算法探索还在路上

随着比特币、莱特币矿机相继出现，大家已经认识到没有不能开发矿机的算法，想通过改进算法来彻底阻止矿机和矿池的出现是不可能的。

区块链核心算法一：拜占庭协定

拜占庭的故事大概是这么说的：拜占庭帝国拥有巨大的财富，周围10个邻邦垂诞已久，但拜占庭高墙耸立，固若金汤，没有一个单独的邻邦能够成功入侵。任何单个邻邦入侵的都会失败，同时也有可能自身被其他9个邻邦入侵。拜占庭帝国防御能力如此之强，至少要有十个邻邦中的一半以上同时进攻，才有可能攻破。然而，如果其中的一个或者几个邻邦本身答应好一起进攻，但实际过程出现背叛，那么入侵者可能都会被歼灭。于是每一方都小心行事，不敢轻易相信邻国。这就是拜占庭将军问题。

在这个分布式网络里：每个将军都有一份实时与其他将军同步的消息账本。账本里有每个将军的签名都是可以验证身份的。如果有哪些消息不一致，可以知道消息不一致的是哪些将军。尽管有消息不一致的，只要超过半数同意进攻，少数服从多数，共识达成。

由此，在一个分布式的系统中，尽管有坏人，坏人可以做任意事情（不受protocol限制），比如不响应、发送错误信息、对不同节点发送不同决定、不同错误节点联合起来干坏事等等。但是，只要大多数人是好人，就完全有可能去中心化地实现共识。

区块链核心算法二：非对称加密技术

在上述拜占庭协定中，如果10个将军中的几个同时发起消息，势必会造成系统的混乱，造成各说各的攻击时间方案，行动难以一致。谁都可以发起进攻的信息，但由谁来发出呢？其实这只要加入一个成本就可以了，即：一段时间内只有一个节点可以传播信息。当某个节点发出统一进攻的消息后，各个节点收到发起者的消息必须签名盖章，确认各自的身份。

在如今看来，非对称加密技术完全可以解决这个签名问题。非对称加密算法的加密和解密使用不同的两个密钥.这两个密钥就是我们经常听到的”公钥”和”私钥”。公钥和私钥一般成对出现,
如果消息使用公钥加密,那么需要该公钥对应的私钥才能解密;

同样，如果消息使用私钥加密,那么需要该私钥对应的公钥才能解密。

区块链核心算法三：容错问题

我们假设在此网络中，消息可能会丢失、损坏、延迟、重复发送，并且接受的顺序与发送的顺序不一致。此外，节点的行为可以是任意的：可以随时加入、退出网络，可以丢弃消息、伪造消息、停止工作等，还可能发生各种人为或非人为的故障。我们的算法对由共识节点组成的共识系统，提供的容错能力，这种容错能力同时包含安全性和可用性，并适用于任何网络环境。

区块链核心算法四：Paxos 算法（一致性算法）

Paxos算法解决的问题是一个分布式系统如何就某个值(决议)达成一致。一个典型的场景是，在一个分布式数据库系统中，如果各节点的初始状态一致，每个节点都执行相同的操作序列，那么他们最后能得到一个一致的状态。为保证每个节点执行相同的命令序列，需要在每一条指令上执行一个“一致性算法”以保证每个节点看到的指令一致。一个通用的一致性算法可以应用在许多场景中，是分布式计算中的重要问题。 节点通信存在两种模型：共享内存和消息传递。Paxos算法就是一种基于消息传递模型的一致性算法。706878

区块链核心算法五：共识机制

区块链共识算法主要是工作量证明和权益证明。拿比特币来说，其实从技术角度来看可以把PoW看做重复使用的Hashcash，生成工作量证明在概率上来说是一个随机的过程。开采新的机密货币，生成区块时，必须得到所有参与者的同意，那矿工必须得到区块中所有数据的PoW工作证明。与此同时矿工还要时时观察调整这项工作的难度，因为对网络要求是平均每10分钟生成一个区块。

区块链核心算法六：分布式存储

分布式存储是一种数据存储技术，通过网络使用每台机器上的磁盘空间，并将这些分散的存储资源构成一个虚拟的存储设备，数据分散的存储在网络中的各个角落。所以，分布式存储技术并不是每台电脑都存放完整的数据，而是把数据切割后存放在不同的电脑里。就像存放100个鸡蛋，不是放在同一个篮子里，而是分开放在不同的地方，加起来的总和是100个。

算法演进之路

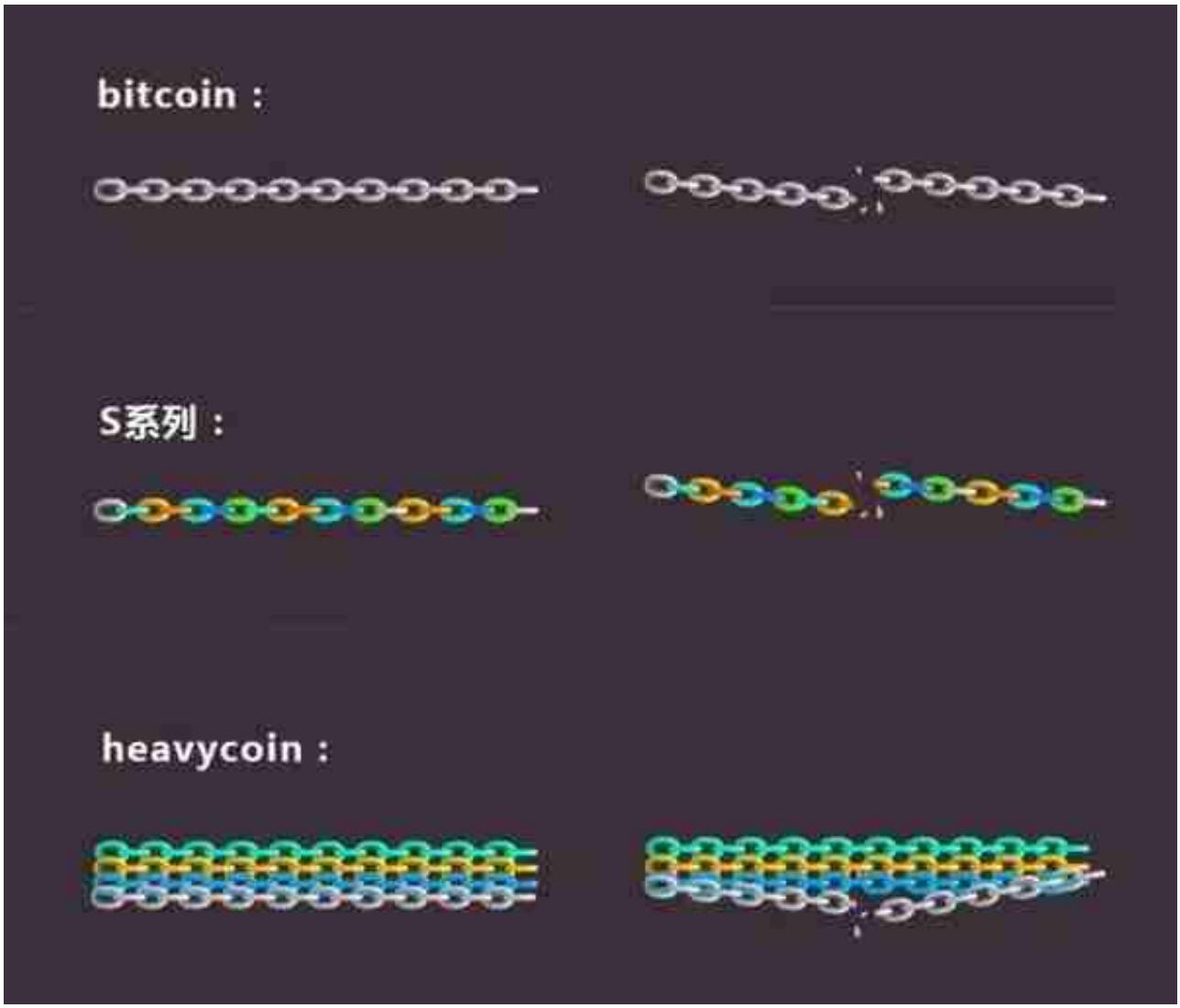
算法演进

关于“算法”一词，目前国内用户使用的比较模糊，有时指共识机制，比如POW算法，POS算法；有时指具体的Hash算法，比如SHA256，SCRYPT。应该说这是由于早期从外文资料翻译过来概念模糊导致的错误，后来人云亦云。共识机制（以前一般叫Proof，现在经常使用Consensus）和算法（Algorithm）在英文资料里语义清晰，不能混为一谈，两者都是区块链技术体系里的重要支柱。

因此当我们说“X币使用Y算法”的时候，其实具体指的是采用何种Hash算法，而且隐含的前提条件是这个币使用POW证明方式。只有在POW下讨论选取何种算法才有意义，算法的各种复杂设计才能体现其用处。为什么呢，中本聪在设计比特币的时候其实有很多地方用到Hash函数，比如计算区块ID，计算交易ID，构造代币地址等。我们说的算法具体是指用何种Hash函数计算区块ID，所谓算法创新也就是在这个地方下功夫。此外其他任何用到Hash函数的地方，对计算难度没有要求，而且应该选用可以快速运算的算法，尤其在计算交易ID时候，不然影响区块链同步速度。因此如果选用POS方式，计算区块ID也应该使用容易运算的算法。

Hash函数

如上所言，我们经常说的POW算法本质是一个Hash函数。Hash函数是一个无比神奇的东西，说他替中本聪打下了半壁江山一点不为过，学习比特币应该从学习Hash函数入手，理解了Hash函数再去学比特币原理将事半功倍，不然将处处感觉混沌，难以开窍。而中本聪也将Hash函数的所有特性使用得淋漓尽致：



之所以首先进行一轮HEFTY1 哈希，是因为HEFTY1 运算起来极其困难，其抵御矿机性能远超于SCRYPT。但与SCRYPT一样，安全性没有得到某个官方机构论证，于是加入后面的四种安全性已经得到公认的算法增强安全。

对比串联和并联的方法，Quark、X11，X13等虽使用了多种HASH函数，但这些算法都是简单的将多种HASH函数串联在一起，仔细思考，其实没有提高整体的抗碰撞性，其安全性更是因木桶效应而由其中安全最弱的算法支撑，其中任何一种Hash函数遭遇碰撞性攻击，都会危及货币系统的安全性。

HVC从以上每种算法提取64位，经过融合成为最后的结果，实际上是将四种算法并联在一起，其中一种算法被破解只会危及其中64位，四中算法同时被破解才会危及货币系统的安全性。