称加密
2. 哈希
3. 数字签名

分层确定性钱包

Hierarchical Deterministic Wallet, HD钱包

- BIP32: HD 钱包的核心提案，说明了自私钥生成方法以及树状结构的构造方式；
- BIP39: 助记词提案
- BIP43: 为 HD 钱包子私钥派生路径增加有广泛共识的段；
- BIP44: 确定支持多链 HD 钱包子私钥派生路径的标准格式；

Metamask钱包

1. 创建钱包
2. 切换网络
3. 获得测试以太币
4. 向以太坊发送以太币
5. 交易记录

账户

一个账户，就是一个地址

> 0x8A8A6943A01c0228d5D7f3a06465B69c703745A0

外部账户：管理以太币、发起交易

内部账户（合约账户）：智能合约、发起消息

1. 私钥：随机生成 1-0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364140
2. 公钥：椭圆曲线 secp256k1

$$K = k * G$$

$$0x04 + x + y$$

3. 地址：keccak-256哈希，低20字节，40位16进制数

   EIP-55重编码

以上单向衍生，无法逆运算

智能合约

智能合约是其能够称为“计算机”的根本原因，合约提供了执行足够复杂脚本的能力，且合约可以继续调用其他合约，从而能够构建复杂的逻辑。

```
// @file faucet.sol
// @dev 水龙头合约
pragma solidity ^0.4.0;

contract Faucet {
  function withdraw(uint withdraw_amount) public {
    require(withdraw_amount <= 100000000000000000);
    msg.sender.transfer(withdraw_amount);
  }
  function () public payable {}
}
```

1. 开发
2. 编译
3. 测试
4. 部署

交易（TRANSACTION）

交易是事务的，具有ACID特性。是一切状态变化（更新余额、执行合约代码、更改区块链状态）的开端。

```
{
  "jsonrpc": "2.0",
  "id": 2,
  "result": {
    "raw":
"0xf883800182033394 07a565b7ed7d7a678680a4c162885bedbb695fe080a44401a6e40000000000000000
0000000000000000000000000000000000000000000001226a0223a7c9bcf5531c99be5ea7082183816eb2
0cfe0bbc322e97cc5c7f71ab8b20ea02aadee6b34b45bb15bc42d9c09de4a6754e7000908da72d48cc77049
71491663",
    "tx": {
      "nonce": "0x0",
      "gasPrice": "0x1234",
      "gas": "0x55555",
      "to": "0x07a565b7ed7d7a678680a4c162885bedbb695fe0",
      "value": "0x1234",
      "input": "0xabcd",
      "v": "0x26",
      "r": "0x223a7c9bcf5531c99be5ea7082183816eb20cfe0bbc322e97cc5c7f71ab8b20e",
      "s": "0x2aadee6b34b45bb15bc42d9c09de4a6754e7000908da72d48cc7704971491663",
      "hash": "0xeba2df809e7a612a0a0d444ccfa5c839624bdc00dd29e3340d46df3870f8a30e"
    }
  }
}
```

- `raw` 是已签名交易的 RLP（Recursive Length Prefix）编码形式。
- `tx` 是已签名交易的 JSON 形式。

nonce：顺序保证、重复保护

交易传播：P2P泛洪

参考文献

[1]《精通以太坊》

[2] 分层确定性钱包 HD Wallet 剖析：设计和实现， https://www.arcblock.io/blog/zh/post/2018/12/01/hd-wallets-design-and-implementation

推荐阅读

1. 《精通以太坊：开发智能合约和去中心化应用》（Mastering Ethereum: Building Smart Contracts and DApps）
2. DApp入门教程：https://cryptozombies.io/（包含智能合约、前端页面、以太坊交互）