区块链技术演化

区块链的演化

- 区块链 1.0 比特币
- 区块链 2.0 以太坊(智能合约)
- 区块链 3.0 hyperledger

数据结构+算法 = 计算机程序设计

区块链1.0 比特币

- 数据结构
  - 张三 100
  - 李四 55
- 算法(转账)
  - 张三 100 -10 = 90
  - 李四 55 + 10 = 65
- 世界状态变化
  - 100, 55 → function() → 90,65

区块链2.0 以太坊

- 数据结构
  - 整形,数组,map,结构体...
- 算法(智能合约)
  - 图灵完备虚拟机中执行的函数
- 世界状态变化
  - 00110011 → function() → 10110110

区块链3.0 hyperledger

- 数据结构
  - 任意数据结构
- 算法(智能合约)
  - Nodejs , java, go, python编写的chaincode
- 世界状态变化
  - 00110011 →全功能 function() → 10110110

区块链与分布式技术

- 区块链是一个自带对账功能的分布式账本

区块链的分类

- 公有链
- 私有链
- 联盟链

区块链关键技术

- 抗抵赖与隐私保护(密码学,hash,数字签名…)
- 分布式共识(pow,pos,dpos,poe)

共识协议

- **POW：Proof of Work，工作证明。**
- 比特币在Block的生成过程中使用了POW机制，一个符合要求的Block Hash由N个前导零构成，零的个数取决于网络的难度值。要得到合理的Block Hash需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的Block Hash值，说明该节点确实经过了大量的尝试计算，当然，并不能得出计算次数的绝对值，因为寻找合理hash是一个概率事件。当节点拥有占全网n%的算力时，该节点即有n/100的概率找到Block Hash。
- **POS：Proof of Stake，股权证明。**
- POS：也称股权证明，类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。简单来说，就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明POS模式下，有一个名词叫币龄，每个币每天产生1币龄，比如你持有100个币，总共持有了30天，那么，此时你的币龄就为3000，这个时候，如果你发现了一个POS区块，你的币龄就会被清空为0。你每被清空365币龄，你将会从区块中获得0.05个币的利息(假定利息可理解为年利率5%)，那么在这个案例中，利息 = 3000 * 5% / 365 = 0.41个币，这下就很有意思了，持币有利息。
- **DPOS：Delegated Proof of Stake，委任权益证明**
- 比特股的DPoS机制，中文名叫做股份授权证明机制（又称受托人机制），它的原理是让每一个持有比特股的人进行投票，由此产生101位代表，我们可以将其理解为101个超级节点或者矿池，而这101个超级节点彼此的权利是完全相等的。从某种角度来看，DPOS有点像是议会制度或人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的超级节点来取代他们。DPOS的出现最主要还是因为矿机的产生，大量的算力在不了解也不关心比特币的人身上，类似演唱会的黄牛，大量囤票而丝毫不关心演唱会的内容。
- **POE: Proof of elapsed time ,消逝时间证明**
- Intel 公司芯片级别的共识协议, 耗电量少

交易性能

- 比特币 7笔/秒
- 以太坊 15笔/秒
- VISA / hyperledger 百万笔/分钟

认识误区

- 区块链不是比特币
- 区块链不是数据库
- 区块链并不是一个颠覆万能的技术

现有落地产品

- 比特币 (c++)
- 以太坊 (Java,Python,Rust,Ruby,C++,Go)
- Hyperledger (go,nodejs,python)
- Corda (kotlin)