比特币

比特币是人类历史上第一种数字货币。

什么是数字货币？一句话概括，数字货币是基于数学加密原理构建的不可伪造的货币系统，而比特币是第一个基于数学加密原理构建的分布式数字货币系统。

比特币和区块链有什么关系？一句话概括，比特币使用区块链技术实现了数字货币的可信支付。

比特币的历史可以追溯到2008年10月，一个名叫中本聪的神秘人物在一个密码学朋克论坛上发表了一篇比特币：一种点对点的电子现金系统的文章，这篇文章被看成是比特币的白皮书。

随后在08年11月，中本聪发布了比特币的第一版代码。09年1月，中本聪挖出了比特币的第一个区块——创世区块，比特币网络正式开始运行。

到现在，比特币已经运行了11年多。

数字货币 vs. 电子货币

说起货币，我们想到的就是日常生活中使用的纸币。但是，纸币并不是天生就出现的。如果追溯到三千多年前，人类社会并没有任何货币，部落之间的贸易是物物交换。随着经济和贸易的发展，迫切需要一种“一般等价物”来作为商品交换的“中介”，这种一般等价物就是货币。最早的货币是贝壳，后来由于金属冶炼技术的进步，出现了铜、铁铸造的货币。金属货币由于体积小，容易分割和铸造，逐渐获得了广泛的使用。最终，世界各国的金属货币都落到了金、银这几种贵金属上。

随着经济的继续发展，金属货币因为沉重并且不易携带，因此，人们发明了纸币。世界上最早的纸币出现在中国宋朝，称为“交子”。纸币的发行机制决定了必须由政府发行，并且强行推广使用，因此纸币又称法币。

随着计算机技术的发展，银行系统经过几十年的发展，已经用计算机系统完全代替了人工记账，纸币也实现了电子化。现在，我们可以自由地使用网银、支付宝这样的工具实现随时随地转账付款，就得益于纸币的电子化和网络化。

电子货币本质上仍然是法币，它仍然是由央行发行，只是以计算机技术把货币以实体纸币形式的流通变成了银行计算机系统的存款。和纸币相比，电子货币具有更高的流动性。我们每天使用的网上银行、支付宝、微信支付等，都是这种方式。

而比特币作为一种数字货币，它和电子货币不同的是，比特币不需要一个类似银行的中央信任机构，就可以通过全球P2P网络进行发行和流通，这一点听上去有点不可思议，但比特币正是一种通过密码学理论建立的不可伪造的货币系统。

比特币解决的问题

比特币通过技术手段解决了现金电子化以后交易的清结算问题。

传统的基于银行等金融机构进行交易，本质上是通过中央数据库，确保两个交易用户的余额一增一减。这些交易高度依赖专业的开发和运维人员，以及完善的风控机制。

比特币则是通过区块链技术，把整个账本全部公开，人手一份，全网相同，因此，修改账本不会被其他人承认。比特币的区块链就是一种存储了全部账本的链式数据库，通过一系列密码学理论进行防篡改，防双花。

如果我们从现金和存款的角度看，现金是M0，而银行存款是M1和M2。银行存款本质上已经不是现金，而是用户的资产，对应着银行的负债。因为银行只记录用户在银行的资产余额，因此，用户A通过银行把100元转账给用户B的时候，用户A的资产减少100元，相应的，用户B的资产增加100元，银行对用户A和用户B的总负债不变。换句话说，存款是用户的“提款期权”。

而现金则是由用户自己负责保存的货币。如果用户A把100元现金给用户B，那么此交易并不需要通过银行，因为使用现金时，用户与银行之间没有资产和负债关系。

通过银行转移存款，对用户来说很方便，但永远绕不过中央信任机构，并且用户必须信任银行不会篡改余额。通过现金交易，用户并不需要金融中介，但是需要当面交易，以及会遇到现钞的防伪、防盗等问题。

比特币解决的是现金电子化后无需中央信任机构的交易问题，即M0如何通过网络进行价值传输。我们已经习惯了通过互联网对数字化的新闻、音乐、视频进行信息传输，因为信息传输的本质是复制，但现实世界的现金可不能复制。想象一下我们如何把100元现金通过网络发送给另一个人，同时确保交易前后两个人的现金总额保持不变。所以，中本聪的白皮书把比特币定义为“点对点的电子现金系统”。

小结

总的来说，比特币具有以下特点：

- 创建了无需信任中心的货币发行机制；
- 发行数量由程序决定，无法随意修改；
- 交易账本完全公开可追溯，不可篡改；
- 密码学理论保证货币防伪造，防双花；
- 数字签名机制保证交易完整可信，不可抵赖和撤销。