1. 比特币与区块链

1.1 比特币的概念

比特币（Bitcoin）的概念最初由中本聪在2008年11月1日提出，并于2009年1月3日正式诞生 。根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的虚拟的加密数字货币。点对点的传输意味着一个去中心化的支付系统。

与所有的货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。

1.2 历史

- 2008年11月1日，中本聪发表《白皮书》
- 去中心化的电子记账系统

1.3 比特币系统记账原理

假定比特币系统中存在A、B、C、D 4个用户。A用户支付10比特币给B，这个交易活动A会向B、C、D进行广播；B支付5比特币给C，B会向A、C、D进行广播；C支付2比特币给D，C会向A、B、D进行广播。类似这样，每一条交易，交易的发出人都会向全网广播（此时就是A、B、C、D），全网的每个人都能收到所有的交易记录。为了便于管理，我们将这些交易记录打包为“区块”，每个区块大小为1M左右，包含4000条左右交易记录，区块还包含一些摘要信息（后面会说）。随着交易的继续，产生的区块会越来越多，我们将这些区块链接起来，就形成了一个链条，这就是“区块链”。

1.3.1 为何要记账

比特币系统中的每一个参与者都需要记账，也都有将账目打包为“区块”的权利。中本聪在设计比特币系统时，规定每10分钟打一个区块，系统会对成功的“区块”打包者进行奖励，前4年每个“区块”的奖励为50比特币，第2个4年的奖励为1/2*50比特币，第3个4年奖励 1/2 * 1/2 * 50比特币，依次类推，这样算起来所有“区块”打包的奖励总共为：

```
50 * 6 * 24 * 365 * 4 * ( 1 + 1/2 + (1/2)^2 + ...) = 2100万
```

基于上述原因，比特币总共只有2100万个。

1.3.2 记账以谁为准

比特币系统的每一个参与者都可以打包“区块”，这就涉及到底以谁为准的问题，也就是挖矿原理的问题。挖矿使用哈希函数sha256算法进行，这个算法的特点是正向哈希计算容易，反哈希困难。每一个“区块”内部包含有区块头和账目信息。哈希算法对块头ip、账单、时间和随机数组成的字符串进行两次哈希运算，最终生成一个数值。比特系统要求这个数值的前n位应该是0，如果运算结果前n位不是0，可以修改随机数重新运算，直到满足前n位都是0的目标。而前n位都是0的概率是1/2*1/2*...* 1/2=(1/2)^n，需要计算2^n次。假定比特系统中有

10000台矿机参与运算，每台矿机的哈希运算速度为14T/s，也就是每秒运算1.4*10^13次，由于每10分钟打包一个“区块”，在10分钟内10000台矿机可以运算1.4 * 10^13 * 10^4 * 600 ≈ 8 * 10^19次，也就是2 * n = 8 * 10^19，计算可得n=66。优先算出前66位为0的哈希值的机器获得了记账权限，它可以发布打包好的区块。

1.4 如何进行身份认证

比特币使用公钥进行电子支付身份认证。用户在比特币系统注册时，系统会分配给用户一个私钥、公钥和地址，用户需要妥善保存私钥，而公钥和地址则是公开的。 假定现在A发布一条账单信息，此时A会对账单信息进行hash运算，从而形成一个摘要，接下来A使用私钥对摘要进行加密，从而形成一个密文，最后A将账单信息、公钥和密文在系统内广播；此时假定B收到了A的广播，为了确定A的身份，B会使用A的公钥对密文进行解密，从而获得摘要1，然后B对A发送的账单进行哈希运算，从而获得摘要2，接下来对比摘要1和摘要2，如果相等，则可以确认信息来源的正确性，否则忽略该广播。

1.5 如何确认余额信息

比特币系统中的用户会对区块链进行追溯，从而查询用户的余额。

1.6 如何解决双重支付问题

假定A只有10比特币，A确发送两条消息，一条是转给B 10比特币，另外一条是转给C 10比特币；这两条消息在网络上传输，收到这两条消息的用户可以通过追溯来确认A的余额，所以A的双重支付只会有一条被确认，此时挖到矿的用户可能会接收第一条消息的同时忽略第二条消息，也可能接受第二条消息的同时忽略第一条消息，总之A的支付记录只有一条被打入“区块”中。接下来未挖到矿的用户就自动接受新增“区块”的记录了。

1.7 如何放置伪造

假定一个用户想伪造交易记录，那么他需要在某一个区块的位置加入自己伪造的“区块”，并在后续不断链接区块。但是由于区块链系统默认会承认最长的区块链，伪造者并不能成功。但是如果伪造者有着超强的挖矿能力，它就能构建最长的区块链，从而实现伪造的目的，但如果有此实力，其实并不需要伪造了。