

看涨比特币的理由

Vijay Boyapati 文

本文由币信原创编译，原文链接：### <https://medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1>

本文版权归原作者所有，仅代表作者本人观点，不代表币信的观点或立场。

本文约17000字，阅读全文需约40分钟。

随着比特币价格在2017年飙升至新高，投资者看涨比特币的理由可能看起来一目了然，无需说明。另一方面，投资一种没有任何商品或政府背书的数字资产似乎又是愚蠢的，它的价格上涨促使一些人将其与郁金香狂热或互联网泡沫进行比较。以上两种说法都不对；看涨比特币的理由令人信服，但远非显而易见。投资比特币存在重大风险，但正如我所说，仍然存在巨大的机会。

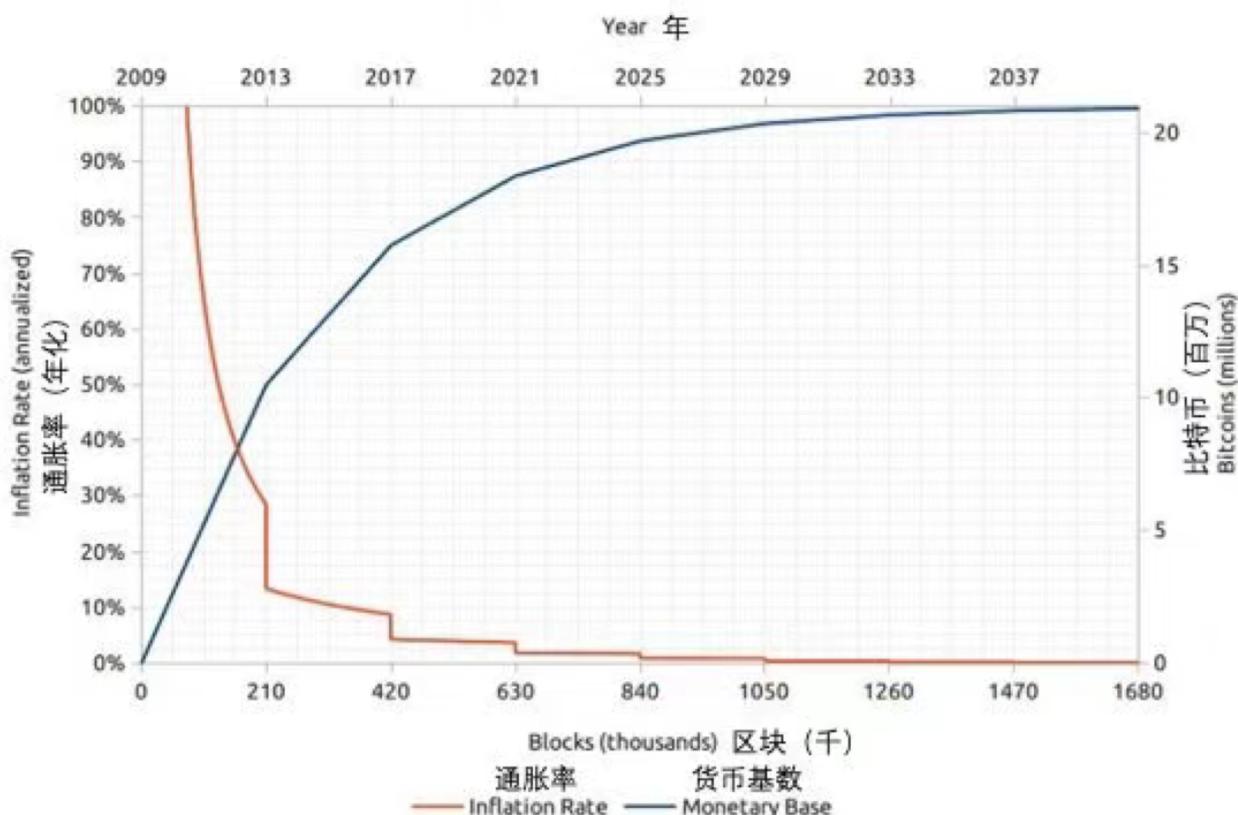
创世

世界历史上从不可能在不依赖可信中间人（如银行或政府）的情况下在两人之间远距离转移价值。2008年，身份至今无人知晓的中本聪（Satoshi Nakamoto）发表了一篇9页长的方案，一举解决了计算机科学领域内长期存在的拜占庭将军问题。中本聪的解决方案和他所构建的系统——比特币，让人们有史以来第一次可以以一种完全无需信任的方式远距离快速转移价值。比特币的创造对经济学和计算机科学都有着深刻的影响，因此中本聪应该是第一个有资格同时获得诺贝尔经济学奖和图灵奖的人。

对投资者而言，比特币系统发明的一大突出事实，是它创造了一种全新的稀缺数字商品——比特币。比特币是可转让的数字代币，在比特币网络上创建它的过程被称为“挖矿”。比特币挖矿大致类似于黄金开采，只是其生产遵循着一个设计好的、可预测的时间表。根据设计，只有2100万比特币等待开采，其中大部分都已经被挖出来了——在撰写本文时（注：本文发表于2018年3月2日），已开采出约1680万比特币。每隔四年，挖矿所生产的比特币数量将减半，新比特币的生产将在2140年完全结束。

Bitcoin Inflation vs. Time

比特币通货膨胀对时间



比特币没有任何实体商品背书，也不受任何政府或公司担保，这为新的比特币投资者提出了一个明显的问题：比特币为什么有价值？与股票、债券、房地产、甚至石油和小麦等商品不同，比特币不能通过标准贴现现金流量分析，也不能通过用于生产高阶商品的需求来估价。比特币属于完全不同的商品范畴，被称为货币品（monetary goods），其价值由博弈论设定，即每个市场参与者对商品的估值基于他们对其他参与者如何对其估值的评估。要理解货币品的博弈论本质，我们需要探索货币的起源。

货币的起源

在最早的人类社会中，人与人之间的贸易是通过易货贸易来进行的。易货贸易所固有的令人难以置信的低效率，极大地限制了贸易可能发生的规模和地理范围。易货贸易为基础的贸易有一个主要缺点，即需求问题的双重巧合。例如，苹果农可能希望与渔民进行贸易，但如果渔民在同一时刻不想要苹果，交易就会无法发生。随着时间的推移，人们开始渴望拥有某些收藏品，因为它们具有稀有性和象征性价值（例如贝壳、动物牙齿和燧石）。事实上，正如尼克·萨博（Nick Szabo）在他精彩的《关于货币起源的论文###》中所说的那样，人类对收藏品的渴望为早期人类超过其最接近的生物竞争对手，即尼安德

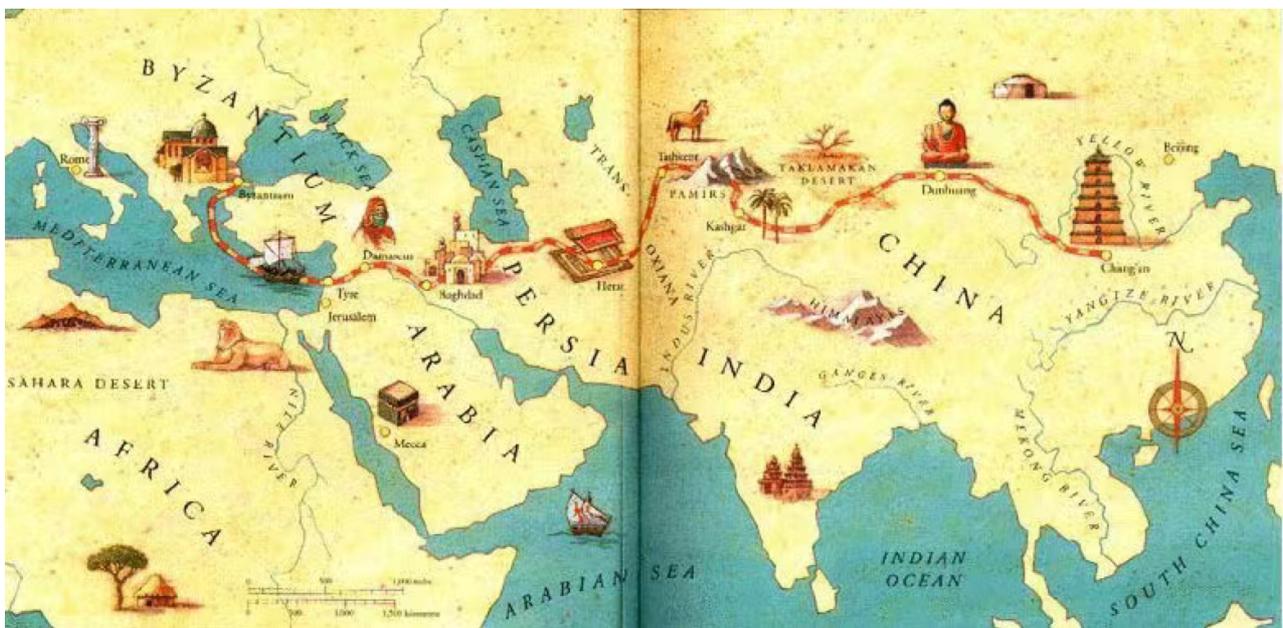
特人，提供了一种独特的进化优势。

收藏品的主要和最终进化功能是作为一种储存和转移财富的媒介。

通过在其他敌对部落之间进行贸易，并允许财富在世代之间转移，收藏品可以作为一种“原始货币”。在旧石器时代的社会中，收藏品的交易和转让很少见，这些商品更像是一种“价值储存”而不是我们对现代货币所认知的“交易媒介”的角色。萨博解释说：

与现代货币相比，原始货币的流度非常低——在一般人的一生中，它可能只会被转移几次。尽管如此，耐用的收藏品，今天我们称之为传家宝，可以持续很多代，并在每次转让时增加实质价值——经常使转移成为可能。

在决定收集或创造哪些收藏品时，早期人类会遇到一个重要的博弈论困境：其他人会想要哪些物品？通过正确地预测人们会需要哪些物品的可收藏价值，持有者就可以完成交易并获取财富，得到巨大的利益。一些美洲原住民部落，如纳拉甘西特族（Narragansetts），专门制造并无他用的收藏品，仅仅是因为它们它们在贸易中的价值。值得注意的是，对未来对可收藏品需求的预期越早，赋予其拥有者的优势就越大；它可以比被广泛需求时更便宜地获得，并且，随着需求扩大的人口增长，其贸易价值会升值。此外，希望一件商品成为未来的价值储存而获得它，因此加速了它的采用。这种循环实际上是一个反馈环路，它促使社会迅速凝聚到一个单一的价值储存中。在博弈论术语中，这被称为“纳什均衡”（Nash Equilibrium）。实现价值储存的纳什均衡是任何社会的一大福音，因为它极大地促进了贸易和劳动分工，为文明的出现铺平了道路。



几千年来，随着人类社会的发展和贸易路线的发展，各个社会中出现的价值储存开始相互竞争。商人和交易者将面临选择，是将他们的交易收益存储在他们自己社会的价值储存里，还是存储在和他们交易的社会的价值储存里，或在两者中取得平衡。保持存储在外国价值储存的好处，是增强了在相关外国社会中完成贸易的能力。存储在外国价值储存的商

人也有动力鼓励在自己的社会中采用它，因为这会增加他们储蓄的购买力。进口外国价值储存的好处不仅在于进口商人身上，也体现在社会本身。两个社会聚集在一种单一的价值储存中，彼此完成贸易的成本会大幅下降，随之而来的是以贸易为基础的财富增长。事实上，19世纪是世界大部分地区第一次聚集于单一价值储存——黄金——这一时期是世界历史上最大的贸易爆炸。在这个宁静时期，凯恩斯勋爵写道：

那个时代是人类经济进步中一个多么非同寻常的章节啊.....任何有能力或有些特点的人都能超过平均水平，进入中层和上层阶级；那个时代以低成本和最少的麻烦为他们的生活提供便利、舒适和愉快，这甚至超越了其他时代最富有、最强大的君主的水平。伦敦的居民可以一边在床上啜饮他的早茶，一边通过电话订购他认为数量合适的全球各种产品，并合理地期望它们被早早地送到他的家门口。

好的价值储存的属性

当价值储存相互竞争时，一种好的价值储存所具有的特定属性让某种价值储存在边际上脱颖而出，并随着时间的推移增加对它的需求。虽然许多商品被用作价值储存或“原始货币”，但出现了某些特别需要的属性，具有这些属性的物品将胜过其他物品。理想的价值储存将是：

- 耐用的：该物品不能轻易腐烂或容易被破坏。因此小麦不是理想的价值储存。
- 便携的：该物品必须易于运输和储存，从而可以防止丢失或被盗，并使其便于长途贸易。因此，一头牛不如一个金手镯理想。
- 可互换的：任何一件该物品，应该可以与另一件等量的物品互换。离开可互换性，需求的巧合问题仍然没有解决。因此，黄金比钻石更好，钻石的形状和质量都不规则。
- 可验证的：该物品必须易于快速识别和验证为真的。简单的验证增加了其接收者对交易的信心，并增加了交易完成的可能性。
- 可分割的：该物品必须易于细分。虽然这种属性在贸易不频繁的早期社会中并不那么重要，但随着贸易的蓬勃发展和交换的数量变得越来越小，越来越精确，这一点变得越来越重要。
- 稀缺的：正如尼克·萨博所说，货币品必须具有“不可伪造的成本”。换句话说，商品的数量不得丰富或容易大量获取或生产。稀缺可能是一种价值储存的最重要属性，因为它正好利用了人类渴望收集稀有物品的天性。它是价值储存的原始价值来源。
- 历史悠久的：该物品被社会认为有价值的时间越长，其作为价值储存的吸引力就越大。一个历史悠久的价值储存将难以被新贵所取代，除非通过征服的力量，或者如果该新贵在上述其他属性中具有显著优势。
- 抗审查的：抗审查是一种新的属性，它在我们监视无处不在的现代数字化社会中变得

越来越重要。也就是说，对于诸如公司或国家这样的外部方来说，阻止物品的所有者保留和使用它有多么困难。一些人所处的政权试图实施资本管制或禁止各种形式的和平贸易，对于这些人来说，具有审查能力的物品是理想的选择。### *

下表根据上面列出的属性对比特币、黄金和法币（如美元）进行评级，然后对每个等级进行逐一解释：

	Bitcoin 比特币	Gold 黄金	Fiat 法币
Durable 耐用	B	A+	C
Portable 便携	A+	D	B
Fungible 可互换	B	A	B
Verifiable 可验证	A+	B	B
Divisible 可分割	A+	C	B
Scarce 稀缺	A+	A	F
Established History 历史悠久	D	A+	C
Censorship Resistant 抗审查	A	C	D

耐用性：

黄金是无可争议的耐用之王。绝大多数曾经被开采或铸造的黄金，包括法老们的黄金，今天仍然存在，并且很可能在一千年后可用。在古代用作货币的金币今天仍然保持着重要的价值。法币和比特币基本上是数字记录，可能采取物理形式（如纸币）。因此，不应考虑其耐久性的物理表现（因为破旧的美元钞票可以换成新的钞票），而是发行它们的机构的耐久性。在法币的情况下，许多政府已经过去几个世纪，它们的货币随之消失。魏玛共和国的纸马克、租马克和帝国马克都不再具有价值，因为发行它们的机构已不复存在。如果遵循历史的指引，认为法币从长期来看具有持久性就是愚蠢的——在这方面，美元和英镑相对异常。没有发行机构的比特币可以被认为是持久的，只要保护它们的网络仍然存在。鉴于比特币仍处于起步阶段，现在就其耐久性得出强有力的结论还为时过早。然而，有令人鼓舞的迹象表明，尽管各国一直试图监管比特币，多年来黑客也一直在攻击它，网络仍在继续发挥作用，显示出极高程度的“反脆弱性”。

便携性：

比特币是人类有史以来最便携的价值储存。代表数亿美元的私钥可以存储在一个小巧的U盘里，轻松携带到任何地方。此外，同样价值的金额可以即时地在地球两端的人们之间传输。法币基本上是数字化的，也非常便携。但是，政府监管和资本管制意味着大量的价值转移通常要耗时数天，甚至根本不可能。现金可以用来避免资本管制，但随后的存储风险和运输成本变得很大。实物黄金的密度极大，是迄今为止最不便携的。毫无疑问，大多数金条从未被运输过。当金条在买方和卖方之间转移时，通常只转移黄金的所有权，而不是实物金条本身。远距离运输实物黄金是昂贵、危险和耗时的。

可互换性：

黄金提供了可互换性的标准。当熔化时，一盎司黄金与另一盎司基本上无法区分，黄金一直以这种方式在市场上交易。另一方面，法币只有发行机构允许的货币才具有可互换性。虽然接受法定钞票的商人通常对待每张钞票都是一样的，但有些情况下大面额钞票的处理方式与小钞票不同。例如，印度政府试图摧毁印度的未征税灰色市场时，将其500卢比和1000卢比的钞票完全非货币化。这种非货币化使500卢比和1000卢比的票据以低于其面值的价格进行交易，这使得它们不再真正与其较低面额的票据具备可互换性。比特币在网络层面是可互换的，这意味着每个比特币在传输时在比特币网络上都是相同的。但是，由于比特币在区块链上是可追溯的，因此特定比特币可能因其在非法贸易中的使用而受到污染，商家或交易所可能被迫不接受这种受污染的比特币。如果不改善比特币的网络协议的隐私性和匿名性，就不能认为比特币是像黄金一样可互换的。

可验证性：

大致来说，验证法币和黄金的真实性都相对容易。然而，尽管在他们的钞票上提供了防止伪造的功能，各个国家及其公民仍然面临被伪钞欺骗的可能性。黄金也不能免于被伪造。老练的罪犯用镀金钨来欺骗黄金投资者购买假黄金。另一方面，比特币可以用数学确定性来验证。使用加密签名，比特币的所有者可以公开证明他拥有他所说的比特币。

可分割性：

比特币可以被分割为一个比特币的亿分之一，并以这种微小的数量传输（但网络费用会使小额传输变得不经济）。法币通常可以分割成口袋里几乎没有购买力的零钱，这使法币在实践中足够可分。黄金虽然在物理上可分割，但在分成足够小、对于低价值的日常交易可用的数量时变得难以使用。

稀缺性：

最明确区分比特币与法币和黄金的属性是其预定的稀缺性。按照设计，最多可以创建2100万比特币。这使得比特币的所有者知道他们占可能总供应量的百分比。例如，持有有10个比特币的人会知道，地球上最多210万人（不到世界人口的0.03%）可能拥有与他们一样多的比特币。黄金虽然历史上仍然非常稀缺，但并不能免受供应增加的影响。如果采用新的采矿或获取黄金的方法变得经济，黄金的供应可能会急剧上升（如海底或小行星采矿）。最后，法币虽然只是历史上相对较新的发明，但已证明其供应量在不断增加。各国表现出持续倾向于扩张其货币供应以解决短期政治问题。世界各国政府的通货膨胀倾向，使得法币持有者的储蓄的价值可能会随着时间的推移而减少。

历史悠久：

没有任何其他货币的历史像黄金一样悠久和传奇，只要人类文明存在，黄金就会一直被视为有价值的。在遥远的古代铸造铸造的硬币，在今天仍然保持重要价值。法币就并非如此了，它是历史上相对较新的反常事物。从一开始，法币就几乎普遍倾向于归零。用通货膨胀来作为对公民进行无形征税的阴险手段，一直是历史上很少有国家能够抵制的诱惑。如果法币主导全球货币秩序的20世纪确立了任何经济真理，那就是不能信任法币能在长期甚至中期维持其价值。比特币虽然存在时间短，但已经在市场上经受了足够的考验，它很可能不会很快作为有价值的资产消失。并且，林迪效应（Lindy Effect）表明，比特币保持存在的时间越长，社会对它将在未来继续存在很长一段时间的信心就越大。换句话说，社会对一种新货币品的信任在本质上是渐近的，如下图所示：



如果比特币存在了20年，那么人们就会有信心认为它会永远存在，就像人们认为互联网是现代世界的永久特征一样。

抗审查性：

比特币早期需求的最重要来源之一，是它们在非法毒品贸易中的使用。许多人后来错误地推测，对比特币的主要需求是由于他们表面上的匿名性。然而，比特币远非匿名货币；在比特币网络上传输的每笔交易都会永久记录在公共区块链上。交易的历史记录允许稍后的取证分析以识别资金流的来源。就是靠着这样的分析，著名的MtGox盗窃者被绳之以法。虽然一个足够小心和勤奋的人在使用比特币时可以隐瞒自己的身份，但这并不是比特币在毒品交易上如此受欢迎的原因。使比特币对违禁活动有价值的关键属性，是它在网络层面是“无需许可”的。当比特币在比特币网络上传输时，没有人为干预决定是否应该允许交易。作为一个分布式的点对点网络，比特币本质上是设计来抗审查的。这与法定银行系统形成鲜明对比，在法定银行系统里，国家监管的银行和其他货币转移的看门人会报告和防止货币品的非法使用。受监管货币转移的典型例子是资本管制。例如，富裕的百万富翁可能会发现，如果他们希望逃离一个压迫性的政权，就很难将他们的财富转移到新的住所。虽然黄金不是由国家发行的，但其物理性质使其难以远距离传播，使其比比特币更容易受到国家监管。印度的“黄金管制法”就是这种监管的一个例子。

比特币在上面列出的大多数属性中表现优异，使其能够在边际上超越现代和古代货币品，并为其日益普及提供强大动力。特别是，审查抵制和绝对稀缺的有效结合一直是富有投资

者将其部分财富配置给新生资产类别的强大动力。

货币的演变

现代货币经济学痴迷于货币的交换作用。在20世纪，各国垄断了货币的发行，并不断破坏其作为价值储存的用途，造成了一种错误的信念，即货币主要被定义为交换媒介。许多人批评比特币不宜用作货币，因为它的价格太不稳定而不适合作为交换媒介。然而，这是本末倒置的。货币总是分阶段演变的，而价值储存的作用要先于在交换媒介的作用。边际主义经济学的创始人之一威廉·斯坦利·杰文斯（William Stanley Jevons）解释说：

从历史上看，.....黄金似乎首先作为一种有价值的商品用于装饰目的；其次，作为储存的财富；第三，作为交换媒介；最后，作为衡量价值的尺度。

使用现代术语来说，货币的演变总是遵循以下四个阶段：

- 1 收藏。**在其演变的第一阶段，货币将完全基于其特有的属性，通常会成为拥有者的一时兴起。在后来转变为更为人所知的货币角色之前，贝壳、珠子和黄金都是收藏品。
- 2 价值储存：**一旦其特质被足够多的人需要，货币将被视为一种随着时间的推移保持和储存价值的手段。随着一种物品被广泛视为一种合适的价值储存，其购买力将随着更多人为此目的的需求而增加。一种价值储存的购买力最终会在其被广泛持有，并且希望用它来作为价值储存的新人涌入减少时达到稳定水平。
- 3 交换媒介：**当货币完全被确立为价值储存时，其购买力将稳定下来。在稳定购买力后，使用货币完成交易的机会成本将降低到适合用作交换媒介的水平。在比特币最早期，许多人并不了解使用比特币作为交换媒介而非初期价值储存的巨大机会成本。有人用10,000比特币（在撰写本文时价值约9400万美元）换两个披萨的著名故事说明了这种混淆。
- 4 记账单位。**当货币被广泛用作交换媒介时，商品将以其来定价。即，大多数商品都会有这种货币的兑换率。人们常常误以为今天许多商品都有比特币价格。例如，虽然可以使用比特币购买一杯咖啡，但所列价格并不是真正的比特币价格；而是在当前的美元/比特币市场汇率下，商家所希望的美元价格转换为比特币价格。如果比特币对美元的价格下跌，商家要求的比特币数量将相应增加。只有当商家愿意接受比特币支付而不考虑比特币对法币的汇率时，我们才能真正认为比特币已成为一种记账单位。

尚未成为记账单位的货币品可能会被视为“部分货币化”。今天，黄金充当了这样一个角色，成为一种价值储存，却被政府干预剥夺了其交换媒介和记账单位的角色。一种物品也有可能扮演货币的交换媒介角色，而另一种物品则扮演其他角色。在阿根廷或津巴布韦等国家功能失调的国家，情况通常如此。纳撒尼尔·波普尔（Nathaniel Popper）在他的《数

字黄金》（Digital Gold）一书中写道：

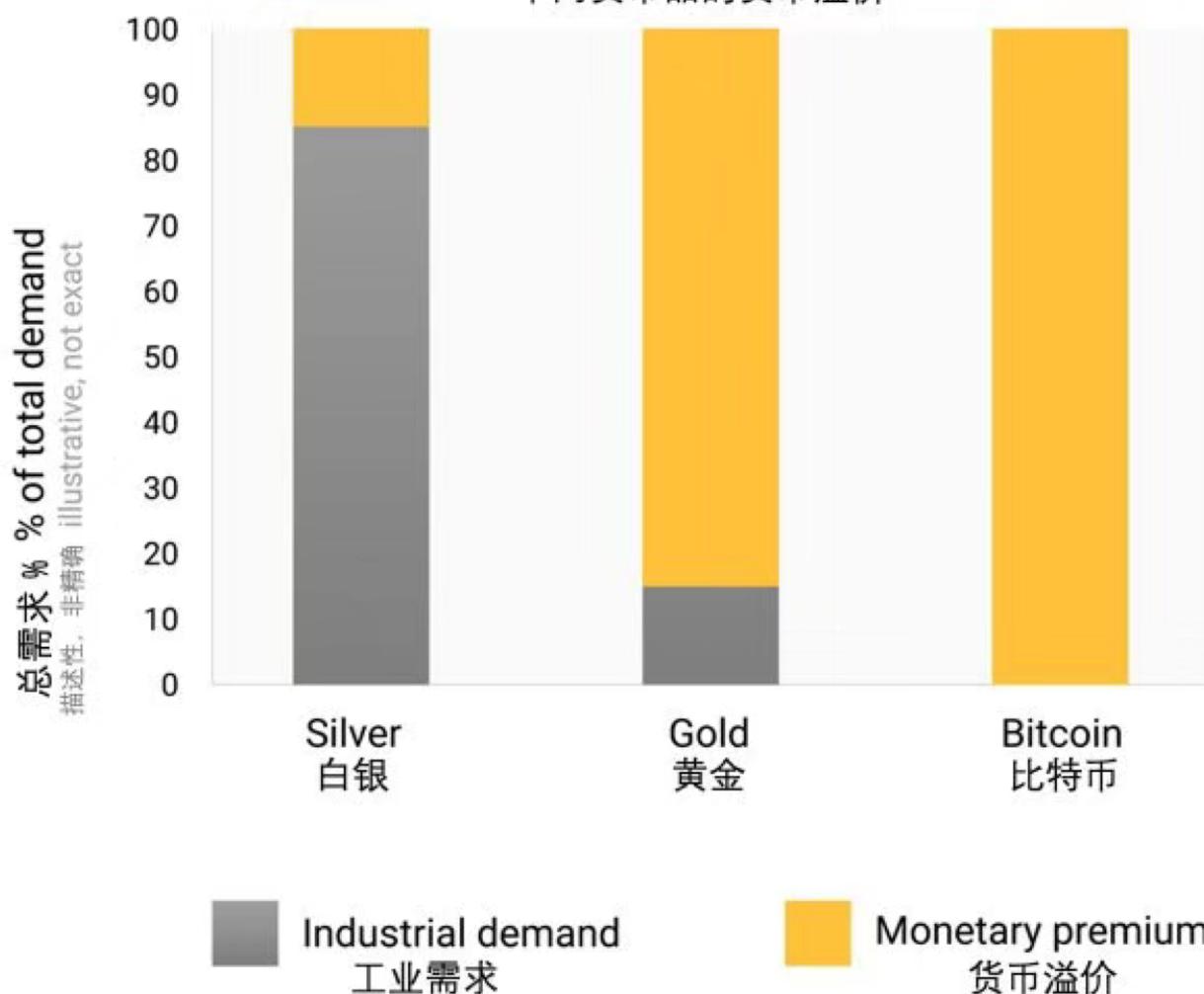
在美国，美元无缝地服务于货币的三个功能：提供交换媒介，衡量商品成本的单位，以及可以存储价值的资产。另一方面，在阿根廷，比索被用作交换媒介——用于日常购买——而没有人用它作为价值储存。用比索来储蓄相当于扔钱。所以人们把他们想要存的比索换成美元，它们的保值能力强于比索。由于比索非常不稳定，人们通常会记住以美元计的价格，它提供了一个更可靠的衡量单位。

比特币目前正在从货币化的第一阶段过渡到第二阶段。比特币从初期的价值储存转变为真正的交换媒介可能需要几年的时间，而实现这一目标所需的路径仍然充满了风险和不确定性。值得注意的是，同样的过渡黄金也需要花费几个世纪。没有人见过一种物品的实时货币化（就像比特币在发生的一样），所以对于这种货币化的道路，我们几乎没有什么经验。

路径依赖

在货币化的过程中，货币品的购买力将会飙升。许多人评论说，比特币购买力的增加造成了“泡沫”的出现。虽然这个术语通常贬低地表明比特币被严重高估，但它无疑是恰当的。所有货币品共有的一个特征是，他们的购买力高于仅凭其使用价值所证明的购买力。实际上，历史上许多货币都没有任何使用价值。货币品的购买力与其固有用途所指示的交换价值之间的差异可以被认为是“货币溢价”。随着货币品在货币化阶段的转变（在上文中列出），货币溢价将会增加。然而，溢价不是一条笔直的、可预测的线。正在货币化过程中的一种物品X可能会被另一种更适合作为货币的物品Y所击败，而X的货币溢价可能会下降或完全消失。白银的货币溢价在19世纪后期几乎完全消失，当时世界各国政府基本上放弃了它作为货币而转向黄金。

Monetary premium for different monetary goods 不同货币品的货币溢价



即使在没有诸如政府干预或其他货币品竞争等外部因素的情况下，新货币的货币溢价也不会遵循一条可预测的路径。经济学家拉里·怀特（Larry White）观察到：
当然，泡沫论的问题是，它与任何价格路径一致，因此并没有解释一条特定的价格路径。

货币化的过程是博弈论的；每个市场参与者都试图预测其他参与者的总需求，从而预测未来的货币溢价。由于货币溢价不受任何固有用途的影响，因此市场参与者在确定货币品是否便宜或昂贵以及是否购买或出售时，往往会默认过去的价格。当前需求与过去价格的联系被称为“路径依赖”，它可能是在理解货币品价格变动时，最让人困惑的地方。

当一种货币品的购买力随着采用率的增加而增加时，市场对“便宜”和“昂贵”的预期会相应发生改变。同样，当货币品的价格崩溃时，预期也会随之转变，普遍认为先前的价格是“非理性的”或过度夸大的。著名华尔街基金经理约什·布朗的这番话说明了货币的路径依赖：

我在大概2300美元购买了【比特币】，并且在我手上立即翻了一倍。然后我开始说，“我不能再买更多了”，因为它涨了，尽管这只是一个锚定的意见，除了我最初的购买价格之外毫无根据。然后，因为中国取缔交易所上周币价下跌，我开始对自

己说：“哦，好，我希望它会被杀死，这样我可以买得更多。”

事实上，“廉价”和“昂贵”的概念在货币品方面基本没有意义。货币品的价格并不反映其现金流量或其有用程度，而是衡量它能多么广泛地承担货币的各种功能。

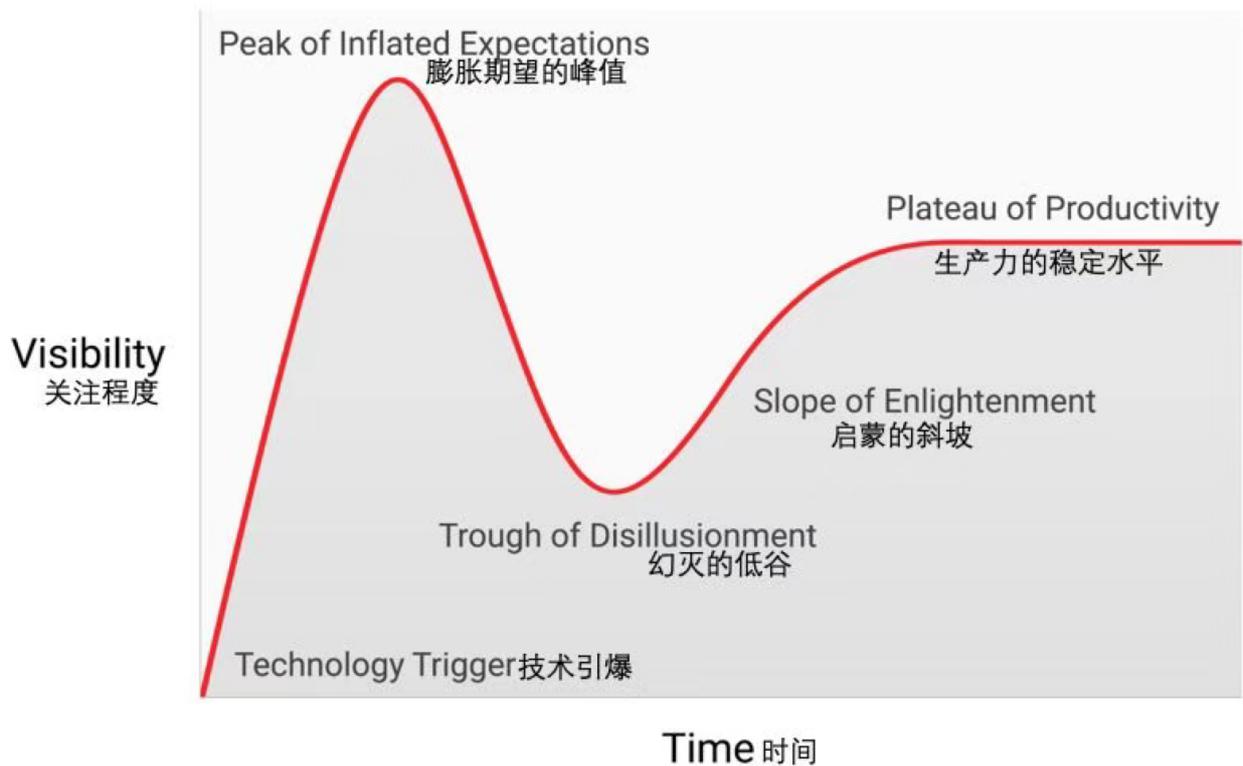
使货币的路径依赖性进一步复杂化的是，市场参与者不仅仅是冷静的观察者，一边预测货币溢价在未来的变动，一边进行买卖，他们还充当积极的布道者。由于没有客观正确的货币溢价，鼓吹货币品的优越属性比鼓吹普通物品更有效，普通物品的价值最终取决于现金流量或使用需求。我们可以在各种在线论坛中观察到比特币市场参与者的宗教热情，在这些论坛中，持币人积极地宣传比特币的好处以及通过投资可以赚取的财富。在观察比特币市场时，利·德罗根（Leigh Drogen）评论到：

你会认识到这是一种宗教——一个我们都互相告诉并同意的故事。宗教是我们应该考虑的接受曲线。它几乎是完美的——一旦有人进来，他们会告诉所有人并出去布道。接着他们的朋友进来，然后他们开始布道。

虽然跟宗教相提并论可能会给比特币带来一种非理性信仰的气质，但对于个人持有者来说，布道一种出众的货币品，以及对整个社会来说，用标准去检验它，都是完全理性的。货币是所有贸易和储蓄的基础，因此采用优质货币对社会所有成员创造财富有巨大的倍增效益。

货币化的曲线

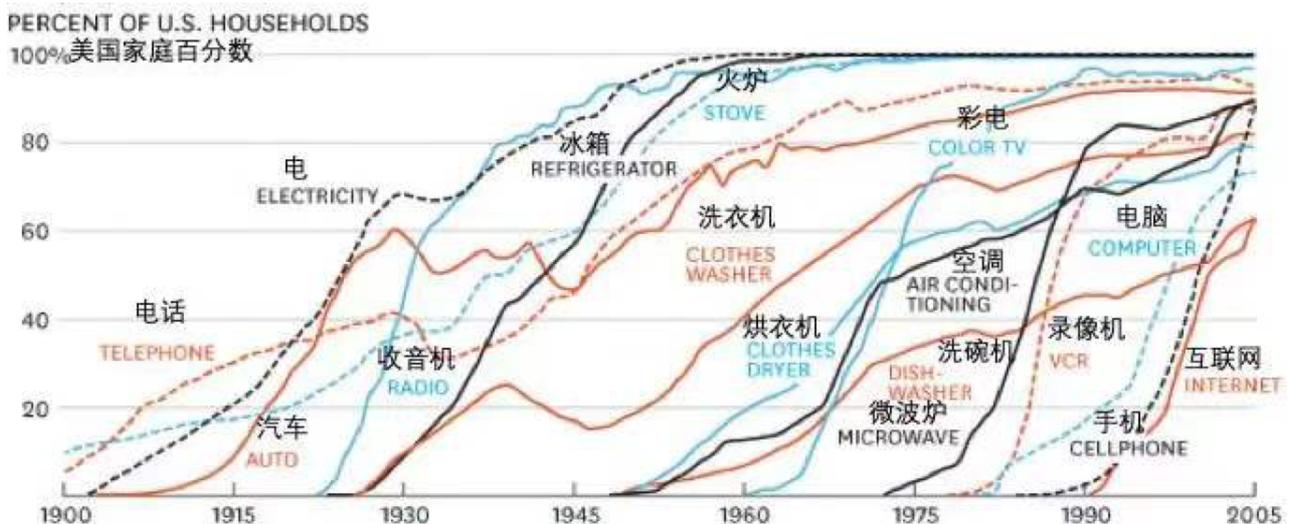
对于一种货币品在货币化过程中所采取的路径，虽然没有先验的规则，但在相对简短的比特币货币化历史中出现了一种奇怪的模式。比特币的价格似乎遵循增长量级的分形模式，其中分形的每次迭代都与加德纳炒作周期（Gartner hype cycle）的经典形状相匹配。



在其《### 推测性比特币接受/价格理论》

推测性比特币接受/价格理论

一文中，迈克尔·凯西认为，不断扩大的加德纳炒作周期代表了一条采用标准S曲线的不同阶段，许多在社会中被普遍使用的变革技术都遵循了这种曲线。



每条加德纳炒作周期都始于对新技术的热情，价格由在该次迭代中“可触及”的市场参与者提高。加德纳炒作周期中最早的买家通常对他们投资的技术变革性持强烈信念。最终市场的热情逐渐增强，因为在周期中可以达到的新参与者的供应已经耗尽，并且购买变得更受投机者的支配，投机者对快速获利比对基础技术更感兴趣。

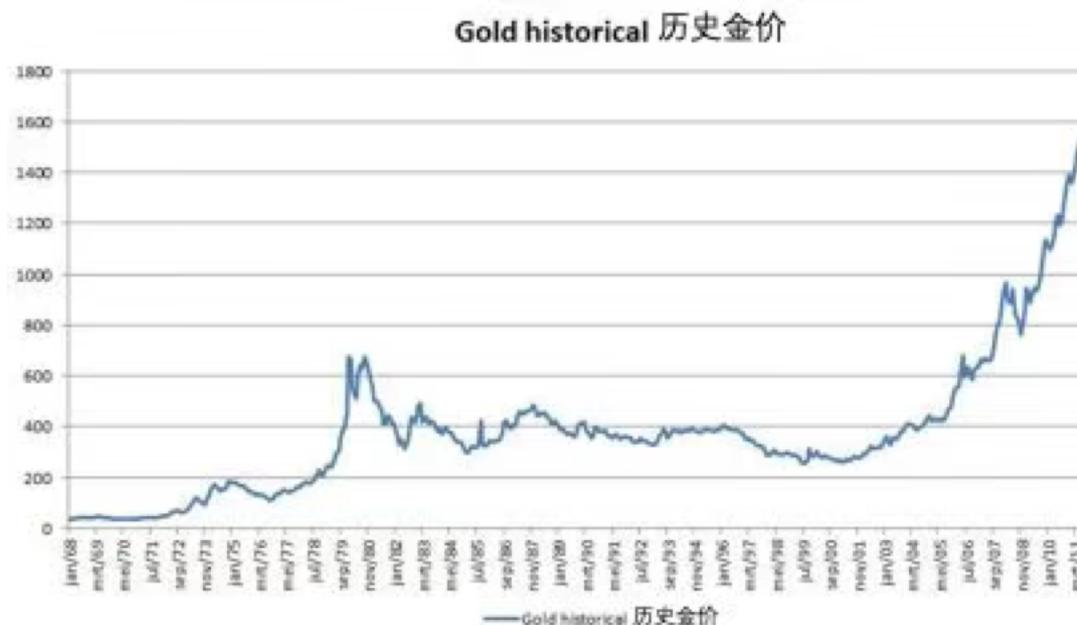
在炒作周期达到顶峰之后，价格迅速下跌，投机热情被绝望、公众嘲笑和技术根本没有变革的感觉所取代。最终价格触底并形成平台，在那里，一群能够承受崩盘之痛并欣赏

该技术重要性的新队友，加入了具有强烈信念的原始投资者。

平原会持续很长一段时间，正如凯西所说，形成了一种“稳定、无聊的低谷”。在平原期间，公众对该技术的兴趣将会减少，但它将继续发展，强大的信徒群体将会慢慢增长。接着是为炒作周期的下一次迭代奠定新的基础，因为外部观察者会认识到技术不会消失，并且投资它可能没有在周期的崩盘阶段看起来那样危险。炒作周期的下一次迭代将带来更大的接受群体，并且在量级上要大得多。

参与加德纳炒作周期迭代的人很少会正确预测该周期的价格会有多高。在周期的最初阶段，价格通常会达到对大多数投资者而言似乎荒谬的水平。当周期结束时，媒体通常会把崩盘归罪于一个热门的原因。虽然所述原因（如一个交易所破产）可能是一个引发事件，但这并不是该周期结束的根本原因。加德纳炒作周期结束是因为在这个周期中可以触及的市场参与者已经耗尽。

这说明从20世纪70年代末到21世纪初，黄金遵循加德纳炒作周期的经典模式。人们可能会推测，炒作周期是货币化过程中固有的社会动态。



加德纳群组

自2010年有了第一次交易所交易价格以来，比特币市场已经见证了四次大的加德纳炒作周期。事后来看，我们可以精确地确定，在比特币市场里先前炒作周期的价格范围。我们还可以定性地确定与先前周期的每次迭代相关联的投资者群组。

0美元-1美元（2009年 - 2011年3月）：比特币市场的第一个炒作周期由密码学家、计算机科学家和赛博朋克们主导，他们最早认识到中本聪突破性发明的重要性，并且首先确定

比特币的协议没有技术缺陷。

1美元–30美元（2009年 - 2011年7月）：第二个周期吸引了新技术的早期接受者和源源不断的意识形态投资者，他们倾倒在一种无国籍货币的潜力。像罗杰·维尔（Roger Ver）这样的自由主义者被比特币所吸引，因为如果新技术被广泛采用，反建制活动将成为可能。文斯·卡萨维斯（Wences Casares）是一位才华横溢且人脉广泛的连续创业者，他也是第二次比特币炒作周期的一员，向硅谷的一些最杰出的技术专家和投资者布道了比特币。

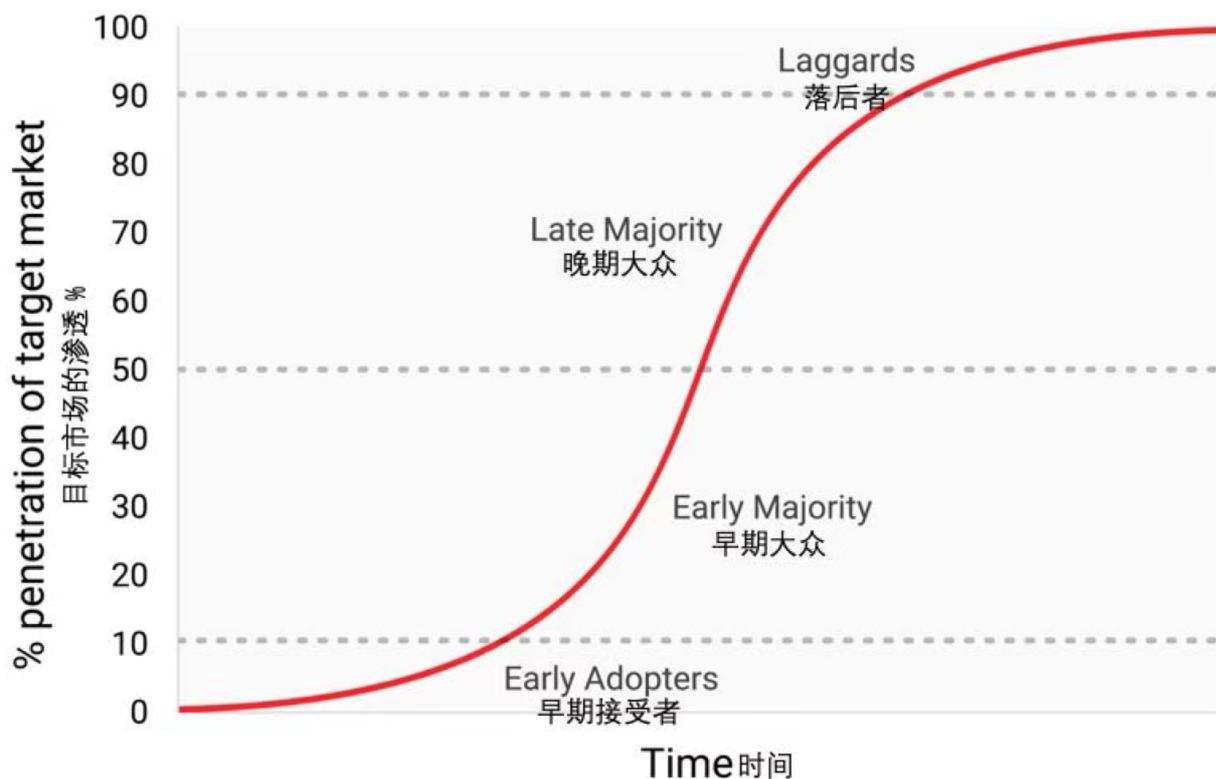
250美元–1100美元（2013年4月 - 2013年12月）：第三个炒作周期见证了早期小额和机构投资者的入场，他们勇敢地面对了极其复杂、流动性存在风险的比特币购买渠道。在此期间市场流动性的主要来源是日本的MtGox交易所，该交易所由恶名远扬、行为不检的马克·卡佩莱斯（Mark Karpeles）经营，他后来因在交易所破产中扮演的角色而在监狱中度过了一段时间。

值得注意的是，在上述几个炒作周期中，比特币价格的上涨主要与流动性的增加和投资者购买比特币的难易程度相关。在第一个炒作周期中，没有可用的交易所，获得比特币主要是靠挖矿或与已经挖到比特币的人直接交换。在第二个炒作周期中，基本的交易所变得可用，但从这些交易所获得和存放比特币对于除技术最精通的投资者之外的所有人来说仍然过于复杂。即使在第三个炒作周期中，对投资者来说，将资金转移到MtGox以获取比特币仍然存在着重大障碍。银行不愿意与交易所打交道，而促进转账的第三方供应商往往不称职，或者不道德，或者两者兼有。此外，许多确实设法将资金转移到MtGox的人，最终在交易所遭到黑客攻击并随后被关闭时面临了资金损失。

只有在MtGox交易所倒闭，比特币市场价格经过了两年平静之后，才形成了成熟而有深度的流动性来源，例如GDAX这种受监管的交易所，以及坎伯兰矿业这样的场外交易商。到2016年第四次炒作周期开始时，小额投资者才能相对容易地购买和存放比特币。

1100 美元–19600美元？（2014年-？）：

在撰写本文时，比特币市场正在经历其第四个炒作周期。被迈克尔·凯西称之为“早期大众”的小额和机构投资者，主导了当前炒作周期。



随着流动性来源深度越来越大，越来越成熟，大型机构投资者现在有机会通过受监管的期货市场参与。受监管的期货市场的存在为创建比特币ETF铺平了道路，也将在随后的炒作周期中迎来“晚期大众”和“落后者”。

虽然我们不可能预测当前炒作周期的确切幅度，但可以合理推测在这个周期中，峰值将达到2万美元到5万美元之间。如果高于这个范围，比特币将占据黄金总市值的很大一部分（在编写本文时，如果比特币价格约为38万美元，黄金和比特币将达到相同的市值）。黄金市值的很大一部分来自央行的需求，央行或各国不太可能参与这个特定的炒作周期。

各国的进场

当各国开始囤积比特币来作为外汇储备的一部分时，比特币将开启最后的加德纳炒作周期。比特币的市值目前太小，无法被视为大多数国家储备的可行补充。然而，随着私营部门兴趣的增加，以及比特币市值接近1万亿美元，它的流动性将变得足够大，以便大多数国家进场。第一个正式将比特币加入其储备的国家的进场，可能会引发其他国家的蜂拥而至。如果比特币最终成为全球储备货币，那么最早接受比特币的国家将会在其资产负债表上得到最大的利益。不幸的是，拥有最强行政权力的国家——像朝鲜这样的独裁政权——可能在囤比特币上速度最快。由于不愿意看到这些国家改善其财政状况，以及西方民主国家所固有的弱势行政部门，将导致它们犹豫不决并在囤比特币作为储备上落后。

讽刺的是，美国是目前对比特币监管立场最开放的国家之一，而中国和俄罗斯则是最敌对的国家。如果比特币取代美元成为世界储备货币，美国的地缘政治地位将面临最大的下行风险。在20世纪60年代，夏尔·戴高乐批评美国从1944年布雷顿森林协议所制定的国际货币秩序中获得了“过高的特权”。俄罗斯和中国政府尚未意识到比特币作为储备货币的地缘战略利益，目前正专注于其对内部市场可能产生的影响。20世纪60年代的戴高乐为了回应美国过高的特权，威胁要重建古典金本位，和他一样，中国和俄罗斯将适时看到把一大部分储备放在一种非主权价值储存里的好处。由于比特币算力大量集中在中国，中国在其储备里增加比特币的潜力已经具有明显的优势。

美国以自己是一个创新国家而自豪，硅谷是美国经济皇冠上的明珠。迄今为止，硅谷在很大程度上主导了监管机构应该就比特币采取什么样的立场。然而，银行业和美联储终于初步了解到，如果比特币成为全球储备货币，它会对美国货币政策构成生存威胁。以美联储传声筒著称的《华尔街日报》发表了一篇关于比特币对美国货币政策构成威胁的评论：
还有另一个危险，从央行和监管机构的角度来看可能更为严重：比特币可能不会崩溃。如果对加密货币的投机热情仅仅是它被广泛用作美元替代品的前兆，那么它将威胁央行对货币的垄断。

在未来几年，硅谷的企业家和创新者（他们将试图保持比特币不受国家控制）与银行业和央行（他们将竭尽全力监管比特币以防止他们的行业和发钞权力被破坏）之间将会有一场激烈的斗争。

过渡到交换媒介

货币品在被广泛认为有价值之前不能过渡为一种被普遍接受的交换媒介（“货币”的标准经济定义），换言之，不被认为有价值的商品不会在交易中被接受。在被广泛认为有价值——并因此被当做一种价值储存——的过程中，货币品的购买力将会飙升，从而产生放弃其在交换中使用的机会成本。只有当放弃一种价值储存的机会成本降到适当的低水平时，它才能转变为普遍接受的交换媒介。

更准确地说，当机会成本和交换中使用它的交易成本之和，低于不靠它完成一笔交易的成本时，一种货币品才适合作为交换媒介。

在一个基于易货交易的社会中，即使货币品的购买力在增加，也可能发生从价值储存向交换媒介的转变，因为易货交易的交易成本非常高。在交易成本较低的发达经济体中，尽管在非常有限的范围内，也有可能将像比特币这样的新生且快速升值的价值储存用作交换媒介。一个例子是非法药物市场，买家愿意牺牲持有比特币的机会，以尽量减少使用法币购买药物的巨大风险。

然而，在发达社会中，一种新兴的价值储存要成为被普遍接受的交换媒介，还有很大的制度障碍。各国通常会利用税收的有力手段，来保护其主权货币免受竞争货币的冲击。主权

货币不仅享有持续需求来源的优势，而且只能用它来支付税收，但竞争货币品只要在交易时升值了就会被征税。后一种税收对使用一种价值储存来作为交换媒介造成了巨大的摩擦。

然而，基于市场的货币品的劣势，并不是将其用作被普遍接受的交换媒介的不可逾越的障碍。如果人们对一种主权货币丧失信心，其价值就会在被称为恶性通胀的过程中崩溃。当一种主权货币出现恶性通胀，它对社会中流动性最大的商品（如黄金或美元等外币，如果有的话）的价值首先会崩溃。如果没有流动性商品或其供应有限，恶性通胀的货币就对实物（房地产和商品等）崩溃。恶性通货膨胀的典型形象是一家空无一物的杂货店，因为消费者逃离了他们飞速贬值的国家货币。



最终，当信心在恶性通胀期间完全丧失时，任何人都不再接受主权货币，社会将转向易货交易，或者货币单位将被完全取代为一种交换媒介。这一过程的一个例子是用美元取代津巴布韦元。由于外国货币的稀缺，以及缺乏外国银行机构来提供流动性，用外国货币来置换主权货币变得更加困难。

由于比特币能轻松地跨境传输，并且不需要银行系统，对饱受恶性通胀之苦的人来说，比特币成为了一种理想的货币品。在未来几年，随着法币继续遵循其历史趋势走向归零，比特币将成为全球储蓄逃往的一个越来越受欢迎的选择。当一个国家的货币被抛弃并被比特币取代时，比特币将从该社会的价值储存转变为普遍接受的交换媒介。丹尼尔·克拉维茨

(Daniel Krawisz) 创造了“超级比特币化 (hyperbitcoinization###)
”这个术语来描述这个过程。

常见误解

本文的大部分内容都集中于比特币的货币性质。有了这一基础，我们现在可以提出一些关于比特币最常见的错误观念。



比特币是一个泡沫

和所有基于市场的货币品一样，比特币也有一个货币溢价。该货币溢价引起了普遍的批评，即比特币是一个“泡沫”。然而，所有货币品都会有一个货币溢价。实际上，这种溢价（超出使用-需求价格的部分）正是所有货币的决定性特征。换句话说，不论何时何地，货币总是一个泡沫。矛盾的是，一种货币品既是泡沫，也可能被低估——如果它处于其被接受为货币的早期阶段。

比特币太不稳定了

比特币的价格波动是其新兴的功能。在刚开始的几年里，比特币表现得像低价股，任何大买家——比如温克莱沃斯兄弟——都可能引起价格暴涨。随着多年来接受度和流动性的增加，比特币的波动性相应减少。当比特币的市值超过黄金的时候，它将呈现出类似的波动水平。由于比特币超过了黄金的市值，其波动性将降低到适合作为广泛使用的交易媒介的水平。如前所述，比特币的货币化发生在一系列加德纳炒作周期中。在炒作周期的稳定期，波动率最低，而在周期的峰值和崩盘期，波动率最高。每个炒作周期的波动性都比之前的低，因为市场的流动性增加了。

交易费太高

最近对比特币网络的批评是，传输比特币的费用增加使其不适合作为支付系统。然而，费用的增长是健康和符合预期的。交易费是支付给比特币矿工通过验证交易来保护网络所需的成本。矿工可以通过交易费或块奖励（这是一种由当前比特币所有者承担的通胀补贴）来支付。

鉴于比特币有着固定的供应计划——这种货币政策使其非常适合作为价值储存——区块奖励最终将降至零，网络最终必须由交易费来保障。一个“低”费用的网络是一种安全性很低且易于外部审查的网络。那些吹捧比特币替代品费用低的人，在不知不觉中说出了这些所谓“山寨币”的弱点。

对比特币“高”交易费的批评，有着一个似是而非的根源，即相信比特币应该首先成为支付系统，然后才能成为价值储存。正如我们从货币的起源看到的那样，这种信念本末倒置了。只有当比特币成为一种完善健全的价值储存时，它才会成为一种交换媒介。此外，一旦交易比特币的机会成本达到适合作为交换媒介的水平，大多数交易将不会发生在比特币网络本身，而是发生在费用低得多的“第二层”网络上。第二层网络，例如闪电网络

（Lightning Network），相当于19世纪转移黄金所有权的本票。银行使用本票，因为转移底层金条的成本远远高于转移代表黄金所有权的票据。然而，与本票不同，闪电网络将允许以低成本转移比特币，同时很少或不需要银行等第三方的信任。闪电网络的开发是比特币历史上一项非常重要的技术创新，其价值将在未来几年得到发展和采用。

竞争

作为一种开源软件协议，人们总是可以复制比特币的软件并模仿其网络。多年来，已经诞生了许多模仿者，从模仿复制的莱特币，到像以太坊这样的复杂变体，它承诺允许使用分布式计算系统来执行任意复杂的合约安排。一个对比特币的常见投资批评是，既然我们能够轻松创造出竞争者，并吸收最新创新和软件功能，比特币无法保持其价值。



这一论点的谬论是，多年来创造出的大量比特币竞争者缺乏该领域首个和主导技术的“网络效应”。网络效应——使用比特币的价值不断增长仅仅因为它已经是主导网络——本身就是一种特性。对于任何具有网络效应的技术来说，网络效应就是其最重要的特性。

比特币的网络效应包括其市场的流动性、持有它的人数，以及维护和改进其软件及其品牌知名度的开发者社区。包括各国在内的大型投资者都会寻求最具流动性的市场，以便他们能够在不影响价格的情况下迅速进入和退出市场。开发人员将涌向拥有最优秀人才的优势开发社区，从而加强该社区的实力。品牌意识是自我强化的，因为自称比特币竞争者的人总是在比特币本身的背景下被提及。

挡道的分叉

一种在2017年变得流行的趋势是，不仅模仿比特币的软件，还要复制其过往交易的整个历史（被称为区块链）。将比特币的区块链复制到一个特定的点，然后分裂到一个新的网络，这个过程被称为“分叉（forking）”，通过这样，比特币的竞争者们能够解决将其代币分发给一大群用户的问题。



这种分支中最重要的一个发生在2017年8月1日，当天诞生了一个名为比特币现金（BCash）的新网络。在2017年8月1日之前持有N个比特币的人，将拥有N个比特币和N个BCash代币。BCash支持者的社区虽小却声势浩大，他们通过给自己的新网络命名，并发起运动说服比特币市场中的新手Bcash是“真正的”比特币，不知疲倦地试图把比特币的品牌认知据为己有。这些尝试在很大程度上失败了，这种失败反映在两个网络的市值上。然而，对于新投资者而言，仍然存在着一个明显的风险：某个竞争者可能会克隆比特币及其区块链并在市值上成功超越它，从而成为事实上的比特币。

从比特币和以太坊网络的主要分叉里，可以得出一条重要的规则。大多数市值将落在保留最高水平和最活跃开发者社区的网络上。虽然比特币可以被看作是一种新兴货币，但它也是一个计算机网络，建立在需要维护和改进的软件上。如果一个网络没有开发者支持或开发者经验不足，购买其代币就类似于购买没有微软最佳开发人员支持的微软Windows系统。从2017年分叉的历史可以清楚地看出，最优秀、最有经验的计算机科学家和密码学家致力于为原始比特币开发，而不是从中创造出的越来越多的模仿者。

真正的风险

尽管媒体和经济学界对比特币的常见批评是不当的，并且基于对货币的错误理解，但投资比特币的确存在着实际而值得注意的风险。在考虑对比特币进行投资之前，对于未来的比特币投资者来说，理解并权衡这些风险是明智的。

协议风险

比特币协议及其使用的加密原语可能被发现存在某个设计缺陷，或者可能随着量子计算的

发展而变得不安全。如果在协议中发现一个缺陷，或者某些新的计算方法使得破解支撑比特币的密码学成为可能，那么对比特币的信任可能会受到严重损害。在比特币发展的早期阶段，协议风险最高，即使是对经验丰富的密码学家来说，当时也不清楚中本聪实际上是否已经找到了拜占庭将军问题的解决方案。多年来，对比特币协议中存在严重缺陷的担忧已经消散，但鉴于其技术性质，协议风险将始终存在于比特币中，即使可能性很低。

交易所的关闭

比特币的设计是去中心化的，它在面对各国政府为监管或关闭它的多次尝试中，表现出了极强的韧性。然而，比特币兑法币的交易所是高度中心化的，易被监管和关闭。如果没有这些交易所，没有银行系统愿意和它们做生意，比特币的货币化过程将会严重受阻——如果不是完全停止的话。虽然比特币有其他流动性来源，如场外交易商和买卖比特币的去中心化市场（如localbitcoins.com），价格发现的关键过程发生在流动性最强的交易所，而它们都是中心化的。

司法套利会减少交易所关闭的风险。创立于中国的著名交易所币安，在中国政府叫停其在中国的业务后，转移到了日本。（注：后来又因为政策原因离开了日本。）各国政府也担心会扼杀一个可能与互联网一样具有重要意义的新兴产业，从而使其他国家获得巨大的竞争优势。

只有协调全球关闭比特币交易所，才能完全停止货币化进程。竞争已经开始，比特币的接受是如此广泛，完全关闭变得像完全关闭互联网一样在政治上不可行。然而，这种关闭的可能性仍然存在，在投资比特币时必须考虑这种风险。正如之前关于各国进场的部分所讨论的那样，各国政府终于意识到非主权、抗审查的数字货币对其货币政策的威胁。在比特币变得根深蒂固以至于对其采取的政治行动都被证明无效之前，他们是否会采取行动应对这一问题，是一个悬而未决的问题。

可互换性

比特币区块链的开放性和透明性使得各国有可能将某些比特币标记为被其在违禁活动中的使用“污染”。虽然比特币在协议层面的抗审查允许传输这些比特币，但如果出现监管禁止交易所或商家使用这种受污染比特币，它们可能变得毫无价值。比特币将失去货币品的一个关键属性：可互换性。

为了改善比特币的可互换性，需要在协议级别进行改进以改善交易的隐私性。虽然以门罗币和大零币等数字货币为先导，在这方面有了新的发展，但在比特币的效率和复杂性及其隐私之间存在着重大的技术权衡。能否把增强隐私的功能添加进比特币，而不以其他方式损害比特币作为货币的可用性，仍然是一个悬而未决的问题。

结论

比特币是一种尚在萌芽期的货币，正在从货币化的收藏阶段过渡到成为一种价值储存。作为一种非主权的货币品，在未来的某个阶段，比特币有可能成为全球货币，就像19世纪古典金本位中的黄金一样。接受比特币作为全球货币正是看涨比特币的理由，早在2010年，中本聪就在与麦克·赫恩（Mike Hearn）的电子邮件交流中阐述过：

如果你想象它被用于世界商业的一部分，而全世界只会有2100万个币，所以每个单位的价值会更高。

杰出的密码学家哈尔·芬尼（Hal Finney）是首个运行的比特币软件发布后不久，由中本聪发送的首笔比特币的接收者，他让这个理由变得更加犀利：

想像比特币成功了，并成为世界各地使用的主要支付系统。那么货币的总价值应该等于世界上所有财富的总价值。目前的全球家庭财富总额我估计在100万亿美元到300万亿美元之间。一共2000万个币，那么每个币价值约1000万美元。

即使比特币不是一种完全成熟的全球货币，只能和黄金竞争作为一种非主权的价值储存，它目前也被大幅低估了。将现存地上黄金供应（约8万亿美元）的市值映射到最大比特币供应量（2100万个），每个比特币的价值约为38万美元。正如我们在前面章节中看到的那样，对于使货币品适合作为价值储存的那些属性，除了历史悠久这一点，比特币在每种属性上都优于黄金。随着时间的推移，林迪效应持续作用，历史悠久将不再是黄金的竞争优势。因此，期望比特币在未来十年接近并可能超过黄金的市值并不是不合理的。本文的一个警告是，黄金市值的很大一部分来自中央银行将其作为价值储存。为了使比特币达到或超过黄金的市值，让各国进场将是必要的。西方民主国家是否会参与比特币的持有权尚不清楚。更有可能，也很不幸的是，蹙脚独裁政权和盗贼统治将是第一批进入比特币市场的国家。

如果没有任何国家参与比特币市场，比特币仍然存在看涨理由。作为仅用于小额和机构投资者的非主权价值储存，比特币仍处于采用曲线的早期阶段——所谓的“早期大众”现在正在进入市场，而晚期大众和落后者仍然需要几年才能进入市场。随着小额尤其是机构投资者的广泛参与，价格在10万美元到20万美元之间是有可能的。

拥有比特币是全世界人都可以参与的为数不多的非对称投注之一。就像看涨期权一样，投资者的下跌空间被限制在1倍以内，而潜在的上涨空间却是100倍或更多。比特币是第一个真正的全球性泡沫，其规模和范围取决于世界公民希望保护其储蓄免受政府经济管理不善的影响。实际上，比特币像凤凰涅槃一样从2008年全球金融灾难——一场由美联储等央行的政策所引发的灾难——的灰烬中崛起。

除了金融理由之外，比特币作为非主权价值储存的崛起将产生深远的地缘政治后果。一种

全球性、非通胀的储备货币将迫使各国将其主要的融资机制从通货膨胀转变为直接税收，这在政治上的可取性要小得多。各国的规模将缩小，以匹配过渡到税收作为其唯一——资金来源的政治痛苦。此外，全球贸易的解决方式将满足戴高乐的愿望，即任何国家都不应该拥有任何对其他国家的特权：

我们认为有必要在世界的巨大不幸之前，在无可争议的货币基础上建立国际贸易，的确如此，并且这个基础不具有任何特定国家标志。

从今50年后，那个货币基础将是比特币。