区块链技术分享

1. 区块链概述

1.1 概念

> 百度百科：区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

- 分布式数据存储
- 点对点传输
- 共识机制
- 加密算法

1.2 分类

- 公链
- 私链
- 联盟链

1.3 应用

- 比特币
- 以太坊
- Fabric

> 问题：比特币的白皮书称比特币是一种点对点的电子现金系统，请问，比特币有价值么？

1.4 区块链行业现状

- 政府高度关注
- ICO / 炒币收益巨大
- 资金盲目恐慌进入
- 各大公司投入技术研究
- 专家认为区块链技术会导致社会变革
- 处于不成熟时期
- 缺乏杀手级应用
- 以区块链概念的传销、庞氏骗局横行

2. 比特币详解

> 比特币是基于区块链的第一个应用，区块链技术脱胎于比特币。

2.1 比特币概述

- 比特币的目的：电子现金系统
- 技术难点：使用信息来表示价值
- 价值的表现方式：现金和记账
- 加密和签名：如何让记账不可抵赖
- 挖矿和矿工：解决重花问题、解决货币发行

> 所有的技术结合起来，形成一个完美的轮回，解决货币的发行、验证、交易等功能。

2.2 技术细节

2.2.1 数据结构

- 比特币是点对点网络组成，因此没有服务器概念，运行比特币程序的电脑，称之为**节点(node)**。
- 每个节点记录着相同的**账本(ledger)**。
- 账本的数据结构由**区块(block)**组成，每个区块通过hash指针，指着上一个区块，组成**区块链(block chain)**。区块链很像数据结构中的单链表。区块链数据结构由于相互通过哈希锁定，因此不可能被修改。
- 区块中保存了合法的**交易(transation)**，交易由**输入**和**输出**组成，没有交易出去的输出，称为**UTXO(Unspent Transaction Output)**。
- 如果你想把 UTXO 转账给其他人，你必须有该 UTXO 对应的**私钥(private key)**。
- 如果你想收到别人的转账，你必须有**钱包地址(wallet address)**，或者简称**地址**，地址由**公钥(public key)**按照算法生成。

2.2.2 点对点网络

- 所有节点通过**点对点**协议连接，类似 BT 网络。
- 一个用户发起转账，导致的账本变化，通知到全网过程中有延迟。
- 需要有一个节点来对账本变化进行确认。
- 由于对记账有奖励，因此有些节点，会努力争取记账权。争夺记账权的过程，称之为挖矿。争夺记账权的节点，称之为矿工。

2.2.3 工作量证明

- 为了争夺记账权，每个矿工都要努力计算哈希值。
- 如果某个矿工算出的哈希值符合条件（往往条件是小于某个值），则获得记账权。
- 获得记账权的矿工，把过去一段时间（比特币大约是 10 分钟，以太坊大约是 15 秒）内发生的交易，打包到区块中。
- 完成记账的矿工，可以得到系统的奖励（一开始是 50 比特币，现在是 12.5 个比特币）。
- 计算哈希值，就是叫做工作量证明，这种证明很难被攻破，但是缺点是耗电很多。

3. 以太坊

3.1 比特币的缺点

- 没有管理。
- 工作量证明，耗电多。
- 没有价值背书。
- 只是记账工具，脚本功能偏弱。

3.2 以太坊

- 可以写智能合约，具备强大的脚本功能。
- 有基金会管理。
- 以太币有使用价值（智能合约的运行，需要使用以太币）。

> 以太坊的目标是成为全球计算机。

3.3 智能合约

- 以太坊支持图灵完备的脚本，用于编写智能合约。
- 智能合约能用于众筹、博弈、记账、投票、拍卖等等。
- 智能合约的每个指令执行必须要耗费 Gas，以避免滥用。
- Gas 最后使用以太币来结算。

3.4 代币和 ICO

- ERC 20
- ERC 721

3.5 缺陷

- 性能
- 安全性

4. 创富机会

- 挖矿
- 炒币
- DAPP
- 媒体
- 培训
- 交易所
- 公链
- 私链和联盟链

5. 链接

- Mobilefish 的区块链入门课程
- Solidity 官方文档
- 比特币区块查看
- 以太坊区块查看
- Ethereum DAPP 开发入门教程
- 比特币 Github 地址
- 以太坊 Github 地址
- 创建安全的纸钱包