



接触比特币以来，一直在探寻一个问题：比特币到底是什么？

有人说是数字黄金，有人说是跨境支付的工具，有人说是风险资产，有人说它是“郁金香泡沫”，还有人则直截了当的回答——不知道它是什么……

十年过去了，站在这个时间节点，回顾比特币的前世今生——它的诞生的理想是什么，有哪些并未实现，它将会改变什么，这样可能让我们更加接近真理。

理想之国

2008年10月31日，中本聪发布了比特币白皮书。他在白皮书中写道：

互联网商业几乎完全依赖金融机构作为可信的第三方去处理电子支付。虽然对大多数交易来说，这个系统还算不错，但它依然被基于信任的模型所固有的缺陷所拖累。

尽管这句话翻译成汉字不足百字，但意义非凡，此前，从来没有谁像中本聪那样通过区块链技术，不仅质疑了第三方机构存在的合理性，而且提出了可实操的方案。

他在比特币创世区块里再次写下了第三方机构存在的问题。“2009年1月3日，财政大臣正处于实施第二轮银行紧急援助的边缘。”他讽刺的是美国政府，当时正值经济危机，中心化控制的银行失去了信用。

中本聪给出的解决方案是，要实现一种完全通过点对点技术实现的电子现金支付系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何中心化的金融机构。

为了对密码朋克表示致敬，中本聪还用

密码技术保

护个人隐私，不受其它人、或者政府的侵犯。人们在比特币网络空间中进行支付，就像在物理空间的一个蒙面集市上，谁都不知道谁，但所有的支付信息都公开透明可查。

随着创世区块被挖出，比特币从最初白皮书的设想变为了现实，并且走上了和物理空间价值结合的道路。

2010年，美国佛罗里达一位名为LaszloHanyecz的程序员，用10,000枚比特币买了两个“约翰爸爸”（Papa John）的披萨优惠券，现如今，这10,000个比特币价值几亿多人民币。

当然，通过比特币买披萨饼仅是人们有趣的实验。后来，令人意想不到的是，随着比特币开始流行，它的价值也越来越高。

此时，一个普遍疑惑摆在人们心头：既然地球上已经有数以百计由国家和地区发行的纸质货币，为什么还需要在互联网上另外创造一种虚拟货币？

技术是思想异化的产物。后来人们发现，中本聪创造的比特币和奥派经济学家哈耶克的货币自由竞争理论非常契合。

哈耶克曾经说过：“从好人假设出发，只会设计出坏制度，从坏人假设出发，才会设计出好制度。”

过去的法币体系无疑都是从好人假设出发的，他们的假设是：所有银行都会合法合规，为了维护所有公民的权益不会随便乱发纸币。这里的银行是理性而且被神化，即会支撑经济繁荣，又愿意将财富发放给民间藏富于民。

哈耶克认为，社会上流通的货币不应是单一的，而是各种货币都有的自由竞争市场。中本聪创造比特币恰是符合哈耶克的愿景，在法币之外存在别的货币流通于市场。

然而，中本聪低估了比特币在现实世界的发展难度。

失落之塔

十年来，比特币改变了很多，比如价格飞涨实现了有价资产功能，越来越多人认识到比特币理念，可以作为临时跨境的支付的工具，普及区块链技术，等等；然而，从某些方面来看，比特币又无疑有它失落的地方。

首先是社区共识的分裂。

为了保证比特币区块链系统的安全和稳定，中本聪决定临时将区块大小限制在1MB。

一开始因为用户很少，交易量也不是很大，1MB的区块对系统并没有产生大的影响；然而，随着比特币价格猛涨，社区用户体量越来越大，比特币网络拥堵、交易费用上升问题开始凸显。

为了解决比特币区块链大小问题，以比特大陆为代表的算力巨头对比特币区块进行了扩容升级，将区块大小扩容到了8M，分叉币BCH就此诞生。

然而，随着BCH社区日益壮大，此次扩容并没有完美的解决比特币社区的分歧。BCH社区也面临着分裂的危机，比特大陆为代表社区力量正在进行虫洞计划。

其次，小额现金交易服务实现难行。

中本聪在白皮书中明确表示，其发行比特币的初衷是提供互联网小额现金交易服务，制定的去中心化电子现金系统框架至今没有变化，但由于币值升高，考虑将其用于小额交易的人不会很多。目前，缺乏有效手段保持比特币币值的稳定性，比特币作为稳定的交易媒介还存在较大问题。

中本聪公开表示过，期望通过比特币这个实验性产品来解决通货膨胀的问题，目前来看，作为货币的比特币也没有完全达到当初的目的。中本聪曾在公开言论以及私人邮件交流中表示，“如果十年后电子货币还没有普及，我会感觉很奇怪。”十年过去了，数字货币的普及方式已经脱离了中本聪最初的想象。

按照其最初的设想，比特币首先在小的细分市场上先应用起来，比如积分奖励、礼品卡、游戏币、付费邮件等等小额交易上。但矿池的形成以及后续的炒作完全脱离了中本聪的想象。

再者，从去中心化趋向中心化。

比特币最吸引人的是其去中心化的价值，然后十年来挖矿技术的进步，完全的去中心从现在来看是一种乌托邦的设想。

十年来，挖矿一开始用电脑客户端，然后用GPU，为了省电，开发出FPGA，最后ASIC化。前三个阶段，市场很零散，主要是技术极客在玩，算力垄断几乎很难实行；然而，随着ASIC矿机诞生，比特币区块链网络算力垄断变得可行。

最早的去中心化理论是基于，每一个人都有节点记账的权利，任何人只要启动挖矿程序就可以参与挖矿记账。但实际上，现在参与挖矿，只要把矿机连到矿池即可。按照现有的全球矿池统计，比特币挖矿基本是十几家矿池在相互竞争，最大的几家矿池甚至垄断约80%的份额。换句话说，挖矿变成了一种只有BOSS才有权利玩的游戏。

最后一个问题是隐私的问题。

匿名性是比特币另外一个吸引人的特点，然而在人们实际买卖过程中，要实现匿名性是非常难的。比如，现在各大交易所都有KYC制度，用户信息即被掌握在这些交易所手中。另外，银行、第三方支付等系统，通过数据监控是可以把区块链网络中交易对象映射到物理空间，这意味着用户交易过程也毫无隐私可言。

未来之路

站在过去十年和下一个十年的交点，比特币区块链的未来可以从两个维度来看。

第一个维度是其本身的发展。

首先，通过技术迭代完善交易支付功能，逐渐应用到人们的生活中，实现一些小额支付功能。

其次，硬分叉BCH后它或许能够借助比特大陆的虫洞计划，自身逐渐“进化”成像以太坊那样支持智能合约，可以跑DApp的公链，成为支持全球金融的基础设施。当然，这条区块链网络早已超脱了中本聪最初的设想。

第二个维度是其比特币理念的传播，实现“一花开五叶，五叶自然成”。

当年，达摩东渡传法于二祖至到六祖，这一花代表的是初祖达摩，五叶代表的是慧可、僧璨、道信、弘忍、慧能。这五位祖师让禅宗在中国扎根，深深影响此后的中华文化。

打一个不恰当的比喻，比特币意义就像当年的达摩东渡，它开启了全球区块链经济时代。它是区块链宣言书，它是区块链宣传队，它是区块链的播种机。

此后的以太坊、EOS，以及其他的区块链网络莫不是从比特币那里继承来的，后来的通证经济思想、ICO、STO也莫不是从比特币那里发展演化来的。所以，这个角度可能更能反映比特币的理念价值。

下一个十年，比特币内在的理念精神将继续在世界各地传播，它会越来越普及到人们生活，吸引无数人奔往区块链新大陆。

在这里，火星财经也与大家一道——

在凛冽的寒冬里，依然追寻太阳的光芒，踏上新的大陆。

更多专题报道：

「人物篇」链圈币圈：区块链世界的千面英雄

「行情篇」激荡十年：从0到3000亿美元，比特币行情全面回顾

「技术篇」比特币十年：一部慷慨激昂的技术进化史

「展望篇」未来之路：那些即将被区块链改变的行业

本文为火星财经原创稿件，版权归火星财经所有，未经授权不得转载，转载须在文章标题后注明“文章来源：火星财经（ID：hxcj24h）”，若违规转载，火星财经有权追究法律责任。