比特币的理论、实践与影响

贾丽平

内容摘要：比特币是一种纯 P2P 的虚拟货币，能够满足去中心化、严格控制货币供给速度、预估货币流通总量、有效遏制通货膨胀的需求。比特币基本上具有货币的功能，拥有货币的部分属性，但不一定是真正的货币。它未来能否过渡为真正货币取决于人们对比特币的信任、对一整套机制所营造的信心。本文分析了比特币能够成为真正货币必须克服的一些现实问题，其中涉及经济、互联网金融、法律、网络技术和信息传播等领域。最后提出比特币作为一种全新的无政府虚拟货币，一场数字货币的革新，代表了世界政治经济一体化思潮，具备一定的革命性。

关键词：比特币　个人对个人直接信贷　数字货币　传统货币

中图分类号：F831　　**文献标识码**：A

人们对任何形式货币的需求，总会选择使得商品交换、价值储存、记账更加便捷的货币作为最适合的货币。货币同质化会引起相同的风险敞口，而维护金融体系稳健运行，需要多种异质风险偏好的货币并存。互联网金融条件下的虚拟货币灵活多样、方便快捷，金融服务和金融资源呈现出异质性的特征。目前，一种新型虚拟货币比特币成为全球增速最快、使用最为广泛的虚拟货币，在世界范围内迎来高速发展期。从创新的角度讲，货币是金融行业的基础设施，比特币全新的发行技术、交易模式对货币的内涵结构、形式内容、职能特征、作用机制和社会效应产生了深刻影响，从基础设施上对现有货币体系进行颠覆性创新，形成独立存在的货币系统，创造了一种有力的价值存储手段和金融模式，改变了人们的消费模式，产生了新型产业，是信息科技时代国际货币体系演变的标志性事件。

一、比特币的产生与运行机制

21 世纪功能强大的计算机和互联网使得虚拟货币容易创造和管理，2008 年 11 月 1 日，一名自称中本聪（Satoshi Nakamoto）的人设计了一种任何人都能够创造和管理，用于各种交易的新型虚拟货币——比特币。设计者期望这一货币能替代美元和欧元甚至全球货币，彻底改革金融业。

（一）比特币的界定

比特币（Bitcoin）是通过开源的算法产生的一套密码编码，是世界上第一个分布式匿名数字货币。通常也用来标识商品或服务价值，作为虚拟货币的基本单位，简写为 BTC，如 100BTC。比特币使用遍布整个 P2P 网络节点的分布式数据库来管理货币的发行、记录货币的交易和账户余额信息，并使用密码学的设计核

作者简介：贾丽平，硕士，山西财经大学财政金融学院副教授、硕士生导师。

查重复消费，保证货币流通各个环节的安全性。

比特币具有五个显著特性。第一，属于“信息货币+私人货币”。信息货币是人们为了方便交换不同的物质资源抽象出来的数量单位。由分布式的网络节点，以信息化的方式分散发行，而非中央银行集中控制，与服务、自我服务本身内在相连，其价值取决于承载的信息内容，是一种附加信息的货币卡，具有混合价值形态。私人货币的特点是允许私人发行货币，自由竞争产生货币。第二，不会发生通胀、通缩。生成比特币的上限时间和上限数量被设定为固定值，自动化的技术手段保证了货币供给以预定的速度增长。在最初的四年有1000万个比特币被制造出来，每10分钟向网络中释放50个比特币，这个数值每四年逐步减半。[①]现存的比特币总数是区块（Block）的总数乘以每个区块的比特币值。比特币固定了基础货币的投放总量，至2140年全部比特币被挖掘出来，达到2100万个，之后不再增加，因此不会发生通胀。如果比特币长期升值，发生货币囤积，流通货币总量不足或者经济困难需要调节货币供给量时，这种货币管理机制可以因需调整，即每个比特币可以切割为10的8次方份，实现比特币供给量与经济活动水平所对应的合理货币量恰好匹配，不会出现流通中货币量不足而影响流通，发生通货紧缩（黄金萍，2011）。第三，高度匿名。交易双方可以随意生成自己的私钥，将与其对应的公钥告知付款人即可收到款项。下次再使用时，重新生成一对公私钥进行交易。这种一次一密的做法实现了高度匿名交易，且交易不可逆（洪蜀宁，2011）。第四，使用方便。达成协议的双方直接进行支付，不需要依靠第三方机构，克服了地理空间的限制和市场的地域分割，提高了金融资源的配置效率，使金融资源配置获得更大的地域弹性。有些网站开发了手机钱包，通过手机使用比特币，满足了互联网时代全球电子货币交易一体化的需求。第五，交易成本低廉。每笔交易收取约1比特分的交易费，跨境交易支付比特币时不存在汇率问题。

（二）比特币的产生机制

任何人都可以下载并运行比特币软件参与比特币生产，这种生产模式模拟了贵金属黄金的生产过程，被称为挖矿（Mining）。挖矿需要强大的计算能力（反复运行散列算法），找一个最小的散列值，生成比特币网络所搜寻的64位数字，创建一个区块，便可以获得一个区块中所包含的比特币，每10分钟整个网络出现一个新区块。为了严格控制比特币的生产速度，生成算法会根据当前已产生的比特币存量动态调整算法的复杂度，已经产生的比特币越多，参与挖矿的人数越多，算法就越复杂，挖矿的困难度就越高。挖矿的困难度与一定时间内全网投入制作工作的平均运算能力相关。单一个体和其他用户竞争，他的计算能力高于全网计算能力的综合水平，成为整个网络最早创建新区块的第一人，并把这个新区块发布到全网络，被全网所确认，即挖矿成功。若10分钟内有人抢先挖矿，则以前的计算无效，只能重新再创建另一个新区块。

（三）交易支付机制

比特币交易需要设立一个账户，该账户是一对公、私钥，通过公开密钥算法，采用电子签名的技术进行交易。如果A转给B一笔比特币，A把钱的数量加上B的公钥（即收款地址Bitcoin address），用自己的私钥签名。B看到这个签名，便知道A向他支付款项。

同时，比特币交易需要整个网络作为担保人对交易进行担保。A发起这笔交易时，需要把签过名的交易单公布到全网络，网络上的每个人都可以检查确认这笔交易。B从网络上收到足够多（6个人）的确认信息后，便能确认A发出了这条交易单，B以后可以合法使用这笔比特币。比特币网络并没有记录每一个比特币归属谁，只是在公开日志中以列表的形式记录了比特币诞生以来的每笔交易的详单。一旦法律强制执行时，监管部门可以使用高端网络分析技术追踪交易流量，追溯每一个比特币的去向，找到比特币个人用户。任何人需要确认

[①]2012年11月28日，比特币发行量占发行总量2100万的一半。区块供应量首次减半调整，从之前每10分钟50个递减至25个，即每个区块的币值在2009年的210000个区块中是50BTC，2013年210000区块是每区块25BTC，2017年是12.5BTC、2021年是6.25BTC，以此类推。

一个交易单时，比特币网络都会检查这个列表来确认转出账户上是否有足够多的比特币（洪蜀宁，2011）。

利用 P2P 系统中的节点投票验证把所有交易固化成一个交易链（见图 1），让所有节点都可以验证资金的流向，使用分布式时间戳算法将由网络节点验证后的新交易数据加入到全网认可的交易链中，追溯交易链中的交易判断收款人收到的钱是否被重复支付，解决了比特币的重复使用问题（郑书雯，2011）。

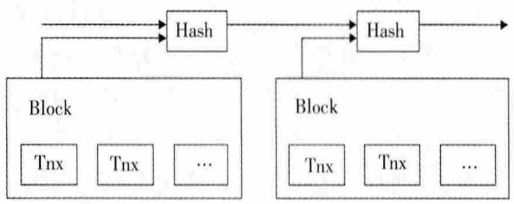


图 1　交易链和块结构①

（四）比特币的获得方式

比特币的获得方式有三种：一是挖矿生产。制造一个新的比特币区块获得比特币。二是进行购买。通过类似于网上交易平台 Mt.Gox②购买。三是捐赠获得。2011 年自由网、互联网、档案馆、自由软件基金会以及其他的一些组织，接受比特币捐赠。

（五）比特币与传统虚拟货币的比较

基于网络社区中虚拟商品制造、交流、支付和使用，对网络的依赖，形成了虚拟世界独特的“分享型经济”，大量用户在网络市场交易商品，虚拟货币在此基础上应运而生。欧洲中央银行根据虚拟货币和实体经济互动程度，将虚拟货币分成三类：第一类是封闭性虚拟货币。几乎与实体经济无联接，用于游戏中各种游戏币，如暴雪娱乐的魔兽金币。第二类是单向流入虚拟经济的虚拟货币。按照买进汇率，现金兑换虚拟货币后，可以购买虚拟商品和服务，虚拟货币一般不能购买实体商品或服务，个别例外可购买实体商品或服务，如 Second Life 发行 Linden Dollars，Facebook 发行 Facebook Credits，亚马逊公司发行亚马逊币，腾讯发行 Q 币。第三类是双向货币流的虚拟货币。按照买进卖出汇率，用于买卖虚拟及实体商品、服务，如比特币。本文把第一类、第二类虚拟货币统称为传统虚拟货币。比特币与传统虚拟货币不同之处在于（见表 1）：第一，发行方式不同。传统虚拟货币有发行主体，其使用范围主要局限在各个网络公司，如 Linden Dollars 用于支付林登实验室提供的游戏和业务。比特币没有发行主体。第二，监管体系不同。我国已经把传统虚拟货币纳入第三方监管体系，给第三方支付发放牌照，对传统虚拟货币交易征税，受到中央银行和政府虚拟货币管理政策、法律和法规的约束。若购买传统虚拟货币的数额增大，滞留在网络公司的真实货币增多，给现实经济带来隐患，政府监管措施可以影响传统虚拟货币的发展。而比特币由比特币网络所有节点集体管理，很难了解比特币的交易情况，对传统虚拟货币的监督方式很难应用于比特币，比特币交易很难征税。第三，匿名程度不同。传统虚拟货币依靠账号系统，掌握交易双方个

表 1　比特币与传统虚拟货币的比较

	比特币	传统虚拟货币
性质	去中心化	有一个运营服务商
交易公开度	匿名	交易公开，可追溯到实名用户
存量	存量有限	无限增发
代码属性	开源	封闭
价值体现	可直接购买商品	可直接购买虚拟商品，个别例外可以购买实物商品
使用范围	没有限定	范围有限

①交易 Tnx 包含以下信息：In（收入来源）、Previous tx（收入来源交易单的散列值）、Index（Previous tx 交易单中的 Out 索引值）、scriptSig（拥有者对该交易的 ECDSA 签名认可）、Out（货币转出信息）、Value（发送的币值）、scriptPubKey（接收方的公钥脚本）。每一笔交易可以有两个 Out 和多个 In，一个 Out 用来指出所付金额，另一个 Out 用来将多余金额返回给自己，Out 的总额应该等于 In 的总额。但是，在交易单里，只会有 Out 的 Value，没有 In 的 Value，通过 In 的 Pervious 与 Index，追溯到上一个交易单的某一个 Out，获得 Value。

②Mt.Gox 是目前最大的比特币交易平台，总部设在东京，处理全球大约 80%的比特币兑换美元业务。除了美元外，还提供英镑、欧元、加元、澳元、日元以及波兰兹罗提与比特币的兑换业务。

人信息进行交易。比特币不依靠账号系统，交易双方公开密钥信息进行交易，可以通过不断变换收款地址，隐匿真实身份。第四，价值不同。传统虚拟货币的价值是个性化的，相对的，无统一标准。正当渠道购买的 Q 币和游戏币与人民币之间有固定的兑换比率。比特币没有限定使用范围，对美元汇率不稳定。

二、比特币的货币属性

货币是从商品中分离出来的特殊商品。货币是一种商品，具有普通的价值（凝结着一般抽象人类劳动，具有社会属性）和使用价值（自然属性所决定的物的有用性）。货币又是一种特殊商品，具有特殊的价值（由其他一切普通商品综合表现出来，货币的对内价值用货币的购买力=1/物价指数表示，货币的对外价值用汇率表示）和特殊的使用价值（货币可以衡量和表现一切商品的价值，具有与一切商品相交换的能力）。货币是商品交换发展到一定阶段的产物。马克思认为货币的本质是一般等价物，具有价值尺度、流通手段、支付手段、贮藏手段、世界货币的职能。价值尺度、流通手段的统一是货币。Frederic S.Mishkin 认为，货币是在商品或劳务的支付中或债务的偿还中被普遍接受的任何东西。普遍被接受的作为购买、支付的手段（隐含着赋予交易对象以价格形态的前提），具有交易媒介、支付工具、价值储藏和计算单位的物品，是市场经济的一般等价形态。凯恩斯经济理论流行以来，“流动性”几乎成为货币的同义语。斯蒂格利茨认为，货币就是货币行使的职能。货币具有四个基本职能：赋予交易对象以价格形态、交易的媒介、支付手段、积累和保存价值的手段。下面以马克思的货币职能，分析比特币的货币属性。

（一）价值尺度是赋予交易对象以价格形态，指货币作为计价标准，充当衡量和表现商品价值大小的社会尺度。比特币是人类历史上第一次由技术群体在自己的领域内对世界的商品计价，且与美元形成比价效应。比特币效仿黄金低产出和有限数量的特点，具备稀缺性，充当价值尺度的社会职能，成为世界最被认可的虚拟货币，网络中的数字黄金。

（二）流通手段是指货币充当商品交换的媒介，是一种现实的货币。比特币具备交易媒介功能，出售商品与服务获得比特币，比特币不但能购买网络虚拟产品和服务、实物产品，而且具有较强的分割能力。1 个比特币可以被分解到小数点后第 8 位，方便微型支付。

（三）支付手段是指发生赊销赊购，用延期支付的方式买卖商品的情况下，货币用于清偿债务时执行的职能，是交易媒介职能的延伸。比特币由于其使用范围不受限制，可以线上线下赊销赊购公司提供的商品与服务，实现未来货币与财富的兑现。

（四）贮藏手段是指货币退出流通领域，作为社会财富的一般代表而加以积累和保存价值的手段，发挥“蓄水池”的贮藏作用。比特币具备价值储藏或购买力储藏的职能，具有专属所有权，运用计算机技术和通信技术将网络中的比特币以数字化形式（二进制数据）被隔离存储在网络或有关电子设备中，只有用户自己操控私钥支付，无人可以获取。携带和保管的成本几乎为零，且不易出现损耗。消费者将来如果需要实现货币购买力，比特币具备保值功能，可以按照交易平台兑换汇率将比特币赎回为现实货币，得到完好无损的财富兑现能力。

（五）世界货币是指当货币超出国界，在世界市场上发挥一般等价物时，执行此职能。世界货币作为国际间的购买手段、支付手段，实现国际间财富的转移。比特币没有国界，适合作为国际间贸易的支付手段。

从以上比特币行使的职能来看，比特币具有五大货币职能，尤其是商品交易中介职能，体现了比特币的使用价值。购入计算机的费用和挖矿时的电耗、时耗等都使比特币天然具有价值，类似开采黄金消耗的社会必要劳动时间固化于黄金本身而使其具有价值一样，挖矿消耗的劳动全部转化为比特币的价值。因此，比特币具有货币的价值和使用价值。

表面上，比特币具有货币功能，但是它的价值还没有得到全社会的认可，因此比特币不是真正的货币，它的本质是商品。任何东西都能成为货币，只要每个人都认同比特币是主要

货币，那么，比特币就能成为主要货币。比特币既缺乏金本位币背后的商品职能，又缺乏信用货币的强制力保证，它的价值取决于有多少人、多少商品和服务愿意接受比特币付款，即人们对比特币的信任、对一整套机制所营造的信心。如果比特币能够在较长的时间内建立投资者的信心，认可度越来越高，交易范围越来越广，影响力增加提升了整个社会公信力，它的货币属性就会越来越强，那么，一种新的货币体系也许就此开始，并最终成为真正的货币。如果比特币使用群落有限，它的货币性能被局限在某些特定领域里，在一定范围具有交换支付手段功能，相当于代金券或者商城购物卡，其商品属性大于其货币属性，货币属性就比较小，是一种特殊商品。现实中，比特币币值波动正是因为比特币使用范围和实际影响不够大，容易被投机者炒作，其内生性的体制约束力还没能充分显现。比特币基金会（Bitcoin Community）评价其为“实验性货币”，项目核心开发成员埃米尔·塔吉认为，比特币符合高德纳的发展规律周期，分为技术萌芽期、过热期、幻觉破灭谷底期、复苏期和生产力成熟期，遵循一种技术从被采用到成熟的理论曲线（周寿英，2013）。2013 年 4 月底，比特币处于幻觉破灭谷底期。法定货币也有过这些经历。只要比特币在发展过程中能够经受住投机者炒作，比特币的价格将在一个比较成熟的市场里趋于稳定。

三、比特币产生的客观经济基础

（一）客观经济发展推动货币的嬗变

货币是时代变革的产物，货币的嬗变过程是不断提高交易效率，降低交易成本的过程，体现在适应客观经济发展、满足交易模式、规避货币波动风险的内在映射上。贵金属货币、信用货币和虚拟货币在不同发展时期、各自领域都有过完美的表现。当前正处在货币史上最困惑不确定的时期，金属货币不再是流通中的货币，信用货币内在价值不稳定，虚拟货币比特币规模还太小。比特币是信息科技时代对货币进化提出新要求的必经过程，代表金本位理念，是信息价值的承载中介，具有流动性和增值性，预示全球金融生态系统正由量变引发质变。下面从贵金属货币、信用货币、比特币作为衡量全球财富的货币嬗变过程，分析比特币产生的客观经济基础。

1.贵金属货币

从农业社会进入商业社会，黄金作为贵金属货币，由于储量低、开采难，内在价值稳定，相当长时间内充当一般等价物，促进了各国范围经济和规模经济的发展。贵金属货币反映了重商主义，促进了国际贸易稳步增长，出现了百年经济繁荣。但是当各国经济达到一定规模，大量商品被生产出来，黄金自然数量过少的问题出现，黄金供求关系失衡，作为媒介商品流通的手段，导致大量商品闲置和价格畸低，出现通货紧缩和经济萧条，金本位制度崩溃。1925 年丘吉尔恢复金本位制，导致通货紧缩、失业增加，重创英国经济。凯恩斯认为金本位制度是“野蛮的遗迹”。国际金融危机后不断有“回归金本位”的观点产生，2013 年上半年国际金价持续跌势，意味着黄金如果作为一般等价物其价格也不稳定，再加上黄金的稀缺性，不能与经济发展保持同步，难以精确微分实现微型支付，回归金本位不可行。

2.信用货币

1971 年布雷顿森林体系解体后，货币从贵金属货币进化到没有商品作为发行保证的信用货币，货币的分散性替代了单一性，呈现出多元主权货币的特征。信用货币不具有内在价值，各国信用货币的信用来自于中央银行体系和国家法律的强制力，只有国家发行的货币才有法定清偿能力，具有名义价值，而且货币名义价值的基础是国家经济实力和偿债能力，从而保证了信用货币较好地实现货币产生的初衷，便利商品交易，满足日常经济生活。未来一段时间内信用货币依然是货币的主流形式。

随着科技进步、微观势力的发展壮大，信用货币反映了工业主义发展的特点，它代表着使用资源的能力。商业银行信用货币创造过程是一个信用发现、评估、定价的过程，信用系统通过信用活动能够为资金需求者创造“恰当数量”的货币，使社会创造稀缺资源的未来潜

力变为现实。这是信用货币繁荣市场经济、信用经济的最大贡献。

但是，分散性主权信用货币币种繁多，商品交易承受汇率风险，增加了额外交易成本。同时，信用货币生产成本低，货币供给具有弹性，避免了黄金等自然货币数量受限的问题。通过增发信用货币满足商品交易的需求，容易导致币值不稳定，持有信用货币的微观个体被动承受货币通胀、贬值的损失。这种失衡的货币格局自然引发货币的自我进化（程实，2013）。

3.比特币

比特币是信用货币进化的阶段性产物，反映了信息对称、个体选择、去中心化和权力制衡的货币特征，映射了货币由分散性向单一性回归的进化需求。比特币是电子商务的产物，让电子商务变得便捷一直是互联网货币设计的理念。互联网是信息生产和流动的网络，金融业是信息敏感产业，互联网与金融业务的融合形成互联网金融。互联网金融是互联网时代金融业发展的主要路径，互联网金融依照金融业务产品化、金融产品标准化，产生规模化效应，淡化了金融业的分工和专业化，最具代表性的是个人对个人直接信贷 P2P。互联网金融有三大支柱：支付方式、信息处理和资源配置。其中，互联网金融的支付方式体现在比特币上，促进了货币全球化进程，为非主权的虚拟货币逐渐成为主流货币创造了条件。

从广度来看，互联网金融在电子化方向的广泛应用推动交易模式的技术改进，降低了金融产品和服务的门槛，成为一种消费引导和客户服务模式，提高了金融包容性，市场参与者更为大众化。从深度上看，金融消费者掌握互联网金融产品和服务水平的能力不断提升，利用互联网可以完成几乎所有的交易，而且互联网金融最大特点是不断创新。金融交易内在的复杂多样和专业性不断提升，与高技术的互联网行业结合在一起，金融体系更加透明、平等、开放，互联网金融可以交由某一个先进的算法进行数字化处理，人们不再是被动的货币产品消费者，而是货币的生产者、创造者，不受任何政府和银行的掌控。

（二）国际货币体系的内在缺陷促进了比特币的产生

金本位制度、信用货币制度和虚拟货币制度都是人类不断探寻促进全球经济活动、解决全球流动性问题的制度安排，但是一直没有找到理想的全球流动性制度安排。国际货币发行国成为现实中的全球中央银行，提供流动性但缺乏统一规则，特别是国际金融危机后，各国际货币发行国竞相采用量化宽松货币政策（Quantitative Easing，QE），尤其是美联储连续四次推出 QE，导致全球流动性泛滥。当前国际货币体系的内在缺陷是比特币产生的客观经济基础。

一是缺乏可信的“锚”。国际货币发行边际成本几乎为零，当国际货币发行国出现经常性账户逆差，弥补国际收支缺口的方式主要有两种：一种是利用增发货币融资，另一种是利用资本账户顺差借入货币融资。如果没有泰勒规则约束，会造成全球流动性供给过剩。国际货币体系对国际货币发行国实行软约束，国际货币发行国中央银行的不良政策和人为干扰造成国际货币多发，诱引其他国家货币出现“超发”的集体道德风险。

同时，国际货币有国内乘数效应和国际货币乘数效应，通过国际货币乘数扩大以后被国外经济体吸收的国际货币转化成非国际货币发行国的外汇储备，再利用借出货币的方式回流到国际货币发行国债券市场。这样，某种国际货币发行越多，非国际货币发行国对此种货币资产的刚性需求越大，就越容易出现货币替代效应，引起全球货币需求不稳定（麦金农，1982）。

二是特里芬难题。特里芬难题是指经常性账户赤字与汇率稳定之间的矛盾。货币是财富的表现形式，多国博弈采用 QE，而 QE 不需要经常性账户赤字，也可以增加国际流动性，导致全球流动性过剩，信用货币币值的不确定性和不稳定性增大。币值不稳定导致财富再分配，各国实行以邻为壑的汇率政策，竞争性货币贬值，出现国际货币发行国之间的“囚徒困境”，货币信用受损。而较早退出 QE 的国家主权货币相对其他未退出 QE 国际货币升值，抑制出

口，QE 面临退出的合作困境。

三是缺乏国际协调机制。每个国际货币发行国都有货币发行权，缺乏国际协调机制，全球流动性过剩，聚集通货膨胀风险却很难找到明确的责任人。QE 导致国际货币发行国降低基准利率，实际利率较低。同时，全球缺少高信用等级资产，量化宽松产生托宾效果即货币与资产的替代效果，通过资产价格上涨带动经济增长。QE 是缺乏规则的相机决策，政策效果具有短期性，出现决策与政策效果的动态不一致，金融资产投机易诱发资产价格偏高，甚至泡沫，积累金融风险。如果全球产业链紧密，汇率体系缺乏完全弹性，全球产出缺口不大，某个国际货币发行国国内产出缺口很大，会增加全球流动性供给（姚余栋，2013）。

在多元主权货币体系下，人类至今一直没有找到可信的“锚”。比特币未来 100 多年内最大货币存量为 2100 万个，形成“锚”。比特币热潮说明各国对国际货币“锚”的渴求，需要建立一个管理全球流动性的“锚”（姚余栋，2013），对国际货币供给实行硬约束。同时，QE 导致通货膨胀，主权货币价值尺度的“度”不准确，媒介物品交换困难，储存价值的功能弱化，社会和个人财富在银行信用泡沫中被侵吞，信任成为主权货币最根本的问题。比特币的供给量不依赖于中央银行的支持或者金融机构的信用担保，避免了货币超发和汇率操控，解决了信任问题，更为安全公正，可能会出现比特币部分替代主权货币的情况。

凯恩斯强调需求管理，没有对供给方面进行结构性改革。弗里德曼的货币数量论设想用一个自动化系统取代中央银行，以稳定的速度增加货币供应量，消除通胀。20 世纪初，奥地利经济学家哈耶克在《货币的非国家化》（Denationalization of Money）中第一次完整论述了一种非主权货币的构想：政府不应该控制货币发行，允许私人自由竞争产生货币。当前需求不足，供给方失调，国际货币体系改革的主要内容应该实行包括量化宽松的需求管理转向供给方面改革，以供给管理为主、需求管理配合，管理全球流动性“总闸门”，为向非主权货币过渡创造条件。

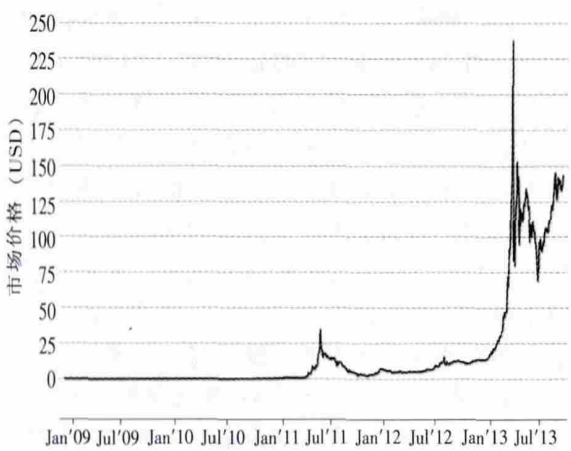
四、比特币发展现状与面临的问题

比特币成为一种逐渐向大众流动的货币，越来越和现实世界交汇。从投资比特币本身，到比特币进入支付环节，再到比特币相关的经济活动，比特币全新的交易模式、产业模式繁荣了比特币经济。

（一）比特币带动全新交易模式、产业模式

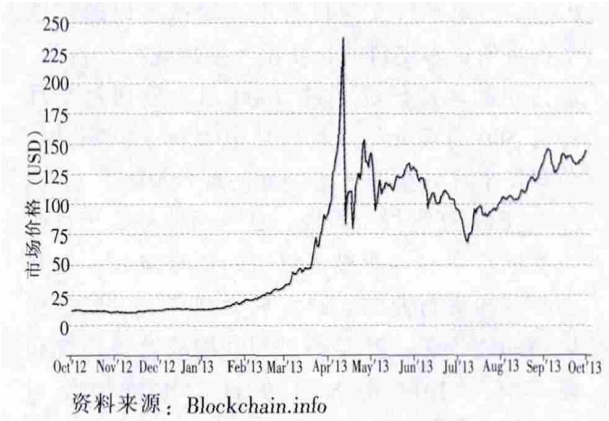
1.比特币成为新型投资品

比特币开始的几年价值被低估，2010 年 4 月 25 日，比特币首次公开交易，1BTC 市场价格 0.03 美元，到 2012 年 10 月，1BTC 市场价格一直没有超过 15 美元（见图 2）。2013 年 1 月 1BTC 市场价格从 15 美元开始暴涨，3 月 10 日，流通中的比特币为 1087 万，总市值 5 亿多美元，拥有人数仅几十万人（中国持有量全球第四），与 10 亿互联网的用户基数相比，平均每百人可获得一个比特币，比特币持有者信心增强（屈丽丽，2013），需求增速快于供给，投资热潮膨胀。4 月 10 日比特币大幅升值至 266 美元，4 月 11 日比特币兑美元汇率跌至 150，一日贬值逾 40%。7 月 10 日，比特币兑美元汇率回归理性，1BTC 价格 76.83 美元，9 月 30 日 1BTC 价格 142.11 美元（见图 3），总市值超过 15 亿美元，流通中的比特币接近 1175 万（见图 4）。



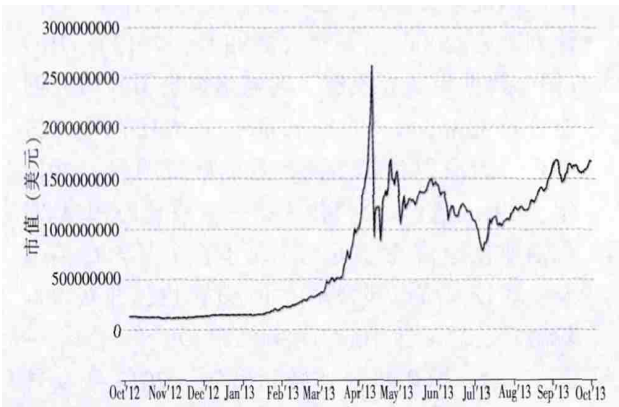
资料来源：Blockchain.info

图 2　2009 年 1 月–2013 年 9 月
比特币市场价格变化（美元）



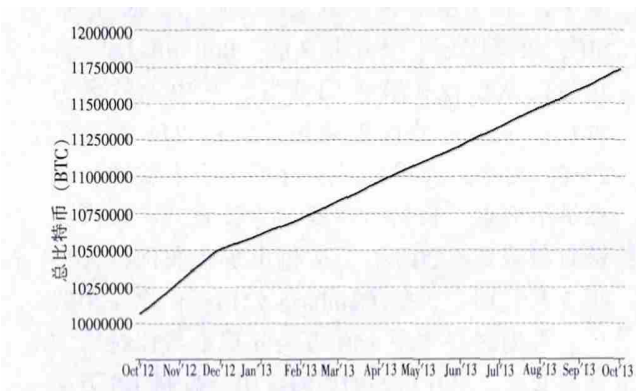
资料来源：Blockchain.info

图 3　2012 年 10 月–2013 年 9 月
比特币市场价格变化（美元）



资料来源：Blockchain.info

图 4　2012 年 10 月–2013 年 9 月
比特币市值变化（美元）



资料来源：Blockchain.info

图 5　2012 年 10 月–2013 年 9 月
流通中的总比特币数量（个）

比特币处于增长趋势中，这股比特币热潮源于三方面：一是塞浦路斯银行挤兑风潮。2013 年 3 月 16 日，塞浦路斯为获得欧盟的进一步援助，提议通过对每个银行存款账户征税，筹集 58 亿欧元的法案，消息一出塞浦路斯储户涌向银行挤兑。比特币成为储户规避税收、实现财富保值增值的方式。2013 年 7 月，塞浦路斯政府为获取储户的信任，以比特币代替本国货币，在塞浦路斯各大银行 ATM 机旁设置了世界上第一款比特币 ATM 机，提供以现金直接兑换比特币的业务。二是比特币政策风险降低。2013 年 3 月，美国货币监管委员会正式将比特币纳入了监管范围（李想，2013）。5 月 30 日，Mt.Gox 宣布将加强鉴定程序，所有的用户账户经过验证之后才能储存和提取真实货币，交易规范化。6 月 27 日，德国议会决定对持有比特币一年以上的将予以免税。8 月 20 日，比特币被德国财政部认定为记账单位，成为一种在德国银行业条例下的金融工具，与“私人货币”更接近，可以用来多边结算，意味着比特币在德国已被视为合法货币（严湘君，2013）。6 月 28 日，Mt.Gox 获得美国财政部金融犯罪执法系统 FinCEN 颁发的货币服务事务（MSB）许可，这一历史性事件说明比特币已经被美国官方作为“货币”对待。[①]三是流动性过剩。2013 年是比特币供给量每四年减半的开始点，也是投资比特币的敏感时间窗口，在流动性过剩背景下，有更多追逐新产品的流动资金，一些投资者把比特币作为全新金融投资渠道。

2.比特币改变了居民消费模式

作为新的购买商品和服务的支付手段，比特币消费表现在：（1）游戏充值。如 Facebook 的游戏 Minesweeper 中使用。（2）购买网络服务。如程序员群体中用比特币换取服务、VoIP 网络电话服务 Lightbox Technologies Inc。（3）购买实物。目前比特币可以在近 30 家网站上购买物品，接受比特币的供应商数量包括网上和线下的供应商。比如，2012 年 10 月，已有超过 1000 家商户通过比特币支付公司 Bitpay 的支付系统接收比特币付款。2012 年 11 月

[①]在美国，比特币作为一种以货币为基础的服务项目，很难用固定的商品或外汇来衡量、判断，在交易性和商品性之间游移不定，还不是真正的货币。

WordPress 宣布接受比特币付款。[①]eBay 上排名第 13 位的书店 Qugelmatic Books 接受比特币。德国一些主要城市的商业街支持比特币的支付，芬兰公司用比特币给员工支付工资。在我国一些城市，比特币已经进入日常生活。2013 年 3 月，美国留学生杰克在位于北京市海淀图书城附近的车库咖啡馆，使用 0.012 比特币购买了一杯咖啡。淘宝网有可以消费比特币的商家，在“我要买”网站上可以用比特币来买防 PM2.5 的口罩，有些电信充值的商家允许用比特币给手机充值。

3.产生与比特币相关的新型产业

除投资比特币本身外，围绕比特币还产生了一系列相关产业和投资品，如比特币交易所、第三方支付平台、新型投资行业、比特币钱包、挖矿机等。

（1）比特币交易所。交易平台 Mt.Gox 每天有大量的比特币进行买卖，交易的最高价、最低价和成交量实时更新。Mt.Gox 比特币与美元的成交汇率是比特币最为主要的参考汇率。此外，出现比特币资讯网站、基于比特币的金融产品和金融交易，如在 mpex、btct 上发行的各种比特币公司的股票，比特币论坛 IPO 发行的股票等。不少比特币论坛 IPO 发行的股票以周为单位进行分红，分红丰厚。目前，我国已经发起一只基金总额为 2000 万元的封闭型比特币投资基金，比特币的期货和股票市场也在建成和完善之中。

中国比较活跃的比特币交易平台 btcchina.com 平台日均成交量 6000 个比特币以上，成交金额 600 万元以上。2013 年 10 月 1 日，btcchina.com1BTC 市场最高价 777.80 元人民币。[②]中国比特币的投资偏重于投机，投资者通过交易平台的手续费获得利润。平台规定，双向收取 0.3%的手续费。2013 年 4 月 25 日，当天成交量约 9400 个比特币，1 个比特币成交均价为 940 元。9400×0.3%×2×940=5.2 万多元手续费，搭建成本几十万元的平台，仅交易手续费一年收益就达上千万元。

（2）第三方支付平台。消费者可以通过 Bitpay 公司平台支付比特币，商家可以通过该平台将消费者支付的比特币转换成现金。目前，该公司的客户已经超过 7000 名，公司每个月进行 500 万美元的交易，从中收取 1%的费用，公司每个月可获得 5 万美元的现金报酬。

（3）新型投资行业。比特币业务处于行业投资期。一些专业投资机构的资金流入，填补了某些投资行业的空缺，成为现有金融服务提供商的竞争者，甚至通过互联网战胜了传统利益群体。2013 年 5 月 9 日，比特币公司 Coinbase 获得了投资基金 Union Square Ventures 的 500 万美元 A 轮投资；7 月 2 日，文克莱沃斯比特币信托基金（Winklevoss Bitcoin Trust）向美国证券交易委员会（SEC）提交 IPO 申请，计划融资 2000 万美元（严湘君，2013）。IDG（国际数据集团）投资了两家虚拟货币领域的创业公司 Coinbase 和 Opencoin。各大比特币交易平台开始取得各界不同产业的融资项目。2013 年，BitcoinATM 公司作为第一家将比特币 ATM 机商业化运营的公司，计划 3–6 个月内在美国及全球较大城市部署比特币 ATM 机，并获得首轮融资，总额达 100 万–300 万美元。

（4）挖矿机、比特币钱包。2013 年 9 月 30 日挖矿困难度为 148,819,199.81，随着挖矿困难度提高，对挖矿机的精密度要求也越来越高。2009 年比特币刚出现时，普通电脑通过运行 CPU 挖矿，2011 年、2012 年需要高效率的显卡，2013 年 2 月，研发出专业挖矿芯片 A-SIC，效率比显卡提升上百倍。Butterfly Labs 公司专门从事挖矿软件的开发，其中一款名为 Bitforce miners 的挖矿软件报价在 274 美元至 23000 美元，公司已经发行了上千个软件，仍然供不应求。目前，以我国为代表的矿机产业链日益成熟，20%的挖矿机出现在我国。2013 年 5 月，旧金山的 Coinbase 公司提供比特币钱包，帮助客户实现 150 万美元现金与比特币的转换交易，从中收取 1%的费用，盈利 1.5 万美元。

（二）比特币发展过程中面临的问题

比特币若要成为真正的货币，必须克服一

[①]肯尼亚、海地和古巴等地区遭受国际支付系统封锁，这一地区的互联网用户可以使用比特币购买商品和服务。

[②]https://btcchina.com/ 2013–10–1

些现实问题，这其中涉及经济、互联网金融、法律、网络技术和信息传播等领域。

1.政府监管

比特币的高度匿名性很可能被用来从事非法交易、洗钱、转移资产、逃税等，政府可能宣布其非法，依靠政治外力将其扼杀。2013 年 3 月 18 日，FinCEN 发布了虚拟货币个人管理条例，首次阐明了虚拟货币所有交易或转移虚拟货币的公司均归类为从事货币服务业务，这些公司必须向政府提供信息，并实施防止洗钱的政策。这项规定导致至少三家北美企业被银行关闭了企业账户，包括纽约比特币交易中心 Bitfloor 公司的账户，其目前仍无法把资金还给客户。5 月 15 日，美国国土安全部发布禁令，责令移动支付服务 Dwolla 关闭 Mt.Gox 的转账支持，冻结 Mt. Gox 拥有的两个银行账户。5 月 28 日，美国国土安全部以涉嫌洗钱和无证经营资金汇划业务取缔了汇兑公司Liberty Reserve 的虚拟货币服务，成为历史上最大的国际洗钱诉讼案，洗钱规模达到 60 亿美元。除此以外，美国商品期货交易委员会（CFTC）、国税局（IRS）和 SEC 主要监管机构都未就比特币监管发表任何官方意见。我国交易平台 btcchina.com 没有 ICP 备案，没有备案的网站可依法关停。若网站公司在国内，网站服务器在国外，我国有关部门也可对该公司进行监管。

2.技术上的安全性

一是比特币用户之间流通的数据量规模庞大，会减缓整个系统的运行速度，危及自身发展。无法修改所有人的节点算法和参数来加快比特币的运行，只有升级所有用户的比特币钱包和相关软件，通过发布补丁才能解决这一问题，但这很难实施。二是黑客攻击。2011–2012 年间发生了至少 4 起较大的黑客事件，涉及金额超过 1000 万美元，导致比特币交易中心 My-Bitcoin 关机，比特币储蓄信托平台（Bitcoin Savings and Trust）关闭，SEC 介入调查（于江，2013）。2011 年 7 月，世界第三大比特币交易中心 Bitomat 记录着 17000BTC（当时约合 22 万美元）的 wallet.dat 文件的访问权限丢失，决定出售服务以弥补用户损失。三是网络故障。2013 年 4 月 10 日，Mt.Gox 软件发生故障，引发大批用户恐慌，比特币交易出现大幅盘整。四是缺乏有效监测网络交易技术。交易平台没有经过相关部门的资质审查，交易者无需进行客户身份识别。在我国只需注册一个用户名，将资金转给中间人的支付宝账户，由中间人将交易者的资金转到交易平台，中间人凭自律帮助交易者完成交易，从中收取 5‰的手续费。由于缺乏有效监测技术，出现了中间人将交易者资金卷走的风险。

3.高额交易风险

比特币交易量小、筹码少，比特币市场价格容易受到庄家控制，出现暴涨暴跌。同时，比特币交易平台 24 小时开放，没有涨跌停限制，很难把握最佳的入市时机，交易风险高于公司证券。

4.高额的获取成本

目前，挖矿需要一台高配置专业挖矿机，市场价格 30 万元人民币。使用的矿机越先进，参与挖矿的极客越多，需要能量成本、时耗成本也越高。2013 年 9 月 30 日，挖矿电力成本 2,994,794.62 美元，每次挖矿交易成本 12.06 美元。①

5.网络货币的泛滥

受比特币系统启发，相继产生了 Litecoin，DevCoin，NameCoin，PpCoin 等八种类似比特币的新型虚拟货币，它们多数用户量和流通量都很小。DevCoin 主要用于支付开源软件工作者的工资，NameCoin 主要用于域名和网络主机支付流通。未来更多虚拟货币将会展开竞争，可能出现比特币的替代品，也可能出现这类虚拟货币的泛滥发行。

五、结　论

虚拟世界的经济是构建在虚拟货币基础上的，这是虚拟货币存在的价值。虚拟货币在电子商务、虚拟经济中发挥基础性作用，虚拟货币的发展是一个不可逆转的趋势。未来货币的发展趋势是向信用货币体系施加虚拟化的压力，在更广泛的区域货币一体化进程中激发人们通

①http://blockchain.info/zh-cn/stats 2013-9-30

过采用虚拟货币的一些技术和理念不断调整、改进信用货币，建立内部协调机制，降低分散性，更好地适应互联网流通和使用的需要。虚拟货币与实体货币并存，成为货币形态的新发展阶段。虚拟货币在科技进步和监管水平提高的促进下逐步成长，每个人或企业都拥有虚拟货币账户，有完备的虚拟货币交易所，不同社区之间虚拟货币可以互相兑换，货币终将变得透明、公平和简单，国际金融体系更加协调、稳定。

比特币是一种全新的无政府虚拟货币，代表数字货币的革新，体现世界政治经济全球化思潮，具备一定的革命性；通过算法控制供给量的做法，具有开创性，将深刻影响金融业；比特币是人们突破地域限制的一种尝试，可靠的电子支付系统的构想为未来的虚拟货币系统的设计提供了经验。

比特币已参与实体经济活动，用于衡量最终用法定货币交易的商品价值，与法定货币可自由兑换，出现比特币股票、基金等金融资产，成为现有货币体系的有益补充。欧洲央行在2012年10月29日发布的《虚拟货币架构》(Virtual Currency Schemes)报告认为，如果虚拟货币的货币创造（money creation）继续处于一个低水平，就不足以对价格稳定构成威胁。目前比特币和经济联系有限，只在一定范围内少量流通，实现流通和支付手段的功能不可能无限扩大，不会冲击金融秩序，危害金融稳定。因此，要从货币嬗变角度规制互联网金融业，既包容创新又确保监管到位，促进其重要社会价值的实现。如果比特币用户庞大，介入实体经济活动创造体系外的M_1、M_2，出现货币替代，产生挤出效应，影响法定货币的流动速度，将会对货币政策与金融稳定形成影响。在这种情况下，需要采取以下措施加强互联网金融的有序竞争。

第一，完善互联网金融监管体系，建立监管协调合作机制。一是明确监管部门的监管职责，将比特币纳入监管范围，构建完善的监管体系。二是推出比特币大型综合交易平台，对比特币交易进行监测，与传统金融行业对接，推动比特币行业的有序化、合法化。三是互联网金融具有跨行业、跨市场的特征，各个部门需要建立金融协调机制。四是信息技术部门要加大网络信息安全的投入，设计比特币评估、表征、簿记、验证等技术环节，设计比特币公钥等监管基础设施，保证国家的金融安全和金融秩序。

第二，完善互联网金融法律制度。用户个人财产安全的法律至为关键。互联网通过用户协议将互联网隐私界定为可以追溯和识别个人身份的基础信息，用实践强行统一了隐私权的标准。这是适应信息技术发展的一种进步，取消了传统空间隐私权的地位。应出台相应的法律保护制度，未经用户许可不得向第三方出售或转让用户隐私，防范利用比特币盗窃、买卖个人财产、洗钱、逃税等犯罪活动，维护其信誉。

第三，建立互联网金融教育的长效机制。中国人民银行金融消费权益保护局需要针对目标群体，把互联网知识和金融知识结合起来，通过多样化的教育模式，建立金融消费者教育的长效机制，提高金融消费者风险意识和自我保护能力。中国人民银行已经开通上海、武汉和西安的金融消费权益保护咨询投诉电话，将来还需要开发网络投诉渠道，畅通互联网金融消费的投诉受理渠道，保护金融消费权益。

（责任编辑　武　岩）

参考文献：

[1] 程实. 货币大动荡预示金融生态加速质变[N]. 上海证券报，2013-4-12

[2] 崔屹东，郑晓彤. 对新型货币比特币的经济学分析[J]. 现代经济信息，2012（16）：8

[3] 哈耶克著，姚仲秋译. 货币的非国家化（第一版）[M]. 北京:新星出版社，2007

[4] 贺艳燕. 数字货币：一种新货币形式[N]. 上海证券报，2013-4-15

[5] 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，2011（10）：61-63

[6] 黄达. 金融学（第三版）[M]. 北京:中国人民大学出版社，2013

[7] 黄金萍. 比特币，史上最危险的货币？[N]. 南方周末，2011-7 -7

[8] 柯白玮. 比特币的实验[N]. 东方早报，2013-6-4

[9] 李想，毛佳楠. 来自塞浦路斯的诱惑—虚拟货币浪潮来袭[N]. 中国经营报，2013-7-15

[10] 屈丽丽. “淘金”比特币[N]. 中国经营报，2013-7-15

[11] 严湘君. 全球首只比特币 ETF 筹备上市[N]. 第一财经日报，2013-7-3

[12] 严湘君. 比特币被德国财政部认可,兑美元汇率触及 123 高点 [EB/OL]. http://www.yicai.com/news/2013/08/2953335.html，2013-8-20

[13] 姚余栋. 关于建立“新布雷顿森林体系”的初步建议[N]. 第一财经日报，2013-5-6

[14] 于江. 新型货币“比特币”：产生、原理与发展[J]. 吉林金融研究，2013（5）：17-23

[15] 郑书雯，范磊. 基于 P2P 网络 Bitcoin 虚拟货币的信用模型[J]. 信息安全与通信保密，2012（3）：73-75

[16] 郑书雯. P2P 网络基于 Bitcoin 虚拟货币的信用模型[D]. 上海交通大学，2012

[17] 周寿英. 比特币走向幻灭[N]. 中国计算机报，2013-4-22

[18] Garcia Flavio D，Hoepman Jaap-Henk. Applied Cryptography and Network Security [M]. Heidelberg：Springer Berlin，2005：271-287

[19] Peserico E. P2P Economies [C]. Computer Communication Review. United States：Proceedings of the ACM Special Interest Group on Data Communication（SIGCOMM），2006

Abstract: Bitcoin is a kind of pure P2P virtual currency and can meet the possible requirement of decentralization. It may help strictly control the speed of money supply, predict the total amount of money in circulation and effectively contain inflation. Bitcoin basically has the function of currency and part of the currency features, but it is not the real currency. Whether bitcoin can be transferred into the real currency depends upon the trust and confidence people have in the currency and the whole mechanism. Based upon this, the paper analyses the real problems for bitcoin to become a real currency, covering the fields of economy, internet finance, law, web technology and information spreading, and etc,. Finally the paper concludes that bitcoin, representing a totally new anarchy virtual currency, an innovation of digital currency, and the global integration of politics and economy, has certain revolutionary nature.

Keywords: Bitcoin; P2P; Digital Currency; Traditional Currency