



随着互联网的发展和银行业务的电子化，从汇票、电报汇款，到网上银行、支付宝、微信支付等，原本以纸币为媒介的支付越来越多地通过电子化、数字化的方式进行。尽管这种货币的本质依然是主权信用货币，但纸币这种自然形态正在被数字这种虚拟形态所取代。从发展趋势看，货币必将甩掉其自然货币的尾巴——纸币，进入数字主权信用货币时期，其人为货币性质将表现得更为彻底。

在反对比特币的声音中，也包括认为比特币只是虚拟的东西，不能够成为货币的观点。现在看来，法币正在快速虚拟化，虚拟不是比特币的缺点，而是货币的现实和未来。

### 3. 比特币是货币吗？

主权信用货币体系的建立证明，人类能够创造出超越自然货币的人为货币。但是，主权信用货币依赖于国家信用，完全由政府掌控，也带来了一系列问题。最大的问题就是通货膨胀，在不受黄金储备限制之后，政府出于扩大财源、刺激经济、讨好

选民等目的，不断增发货币，导致金本位结束后普遍而长期的通货膨胀。这意味着公众财富的持续缩水。

为了消除法币的通货膨胀顽疾，一位化名“中本聪”的人在前人探索的基础上，设计出了一种新的人为货币——比特币。顾名思义，这是要建立一种完全数字化的货币，但其基本特征不在于数字化，而在于剥离货币对主权信用的依赖，转而建立在人人可参与的社会共识机制基础上，即所谓的“去中心化”。

经过多年的数字化，主权信用货币体系本质上已经成为一种记账货币体系，在计算机系统中记录货币的归属和支付交易。这个记账系统在央行的最终控制下由银行体系记录和维护。人为货币的核心问题是如何保证货币归属与交易记录的可靠可信。主权信用货币以央行所代表的可靠可信的国家政权来保证。比特币也是一个记账货币体系，它则是通过四个关键技术或机制，让每个参与者从自身利益出发，共同竞争记录货币归属和支付交易，并保证其可靠、可信。

第一个关键技术是分布式共识机制。

它将法币由央行控制的总账本转变为每个人都可复制保存一份的分布式总账本。货币的归属和支付由超过51%以上的总账本的一致记录为准。当总账本分布在全球的数十上百万参与者手中时，串通篡改或伪造账目的难度超出了黑客攻克任何一家银行系统。

第二个关键技术是区块链技术。

它通过哈希函数把总账本的每个帐页的全部信息压缩成简短摘要，然后嵌入下一个帐页。这样，每个摘要都通过摘要包含了之前所有帐页的信息，从而把整个账本链接为一条信息链，使得：1) 全部细节锁定在最新的一串摘要（即哈希值）中，遍布世界各地的分布式账本之间只需要核对哈希值就可以对账；2) 所有历史交易都锁定在最新的帐页，对历史的任何篡改都会被发现；3) 每个账号信息都与其他账号信息捆绑在一起，篡改一个账号信息，会因损害所有人的利益遭到抵制。这项技术为比特币区块链带来不亚于央行信用的公信力，这种公信力随着总账本的历史数据积累和用户群的扩大而不断增强。

第三个关键技术是非对称加密技术。

它通过两串非对称代码“地址”和“私钥”将现实中的人与总账本中的账号联系起来。这里的地址相当于总账本中的账号，私钥相当于所对应的支付密码。所谓“非对称”指的是：1) 从私钥（密码）可以推算出相应地址（账号），但从地址不能推算出私钥，所以公开地址不会泄露私钥；2) 用私钥对相应账号的转账支付指令



进行签名授权运算后，在不公开私钥的前提下，用相应地址就能够验证这个支付签名授权是否真实。这样，通过掌握私钥，现实中的人就有了对总账本的比特币的实际支配权。

第四个关键技术是工作量证明记账机制。

它用来保证新发生的交易被记录成唯一的新帐页，加入总账本，从而保持分布存储的总账本的一致性。在每个人都可以记账的规则下，通过猜测计算一个满足特殊要求的哈希值，比特币系统实现了让所有人都能参与记账竞争，但每十分钟左右只有一个人能成功记下新帐页，其他人复制该帐页加入自己保存的总账本中。这样就能使分布存储的总账本相互一致。同时，成功记账者能够获得12.5个比特币的奖励，这不但鼓励记账，而且是新币发行的唯一方式。新币记账奖励会每四年左右减少一半，从而消除了主权货币的通货膨胀顽疾。

通过以上四项技术或机制，比特币能够安全可靠地维护一个记账货币系统，并保证每个私钥拥有者对相应地址上货币有实际支配权，通过签名和验证完成安全转账，从而实现了货币的基本支付功能。除了用区块链公信力(本质上是对人的自利本性的信任)取代主权信用之外，比特币作为记账货币系统与法币实现的支付功能没有本质差异。因此，从技术上讲，比特币系统的确是一种货币体系，其中流通的比特币就是一种货币。

#### 4. 比特币被用作货币吗？

比特币系统在技术上具备了货币的功能，那么，有没有人把它作为货币使用呢？答案是：有，而且规模不断增长。

人们所熟知的用比特币达成的第一笔交易是2010年5月22日Laszlo用1万个比特币购买了2个比萨。或许还有更早的，但这是人们最津津乐道的。买比萨算是一次偶然应用，比特币最早被当做货币广泛使用，是在非法交易领域。最著名的是2011年初兴起的“丝绸之路”(Silk Road)网站，它主要使用比特币交易，用户超过100万，其70%的交易与毒品有关。这主要是因为比特币具有很强的匿名性，通过网上支付不像数字化法币那样容易被追查，并且，各国金融监管部门尚不了解比特币，更缺乏相应的监管法律和技术手段。2013年10月丝绸之路被FBI查抄，对比特币的非法应用受到遏制，但此后合法应用迅速兴起。

比特币的创新和开放性吸引了越来越多的支持者，一些支持者在自己的商铺中接受比特币支付，或者说服其他商铺这么做。2013年coinmap.org网站开始免费在地图上登记接受比特币的实体商铺，并提供查询检索服务，目前登记了世界各地近8000家商铺。一些跨国公司也陆续接受比特币支付，包括Paypal、微软、Dell、Expedi

a、Overstock等等。近期，全球最大网上游戏销售平台Steam取消了支付宝支付通道，转而开通了比特币支付。



有人会质疑，国家凭什么让纸币具有那么高的内在价值？其实这跟画家让纸具备更高内在价值并无本质区别。他们都创造了即稀缺又好用的东西，一种东西可供欣赏，另一种可供交换而已。有人会强调法币是因为其发行政府强制兑付而具备了购买力，其自身没有内在价值。但是，索马里政府倒台后，人们依然长期使用该政府发行的纸币。为什么呢？因为，它仍然是稀缺的、有用的，它仍有内在价值。

如果理解了主权背书的纸币具有内在价值，那么理解比特币具有内在价值并不困难。比特币通过分布式共识协议保障了稀缺性，并且具备了相对法币的更多优势，更有助于交换，因此，也就有了内在价值——货币的价值。

货币的价值从实物货币开始一直隐匿于实物的其他用途之中，被人们所忽视，进入主权信用货币这种完全人为货币，其内在价值本应被充分认识，但人们被其金本位纸币的前身和国家背书的法偿性所惑，无法摆脱传统认识。只有到了纯粹数字的、毫无其他用途的、不依赖国家信用的比特币出现，我们才能够更清晰地看到货币的价值，理解以往的各种货币的内在价值。

## 7. 比特币价格为何暴涨暴跌？

既然比特币具有成为更好货币的属性，从而具有内在价值。那么，为什么其价格会暴涨暴跌呢？自2010年8月以来，比特币价格日涨幅超过20%的有32天，最大日涨幅达到173%，而日跌幅超过20%也有10天，最大日跌幅达到64%。国内印象深刻

的是比特币从2013年9月的800元最高飙涨至12月的8000元，又一路跌到2015年1月的900元，到2016年6月又急升至5000元左右。难道内在价值不应该是稳定的吗？

的确，内在价值并不象物品的自然属性，如重量、密度那样稳定。内在价值取决于物品的稀缺性和人们需求之间的关系。而反映为实际的市场价格，还会受到人们对这种关系的认识的影响。比特币的稀缺性尽管是确定的，但人们对它的需求却很不稳定，尤其受到人们对其内在价值和发展前景的预期所影响，这是比特币价格巨幅波动的主要原因。

比特币从零开始到有人买卖、价格不断上涨，主要原因在于越来越多的人开始了解它，意识到它有希望成为更好的货币，从而预期它有可能升值而购买持有。越来越多的人购买持有，其价格就会上涨。当主流媒体或重大事件导致关注和了解它的人数陡然增加时，需求就会迅速增加，价格就会暴涨。比如2011年春天《福布斯》刊登了比特币的报道，推动价格上涨10倍，从86美分到8.89美元；2013年9月中央电视台等主流媒体广泛报道比特币也是此后价格飙涨至8000元的重要原因。

然而，从理论上更好的货币，到现实中的更好货币还有很长的路要走。比特币作为一个人为设计的重大经济机制，仍然具有试验性质，还存在许多不确定性，包括彻底失败的可能性。这些风险主要来自：

### 1) 技术风险。

比如非对称加密算法有可能被破解、协议代码可能存在漏洞、某种方式的网络攻击可能使整个系统瘫痪、系统升级中可能出现技术问题等等。这些是比特币发展早期面临的主要风险，毕竟中本聪势单力孤，其编程技术也并不十分出色。随着更多人才的加入，代码不断更新，很多潜在的技术风险被消除，中本聪也宣布退出了核心开发团队。经过7年的运行，市值过百亿美元之后，比特币已经遭遇过无数次的攻击生存下来了。现在，存在重大技术风险而未被攻击的可能性已经非常小了。

### 2) 竞争风险。

由于比特币是开源的，一个程序员几天就能山寨出一个新的币，此类币被称为“山寨币”，至今已有几千种。还有一些继承了比特币的主要特征，但在某些方面做出改进，对比特币形成一定的竞争压力，可称为“竞争币”，理论上会对比特币的市场和价值形成威胁。不过，威胁最大的可能是央行正试图用区块链技术改造法币而形成的主权数字货币，其他国家也在尝试。但是，相对于比特币，山寨币和竞争币更加脆弱，还需要面对更多考验，而主权数字货币主要是吸收了区块链技术节约信用成本的优势，而主权货币带来的政府过度干预、汇率成本和风险、创新动力不足



等劣势仍然存在。

### 3) 政策风险。

比特币成为货币将对现有货币运行、金融监管、货币政策等产生重大影响，会遇到传统货币金融体系的阻力，也会产生新的社会经济问题，产生新的政策管控问题。2014-2015年价格的持续下跌，很大程度上是受到国内相关政策的影响。尽管2013年以来，包括美国、中国、俄罗斯等国货币当局陆续由抵制转向逐步认同，但随着比特币逐渐进入主流经济，产生的摩擦将会更大，政策层面仍有很大的不确定性。

### 4) 转型风险。

经过7年的发展，比特币积累了相当的经验教训，技术上已经相对成熟，竞争优势业已形成，政策环境也趋向宽松，正在走向主流经济，总体风险较两年前大幅下降。目前，比特币面临的最大的风险是在从小众生态走向主流经济过程中的转型风险。在之前的小众生态阶段主要解决技术风险，系统生态简单，问题和目标明确。而进入主流经济则首先要应对市场迅速扩张对系统容量和稳健性的考验，还要解决更复杂产业生态中的利益相容问题，并且要在系统稳健性、去中心化和扩大市场规模之间做出权衡，而这些问题又都是全球范围内考量的。

作为试图改变世界经济命脉的一场伟大试验，比特币可能的辉煌前景和诸多潜在风险使它的内在价值本身存在很大的不确定性。

而比特币系统及其生态涉及到计算机硬件、编程、密码学、经济学、金融学、货币政策等多领域的知识，充分理解其原理、前景、风险有相当高的学习门槛。即使充分认识，也会对不同的发展方向和风险产生不同的判断，并且会随着形势的发展发生变化。所以，对比特币内在价值及其发展前景的认识和预期，在群体间会有很大差异，在时间上会有很大的波动。在比特币生态中的一个有趣的“粉转黑”的现象很能说明这一点，早期一些强烈支持比特币的“比特粉”，可能突然对比特币系统或其生态丧失信心，转而成为激烈攻击比特币的“比特黑”。

总体上，目前比特币仍是极小范围内流通的货币，只是由于其理论上的优势非常显著，人们对其内在价值的未来预期非常高，才有了较高的需求，推高了市场价格。预期带来的需求和实际需求相比，具有更大的波动性，会随着比特币的技术改进、应用扩张和各种风险的具体表现出现大幅的涨落。只有当比特币的发展前景逐渐在公众中形成共识，前景预期产生的需求逐渐被实际交易需求所取代，这种波动才会显著消减。

## 8. 比特币是一场伟大的社会试验

比特币是人类第一次有意识地创造的可行货币系统。这是一次伟大的经济试验，它将市场的命脉从政府回归市场，并为互联网提供内生的货币，推动经济的全球化和网络化，成为世界经济增长新的驱动力。

市场是人类社会演化形成的最重要的去中心化经济组织，它能将分散的经济主体组织起来，在保障所有权的前提下，配置他们的各种经济资源实现最大产出和最优分配。

市场价格是市场实现其功能的核心信息体系，而货币则是价格的标尺和流通的媒介，称得上是市场的核心。

随着近代市场经济的快速发展和全球化，经济危机成为重大的市场顽疾。为了解决危机，尤其是危机开始阶段的信用紧缩，政府接管了货币，创造出主权信用货币。市场的核心被拿到体外，在医生的干预下跳动。这虽能及时治病，却损害了日常功能，带来其他疾病。比特币以遵循市场去中心化组织原则的方式使货币回归市场，把核心放回体内，对全球市场经济的长期健康成长具有重大意义。

互联网是上世纪末以来最重要的技术创新，是带动第四次工业革命的基础性变革，它不仅缩小了世界，增进了文化交流，还为市场经济全球化提供了前所未有的广阔空间。然而，人们虽然能够通过互联网了解世界各地的经济资源和价格信息，但受制于主权货币的分割，大量交易因汇兑成本、汇兑风险和汇率制度等而无法实施。比特币的出现使得货币超越了主权分割，大幅缩小了国际贸易的交易成本，能够充分地发挥互联网的优势，发掘互联网时代的全球经济增长潜力。为此，比特币与区块链技术也被认为是第四次工业革命中的深度变革。

比特币不仅是一场伟大的经济试验，还是一场伟大的社会试验。人类社会文明进步的重要特征在于每个个体更加自由的发展。个体在智力、劳动、消费、思想等方面更加自由的发展，意味着社会会变得越来越复杂。将复杂社会有序组织起来而又尽可能实现个体自由，是文明进步的永恒主题。市场通过去中心化的自愿交易将自由个体组织起来，促进了文明的进步。比特币也是通过去中心化的技术和机制建立了原本需要人际信任维持的货币体系，使遍布全球的个体更加自由地组织起来，也促进了文明的进步。

不仅如此，  
比特币的货币  
试验还为其他领域  
解决复杂社会的组织问题提供了思路  
和技术。

比特币的核心技术和机制被简称为“区块链技术”，它不仅可以用于构建货币体系，还可以用于各种依赖人际信任的社会经济领域，比如产权、证券、保险、公证、选举、慈善等。目前，各领域的区块链技术应用探索方兴未艾，“区块链”一词的热度甚至已经超越“比特币”。随着这些探索的发展成熟，比特币对人类社会文明进步的重要意义也将进一步显现。

历经7年多，比特币凭借其作为交易媒介的优势，具备了货币的内在价值，取得了初步的成功。但目前仍然是一场试验，正面临着步入主流经济，接受全球市场检验的重大挑战。因此，还存在许多不确定性，价格的暴涨暴跌仍会继续。无论这场货币试验最终是否成功，其创新意义已经日益明朗，应该以更加积极地态度对待它，使其成为推进第四次工业革命和全球经济复苏的重要动力。

（本文首发链得得App）

最好看的得得专栏正式上线，来链得得App给这些币圈链圈最有思想的专业领袖疯狂打Call吧！