蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

比特币区块结构

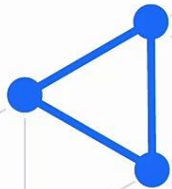
- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解比特币的总体架构
- 了解比特币的区块结构
- 了解比特币的基本运行原理

课程目录

01 比特币分层



区块链系统架构

区块链系统架构采用了分层结构。

应用层	封装区块链的各种应用场景和案例
合约层	封装各类脚本、算法和智能合约
通信层	节点间通信的通信协议
共识层	对区块数据的有效性达成共识
通道层	联盟链中确保隐私安全
网络层	区块链网络中节点与节点之间的信息交流方式
数据层	存储区块链基础数据

比特币分层

比特币其整体架构由下至上可以分层为存储层、数据层、网络层、共识层、RPC层和应用层。

RPC（Remote Procedure Call）远程过程调用，简单的理解是一个节点请求另一个节点提供的服务

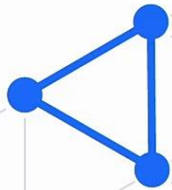
网络层：节点路由、寻址、节点的加入和离开等；区块的广播；发现节点（八卦协议）；

存储层：区块数据存在块文件中；块索引（快速定位，简化验证过程）、UTXO等存在levelDB中；新块的修改

02 比特币区块结构

区块头

区块体



比特币结构

- 比特币是区块链的实现，区块链是比特币的底层技术
- 比特币的区块结构
  - 区块头+区块体<=1M
  - 区块头：80字节
  - 区块体：包含2000个左右的交易，平均每笔交易至少250字节

字段名	大小	描述
区块大小	4字节	这个字段后的区块大小
区块头大小	80字节	包含组成区块头的几个字段
交易数	1～9字节	区块中交易的数量
交易	不固定	记录在区块中的交易信息

- 区块头结构
  - 区块头主要由三组区块元数据组成

	字段名	大小	描述
	版本	4字节	版本信息，用于跟踪软件和协议的更新
第一组元数据	父区块哈希值	32字节	链接前一个区块的散列值
第二组元数据	Merkle树根	32字节	当前区块中所有交易的Merkle树根散列值
第三组元数据	时间戳	4字节	记录在区块中的交易信息
	目标难度值	4字节	当前区块工作量证明算法的难度值
	随机数	4字节	用于工作量证明算法的计数器

典型区块链（共识机制）交易TPS比较

- 比特币POW： 3-7tps
  - 10分钟出一个区块；每个区块2000个交易（0.5M每个区块/250字节每个交易），每个区块包含2000个交易，每秒3.3个交易（2000/600=3.3 ）
  - 如每个区块1M计算（1024kb），每10分钟出一个区块，每笔交易占250字节（ 0.25KB）；每个区块每秒平均打包：1024/600/0.25＝6.82，大概7笔交易

- RBFT：300ms出一个区块；1s 3.3个区块；每个区块2000个交易；每秒 6600个交易，即6600 tps

- Avalanche：1秒内达成共识，每秒一个区块，理论TPS2000，实际tps能达到4500

区块结构——存储结构

- 区块是比特币存储交易的结构，一个区块总是指向其父节点。
- 一个区块包含三个字段：区块头、区块交易数量、交易列表。交易数量受到区块大小限制，输入、输出数量和脚本都会占用区块空间，矿工往往喜欢获得最高费用的交易列表。

区块结构——块结构

原始区块数据被存储在块文件中，这些文件以 blk*.dat 的格式命名，文件大小为 128MB，并以 16MB 为块（chunks）。块索引包含块的基本信息和在原始区块数据中的位置，块索引简化了验证过程。块索引为包含 6 个键的键值集合：

6个键值对：
—区块信息：区块高度、交易数量、区块验证状态、原始数据块文件号
—原始数据块文件信息：文件中的块数、文件大小、最低（高）块高度、最新时间戳
—重建索引标志位：1：正在重建索引；0：不需
—存储标志、可选值：tsnext=true时可用，用来存储原始数据块文件的编号

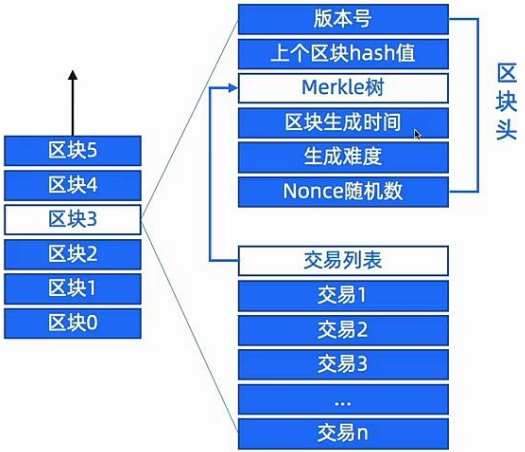
区块结构——区块头

比特币区块头包含了当前区块摘要信息和上一个区块的元信息，我们可以通过这些信息来验证区块体的正确性。

```
class CBlockHeader
{
public:
    // header
    int32_t nVersion;
    uint256 hashPrevBlock;
    uint256
hashMerkleRoot;
    uint32_t nTime;
    uint32_t nBits;
    uint32_t nNon
...
```

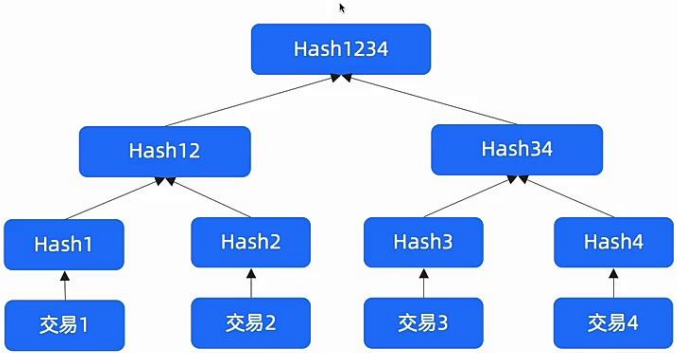
比特币区块头定义中虽然只包含 6 个字段，但每一个字段对于当前区块链的运行都必不可少。

比特币区块数据结构代码描述可见比特币源码的 bitcoin/bitcoin/src/primitives/block.h 文件。



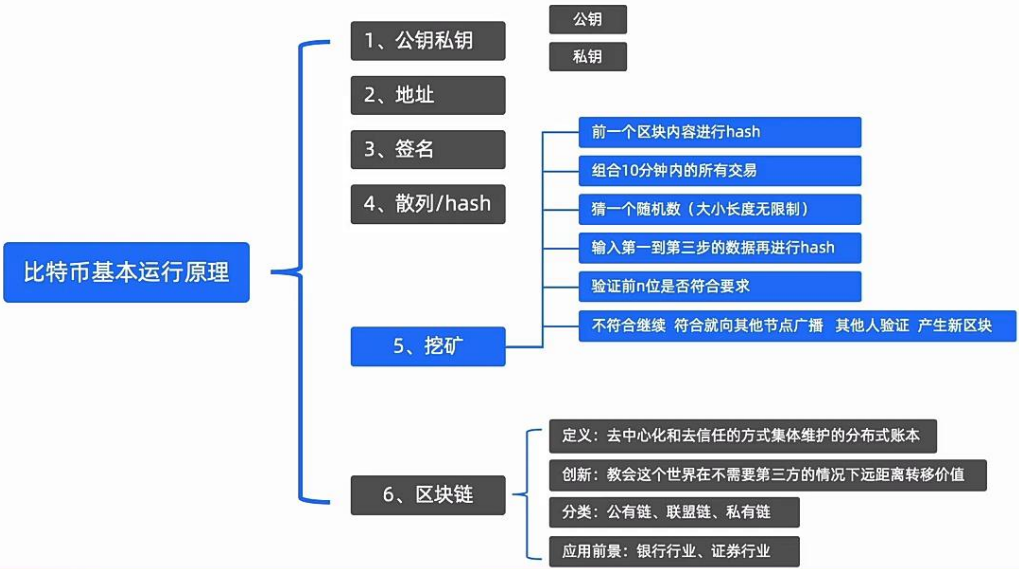
区块结构——区块体

- 比特币区块体用于存储真实的交易记录。
- 区块体包含有序的交易列表，这些交易列表通过默克尔树算法生成的根哈希存储到区块头中，这样可以通过区块头中的少量信息对区块体中的交易进行验证。



03 比特币基本运行原理

比特币基本运行原理


比特币基本运行原理
1、公钥私钥
公钥
私钥
2、地址
3、签名
4、散列/hash
5、挖矿
前一个区块内容进行hash
组合10分钟内的所有交易
猜一个随机数（大小长度无限制）
输入第一到第三步的数据再进行hash
验证前n位是否符合要求
不符合继续 符合就向其他节点广播 其他人验证 产生新区块
6、区块链
定义：去中心化和去信任的方式集体维护的分布式账本
创新：教会这个世界在不需要第三方的情况下远距离转移价值
分类：公有链、联盟链、私有链
应用前景：银行行业、证券行业

总结

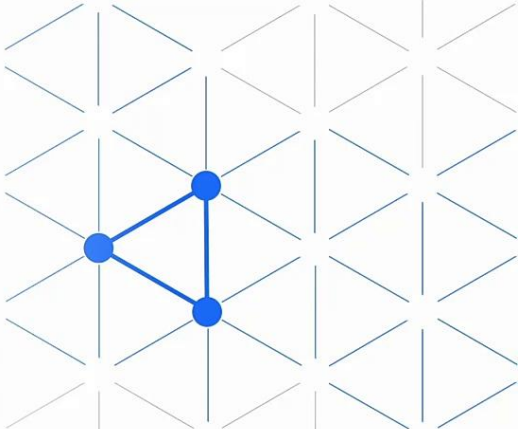
比特币的架构与存储结构

- 比特币的架构组成；
- 比特币的存储结构是由区块体加上区块头构成一个区块，以区块头指向上一个区块体的方式形成链进行数据的存储。

比特币的基本运行原理

- 保证交易的安全性；
- 比特币保证系统稳定运行。

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN