



链滴

初识比特币

作者: [flysea](#)

原文链接: <https://ld246.com/article/1544515794997>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

时常挂网的浪货们，不可能没听过“比特币”，从现在开始我将设法收集网络中的信息，以补充自身比特币的模糊理解。

概念：

比特币（BitCoin）的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及构建其上的P2P网络。比特币是一种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。

与大多数货币不同，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，具有极强稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个（<https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690?fr=aladdin>）

仅从百度百科的定义来看，比特币概念的提出，随之负载了其他几个名词“中本聪”，“P2P网络”“去中心化”，“密码学”，“总量2100万”。

中本聪：Satoshi Nakamoto 中本聪于2008年发表了一篇名为《比特币：一种点对点式的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）的论文，描述了一种被他称为“比特币”电子货币及其算法。2009年，他发布了首个比特币软件，并正式启动了比特币金融系统。2010年，逐渐淡出并将项目移交给比特币社区的其他成员（<https://baike.baidu.com/item/%E4%B8%AD%E9%9C%AC%E8%81%AA/5740822?fr=aladdin>）。百度百科，贴出了中本聪的照片，真是很扯，满络都知道，“中本聪”到目前为止无人认领。从这个名字来看是个和日本有关的博主。

P2P网络：百度百科解释的很清楚，这个名词没有任何可讨论余地，多提一句，当下载混双武打片时那个“种子”就是基于P2P技术实现的。这是很接地气的技术。

去中心化：这个提议在 区块链 也再三被强调，这是区块链，比特币之所以被推崇的最重要的因素。有中央银行。去中心化是比特币安全与自由的保证。这让我想起 庄子的一个说法“圣人不死，大盗不”。

密码学：在区块链中有描述。

总量2100万：很有意思的算法，为何要限制总量，而且限制方式是逐渐收敛。各种经济学者，认为这种方式会导致通货紧缩。以我理解通货紧缩，就是手中的钱越来越值钱，随着时间推移 手中同样货币能买更多的物品，那么会导致大家握紧货币，不去消费。好了，现在可以看出为什么各国都做适量的通货膨胀策略了吧。