引言

为了写一篇关于NFT的文章，需要引用一些关于区块链防篡改的技术细节，就把几年前写的一篇相关文章发布了出来。

文章中有些内容已经过时，还请见谅，但是底层技术是没有什么变化的。

虽然虚拟货币和NFT的妖风都已过去，但是底层设计依旧让人惊艳。也欢迎感兴趣的小伙伴一起交流。

正文

比特币是一个完全开放的去中心化的金融系统，时刻暴露在全球黑客攻击之下仍能安全稳定的运行至今（除了在2010年遭到一次大整数溢出漏洞攻击），用事实证明了比特币系统的安全性和稳定性。

这其中一整套完整的防篡改破坏的安全体系是其最大的安全保障，下面我们就来逐步揭开比特币防篡改特性的面纱，体会一下比特币设计的奥妙。

非对称加密算法

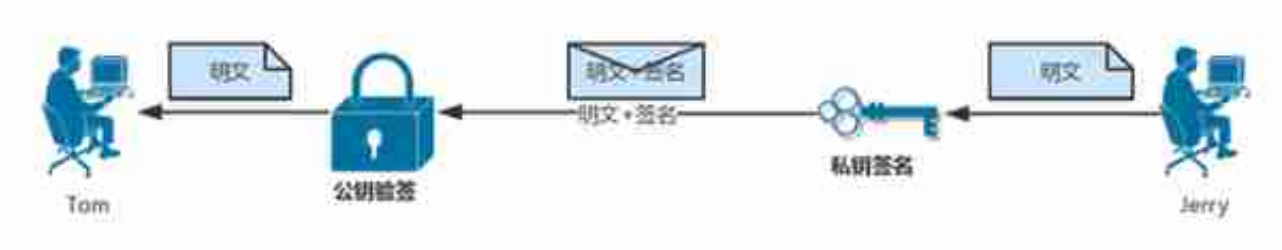
首先我们先复习一下非对称加密的概念：非对称加密都有一对密钥，分为公钥和私钥，两者是一对一的关系。

公钥顾名思义是可以公开的密钥，私钥必须自身严格保存，一旦暴露就相当于银行卡密码被人知道一样的可怕后果。

公私钥有两种用法：

一种是公钥加密数据私钥解密数据：

Tom要给Jerry发信息，Jerry先将自己的公钥发放给Tom，Tom通过Jerry的公钥将明文数据加密成密文，只有Jerry相匹配的私钥才能将密文解密成明文，即使有人截取了Jerry的公钥，也只能用于给Jerry发送加密数据，在没有获得Jerry私钥的情况下，依旧无法破解Tom和Jerry的通信密文。



目前我们常用的非对称加密算法有RSA、ECC和国密SM2等算法。

比特币采用的是ECC椭圆曲线加密算法，用户发起的每笔交易都需要自身的私钥做签名，每个参与记账的节点都可以验证交易是否正确并通过用户的公钥验签信息是否被篡改过。这就完成了比特币防篡改的第一步--单笔交易防篡改。

那么为什么交易信息不加密呢？

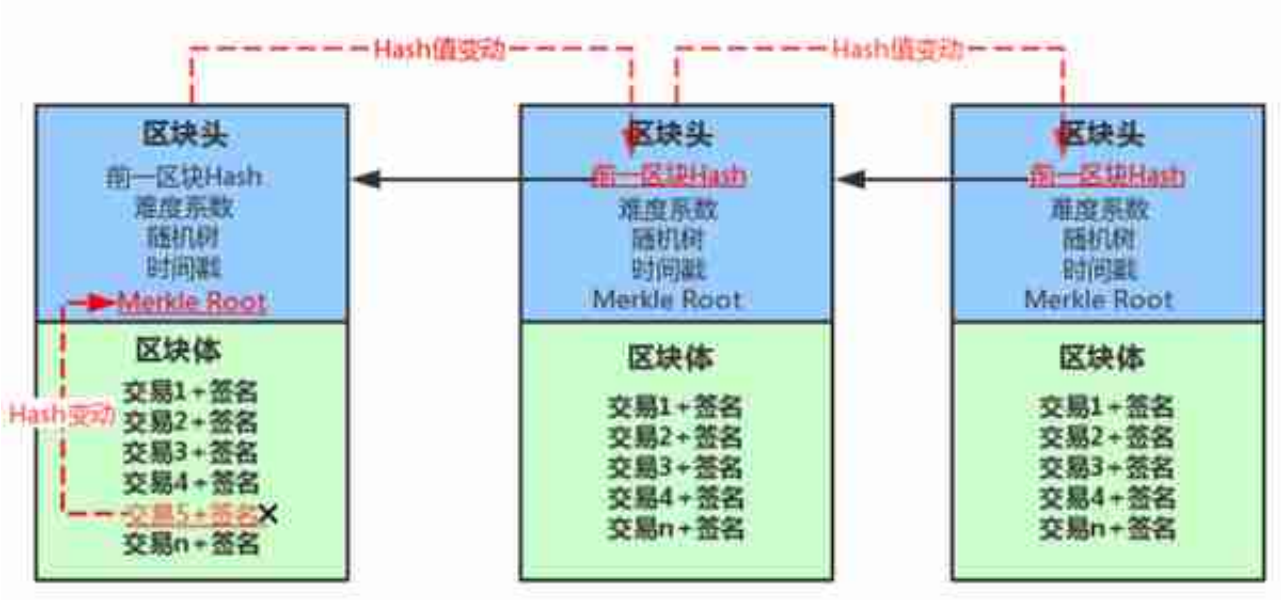
那是因为每一个参与记账的节点都需要验证交易的正确性和完整性，目前比特币参与记账的节点超过40万个，也就是需要用40万个公钥对交易加密40万次，这个计算量和耗时都是不能承受的，而且会影响记账节点的扩展性，所以目前比特币系统中的所有交易都是明文的，但是匿名性弥补了安全方面的不足。

当然，这方面的不足也有解决方案，请参考“零知识证明”、“同态加密”等相关知识，在此不做细述。

另外，因为比特币交易的匿名性，私钥签名就成为了唯一的身份标识，如果私钥丢失，就无法证明比特币是你的，你的比特币也就再也不属于你了。

Merkle树结构

上述比特币通过密钥签名完成了交易防篡改的第一道防线， 比特币交易信息的存储单位称为区块（Block），一个区块包含多笔交易（具体笔数和交易频次、交易数据大小有关），那么一个区块又是如何防篡改的呢？答案就是Merkle算法。



51%算力攻击

上述的多重防篡改机制已经让我们领略了比特币设计的严谨性，通过一环套一环的算法控制，账本很难被篡改。

那是不是基于POW算法的比特币系统就毫无破绽呢？

其实针对所有基于Pow算法的区块链系统，都有一个天生的弱点，那就是著名的51%算力攻击。如果有人控制了全网超过50%的算力（超过越多越容易掌控整个系统），他就能够比其他人更快地找到生成区块的目标Hash值，因此他实际上拥有了决定哪个一区块有效的权力，他就可以对自身的交易发起“双花”攻击（51%攻击、双花攻击概念太过复杂，还会牵扯到比特币UTXO的记账方式，足以单独成文，本文重点介绍防篡改机制，所以略过不表，网上有很多专门论述的文章），简单描述就是可以做交易不花钱。

这已经不是技术问题了，而是一个博弈问题，因为攻击会造成比特币这种去中心代币彻底失去信用，没有信用背书的比特币将变得一文不值。当一个人花费巨大代价获取到超过50%的算力（通过购买矿机或者控制其他人的矿机），并且购置了大量的比特币时，就不会冒着毁灭比特币的风险去攻击整个比特币系统，这样做伤人伤己，没有任何好处，而且以比特币目前的算力体量而且仍然在不断增长，想控制超过半数的算力已经变得越来越困难。

当然比特币的一些分叉系统或者一些较小的采用Pow算法的代币系统，整体算力比较小，实施攻击相对容易，可能就没有安全了。