1.为什么说比特币是高度透明和隐秘的?使用比特币交易后可不可以查看交易双方?通过比特币地址为什么不能查找到人?

答:(1) 透明是说所有的交易信息每人都能查看,隐秘是说:交易双方的信息都是加密的,

(2)可以查看,只能查看最近的交易记录,双方的标识id会变化(加密)

(3)区块链技术作为比特币的底层支撑，可以清晰的记录并查到所有比特币地址、支付以及交易路径，通过分析交易模式，追查到资金的走向以及公钥背后实际的当事人是很有可能的。来自〈http://www.wanbizu.com/news/201705229806.html〉,黑客如果不会洗钱(币),钱就等于是死钱了

2.每产生新的比特币,新的比特币会记录以前的记录吗?如果记录,随着记录的增多,以后产生的比特币会不会疲于更新?如果不同步,也就说明区块链的内容不一样?

答:(1)当前块只会记录(从生产开始算)10分钟内的交易内容

(2)内容的确不一样,但是都是承接的

"可以这么理解，比特币系统是一个巨大的、不断更新的账本。每一页都叫做一个区块，按照时间顺序连起来，就叫做比特币的区块链。每10分钟新增一个区块，里面的内容是过去10分钟系统内发生的一些交易。每一笔交易都会完完整整记录在这个账本里，比特币就是账本里记录的钱"

来自〈http://tieba.baidu.com/p/5606568292〉

3.51%算力攻击

答:所谓51%攻击，就是利用比特币使用算力作为竞争条件的特点，使用算力优势撤销自己已经发生的付款交易。如果有人掌握了50%以上的算力，他能够比其他人更快地找到开采区块需要的那个随机数，因此他实际上拥有了绝对哪个一区块的有效权利

来自〈http://8btc.com/article-1949-1.html〉

交易生效是需要下一个块生成才确定的,如果有人掌握50%算力,就有能力算出另一个(并列)块,因为算力够强,继续生成下一块,而区块链会选择最长的链作为主链,从而虚假块成为主链,真正的交易块被遗弃

但是基本拥有51%算力基本不可能,目前算力是 236万万亿次哈希碰撞每秒 ,而世界第一的神威太湖之光 仅9.3亿亿次每秒,

4.比特币同时多处交易,怎么保证数据的同步?(等6个块)

答:每次交易只部分块记录(块会记录块产生后的10分钟内的所有交易记录),发生一次就在块中记录一次,然后hash不停在计算,更新后面的块,等6个块就完全确定了交易

5.如果比特币只记录10分钟内的记录,那就意味着有些块记录特别少,有些块记录特别多?

答:　是先有交易才会有块,等达到一定的交易量时才会被矿工拿着这些交易记录去挖矿,所以交易记录不会有重复

一次交易流程大致如此:

1.产生新交易:　我产生一个交易A

2.签名加密:　验证这个交易是不是我发起的,钱是不是我的

3.交易在比特币网络中传播:验证完成后,要别人验证,是不是我的钱,钱够不够之类的

4.整合交易&构建新区块:验证交易后，每个比特币网络节点会将这些交易添加到自己的内存池中，内存池也称作交易池，用来暂存尚未被加入到区块的交易记录。而挖矿节点除了收集和验证交易以外，还会将这些交易打包到一个候选的区块中,会把交易A连同其它一些近期被创建的交易整合,打包.挖矿节点需要为内存池中的每笔交易分配一个优先级，并选择较高优先级的交易记录来构建候选区块，在区块被填满后，内存池中的剩余交易会成为下一个区块的候选交易。然后挖矿节点就准备拿候选区块来挖矿

5.挖矿:猜测一个数值(nonce),进行计算(相当复杂的),猜出一个小于nonce值就是正确的hash,即正确的块,获得"记账权",那些交易记录将存在这个块中,节点(矿工)将获得奖励(网络中还有比特币时奖励比特币和交易费,没有比特币就奖励交易费)

6.新区块连接到区块链:比特币交易生命周期的最后一步是将新区块连接至有最大工作量证明的链中。一个节点一旦验证了一个新的区块，它将尝试将新的区块连接到到现存的区块链组装起来。

我有一个交易记录A,交易 A 会被一个或者多个签名加密(这些签名用来说明交易 A 是我发起的,不是别人)。而后，交易 A 被广播到比特币网络中，最快收到广播信息的是相邻的 2- 3 个节点，这些节点都会参与验证这笔交易，于此同时将交易在网络中再次进行广播，直到这笔交易 A 被网络中大多数节点(所有下载比特币客户端的设备都有可能成为这样的节点)接收,最终，交易 A 被一个正在参与挖矿的节点验证，交易 A 连同其它一

些近期被创建的交易一起被打包到一个区块 B ()中，并被添加到区块链上，这时整个区块链就被延长并新增了一个区块 B 。区块 B 获得 6 次以上的“确认”时就被认为是不可撤销的，

来自〈http://www.yixieshi.com/110742.html〉