1. **比特币的发行**

比特币作为“矿”来到这个世界上。通过我们的“计算机”(早期使用CPU或显卡挖掘，而现在都是使用专用的矿机)挖掘。这些“计算机”都在通过一个“密码游戏”，谁最先算出来谁得到这十分钟之内的比特币奖励。比特币十分钟奖励一次称之为一个块。

由于这个游戏会根据完成任务的进度调整难度。参加的机器越来越多，因此个人拿到整个奖励几乎变得不可能。再后来就出现了矿池：大家一起挖，挖到了大家根据工作量分钱。机器也就成了替矿池打工的矿工。比特币也就被分在世界上的各个角落。

事实上，我们在使用电力成本生产比特币。比特币通过电把它与世界紧密的联系到了一起。现在比特币的全网算力152.6P(2014/08/16 00:00)。(早在13年5月比特币全网算力就超过全世界Top500的超级计算机算力之和)



1. **比特币的流通**

下面采用一个例子来说明比特币的流通性：

作为矿工的我辛辛苦苦挖了一点比特币，休息之余约小A,小B，小C打麻将。为了不用每盘给钱，我们采取记账的方式。我们一起做一个记账本，记下每盘的情况。比如这盘我输小C一个比特币。记下“我(应)给她一比特币”。打到最后，依据每盘的记录，我一共输给了小C十个比特币。

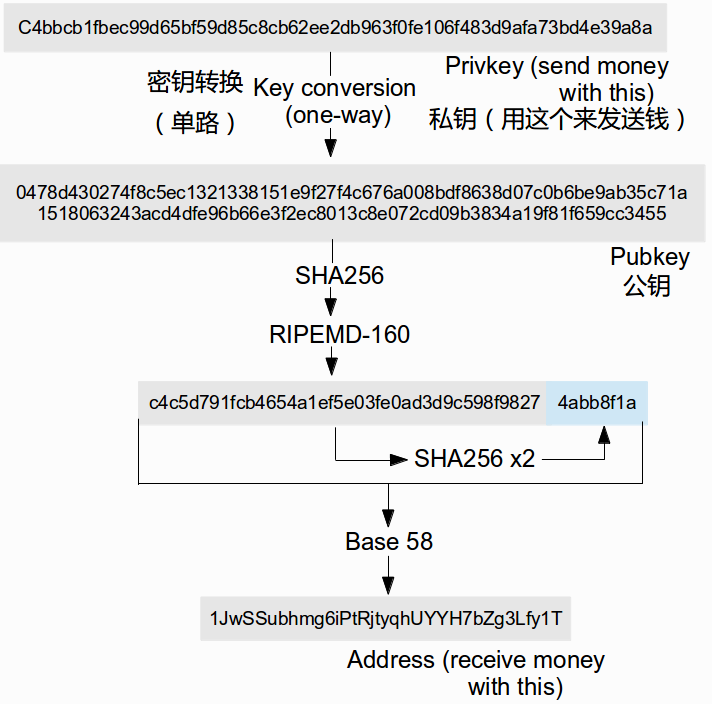
　　比特币采取类似这样的记账的机制，比特币的总量一定数量，总和一定是2100万。由于我与小A小B小C共同记账，因此账本不会出错，每一宗交易都可追溯，比特币就如此流通在世界上了。而这本世界公开账本则储存在比特币核心里，即我们的电脑硬盘里，可供查阅。

1. **比特币的原理**

作为基于密码学的货币，比特币的本质是私钥。

私钥 >> 公钥 >> SHA256(公钥)… >> 比特币地址。

只要保护好你的私钥，谁也没办法拿走你私有财产。



由于比特币是开源的项目，更加的保证了其安全性。迄今为止已经有500多种根据比特币进化改良的虚拟币，使其成为一个更为公平的市场。市场的博弈决定优胜劣汰，同时推动着[虚拟货币](http://www.wanbizu.com/)的进步。

比特币账本分布在世界各个角落。有人为比特币布超级节点，甚至有人准备发射卫星广播比特币区块链。

它是去中心化的，不受任何国家的控制，且永不会增发。

其简单的流通不需要任何第三方机构，其流通成本与现在费用极高的国际转账业务形成巨大的反差。

整个系统的简而美，以至于”It is too simple to crack”。

另外相信存储在我们电脑里的“账本”是全人类最为安全的资料之一，通过在比特币网络上的扩展，或许这个资料也将是最值钱最宝贵的人类财富。