区块链的第一个应用——比特币

2008 年，中本聪把自己的比特币白皮书发布在一个专业研究加密技术的的社区里面，但响应者寥寥。

2009 年 1 月 3 日，中本聪发布了最早的比特币软件，并在赫尔辛基的一个小型服务器上创建了第一个区块，得到 50 个比特币。

在比特币大火之后，大批“信徒”把这一天称为创世日，这个区块也被称为创世区块。

区块诞生的那一天，中本聪写了一句话，这句话也是那天《泰晤士报》的头版标题：2009 年 1 月 3 日，财政大臣正处于实施第二轮银行紧急救助的边缘。

中本聪发明比特币，本意是想创造一种不经过银行，金融机构等中介，能够买卖双方直接交易的去中心化数字货币。

2009 年正是全球金融危机的高潮，中本聪写下这句话，正是想讽刺全球金融体系。

二

说到比特币的发展，就不得不提起一个人：**加文安德烈森。**

比特币最初无人问津，非常之小众。

加文安德烈森作为一个程序员，了解比特币构思及源码后便积极投身比特币宣传事业，创办 https://freebitcoins.appspot.com 网站。

而此时，中本聪则渐渐走向幕后。

2010 年 5 月，佛罗里达一位软件设计师拉斯诺悬赏 1 万个比特币让人送披萨饼，5 月 22 日，加利福尼亚州的一个人打电话帮他支付了美元购买了两个披萨，送到拉斯诺手中。

后来，5 月 22 这一天被定为比特币披萨日，这是比特币第一次购买实物。

2010 年 7 月，位于日本东京的 MT.Gox 门头沟比特币交易所成立。

2011 年，为了更好的推广比特币，加文·安德烈森提议成立非营利性的比特币基金会。

一年后比特币基金会正式成立。

比特币渐渐走入公众视线，并在 2013 年获得德国正式承认的合法地位。

三

什么是比特币？

先来看一下官方解释版本：**比特币(BitCoin)是一种 P2P 形式的数字货币。**

点对点的传输，意味着一个去中心化的支付系统。

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。

概念看过了，怎么理解呢？

首先我们先看看人民币是什么?

我们现在常说央行又“印了“多少多少钱，很多时候并没有真实的“印钞“的过程。

准确说应该叫“投放“，更直白点说，央行就是改了一个数字:我在你银行的总资产上加了一个数字(同时负债上也加一个数字)。

银行同志，现在你可以“贷＂更多的钱出去了。“印“这个动作就完成了。

我们现在又听说，央行要发行自己的数字货币。这又是什么意思呢，难道央行要搞一个新的币种?

并没有，央行的意思是说，它想借鉴区块链，这种支付技术，应用到人民币的支付清算当中去。

那么，人民币本质上是什么?

它其实是个抽象概念，它的存在形式可以是现金、银行户头里的数字，或者数字货币。

而它本质上，其实就是个有用的数字。你有多少人民币，那其实是个数字。

这个数字是你通过和别人不断进行加减运算(经济活动)得来的。

一个国家一共发行多少人民币，那也是个数字，这个数字是央行“根据社会活动需要“拍定下来的。

那么比特币是什么？

比特币其实也是个数字。

只是目前人民币承载在一个中心化的支付系统上，而比特币承载在一个去中心化的支付系统上。

如果有一天央行也将人民币用比特币的支付技术数字化了。那人民币和比特币还有什么区别呢?

至少在技术层面上，它们就没有什么区别了。

它们最大的区别就在于，人民币是央行印的，比特币是中本聪印的。

我们来想象一个这样的场景：在一个电话推销公司中，为了鼓励员工的积极性，会对每 10 分钟内最先达成交易的员工给予双倍提成奖励，奖励以记账形式登记，每月月底再进行结算。

为了避免产生争执，需要以下措施：不再由经理统一记录，每一个员工都需要各自记录，不管最新达成交易的是不是你。

在这个场景中，账本上的奖励就相当于比特币；公司员工组成的网络就是一个 p2p 网络；每个员工都是一个节点；同事加记账共同组成的系统就是一个区域链；不再由经理统一记录就是去中心化；最先达成交易的员工会得到双倍奖励，这个就是挖矿。

四

很多人说比特币不是中本聪印出来的，是挖矿挖出来的，这个我觉得对，但也不全对。

你可以说比特币不是中本聪持有的，但我觉得它是中本聪印出来，或者说投放出来的。只是说他投放出来后，没有交到自己手里。

前面的例子中我们说过，最先达成交易的员工会得到双倍奖励，这个就是挖矿。

比特币是没有中心化发行机构的，中本聪在设计比特币时设立了奖励机制，用户通过贡献 CPU 的算力，最先找到特解，挖出新的区块的人便能得到比特币奖励。

最开始每 10 分钟生成 50 个比特币，每 21 万次后，比特币的单次产量减半。

自比特币诞生以来，已经产出了 1700 余万比特币，占到比特币总量的 83%。

而比特币除了区块链的公开透明，去中心化，不可篡改等特点外，还有发行上限，任何人不能更改，所以也具有抗通胀性。

比特币从诞生之日起，就被寄予去中心化、改变人类社会经济形态的厚望。

虽然直到今天还有一部分人不认可它，但它所代表的人类货币数字化的大趋势是不会改变的。