

比特币发行流通机制及其价格波动研究

唐晓瞳 上海交通大学

摘要: 2013 年底的比特币价格过山车走势及央行颁布的《关于防范比特币风险的通知》将比特币推向了风口浪尖，一时争议不断。进入 2014 年，看似趋向平稳的比特币市场又突然遭受东京比特币交易所破产的重创。作为一种虚拟货币，比特币将在多大程度上影响金融体系运转、其未来的发展空间究竟几何是一个值得深思的问题。本文主要从货币属性方面来研究比特币，分析比特币所代表的货币发行流通理念是否具有广泛推广使用的潜力和价值以及比特币的发展轨迹对于其他新兴货币设计的参考意义。首先本文系统的分析了比特币的理论基础、发行机制和流通产业链，其次，本文从发行方式、发行量、发行成本、退出机制等方面对比了比特币和其他货币，最后，本文从货币的五大职能入手分析了比特币在成为货币的道路上的前景。

关键字: 比特币 货币属性 去中心化

一、引言

米尔顿弗里德曼曾经说过，货币是一件如此严肃的事情，因此绝对不能由中央银行一手遮天。这一思想便是比特币出现的根源。手握货币发行权的政府无论是出于对铸币税的追求或者是迫于经济压力不得以超发货币的行为都会导致法定货币的贬值，手握大量存款及现金的民众因此而蒙受损失。因此，出于对于政府维持币值稳定的能力和意愿的不信任，货币“去中心化”（即在货币发行机制中不设置具有货币发行权的组织或个人）的讨论甚嚣尘上。2009 年初，网络神秘人物“中本聪”的一篇名为《比特币：一种点对点的电子现金系统》的论文将这一构想变为现实，同年 1 月 3 日，中本聪在位于芬兰的一个小型服务器上挖出了第一批 50 个比特币，正式宣告“去中心化”货币从理论讨论走入现实。比特币受到学界关注的主要原因并非其“电子货币”的属性，而在于它是“去中心化”货币的先驱。

随着比特币影响力的逐渐增强，这一新兴货币也成功吸引了各国政府的关注，而政府的政策导向也直接影响到了比特币的价格走势。

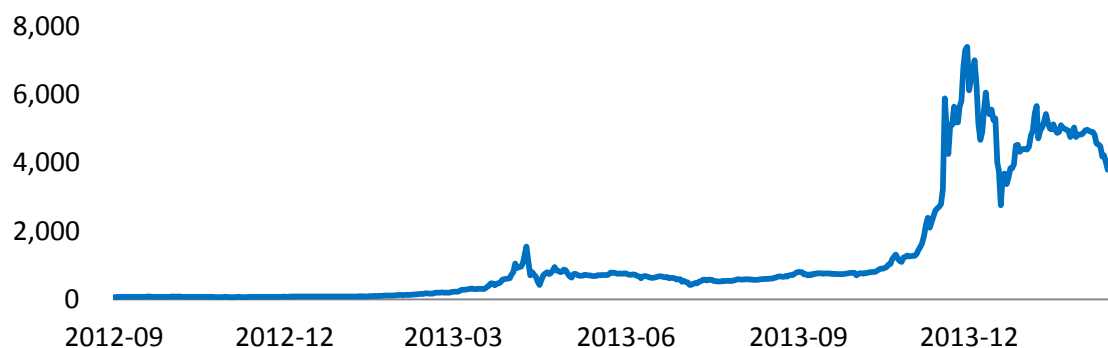


图 1：比特币价格走势受政策影响图/RMB

自 2009 年比特币出现至 2012 年底，比特币价格一直在 10 美元左右震荡。比特币第一次价格大幅上涨始于 2012 年 12 月法国比特币中央交易所的诞生，这是世界首家受到官方认

可的比特币交易所,使得比特币不再仅仅局限于小范围的交易支付,而获得了成为金融产品的必要条件。美国《虚拟货币个人管理条例》的颁布又为这一波涨势推波助澜,该条例承认了比特币作为虚拟货币的地位。在美国和法国政府的共同推动下,比特币的价格在5个月内大涨2300%。与美法德等政府的支持态度不同,中国和泰国政府则对比特币表现出了强硬的态度,泰国中央银行在2013年7月发文禁止了比特币的流通交易,并且暂停了当地企业的比特币结算业务。中国央行于2013年12月颁布的《关于防范比特币风险的通知》更是直接终结了比特币2013年四季度的大涨行情,央行在《通知》中明确了比特币的性质,认为比特币不是由货币当局发行,不具有法偿性与强制性等货币属性,并不是真正意义的货币。各国政府关于比特币的不同态度究其根源在于对比特币未来发展和对国家金融体系的影响有不同的考量,因此,作为一种虚拟货币,比特币究竟是否是一种真正意义的货币,将在多大程度上影响金融体系运转、未来的发展空间究竟几何是一个值得深思的问题。

随着比特币在一些国家受到限制,一批与比特币类似的虚拟货币如雨后春笋般出现,如莱特币、泽塔币、便士币等等,这些货币都具有“去中心化”的特点,仅在产生软件和发行量等方面有些许差别。Litecoin 莱特币放松了对计算机计算能力的要求,使得玩家可以通过普通电脑参与; namecoin 在比特币的匿名性上更进一步,直接给玩家分配域名服务器地址,由此脱离 ICANN 的管制; primecoin 也是一种对比特币产生算法进行改进的去中心化虚拟货币。比特币不是虚拟货币的先驱,在比特币之前 Q 币等就已经成长为成熟的虚拟货币,然而,比特币确是虚拟货币跨时代的里程碑,标志着虚拟货币不再仅仅是真实货币的附属,而成为具有创新的发行方式的独立货币。探究比特币所代表的货币发行流通理念是否具有广泛推广使用的潜力及价值对于把握诸多新兴货币的未来走向有至关重要的作用。

二、比特币的经济学分析

2.1 比特币的发行流通机制

2.1.1 比特币的理论基础

比特币的设计理念最早可以追溯到诺贝尔经济学奖得主哈耶克的“货币非国家化”理论。哈耶克认为自由竞争可以使得一般商品、服务市场达到帕累托最优,那么也应该尝试在货币领域引入自由竞争。因此哈耶克建议废除中央银行制度,通过允许私人发行货币来将自由竞争引入货币市场。这样可以打破政府对于货币发行权的垄断,发行“币值稳定”和“能够有效维护市场经济稳定”的“最好的货币”。在此基础上,另一位诺贝尔经济学奖得主米尔顿·弗里德曼提出使用计算机技术建立比国家信用更为可靠的货币体系。计算机技术的进步和互联网应用的普及使得上述构想有了成为现实的条件,“非国家化”即“去中心化”的货币所需要的技术已经成熟,因此,完整的理论框架与先进的计算机技术相结合孕育出了一种全新的货币形式——比特币。

2009年问世的比特币与传统货币最大的不同之处在于其运行机制不依赖于任何政府、组织或个人的信用支持或担保。比特币的发行实质上是一种对等网络中种子文件所达成的网络协议,这一设计确保了比特币的发行量不受任何人的操纵,以此来规避人为的通货膨胀的产生。同时,比特币在设计之初还设置了供应量上限的限制,在比特币的发行总量达到2100万个时比特币将关闭发行系统,以此来控制通货膨胀风险。比特币的上述设计是对于哈耶克“货币非国家化”理论的一种实践和拓展,将不易实现的“货币私人发行”通过计算机技术转化为货币的“去中心化”发行。

2.1.2 比特币的发行机制

比特币的产生是通过“挖矿”的行为来实现的,这一过程的最主要特点就是存在真实的发

行成本,该成本包括购买“矿机”的成本或者占用的个人数据终端的运算能力所产生的机会成本。“挖矿”活动的过程如下:在每个节点,比特币的挖掘者们将收集所有的还没有得到证实的交易,并通过矿机移动到一个数据块,将此数据块和之前产生的数据块整合。矿工节点被附加了一个随机调整,前面的数据块的 SHA-256 哈希值将由此计算得出。采矿节点不断地尝试来调整计算值,直到找到使哈希值低于某个目标所需要的一个随机数。因为散列操作是不可逆的调整,因此满足该随机数的要求是非常困难的,需要反复的试验过程,用总数估计来替代目标变量。在这个时候,工作量证明机制将发挥作用。当一个节点结果符合要求,它们可以传播到整个网络中寻找自己的解决方案。其他节点可以接收这个新的解决方案计算出来的数据块,并验证其是否符合规则。如果通过计算所得出的散列值中的其他节点都不符合要求(即比特币需要计算的目标),则该节点的数据块是唯一有效的,其它节点将接受该数据块和附加到其上散列链。完成这一过程的矿工将获得相应的比特币^[8]。

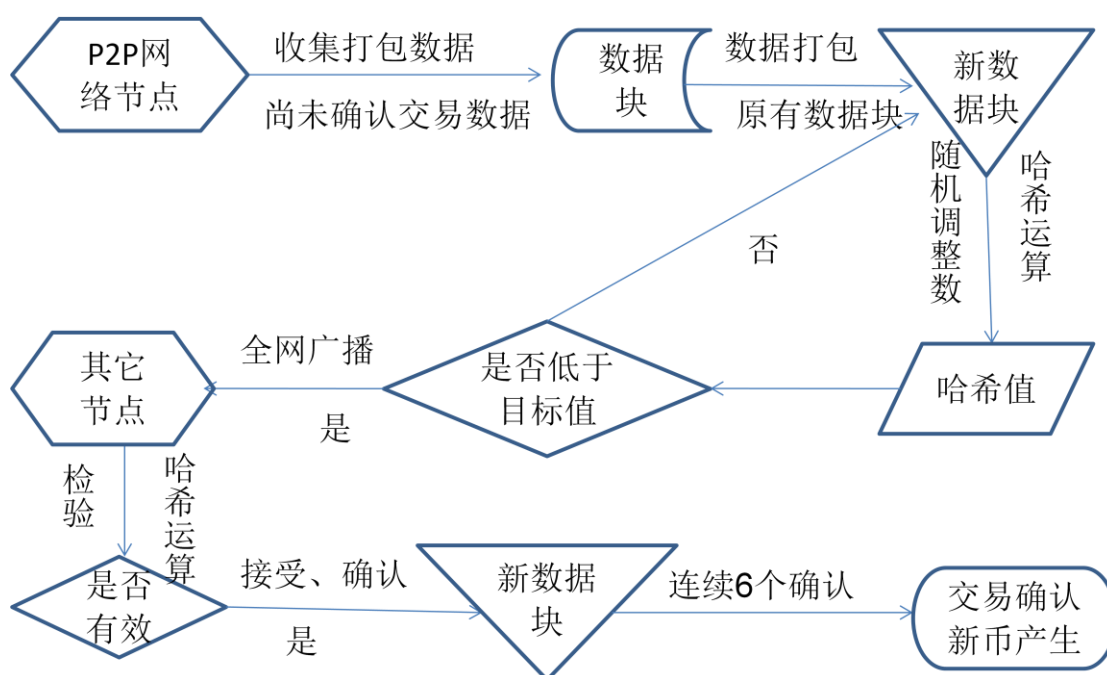


图 2 比特币产生原理

比特币的运行系统整体上限问题设置如下:首先,一个内置的反馈系统,在系统内使得区块解析速度符合参与比特币采矿变化矿工人数的速度变化,参与制作的人数越多比特币解析速度越慢,比特币系统中的当前水平使平均每十分钟确认一个区块。比特币系统是将整个分布式网络分析作为一个整体,根据 2016 年之前的区块的生产时间而进行分析的。因此制造时间取决于整个网络的某些时期到与平均计算功率生产工作的难度。单个人的问题是建立在整个网络的计算能力和计算能力超过了全面的比较新区块的可能性之上的。

货币乘以每个区块的比特币的数量的总数是现有货币的总比特币数。每个区块产生比特币的数量是随着区块的数量递减的。在最初,每个区块可以产生 50 个比特币,然而,当区块数量达到 21 万后,每个区块能产生的比特币数量就减少到 25 个,再过 21 万个区块,这一数字将减少至 12.5 个,以此类推。到 2140 年,每个区块所产生的比特币数量将变成 10 的负无穷次方,届时,比特币的数量将稳定在 2100 万个。

这一发行方式使得比特币面临着通缩的风险。

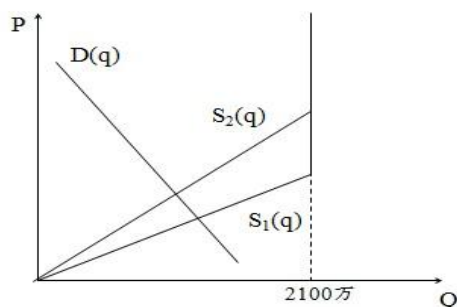


图3 比特币供给需求曲线

货币一般用利率来作为价格度量，然而，比特币没有相关金融产品，且目前其主要以人民币和美元报价，因此本文中用汇率来衡量比特币的价格。对于金融产品而言，无套利定价比供给需求理论更加实用，但是，对于比特币而言，其货真价实的生产成本却使得供给需求理论在此同样适用。

比特币的生产成本随着比特币数量的增加而增加，供给曲线斜率增加，推高价格。在比特币数量达到 2100 万上限之后，其供给曲线将变成一条垂直的直线，因此随着需求曲线向外移动，需求增加，比特币价格也将继续上行。

2.1.3 比特币的流通产业链

在比特币出现之初仅仅是少数电脑爱好者的游戏以及非法交易行为的庇护所，4 年后的今天，比特币已经融入了实体经济，比特币的生产和流通也越来越受到普通民众的关注。如今围绕比特币的生产、储存和支付已经形成了包含矿机生产商、虚拟商品提供商、实物商品提供商和比特币金融服务提供商的完整产业链。



图4 比特币产业链

矿机生产商：随着比特币发行量的增加，比特币的“挖矿”难度也在与日俱增。在比特币出现之初，最先参与游戏的玩家仅仅通过因特网或者超微半导体的中央处理器就可以实现比特币的挖掘。然而时至今日，使用个人电脑的中央处理器可以挖到比特币的概率已经无限趋近于零。2013 年初，采用现场可编程逻辑器件的矿机问世，然而这种矿机本质上依然是使用中央处理器实现区块技术。2013 年中旬，特定用途集成电路（ASIC）矿机大量上市并迅速强制市场，至此，通过因特网或者中央处理器进行挖矿已经无法产生收益。目前，一种计算能力在 5THash/s 以上的集群式特定用途集成电路矿机已经问世，矿机产业正呈现出一种高速新陈代谢的状态。较高的创新要求使得该产业目前处于垄断竞争的市场状态，主要的矿机生产商有 GHash.10、BTCGuild 和 BITMATH。

基础运营平台提供商：比特币的运营平台提供商为比特币玩家提供兑换、存储、交易和

支付平台。目前，比特币中国（btcnCNY）是全球最大的运用平台提供商，也是全球最活跃的比特币交易平台，并有望于 2014 年 5 月成为第一家推出比特币交易型开放式指数基金（ETF）的运营平台。提到比特币运营平台提供商，就不得不提及位于日本东京的 Mt.Gox，这一曾经承担了世界 80% 比特币交易的交易平台于今年 2 月 25 日正式申请法院破产保护。据媒体报道，Mt.Gox 因为受到黑客攻击，总共 744408 个比特币失窃，价值 3.5 亿美元，该平台因此资不抵债而申请破产。黑客攻击一直是笼罩在比特币发展之路上的阴影，由于专业所限，本文无法预测比特币软件漏洞的发生频率以及是否存在绝对安全的电子支付方式。然而不能忽视的是，比特币并非唯一饱受安全问题困扰的电子支付手段，网银、余额宝、微信支付等也时有此类新闻爆出。安全问题是一个技术层面必须正视的问题，完善的用户安全保障方案是电子支付手段繁荣发展的必备条件，但是，关于比特币的探讨也绝不应该在技术层面里固步自封。

商品提供商：由于比特币的匿名性和不可追踪性，最初比特币的商品交易主要集中在军火和药品，例如著名的丝绸之路网站（一家专门提供非法药品和服务的网络黑市）。同时，资金反追踪和洗钱业务也是比特币可以一展身手之处，网络工程师通过将法定货币转成比特币，就可以在电子货币上附加高级别的随机密码保护，完全抹去资金流向。如今一些时尚的商品卖家也会接受比特币支付，但关于此部分的税收条款各国不尽相同，如德国认同比特币作为税收支付手段者有之，如中国坚持本币支付者亦有之。

金融服务提供商：比特币概念的大热催生了依托比特币的一批金融衍生产品，比特币价格的高波动率也吸引了一批投资者进入这一市场。目前，在世界主要比特币交易所交易的比特币金融产品主要有比特币期货、比特币期权和比特币炒币基金等，标的多为比特币对美元或对人民币汇率。提供这些比特币金融服务的提供商主要有烤猫、Labcoin 和 BTCGrowth 等。

2.2 比特币与其他货币对比

表 1 不同支付手段对比

	比特币	Q 币	黄金	美元
发行方式	去中心化	中心化（需求导向）	去中心化	中心化（供给导向）
发行量	有限	无限	有限	无限
发行成本	有	无	有	有
价格（对 RMB 汇率）	浮动	固定（1 比 1 兑换）	浮动	管理浮动
退出机制	无	有	无	有

比特币作为一种依托互联网产生流通交易的虚拟货币，在直观上与传统虚拟货币有相似之处，因此许多人往往过度关注于比特币的虚拟货币属性。为了更清晰的阐明比特币与传统虚拟货币的差异，本文选取了 Q 币与比特币进行对比，以此剖析基于“点对点”的互联网交易方式对比特币的影响；比特币产生之初甚少有人会将其与黄金联系起来，因为“虚拟”世界的光芒掩盖了比特币创新的实质。然而，随着比特币的发展，人们越来越多的关注到了它与黄金的相似之处；美元可以说是比特币的反面，比特币在设计之初就是以推倒美元体系为初衷的，但是，分析美元的流通机制对于剖析比特币的不足之处大有裨益。

2.2.1 Q 币与比特币

Q 币是腾讯公司所推出的一种针对网络即时聊天工具 QQ 的会员的虚拟货币。Q 币的主要用途是用来购买腾讯公司的 QQ 服务，例如 QQ 游戏装备、QQ 皮肤美化等。Q 币的发行权由腾讯公司所有，腾讯公司有主动发行和被动发行两种方式并以由需求导向的被动发行为主。Q 币从产生之初其购买价格就是 1RMB/Q 币，只要 QQ 用户用购买 Q 币的需求并按照

一比一的价格支付，腾讯公司就会发行 Q 币。腾讯公司的主动发行行为多发生于 QQ 游戏奖励制度中，资深玩家可以通过游戏通关来活动 Q 币。Q 币的退出是通过 QQ 用户的购买行为来实现的，QQ 用户可以使用 Q 币购买腾讯公司的虚拟产品，从这一角度而言，Q 币更像是腾讯公司所发行的一种期货，Q 币持有者拥有对腾讯公司未来商品和服务的所有权。Q 币的发行由于是以需求导向为主，所以腾讯公司没有能力也没有动机实现 Q 币的超发，如果腾讯公司在游戏中向买家大量发行 Q 币，则在黑市（淘宝）中 Q 币的价格会相应下降，腾讯公司无法获得 Q 币超发而带来铸币税，因为虽然与法币一样，Q 币发行也是一种负债，但这种负债不是以未来的 Q 币来偿还的，而是以腾讯公司的商品和服务偿还，这一特点从本质上决定了 Q 币不是一种自洽的独立货币，而仅仅是法定货币的一种附属，因此 Q 币与人民币锚定的兑换比例也就不足为奇了。

因此，比特币与 Q 币并没有许多可比之处，虽然同是虚拟货币，Q 币只是一种人民币在网络环境里的支付手段，而比特币则是一种独立的货币形态，除去都需要依托互联网之外，Q 币着实没有资格与比特币相提并论。

2.2.2 黄金与比特币

无论是从发行方式、发行量、发行成本还是从汇率和退出机制角度考虑，比特币与黄金都如同双生子一般的相似。黄金的发行方式是最为接近比特币去中心化特点的，虽然，黄金的勘探开采多受到国家的管制，例如中国的黄金开采是由专业的具有军队建制和番号的黄金部队控制的，个人开采属于违法行为。但是，无论国家如何控制，黄金的发行量都受到黄金储量的限制，因此，自然条件的限制使得黄金同比特币一样不必担忧货币超发的问题。除此之外，比特币与黄金还有许多相似之处，例如与黄金对比，比特币挖矿的速度与黄金储量增长率一致，并且与世界人口增长和财富增长率相吻合。比特币是一种技术进步所带来的福利，它没有黄金交易所存在的交易成本，便于携带和使用。因此，许多人认为比特币是一种黄金的改良版货币。

但是，比特币与黄金的差异也不应被忽略，其中最大的不同就是二者价值来源的不同。黄金成为贵金属而被人们重视的过程一直是经济学家和史学家津津乐道的话题，亚当斯密甚至说过黄金成为硬通货是源于人类对黄色的天然崇拜。而黄金在中国、印度和古埃及更受重视的事实也被赋予了很多人关于种族宗教的文化内涵。更具参考价值的观点认为黄金的兴盛和钻石成为奢侈品的过程一样是一种营销的成功。这种价值远远大于使用价值的物品对于比特币是有参考价值的。迄今为止黄金已经走过了价值建立的阶段，它的价值就是来源于其贵金属的特性，更准确的说是被全世界承认的贵金属特性。而比特币如今还在价值建立的阶段，生于互联网的比特币没有任何使用价值，它的其价格增长来源于需求增长与供给增长的不均衡。因此，比特币的价格取决于人们对它的认同和需求，就目前而言，比特币的营销和炒作十分成功，不仅通过媒体网络电影电视引起了普通民众的关注，政府的关注也着实有效提升了比特币的影响力，另外神秘游资的炒作也是比特币价格的主要推手之一。因此，比特币的成功与否与其营销手段和幕后推手的资金实力密不可分。

2.2.3 美元与比特币

美元的发行流通系统是目前世界上最完善的发行流通系统，通过机制设计实现了“中心化”货币的币值稳定，因而，分析美元的发行流通机制可以很直观的看出比特币发行流通机制中存在的问题。

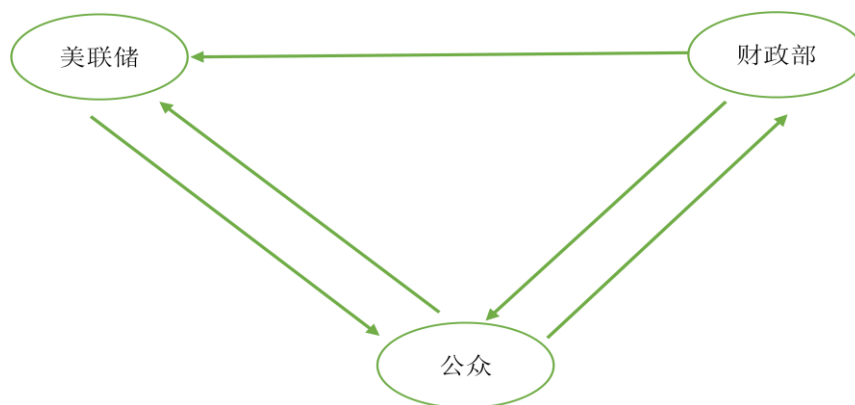


图5 美元循环周转流程

美国买入国债发行美元的货币循环周转流程可以有效的规避政府因追求铸币税而超发货币的风险，同时政府可以利用货币政策来平滑经济周期。首先，在经济低迷的时期，政府为了刺激经济会增加政府支出，此时，财政部会发行国债，以增加政府赤字的方式进行融资，资金的流向是由公众流向财政部；第二步，为了发行美元，美联储将从公众手中购买国债，此时，国债是美联储的资产也是财政部的负债。在这一过程中美元从美联储流向公众，弥补公众支付给财政部用于购买国债的美元，市场上货币供给增加，这一过程实现了美元的发行；第三步，财政部将发行国债募集的美元投入实体经济已经公众用美联储发行的美元进行生产经营活动，随着经济的发展，公众需要按照要求向财政部缴纳税收，缴纳税收的过程使得美元从公众手中流回财政部，这一过程不涉及国债流动，此时，国债依然是美联储的资产和财政部的负债；第四步，当国债到期，财政部用税收偿还美联储持有的国债，国债消失，发行的货币随之退出流通。

美元的发行流通机制的精妙之处在于它在货币中心化发行的前提下规避了货币超发的风险，因为货币的发行并不能给政府带来铸币税的收益。货币通过国债发行，政府今天发出的货币需要财政部在未来使用税收的收益来偿还。同时，政府也通过税收保证了美元的法定货币的地位，因为无论是比特币也好还是各类信用卡的普及也好，只要公众必须用美元偿付税收，这就保证了这个体系的运行和美元的地位。

与美元相比，比特币的发行方式是直线型的，并不存在一个发行、流通和退出的闭环循环。更为致命的是，比特币不能如美元一样对经济形势作出反馈。当经济低迷时，财政部可以赤字融资，美联储发行货币，反之，当经济过热时，美联储可以出售国债使美元退出流通。但是比特币的发行是在其诞生之初就已被锚定的，四年一个发行周期，每四年新增比特币数量减半直到2140年达到2100万个。同时，比特币不存在耗损的问题，发行出来的比特币将永远存在。所以，比特币的发行本身不能对经济形势做出反馈；其次，如果比特币替代美元，政府的货币政策和财政政策效果将大打折扣，因此，政府会全力维护美元地位；再次，政府有通过税收维护美元地位的能力，聪明的政府甚至不用采取法律手段抵制比特币，它们只需守住税收的底线就自然可以限制比特币的发展。

通过以上对比可以看出，作为一种虚拟货币，比特币与传统虚拟货币大相径庭，虚拟这一概念不是比特币的创新也不是比特币的核心，去中心化发行才是比特币的精髓。但是去中心化货币的成功与否依赖于公众的需求，同时，去中心化也不是防止恶性通胀的唯一选择。

2.3 比特币的货币职能分析

关于货币的定义，西方经济学给出了五花八门的概念，从最初的用于支付商品劳务以及清偿债务的物品，到充当一般等价物的特殊商品，再到与国民收入最大相关的流动性资产。但在货币职能的问题上，学界已经有较为统一的意见，本文也将从货币的五大职能的角度来

分析比特币，即支付手段、流通手段、价值尺度、贮藏手段和世界货币。

2.3.1 支付手段、流通手段和世界货币

支付手段和流通手段的货币职能都是在交易的过程中实现的。当货币充当商品交换的媒介时，货币所行使的是流通手段的职能，当货币充当独立的价值度量形式时（如支付租金、清偿债务），货币所行使的是支付手段的职能。因此，支付手段和流通手段这两个职能是相辅相成密不可分的。

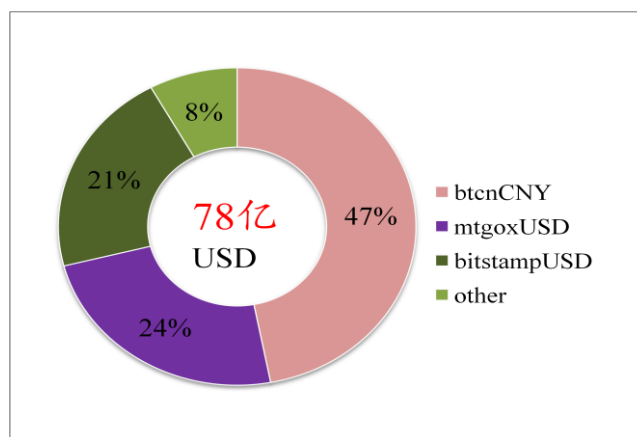


图6 比特币用途分布

从上图可以看出，在总量已达到78亿美元的比特币中，用于交易支付的比特币不足比特币总量的8%，超过90%的比特币仅仅在交易所中流通，并不参与实体经济，造成这一局面的原因主要有两个，其一，比特币的匿名性，其二，政府的税收阻击。

比特币的匿名性源于它的点对点（Peer to Peer）技术，该技术实现了支付的去中介化，使得一方可以发起交易并直接支付给另一方。目前的基于网络的支付方式是基于数字签名（Digital signatures）的，数字签名仍然需要第三方的参与，否则将造成双重支付的问题。而点对点的交易中，网络通过随机过程给每笔交易加上时间戳，并将它们纳入一个基于随机变量的不断延伸的链条中，使得每笔交易都获得各种的时间序列证明，以此来规避双重支付。数字签名技术交易过程如下：一枚电子货币的实质就是基于随机序列的一条数字签名，所以者在签署随机数列的数字签名时不仅要关注该枚比特币的前一次交易，还需要考虑下一位交易者所拥有的公钥（Public key），这个签名将被附加在这枚电子货币的货币尾端，而电子货币的收款人通过电子签名验证身份从而获得这枚货币。这一过程使得电子货币的交易历史被保留，因此，现有的电子货币不能有效保护交易信息。但是，该交易的优势是货币在交易过程中不经过背景数据库处理，为线下交易开放了可能性。与之相对比的点对点技术，正如上文所谈到的，它涉及信息区块的处理和向全网的广播，交易过程中对信息处理的要求成倍增加，因此，如果比特币进入实体交易，其线下设备的成本将大幅高于如今涉及第三方的POS机等设备，因此，公众需要在匿名性带来的收益和交易成本的飙升之间进行选择。更进一步，对于大多数普通公众而言，匿名性并不是一项“福利”，它在隐藏自身交易身份的同时也使得对手的身份无据可查，在现实中，合法交易者还是更乐于留存交易记录的。

匿名性是比特币内在对支付和流通设置的限制，政府的税收阻击就是外部对比特币的支付和流通造成的限制。如果比特币成为某国的统一货币，该国政府将会损失税收以及货币政策相机抉择的权利。首先，对于如中国以负债换取资产发行货币的国家来说，比特币的合法化将使得政府丧失铸币税的收入；其次，比特币的匿名性决定了，如果比特币成为交易媒介，政府将缺乏相应的税收征收依据，交易主体可以规避缴纳税负；再次，当比特币成为某些国家的统一货币，各国将不可避免的失去独立的货币政策，并将面临通缩的风险，这是各国央行所不能接受的，因此，只要政府还是社会经济的组织者，比特币就不会成为主流货币。当

然，政府阻击比特币的意愿和其阻击比特币的能力同时决定了比特币的未来，不幸的是，在阻击比特币这件事上，政府既有意愿亦有能力。在阻击方法上，各国有不同的选择，既有简单粗暴式的，也有迂回隐蔽式的。中国政府采取的无疑是简单粗暴的做法，去年年底，央行发文明确比特币不是货币，近日，央行要求国内商业银行关闭比特币账户。欧美则采取了相对温和的抵制方法，美国《虚拟货币个人管理条例》的颁布承认了比特币作为虚拟货币的地位，德国是世界上首个承认比特币货币地位的国家。然而，这并不意味着欧美国家政府就可以接受损失税收以及货币政策相机抉择的权利，他们只是换了一种更为隐蔽的控制方式：税收控制。税收的重要性要远远超过它直观表现的样子，税收并不只是一种购买支付行为，而是整个货币发行体系中重要的一环，与货币的退出机制息息相关。正如前文论述的那样，美元发行体系中，财政部会发行国债，以增加政府赤字的方式进行融资，为了发行美元，美联储将从公众手中购买国债。在这一过程中美元从美联储流向公众，弥补公众支付给财政部用于购买国债的美元，市场上货币供给增加；之后财政部将发行国债募集的美元投入实体经济已经公众用美联储发行的美元进行生产经营活动，随着经济的发展，公众需要按照要求向财政部缴纳税收，缴纳税收的过程使得美元从公众手中流回财政部；当国债到期，财政部用税收偿还美联储持有的国债，国债消失，发行的货币随之退出流通。因此，政府守住了税收，就保证了美元的货币地位。

货币的世界货币职能主要指货币用作国际支付手段，用以平衡国际收支的差额。支付手段职能是成为世界货币的前提，因而，当比特币在支付手段职能上受到限制时，其作为世界货币的职能更是无从谈及。

2.3.2 价值尺度和贮藏手段

比特币所提供的“挖矿”模式，是旨在为公众提供一种可以替代现金和电子账户的电子货币，因而，交易媒介和保值手段一直是比特币所追求的货币职能目标，然而，纵观比特币的发展，不得不承认的是，比特币从初始就没有找对方向，交易媒介的局限性已经在上一节中做出了阐述，而对于保值手段来说，这种需求的存在性备受质疑，近几十年来，美元在保值手段上表现良好，并在可以预见的未来，几乎没有人会相信美元的购买力会大幅缩水。

如果，比特币将重点转向另一种货币职能——价值尺度，也许会取得更好的效果。货币价值尺度的职能，是将货币视为一种记账单位，这是基本经济计量标准的一种，学界和商界都在计量体系方面投入了极大的热情。

1967年产生于智利的名为“发展单位”的通货膨胀指数是货币价值尺度职能与其他货币职能分离的先驱。比索是智利的国家货币，“发展单位”与比索的换算比例是根据 valoruf.cl 网站发布的数据确定的，用“发展单位”的定价乘以换算比率就是以比索计价的价格。这种方式使得通货膨胀价格指数的设定变得更加容易，例如，在房租市场，涨价将损害租客的利益，因此租客可能需要对冲通货膨胀。在智利，许多房东会使用“发展单位”设定租金，并不对其进行调整，这一方法降低了通货膨胀的菜单成本，也解决的重新定价所带来的摩擦。“发展单位”作为一种脱离了货币其他职能的记账单位，重塑了人们的思维，也为货币的创新提供了一种全新的思路。借助计算机技术，“发展单位”可以有更大的发展。首先，“发展单位”的本质就是一种“篮子”，参照最基本的形式，“发展单位”篮子构成与CPI篮子的构成一致，通过设定基准年份，“发展单位”实现了随着通货膨胀而变化；第二步，通过信用卡公司设定一种电子机制，使得人们可以方便的将以“篮子”计价的传统货币汇至世界各地，传统货币可以随意指定，美元、比索甚至“篮子”本身。将“篮子”设置为计价货币就意味着以本币价格汇出资金；第三步针对记账单位的改进将着眼于整个系统，针对不同项目开发不同“篮子”，例如，针对人口老龄化开发“高级篮子”，针对低保人群开发“衣食篮子”。除了基于CPI的记账单位，也有学者建议使用基于GDP或者人均消费额的记账单位。这两种模式都可以用于养老金和社保福利的发放，使得两代甚至更多人共同承担风险。这些“篮子”式的记账单位可以

更简单的确定价格，在签订长期合同时更容易达成一致。在比特币设计之初，如果将目光更多的投向货币价值尺度的职能，而不是一味寻求支付手段和价值贮藏，比特币将会在实现对抗通胀的同时可能有更大的作为。

从货币的五大职能考虑，比特币在成为货币的道路上实在前途堪忧。匿名性和政府对税收以及货币政策的追求限制了比特币的交易手段职能，不稳定的比特币价格和稳定的美元购买力又堵死了比特币价值贮藏之路，最迫切需要的记账单位职能又在比特币设计之初被忽视了。

同时，作为一种全新的电子货币形式，比特币已经表现出了投机泡沫的特征——人们争相持有一种资产并期待通过该资产的升值来获取财富。如今比特币交易所的活跃和各类比特币衍生产品的活跃也印证了这一观点，目前在背离货币的道路上渐行渐远的比特币正以一种金融产品的姿态活跃于公众的生活之中。

三、结论及建议

本文首先系统的分析了比特币的理论基础、发行机制和流通产业链。比特币的设计理念源于“货币非国家化”理论，其运行机制不依赖于任何政府、组织或个人的信用支持或担保，以此来规避人为的通货膨胀的产生。比特币的发行实质上是一种对等网络中种子文件所达成的网络协议，产生成本随着数量的增加而增长，并在比特币数量达到设定上限时成本达到正无穷。围绕比特币的生产、储存和支付已经形成了包含矿机生产商、基础运营平台提供商、实物商品提供商和比特币金融服务提供商的完整产业链，基础运营平台提供商在产业链中起到了核心的作用。之后，本文从发行方式、发行量、发行成本等方面对比了比特币和其他货币，发现作为一种虚拟货币，比特币与传统虚拟货币大相径庭，虚拟这一概念不是比特币的创新也不是比特币的核心，去中心化发行才是比特币的精髓。但是去中心化货币的成功与否依赖于公众的需求，从货币的五大职能考虑，比特币在成为货币的道路上实在前途堪忧。匿名性和政府对税收以及货币政策的追求限制了比特币的交易手段职能，不稳定的比特币价格和稳定的美元购买力又堵死了比特币价值贮藏之路，最迫切需要的记账单位职能又在比特币设计之初被忽视了。同时，作为一种全新的电子货币形式，比特币已经表现出了投机泡沫的特征——人们争相持有一种资产并期待通过该资产的升值来获取财富。如今比特币交易所的活跃和各类比特币衍生产品的活跃也印证了这一观点，目前在背离货币的道路上渐行渐远的比特币正以一种金融产品的姿态活跃于公众的生活之中。

综合以上结论，本文主要从政府、投资者和电子货币设计者三方面给出建议。

首先，对于中国政府和央行，采取行政手段干预比特币是一个合理的选择。首先，美欧国家可以通过市场手段干预比特币的前提是其货币发行流通退出机制的完善，正如本文第二章介绍的那样，美元发行体系中，财政部会发行国债，以增加政府赤字的方式进行融资，为了发行美元，美联储将从公众手中购买国债。在这一过程中美元从美联储流向公众，弥补公众支付给财政部用于购买国债的美元，市场上货币供给增加；之后财政部将发行国债募集的美元投入实体经济已经公众用美联储发行的美元进行生产经营活动，随着经济的发展，公众需要按照要求向财政部缴纳税收，缴纳税收的过程使得美元从公众手中流回财政部；当国债到期，财政部用税收偿还美联储持有的国债，国债消失，发行的货币随之退出流通。因此，政府守住了税收，就保证了美元的货币地位。然而，人民币买外汇发人民币的方式是直线型的，税收是游离在整个货币发行体系之外的，所以，如果比特币成为国际交易支付中可以接受的主流货币，中国政府将无力仅仅通过控制税收就控制整个货币运行体系；其次，人民币对内贬值、对外升值的现状使得人们对人民币失去信心的同时又无法通过配置外汇来分担风

险，所以只能转而寻求其他抗通胀的产品，这也是中国比特币交易市场可以稳坐全球第一的主要原因，比特币在中国的迅速发展暴露出了许多安全隐患，迫使中国政府采取更激进的政策手段。

对投资者而言，在投资组合中配置比特币需要考虑其价格走势、安全隐患以及政策对比特币的影响。由于东京比特币交易平台的破产和央行政策边界的不明晰，导致目前比特币价格波动剧烈，适合投机炒作但还未能发挥其抵御通胀的长期投资价值。

最后，比特币作为不依赖于其他货币的独立虚拟货币的先驱，为未来电子货币的设计发展提供了许多宝贵经验。通过货币发行流通机制设计而抵御通货膨胀的理念是积极的，也有其存在的合理性，但是，抵御通货膨胀并非只有比特币“去中心化”设计这一种形式，美元以及前文所介绍的智利“发展单位”都能发挥抵御通胀的作用。同时，在货币职能的选择上，电子货币不应该将自身限制在交易手段和价值尺度上，发挥货币的其他职能也许能给电子货币的发展提供更加广阔的空间。

参考文献:

- [1]吴 洪,方引青,张 莹. 疯狂的数字化货币——比特币的性质与启示[J]Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition) Vol. 15, No. 3 Jun. 2013
- [2]张光炜,薛京晶. 比特币——金本位复辟式的一厢情愿[J] 现代经济信息, Vol.10, 2013
- [3]郭帝. 比特币发展前景的研究[J]中国证券期货 Vol.07 2013
- [4]CitiFX London Update[R] CitiFX & Local Markets Strategy, November 25, 2013
- [5]于江.新型货币“比特币”：产生、原理与发展[J]吉林金融研究 No.5, 2013
- [6]Gold and Bitcoin: the Currencies of the Future—James Turk[R] The Gold Report, May 15,2013
- [7]洪蜀宁.比特币：一种新型货币对金融体系的挑战[J]中国信用卡. Vol.10, 2011
- [8]张越. 比特世界[J]个人电脑. Vol.6, 2013

