**【杂志独家】****韩锋：从中本聪论文解析比特币奥秘**

*2014-04-15* *韩锋* [清华金融评论](javascript:void(0);)



文/韩锋 清华大学物理系博士生

本文编辑/贾红宇

比特币的发明人中本聪留下过一篇关于比特币算法的论文。本文解析这篇论文，介绍比特币的密码学基础。

比特币是近年来互联网金融创新最引人注目的现象之一。比特币不需要第三方信用支撑，直接把P2P的信用基础建立在密码学协议之上。在经济学上，它实践了哈耶克提出的设想：流通货币应该由市场起决定性作用,优胜劣汰。在密码学上，它解决了数字货币重复支付的难题。在社会学上，它已经开始形成了全球互联网金融生态圈。在未来学上，它给我们提供了以下可能性和发展机遇：可能通过互联网P2P形成全球贸易的“超主权”货币体系，可能在一些通胀异常严重的国家出现通缩性数字货币救市的现象，可能大幅度降低全球贸易的信用成本。

中本聪（Satoshi Nakamoto）在创建比特币时，需要解决三个核心问题：

第一， 交易确认，利用互联网P2P协议，防止货币的重复支付（即防止造假币）。

第二，比特币的发行。

第三，保护比特币系统不受恶意攻击。通过研究中本聪关于比特币的文献《比特币：P2P电子现金体系（Bitcoin: A Peer-to-Peer Electronic Cash System）》，我们可以发现，中本聪设计的比特币，通过挖矿、记账、算力保护，从而“一石三鸟”地解决了上述三个核心问题。

据清华大学密码学专家王小云教授介绍，比特币的发行（俗称“挖矿”），是建立在SHA-256密码系统之上的。SHA是Secure Hash Algorithm的缩写，意思是基于哈希（Hash）函数算法的加密系统。以下我们通过解析SHA-256密码学系统，来分析展示中本聪解决问题的方法和思路。

哈希函数是一种加密算法，一般写为：h=hash(m),h代表哈希值，m代表对应这个哈希值的解（message）。哈希函数的特点：一是已知m，通过h=hash（m）很容易验证出它对应的哈希值h，但反过来很难，就是已知哈希值要求出对应的解m很难。正是由于哈希函数有这样运算的不对称性，或者说不可逆性，所以它特别适合为密码学所用。比如哈希值就适合当加密的“公钥”，可以完全公开，但是人们即使得到了公钥，也几乎不可能一下子算出它的“私钥”，也就是哈希函数的解m。但是反过来，如果我们已知私钥m，却很容易验证它对应的公钥就是哈希值h，这就是所谓“不对称加密算法”。

哈希函数的第二个“宝贵”特性是：如果“解”（即私钥）稍有不同，那么它对应的哈希值就会有很大不同，这叫雪崩效应（avalanche effect）。哈希函数所具有的这个优秀特性，保证了不同的私钥（哪怕只有一点点差别），都不会和对应的公钥搞混！

进一步我们可以了解：SHA-256是基于十六进位制的加密系统，也就是每一位上允许有十六个比特币的不同信息，一般用十个阿拉伯数字和前六个英文字母表示，即0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f。所以，你要是看到这样一个十六进位的哈希值:Hash:00000000000000004cf3aa249551432fa84da4de05e9cfc3e6d95a5ce8bed5f7，这是比特币世界2014-02-08T03:06:30美东时间，刚挖出的一个比特币区块（block）对应的哈希值，不要觉得奇怪！

之所以叫SHA-256，就是因为其哈希值有64位，每一位上有十六比特也就是二的四次方种选择，这样总的哈希值就可以有2的256次方个比特。

真是天文数字！中本聪把SHA-256加密算法选为比特币的挖矿算法，因为哈希值前面每增加一个零，寻找其解m的难度就会增加二的四次方倍。因为SHA-256还没有像王小云教授的SHA-1那样被破解，所以任何一个六十四位的哈希值，要找到其解m，都没有固定算法，只能靠计算机随机的hash碰撞。一个挖矿机每秒钟能做多少次hash碰撞，就是其“算力”的代表，单位写成hash/s,这就是所谓工作量证明机制POW（Proof Of Work）。

正是基于SHA-256这种十六进位制的加密算法，中本聪在他最原始的比特币论文中写道：“工作量证明过程包括扫描SHA-256的哈希数由多少个0开头，每增加一个0，平均工作量都会有指数级的增加，就是二的四次方，增加了多少个零就是多少个二的四次方乘在一起倍数的工作量增加，这些将在解一个哈希数（也就是挖一个比特币区块过程）中得到证明。”

比特币系统就是靠对于挖矿的哈希值前面加零来控制挖币的总量，不管全网算力如何增加，都能通过在哈希值前面加零来保证平均每十分钟每个区块目前都只能挖出25个币(前四年是每十分钟50个币)，这样建立矿工，就自然解决了第二个问题，即比特币发行的问题。

那么比特币是怎样利用密码学挖矿系统来防止重复支付呢？就是靠这些“挖矿”的计算机算力来同时“记账”和盖时间戳（time stamp），每十分钟挖出一个区块，必须记录这十分钟全网的比特币交易和给每一个交易盖上时间戳，每一笔交易必须通过全网产生区块的节点（node） 六次确认，才能算合法交易，这样一个庞大的记账和盖时间戳系统，保证了重复支付的不可行（因为每个时间戳都要检验再次交易之前这些比特币没有支付过，才会 盖上“戳”，这样也保证原比特币持有者无法再支付给此次交易之外的第三方了。）所以，整个比特币系统的“挖矿”，既保证了比特币的正常发行，也保证了它的 记账，从而避免了重复支付的可能。所谓“矿工”，同时也应该叫记账员，特别是等到2040年比特币大部分已经被挖出，矿工们的工作奖励主要靠收取“交易费”时，他们就更应该被称为“记账员”了。

第三个问题，即保护比特币系统不受恶意攻击的问题，中本聪是怎么设计的呢？其实“矿工”对于比特币世界还有一个重要的功能就是“保护”，按照中本聪最初的比特币系统协议，必须持有全网51%算力的人，才有可能攻击比特币系统，并造成重复支付（也就是造假币）。据比特币挖矿资深人士透露，当前算力成本每年维持1G hash/s约需要240元人民币，即现在比特币全网算力的年成本是9.6亿美元，这是保护比特币系统的基础力量，也是它现有价值的支撑。