2008年11月1日，一个自称中本聪(Satoshi Nakamoto)的人在一个隐秘的密码学评论组上贴出了一篇研讨陈述，陈述了他对电子货币的新设想——比特币就此面世。1年后，比特币的首笔交易完成。

概括来说，比特币基于一套密码编码、通过复杂算法产生，这一规则不受任何个人或组织干扰，去中心化；任何人都可以下载并运行比特币客户端而参与制造比特币；比特币利用电子签名的方式来实现流通，通过P2P分布式网络来核查重复消费。每一块比特币的产生、消费都会通过P2P分布式网络记录并告知全网，不存在伪造的可能。

比特币不依靠特定货币机构发行，它通过特定算法的大量计算产生，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。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。这确保了货币所有权与流通交易的匿名性。