RCIF
Research Center for International Finance
中国社会科学院世界经济与政治研究所国际金融研究中心

Working Paper No. 2014W06

Feb. 17, 2014
www.rcif.org.cn

杨晓晨
morn.yang@gmail.com
张　明
zhangming@cass.org.cn

# 比特币：运行原理、典型特征与前景展望

**摘要：**本文通过对比特币运行原理的阐述，剖析了比特币的典型特征，并展望了比特币的可能前景。首先，作为货币发展史上的重大革新，比特币在设计中使用的一系列创新思想和方式是值得借鉴的。它的出现是解决当前国别货币面临问题的积极尝试；其次，由于比特币在寻求以创新途径解决问题的同时，引入了一些难以调和且致命的新问题，导致市场对目前形式的比特币能否持续发展持怀疑态度；再次，比特币的发展前景取决于其自身能否顺利完成转型。无论是在比特币之上建立其他应用层级，还是将比特币作为全球货币体系改革的一个组件，都需要对它进行重新审视和设计。如果设计更为合理，且在实施过程中能更好地协调各方利益，比特币的发展前景虽然路途遥远，但值得世人期待。

**关键词：**比特币　运行原理　典型特征　前景展望

## 一、引言

比特币最初起源于中本聪（Satoshi Nakamoto）在 2008 年题为《比特币：一种点对点的电子现金系统》的论文（Nakamoto，2008）。在此文中，作者描述了一种完全基于点对点（Point to Point，P2P）的电子现金系统，该系统使得全部支付都可以由交易双方直接进行，完全摆脱了通过第三方中介（例如商业银行）的传统支付模式，从而创造了一种全新的货币体系。

最初，比特币只是作为密码学的创新尝试在一小群极客之间传播，并没有人愿意用现有货币与其进行兑换。经过几年的发展，比特币逐渐进入大众视野，越来越多的商家开始接受比特币。从 2011 年起，随着一系列交易市场的建立，比特币的价格也开始迅速攀升。截至 2013 年 11 月底，比特币的价格一度达到每单位 1200 美元，而其人民币价格也突破了每单位 7000 元。

比特币实行 7*24 的全天候交易，而且没有涨跌幅限制，以至于其价格在一天之内的浮动幅度就可以达到数千人民币。因此，中国人民银行等五部委联合下发了《关于防范比特币风险的通知》，不承认比特币的货币属性，不允许其作为货币在市场上流通。但与此同时，以美国和德国为代表的一些国家对比特币却持有相对乐观的态度，并明确表态愿意接受比特币。不同国家为何对一个新兴货币概念持有不同的态度呢？这背后的深层次原因值得探讨。

目前国内外关于比特币的学术文章很少，而且大多集中于技术领域，经济学文献非常有限。Woo 等（2013）讨论了比特币的内在价值，并对比特币的未来持乐观态度。但与此同时，他们也指出，市场投机行为可能造成比特币的汇率大起大落，从而影响其被社会接受的程度。Yermack （2013）的研究表明，一方面，比特币的每日汇率走势与其他主要货币汇率走势没有相关性，使得比特币无法用于风险管理目的，以及比特币的持有者也很难对比特币持有头寸进行套期保值；另一方面，比特币无法用来为消费信贷或其他贷款合同计价，也难以被纳入具有存款保险特征的银行体系。因此，比特币与其说是一种货币，不如说是一种投机性工具。Šurda（2012）从奥地利学派的角度出发，对比特币进行了理论和实证分析，尤其是对比特币的概念与归类进行了深入探讨。Jacobs（2011）和 Grinberg（2012）对比特币的相关法律问题进行了分析，他们均认为比特币面临较大的法律风险。

比特币虽然比较特殊，但依然可以归于电子货币的类别。Marimon （2003）把电子货币视为央行发行货币的有力竞争者。他建立的模型显示，电子货币有助于降低通

货膨胀，以及促进央行货币政策的稳定性。Lotz 与 Vasselin（2013）对纸币和电子货币的相互替代性进行了研究。其模型指出，电子货币取代纸币的必要条件是相关设备（如 POS 机）的购置成本和使用成本足够低，或者持有纸币的风险与电子货币相比足够高。

有学者认为，电子货币的发展为新兴市场国家与发展中国家带来了独特的机遇和挑战。Bassey（2008）指出，电子货币可以加速非洲大陆的发展速度，是非洲在新时期与其他国家保持同步发展的关键。Jack 等（2010）以肯尼亚的电子货币为例，指出电子货币在流动性管理方面面临与传统货币相似的问题。Cassoni 与 Ramada（2013）对乌拉圭电子货币的研究表明，电子货币的使用可以通过促进区内资金流动来增强区域经济活力。周光友（2010）通过对中国电子货币的实证研究，证明电子货币不仅会在形式上替代 M1，而且会改变货币的供给结构、模糊各类金融资产之间的界限。以上四篇文献均在不同程度上提到，电子货币是对央行控制基础货币能力的重大挑战。电子货币可持续发展的前提是政府能够同步提升金融监管能力。这对金融监管水平相对落后的国家而言无疑构成了重大挑战。

本文首先从技术角度阐明比特币的运行原理，然后对比特币进行经济学分析。由于比特币与之前任何货币相比都存在很大差异，且比特币的精华之处也恰好包含在其算法设计中，因此了解其运行原理就变得十分必要。本文剩余部分的结构安排如下：第二部分介绍比特币的运行原理；第三部分从货币的定义出发，探讨比特币作为货币的优缺点，并利用相关数据进行实证分析；第四部分展望比特币的发展前景；第五部分为结论。

## 二、比特币的运行原理

### 1、重要概念

在介绍比特币的运行原理之前，必须首先厘清以下六个重要的基本概念：散列、工作量证明、公开密钥密码体系、交易、区块与挖矿。

**（1）散列（Hash）**

在计算机科学中，Hash 通常被翻译为“散列”。散列函数的功能是将任意长度的不同信息（例如数字、文本或其他信息）转化为长度相等但内容不同的二进制数列（由 0 和 1 组成）。以比特币采用的 SHA256 为例，任意长度的信息输入通过这个函数都可以转换成一组长度为 256 个的二进制数字，以便统一的存储和识别。256 个 0 或 1 最

多可以组合成 $2^{256}$ 个不同的数，这个庞大的集合能够满足与比特币相关的任何标记需要。此外，任意两个不同的信息输入，想要通过 SHA256 产生相同数字输出的概率，可以说微乎其微。因为输入信息的微小变动将会导致输出数字的巨大变化。这就保证了输入信息与输出数字的一一对应。最后，散列还有一个重要特征 ，即想要通过输出数字来反推出输入信息，这是极其困难的。因此，如果想要生成一个特殊的输出数字，就只能通过随机尝试的办法逐个进行正向运算，而不能由输出结果逆向推出输入信息。这个特征是比特币能够顺利运行的重要基石。

**（2）工作量证明（Proof-of-Work）**

倾注了更多更复杂劳动的事物具有更高的价值，这是比特币运行的哲学基础。让我们先以防范垃圾邮件为例来说明什么是工作量证明。不妨做出如下假定，即如果一个人愿意花 10 分钟写一封邮件，他就不会在意再多花一分钟对其进行处理，以证明自己写邮件付出的努力是真实的。而对垃圾邮件的传播者而言，每封邮件都要多花一分钟才能发送，这是完全不能接受的。因此我们可以设立以下规则，即在每次发送邮件之前都要算出一个随机数，以至于将这个随机数和邮件内容一起输入 SHA256 散列函数时，得到的 256 位二进制数的前 10 位均为 0。如前所述，我们无法预先选择一个前十位为 0 的数，并利用 SHA256 算法反推出这个随机数是什么。唯一可行的办法只能是随机抽取一个数，将其和邮件内容放入 SHA256 中进行计算，看结果是否满足要求。如果不满足，就换一个随机数继续进行尝试，直到要求满足为止。只要我们设定的要求足够简单（要求全为 0 的个数不太多），那么寻找这个随机数的过程也就比较简单，只不过要花去一定的时间（例如几秒或几分钟）。对于真实的邮件而言，为了证明自身价值，付出少量时间进行计算是值得的。但对于垃圾邮件而言，这将导致邮件发送者的时间成本急剧上升。因此，上述机制的引入将会显著减少垃圾邮件的产生。对比特币而言，挖矿（Mining）也是使用随机数进行工作量证明的过程。这种过程虽然从表面上来看没有产生任何价值，但却是解决互联网中信任问题的有效办法，是在不可靠的网络环境中一种较为可靠的信用证明。

**（3）公开密钥密码体系**

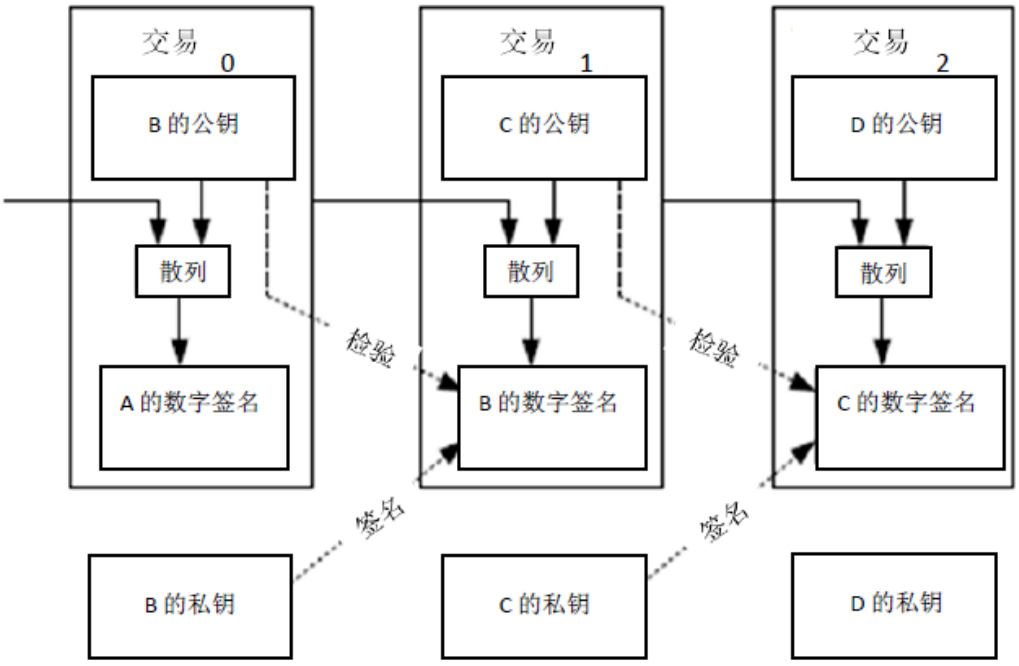
该体系简称公钥体系。在信息传递过程中，发送方通过一把密钥将信息加密，接收方在收到信息后，再通过配对的另一把密钥对信息进行解密，这就保证了信息传递过程的私密性与安全性。而密钥无非是一组数字，通过将原始信息与这组数字放在一起进行特定运算，就能够把信息转换为另外一种格式，从而实现加密。解密过程则刚

好相反。在大多数情况下，一组密钥由公钥和私钥组成。私钥由自己保存，公钥则需要向其他人公开。在信息传递过程中，公钥和私钥相互配合，既能够对持有私钥的发信人进行身份验证，也能够确保发信人对自己发出的信息不能抵赖，还能够保证收发信息的完整性、防止中间环节被截获篡改。如果公钥丢失，还可以通过私钥进行恢复。但试图通过公钥反推出私钥的努力，从理论上来讲是基本不可行的，这就保证了私钥的私密性。

**（4）交易（Transactions）**

交易是指一个用户用比特币向另一个用户进行支付的过程。不过，比特币的交易并非简单的支付货币本身。以图 1 中的交易 1 为例，如果 B 想支付 100 个比特币（100BTC）给 C，那么 B 不仅需要在交易单上注明金额，而且需要注明这 100 个比特币的来源。如图 1 所示，B 的 100BTC 其实来自 A，是 B 通过交易 0 得到的（交易 0 已经通过了全网用户的认证，保存在所有用户的电脑中）。为完成交易 1，B 需要在交易单上填写的信息包括：一是 100BTC 的来源，此处为交易单 0 的 ID；二是 C 的公钥，也即 C 的比特币收款地址；三是将交易单 0 的内容和 C 的公钥输入散列函数，得到一串数字。B 用自己的私钥加密这串数字，作为数字签名放在交易单 1 中。C 在收到交易单 1 之后，可以通过其中存放的 ID 找到交易单 0，并获取 B 的公钥。C 可以使用该公钥对交易单 1 中的数字签名进行解密。与此同时，C 可以把自己的公钥和交易单 0 的内容，按照同样的方式输入散列函数，并将得到的数字与数字签名解密的结果进行比对。如果比对成功，就可以确定如下两个事实：其一，100BTC 的来源属实。因为交易单 0 中包含了 A 的签名，且交易单 0 是经过全网认证过的，即 A 确实将 100BTC 给了 B；其二，交易 1 的确是经由 B 签署的。由于 B 的私钥是唯一的，他无法抵赖这单交易。

**图 1 比特币交易过程**




资料来源：Nakamoto（2008），笔者进行了一定修改。

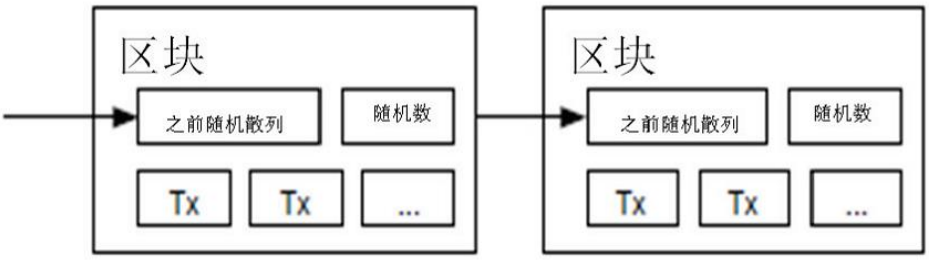
上述过程略显复杂。我们可以换一种不太精确但更容易理解的解释（姚勇，2013）。依然以交易 1 为例，交易单 1 中其实包含以下六种信息：一是交易单 1 的 ID；二是资金的来源，即交易单 0 的 ID；三是 A 对资金的签名，以证明是他把 100BTC 给 B 的；四是资金的去向，即 C 的账号（公钥）；五是资金的数额，即 100 BTC；六是 B 的签名（即 B 用自己私钥进行的数字签名），以证明是他自己签发的交易。由于每笔交易单都记录了该笔资金的前一个拥有者、当前拥有者以及后一个拥有者，我们就可以依据交易单实现对资金的全程追溯。这也是比特币的典型特征之一。最后，当每一笔交易完成时，系统都会向全网进行广播，告诉所有用户这笔交易的实施。

**（5）区块（Block）**

交易和区块的关系，就如同水和瓶子，属于内容和容器的关系。由于每笔交易是相对分散的，为了更好地统计交易，比特币系统创造了区块这一概念。每个区块均包含以下三种要素：一是本区块的 ID（散列）；二是若干交易单；三是前一个区块的 ID（散列）。比特币系统大约每十分钟创建一个区块，其中包含了这段时间里全球范围内发生的所有交易。每个区块中也包含了前一个区块的 ID，这种设计使得每个区块都能找到其前一个节点，如此可一直倒推至起始节点，从而形成了一条完整的交易链条

（图 2）。因此，从比特币的诞生之日起，全网就形成一条唯一的主区块链（Block Chain），其中记录了从比特币诞生以来的所有交易记录，并以每十分钟新增一个节点的速度无限扩展。这条主区块链在每添加一个节点后，都会向全网广播，从而使得每台参与比特币交易的电脑上都有一份拷贝。在现实世界里，每笔非现金交易都由银行系统进行记录，一旦银行计算机网络崩溃，所有数据都会遗失。而在互联网世界里，比特币的所有交易记录都保存在全球无数台计算机中，只要全球有一台装有比特币程序的计算机还能工作，这条主区块链就可以被完整地读取。如此高度分散化的交易信息存储，使得比特币主区块链完全遗失的可能性变得微乎其微。

**图 2 区块链的局部结构**




资料来源：Nakamoto（2008）。

**（6）挖矿（Mining）**

如前所述，比特币的所有交易记录都保存在主区块链中。每十分钟就会有一个新区块生成并加入进主区块链，这个新区块中记录了十分钟内全网的所有交易。由于比特币使用的是 P2P 模式，这意味着网络上的每个节点都是平等的，没有一个中心节点可以用来承担交易记录工作。因此，如此重要的交易记录任务交给谁来完成，就变成一个现实问题。而比特币创始人中本聪给出的答案居然是任何人来完成都可以。由于每笔交易完成后都会被广播给全网，因此每个人在对交易的有效性进行验证后，都可以根据这些交易数据生成新区块。但这又引发了一个新问题，即如何让所有人都信任由一个陌生人生成的新区块？这个新区块中是否记录了虚假交易或重复交易？

要解决这个问题，就要用到前文提到的工作量证明概念。基本思路是，寻找一个随机数，使得将这个数字与新区块的交易信息一起输入 SHA256 后产生的数字，前面 n 位（比如 n=100）都是 0。此项工作的意义在于，由于将会耗费很多时间，如果一个人进行了这项计算且获得成功，那么他提供的区块很可能是真实可信的，因为花费如此大力气作假得到的好处，远远不计花费同样努力从事真实工作得到的好处。此外，

其他所有节点在接收到新区块时，也会对其中包含交易的有效性进行校验，这意味着虚假交易或重复交易很难骗过其他所有用户，这就形成了节点之间的信用保障机制。

挖矿（Mining）就是指产生新区块并计算随机数的过程。具体过程可分为以下六步：第一步，由于网络上的每台计算机都保存有之前的主区块链，某台计算机以其中最后一个区块的内容为输入，计算一个散列值；第二步，该计算机在接收广播来的交易单并逐笔校验交易的准确性之后，把没有被列入之前区块的那些交易进行组合，并纳入一个新区块；第三步，该计算机任意猜一个随机数，其大小和长度没有限制；第四步，该计算机将第一步至第三步产生的数据作为输入，一起放到 SHA256 散列函数中，计算得到一个长度为 256 的二进制数；第五步，检查这个二进制数的前 n 位是否符合要求；第六步，如果该二进制数符合要求，则本轮游戏结束，该计算机会把新区块连同这个幸运随机数一起广播给网络上的其他计算机。其他人在收到这个新区块后，会以同样的方式进行校验。如果结果无误，全网就接受这个新区块，将它连同之前的主区块链一起保存。如果产生的随机数不合要求，则第二步至第六步就会重复进行，直到自己成功或者收到别人发来的新区块（姚勇，2013）。

从上述流程中可以看出，挖矿就是指搜集交易数据并建立新区块的过程。这个过程虽然重要，却耗时费力，为什么所有参与者都趋之若鹜呢？最重要的原因在于，比特币系统规定，每个成功建立新区块的人都将获得 50 个新比特币的奖励，且该奖励将被记录在对应的新区块里。这 50 个新比特币是系统自动产生的，且得到全网的认同。有趣的是，这种奖励的数额每四年减半，即 2009 年至 2012 年年为每区块 50 个比特币、2013 年至 2016 年为每区块 25 比特币、2017 年至 2021 年为每区块 12.5 比特币，如此不一而足。最终，全系统的比特币容量将达到 2100 万个的上限，至此不再增加。从那时起，为保证主区块链能继续不断增长以确保比特币交易能继续正常进行，每个创建新区块的人，都将从新区块包含的交易单中抽取一定的“交易税”作为奖励。这种新的激励机制将保证比特币交易得以延续。

## 2、 运行原理

在上述概念的基础上，我们就可以介绍比特币的运行原理了。作为一种脱离了实物交接的货币形式，比特币需要解决如下几个基本问题：首先，谁来发行比特币并对其进行信用背书？其次，如何建立账户并进行管理？再次，比特币交易如何确认？

### （1）发行和信用背书

与美元等国别信用货币不同，没有中央银行负责比特币的发行，也没有政府为其

提供信用背书。比特币的发行是通过挖矿来完成的。每一次有效挖矿都将产生新的比特币，直至达到数量上限。比特币的信用，则源自所有参与比特币挖矿和交易的用户所付出的大量计算，以及由此消耗的时间和电力等成本。人们为此投入的劳动越多，就意味着对比特币的认可程度越高。比特币系统是一种互联网环境下的新型信用体系，它既不需要任何历史信用记录，也不需要任何机构或个人提供的信用担保。换言之，比特币主要依靠理论和技术的双重保障来保证其信用：一方面，人是理性的，在诚实劳动所能获得的报酬远高于欺骗时，没有人会花费力气进行欺骗；第二，比特币的特征决定了欺骗是极其困难的。要成功进行欺骗，不仅需要经受其他所有用户的检验，也需要具有高于全网总计算能力 51%的计算设备。以目前比特币全网累积的计算能力来看，即便是全球最先进的大型计算机距离这一要求也相差甚远。随着越来越多的新增计算力加入，在比特币的世界里，欺骗的难度将变得越来越大。

**（2）账户管理**

账户管理涉及账户的建立、查询和安全保障，比特币也不例外。对比特币而言，建立账户就是生成一个地址。比特币的账户、地址和公钥等概念是基本重合的。账户就是一个地址（一串数字），相当于银行账户的户名，这当然是公开的。地址是由公钥通过一系列数学计算推导出来的，因此地址仅仅是公钥的另一种形式。有了地址，就可以查询比特币账户的余额。

虽然地址类似于银行账户名，但与银行账户不同，该地址的余额并没有特意记录在某个地方。如前所述，每一枚比特币自诞生之日起的所有交易路径都是可追溯的，都被记录在主区块链中。因此，每个账户的余额都可以通过对主区块链进行计算得到，而不需要单独记录。这种设计看似麻烦，但有着明显的优势：首先，每个使用者可以拥有的账户数量是没有限制的。随着比特币使用者的不断增多，账户数量也与日俱增，为每个账户单独保存余额是对存储空间的极大浪费；其次，对比特币而言，没有中央节点来保存并管理余额信息，想要保存余额信息，就必须将其合并写入到区块中。否则，全网节点在对新生成区块的有效性进行检验时，就不仅需要对新的交易进行检验，还需要对全网所有账户的余额进行追溯检验，这无疑会显著增加工作量。在传统银行里，储户不能仅仅通过户名就对账户余额进行查询。然而，比特币世界允许上述操作，也即任何人都可以通过计算主区块链而查询任何账户的余额。比特币账号是完全匿名的，且每个人可以有多个账号，这就保证了比特币拥有者的个人信息不可能通过分析账号来获得。因此，即使将余额信息完全公开，也可以保证拥有者的个人隐私。

比特币账户的安全管理与传统银行系统完全不同。比特币的所有公开信息（例如交易与公钥）都保存在主区块链中，而主区块链在所有运行比特币软件的计算机上都有完整备份，因此其安全管理的关键在于用户私钥的管理。私钥与公钥一样，都是一长串无规律的数字，很难记忆。而且，私钥是独立存在的，不能被公钥或其他方式反推出来。由于私钥是用户对账户所有权的唯一证明，因此用户每次使用账户时都需要使用私钥。为方便起见，很多用户通常选择将私钥放在文件中或网络钱包中保存，这就使得私钥文件面临着被窃取的风险。而一旦私钥遗失或失窃，就意味着比特币账户的彻底丢失。为防范上述风险，“纸钱包”、“脑钱包”等方法正逐渐被接受。毕竟私钥只是一串数字，完全可以通过写在纸上或打印出来的方式进行保存。这种原始的办法在互联网时代反而是一种非常有效的方式。脑钱包的工作原理与纸钱包完全不同。用脑钱包生成私钥之时，我们可将一句话或一幅图片输入特定函数中，就可得到私钥，且这一过程可以反复进行。因此，脑钱包就把记忆私钥的负担转化为记忆一句话或一幅图片，从而显著降低了记忆的难度。即便这句话或这幅图片不慎被公开，他人也很难猜测其真实用途。

**（3）交易确认**

传统银行账户间的交易是由银行负责确认的，通常在几秒钟内就可以完成。但对比特币而言，任何交易都需要得到全网的确认，而且必须最终进入主区块链才能生效。在挖矿过程中，每个节点在收到其他节点发过来的交易后都要进行验证，验证失败的交易被直接丢弃，而有效交易则会进入区块。由于全网在挖矿过程中可能在同一时间段生成很多有效区块，且由于网络时延的存在，不同地理位置的节点产生的有效区块可能包含不同的交易集合。因此最终哪个区块能够成为当前时间段的正式区块而进入主区块链，就成为一个问题。

如果一个节点收到了周边节点发来的两个不同的有效区块，它会将它们都挂在主区块链的最后，形成一个 Y 形分叉。后续收到的区块都会基于这两个区块产生，这使得分叉会继续向后延伸。最终，哪个分叉的长度最先达到要求，就会正式变成主区块链的一部分，而另一条分叉则会被抛弃。由此可见，一个交易从发生到最终确认，需要等待一段时间。通常来讲，在包含这个交易的区块出现之后，还需要等待 5 至 6 个后续区块生成后，才能确认当前区块是否已经正式进入了主区块链。由于每个区块的生成时间大约为十分钟，这意味着一个交易在发生之后，需要等待较长时间才能够得到确认。这既是比特币自身的一大缺陷，也是 P2P 这种全民投票形式难以克服的弊端。

## 三、比特币的典型特征

### 1、比特币的货币性质

我们将从交易媒介、计价单位与储藏手段这三个层面来分析比特币的货币性质。

货币的最基本功能是充当产品或服务的交易媒介。米什金（2011）指出，某种商品要想充当交易媒介，就必须满足以下要求：一是易于标准化；二是必须被普遍接受；三是易于分割，也即容易找零；四是易于携带；五是不会很快腐化变质。不难看出，比特币能够很好地满足上述要求：第一，比特币具有高度的标准化，它仅仅是存在于互联网中的数字，不存在任何种类和品质的差别；第二，尽管比特币目前还没有被全球普遍接受，但比特币在问世仅仅四年左右，就得到全球范围内的高度关注，以及美国、德国、印度、爱尔兰等国家在不同程度上的认可； 第三，目前比特币的最小单位是 0.00000001BTC，几乎没有其他货币可以做到如此精确的分割。事实上，上述最小单位取决于目前的数据结构。随着比特币价值的上升，这一数据结构可以进一步扩展以满足更小的分割需求。另外，由于比特币的非实物性，人们在支付时可以直接对任意小数金额进行支付，而无需找零；第四，比特币非常便于携带。使用者只需保存好个人私钥，就可以在任意一台装有比特币软件的计算机或终端上使用，用户体验类似于使用密码登录网上银行；第五，比特币仅仅是网络上的数字，既不会损耗，也不会变质。

从计价单位的角度来看，尽管目前接受比特币交易的商品种类还相当有限，但由于比特币与现有主要货币之间都存在交易市场与连续报价机制，因此其他货币的计价功能可以间接传导给比特币。

比特币是否能够充当储藏手段，取决于人们能否长期接受比特币。目前比特币具有一定的价值储藏功能，即人们可以把当前获取的收入以比特币的形式保存起来，并留到未来进行消费。然而，如果比特币的价值过度波动的话，就可能严重损害其价值储藏功能。

综上所述，虽然比特币在较大程度上符合货币的特性，但比特币能否充当货币的关键在于人们是否愿意持续使用比特币进行交易。这又取决于比特币与现行货币相比，是否具有富有吸引力的独特优势。

### 2、比特币的典型特征

比特币在设计理念上试图避免现有货币的诸多缺陷，这也是它备受关注的原因。但比特币的全新特征也引发了一系列全新问题。我们将逐一分析比特币的典型特征。

**首先，比特币成功地实现了去中心化的货币发行与管理方式。**现有货币基本上由央行发行，由一国政府用财政实力担保，这种货币发行与管理方式存在如下缺陷：其一，难免存在多种国别货币，各种货币之间通过外汇市场来兑换，显著提高了国际贸易与投资的交易成本；其二，一旦出现一国政权动荡等意外事件，该国政府发行的货币就会面临巨大的信任危机；第三，货币发行的中心化能免会产生特权，由于货币当局能够轻松征收铸币税，这可能引发货币当局短视自利的机会主义行为。相比之下，比特币在设计之时就致力于去中心化。为解决信用问题，一方面，比特币使用了一套密码学算法，使得参与比特币主区块链构建的所有用户都必须付出相当的努力才能证明其信用；另一方面，比特币产生的过程受到全网的监督，要想骗过全网所有其他用户，需要巨大的计算能力。这从技术上而言并不现实。换言之，比特币成功地利用密码学手段，解决了货币在去中心化发行时面临的信任问题，从而使得比特币的发行不需要依赖任何政府或机构，并且与互联网的去中心化特点高度吻合。

**其次，比特币是一种高度匿名化的货币。**其匿名性主要体现在以下三个方面：其一，比特币账号仅仅是一串数字地址，通过它无法得知拥有者的任何信息；其二，比特币账号的生成过程无需任何实名认证，账号拥有者只能通过私钥证明其所有权；其三，同一拥有者的不同账号之间没有任何关联，这意味着其他人无法得知特定用户的全部比特币持有量。然而，比特币的匿名性是一把双刃剑：它虽然通过技术手段保障了个人财产的私密性，但也为洗钱、贩毒等非法交易提供了天然的温床。此外，匿名性的另一个潜在问题是会影响削弱政府的征税能力。当前全球税收体系主要依靠监控银行账户的变动来防止逃税，这是一种基于账户实名制的有效办法。若一旦资金流动完全匿名化，征税的难度将会显著上升。

**再次，比特币交易具有完整的可追溯性。**对任何一枚比特币而言，其从被挖矿生成到当前所经历的全部状态，都被完整地记录在主区块链中。任何特定账户的全部交易也可以被全程追溯。最为重要的是，追溯过程并不需要认证，任何人都可以对任何账号进行查询。这有助于实现全网的互相监督以保障公平透明的市场秩序。

**第四，比特币交易具有不可逆性。**每笔交易只有成功和失败两种状态，而不允许撤销操作。这种设计的初衷是为了防止付款方利用撤销操作来侵害收款方利益，以及防止退款时因需要重新建立信任关系而额外收集个人信息。针对比特币的不可逆性，存在两种截然相反的看法。支持者认为这种设计可以有效地防范信用风险，而反对者认为人难免后悔或犯错，因此不可逆性会降低比特币被广泛接受的程度。

**第五，比特币的最终总量与生产速度都是事先确定的。**如前所述，比特币的生产速度每 4 年减半，并将在最终达到 2100 万个。支持者认为，这种货币发行模式可以防止滥发货币以维护币值稳定。然而反对者的批评包括：其一，比特币的发行速度逐渐下降且不可调整，这将导致持续的且不断强化的通缩压力；其二，比特币增长速度的下降会形成稳定的升值预期，从而导致人们倾向于持有比特币而不是用其进行交易。这会使得比特币的交易数量日益减少、货币的流动性不断下降；其三，比特币的价值逐渐递增，可能会加剧社会分配失衡。因此，总量固定和增速递减对比特币而言既是突出的优势也是致命的弱点。

**第六，比特币面临巨大的融资难题。**无论是直接融资还是间接融资，均需要以借款人的身份和信用信息作为风险评价依据。但对比特币而言，搜集用户信息与其设计理念是相违背的。此外，为降低搜寻交易对象与撮合交易的成本，借贷双方需要依赖银行或债券市场之类的中介机构，这就必然导致中心节点的出现，而中心节点与比特币的设计理念也是不相符的。这意味着尽管比特币融资在技术上是可行的，但这将会破坏比特币的设计初衷。融资难题将成为比特币发展的重大阻力。

**第七，比特币既不存在货币乘数，也无货币政策可言。**既然无法利用比特币融资，这就意味着比特币没有其他货币均拥有的货币乘数。这固然有助于控制通胀，但也导致比特币难以满足市场的流动性需求。此外，比特币也不存在货币政策的概念。比特币的发行无需政府，这从技术上限制了政府可能对其进行的干预。鉴于比特币的特殊性，基准利率、准备金率与公开市场操作等传统货币政策工具对其而言均是无效的。比特币的这一特征虽然能够避免过度的宏观政策波动以及维持币值稳定，但也排除了通过货币政策进行宏观调控的可能性。

**第八，比特币是天然的全球性货币。**比特币既没有国界，也无需兑换。比特币作为全球性货币的积极一面是有助于降低国际贸易与资本流动的交易成本，而消极一面可能加剧局部危机的传染、放大全球的系统性风险。

**3、针对比特币交易数据的初步实证分析**

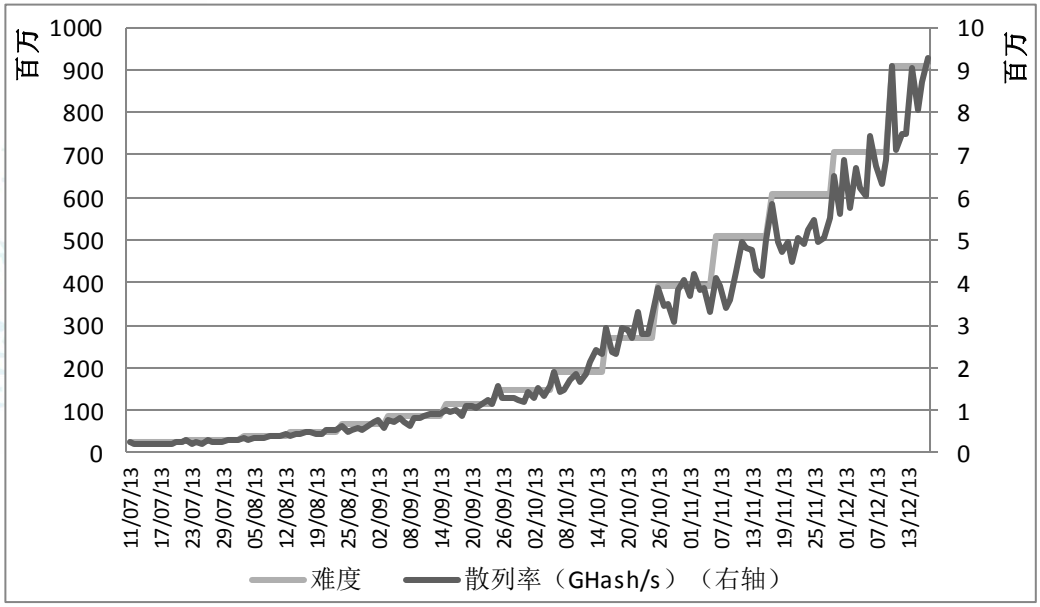
从对比特币典型特征的分析中不难看出，这种货币与传统货币之间存在巨大的差异，以至于经济学中很多典型的货币分析方法对比特币而言并不适用。不过，自比特币诞生之日起，尤其是自 2010 年比特币可以与全球主要货币之间自由兑换以来，各类比特币组织累积了大量的交易数据，我们可以利用这些数据来进行一些初步的实证分析。

**（1）比特币市场价格的决定因素**

比特币的市场价格自 2013 年来呈现出一路飙升态势，从最初的一文不值发展到最高时单位价格突破 1200 美元。有人将比特币的价格上涨归结为市场炒作，但也有人认为这是比特币价值的应有体现。事实上，比特币的市场价格也由供需状况决定。

从供给方来看，获取比特币的源头是挖矿，因此挖矿的成本波动必定会对供给曲线的形状与位置产生影响。图 3 反映了 2013 年 7 月至 12 月期间的全网挖矿难度和运算能力。其中运算能力用散列率表示，代表每秒钟全网进行散列运算的次数。从图中可以看出，随着挖矿者数量的不断增加，全网运算能力显著上升，而运算能力上升的代价是计算机硬件和电力的投入。以 BlockChain 提供的 2013 年 12 月 17 日的数据为例，在当天 24 小时之内，共产生了 5175 个比特币，全网运算能力约为 9,346,953.82 GH/s。目前每 1GHash 运算能力大约需要 650 瓦电力消耗，按照每千瓦时 15 美分计算，产生这 5175 个比特币大约需要耗电 145,812.48 兆瓦时，约合 21,871,871.94 美元。按此计算，每个比特币的生产费用约合 4226 美元。以上仅仅计算了电力消耗成本，还没有考虑计算机的折旧费用。随着全网运算能力的进一步放大，以及考虑到比特币的生产速度每四年减半的特点，比特币的单位开采成本只会越来越大。不过，以上计算的是全网付出的总成本，对每个挖矿者而言，实际成本并没有这么高。因此，在目前比特币单价将近 1000 美元的情况下，挖矿者依然趋之若鹜，说明挖矿依然有利可图。

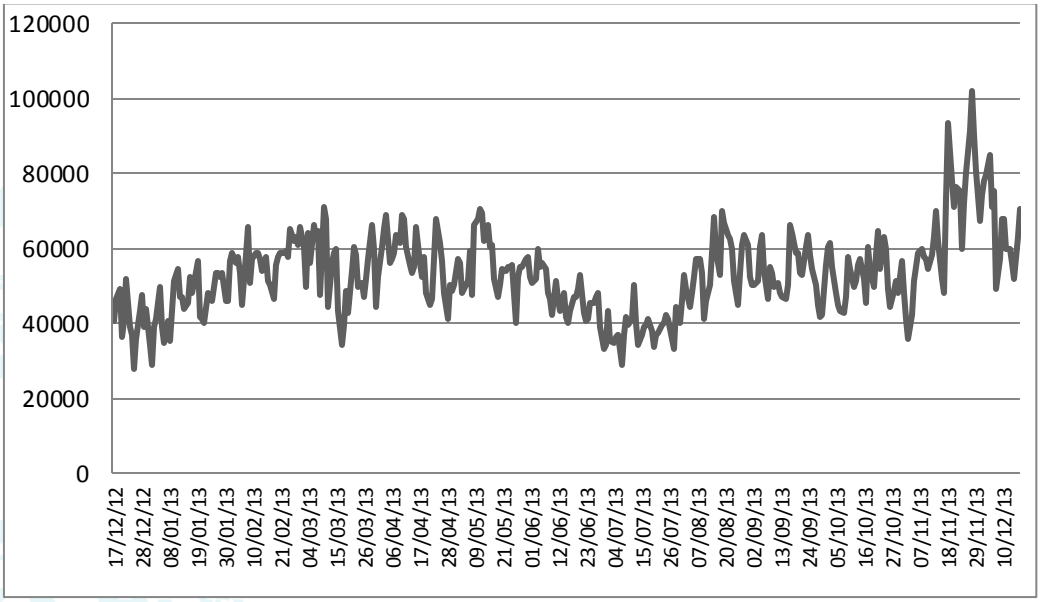
**图 3 挖矿难度**




数据来源：BlockChain。

从需求方来看，目前接受比特币的商家数量还非常有限，因此出于交易目的（而非货币兑换目的）的需求并未呈现出明显的增长态势（图 4）。因此，交易需求并非比特币价格高企的主要原因。

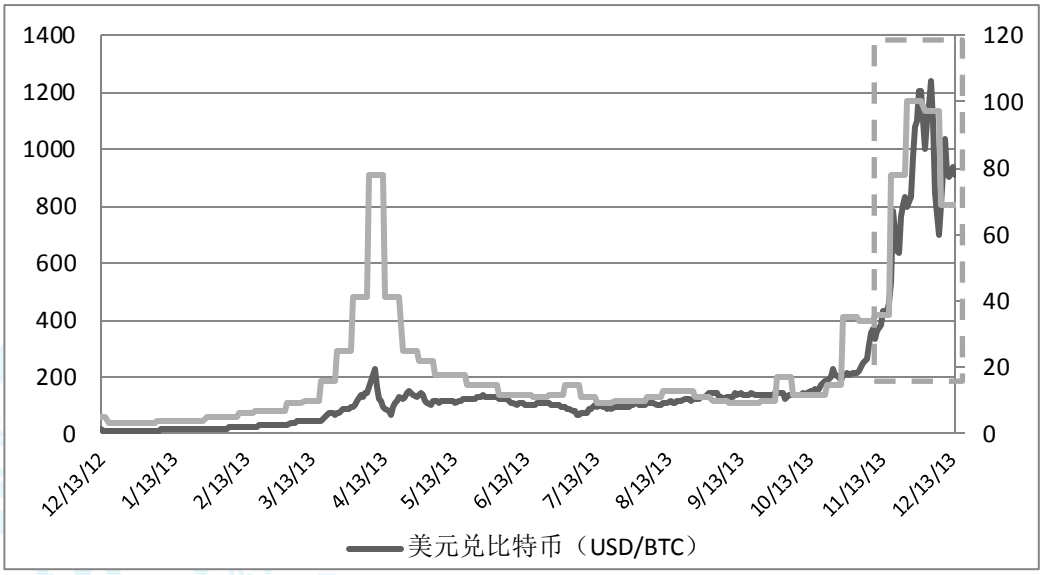
**图 4 比特币日交易次数（交易目的而非兑换目的）**




数据来源：BlockChain。

作为一种天然的稀缺商品，人们对于比特币的价值储藏功能抱有很高期望。为衡量这种期望，我们使用 Google Trends 提供的搜索热度指标代表公众对比特币的关注程度。如图 5 所示，搜索热度与比特币的美元价格走势具有较高的同步性。值得一提的是，2013 年 12 月 5 日，由中国人民银行等五部委联合发文否定比特币的货币属性，造成比特币交易价格在一天内大跌约 50%，而比特币的搜索热度也因此大幅下挫。这说明搜索热度可以大致反映公众对比特币市场前景的预期，因此搜索热度可以被视为反映比特币价格未来走势的参考指标。尽管目前尚无法验证搜索热度与比特币价格之间的因果关系，但我们可以初步判定，公众预期在比特币的价格形成过程中发挥了重要作用。

**图 5 搜索热度 vs 比特币价格（USD/BTC）**



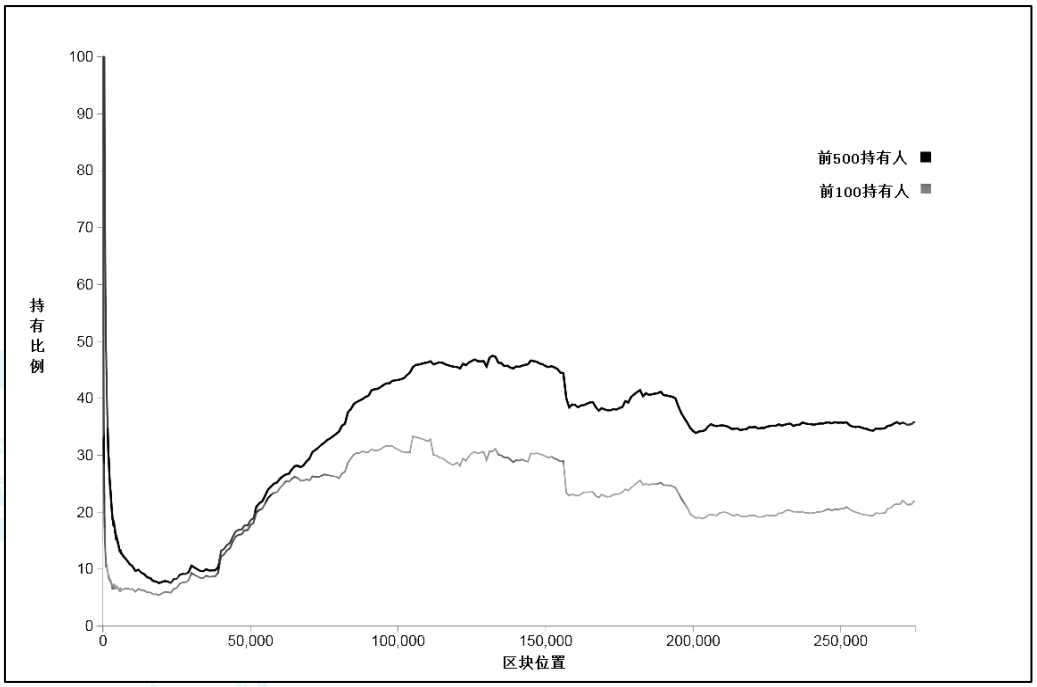

数据来源：BlockChain, Google Trends。

综上所述，比特币的挖矿成本不断上升，导致其供给曲线存在长期左移的趋势。而比特币的需求目前主要与比特币的公众预期密切相关，而与比特币作为交易媒介的需求尚不存在紧密联系。如果将供给与需求结合起来分析，则目前比特币的市场价格主要由公众预期决定。而如果公众预期保持稳定的话，那么从长期来看，比特币的市场价格在成本推动下存在持续走高的可能性。

**（2）市场分布与集中度**

图 6 显示了比特币市场上持币最多的前 100 个和前 500 个账户持币量占比特币总量的百分比。截至 2013 年 12 月，已开采的比特币总量约为 12,131,225 个，排名前 100 的账户持币量为 2,647,870 个，约占总量的 21.8%，而排名前 500 的账户持币量为 4,331,893 个，约占总量的 35.7%。与现行其他货币相比，比特币的市场容量小，持币集中度高。这不仅会影响到比特币市场的流动性，也意味着比特币的币值容易受到操纵。由于比特币的最终总量只有 2100 万个，而目前已开采量超过 1200 万个，即使排名前 500 的账户余额未来不再变动，等到比特币全部开采完毕时，这 500 个账户的比特币持有量也将站到总量的 20%，市场集中度依然很高。

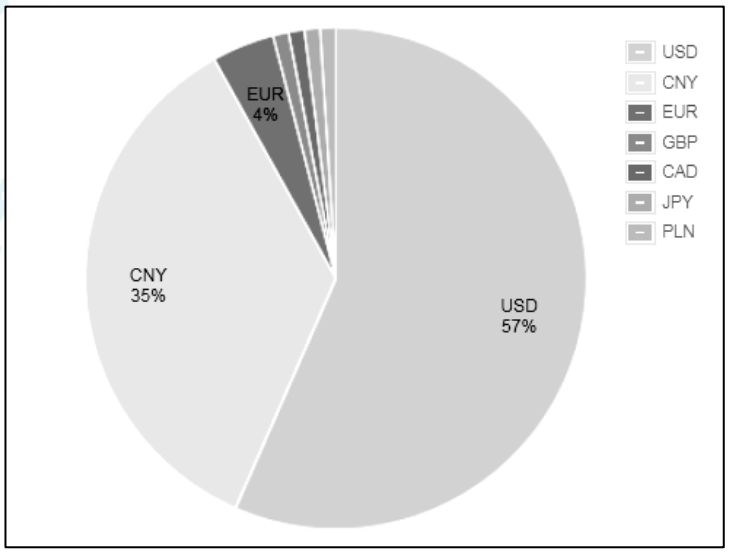
**图 6 比特币持有总量前 500 及前 100 的持有人持币百分比图**




数据来源：BitcoinRichList。

从比特币兑换市场的币种分布来看，最大的三种货币依次是美元（57%），人民币（35%）与欧元（4%）（图 7）。以美元和人民币计价的比特币市场占到了市场总规模的 92%。未来的中美全方位博弈最终会反映到比特币市场上来吗？答案尚不可知。

**图 7 比特币兑换市场币种分布**



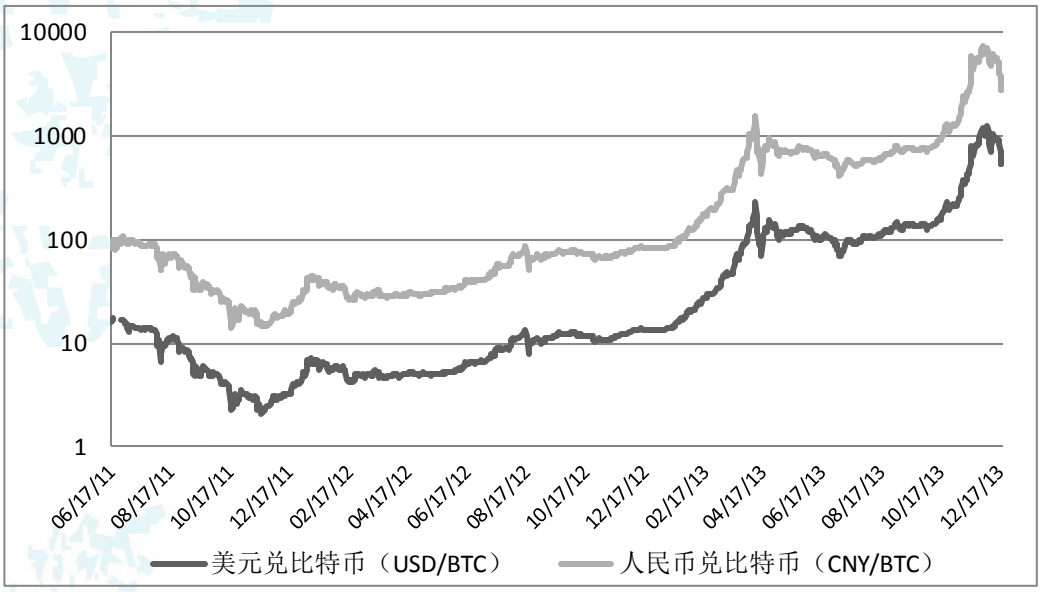

数据来源：Bitcoin Charts。

**（3）资本账户开放下的人民币汇率参考值**

由于资本账户尚未完全开放，且人民币利率形成机制尚未充分市场化，造成计算人民币均衡汇率面临很大困难。而比特币在这方面可能具有天然优势。由于标准化程度高、信息更加透明、没有运输费用、交易成本低、没有资本流动限制，这意味着通过比特币间接计算出的人民币汇率水平，可被视为一旦资本账户全面开放后人民币对美元汇率的参考水平。

图 8 显示了 2011 年 6 月至 2013 年 12 月期间人民币与美元兑比特币的汇率。不难看出，比特币兑人民币与美元汇率的波动趋势具有极强的正相关性，这意味着比特币的跨境套利机制已经存在。

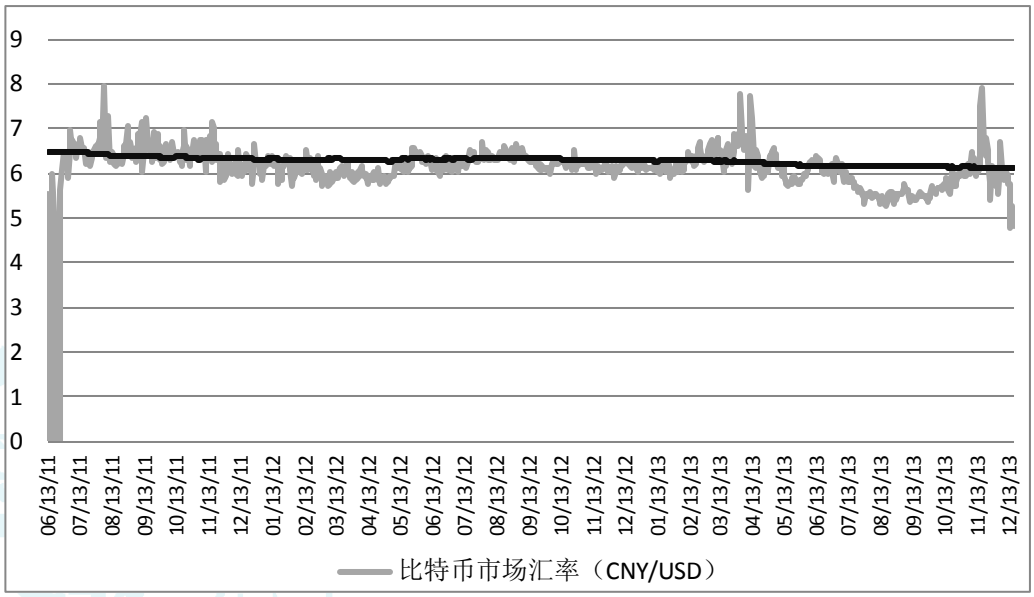
**图 8 比特币兑美元与人民币的汇率**




数据来源：BitCoin Charts。

通过上述两种货币与比特币的汇率而间接计算出来的人民币兑美元汇率，与人民币对美元市场汇率的比较如图 4 所示。可以看出，随着时间的推移，通过比特币市场形成的人民币兑美元汇率围绕着人民币兑美元市场汇率上下波动。人民币兑美元的市场汇率具有很强的稳定性，且在图 9 的时间段内由 6.5 左右缓慢升值至 6.0 左右。相比之下，通过比特币市场形成的人民币兑美元汇率尽管存在较大波动，也一直没有远离该区间。这意味着，即使资本账户全面开放，人民币兑美元汇率也未必会发生持续的升值与贬值。换句话说，这说明当前人民币兑美元的市场汇率已经相当接近于均衡水平。

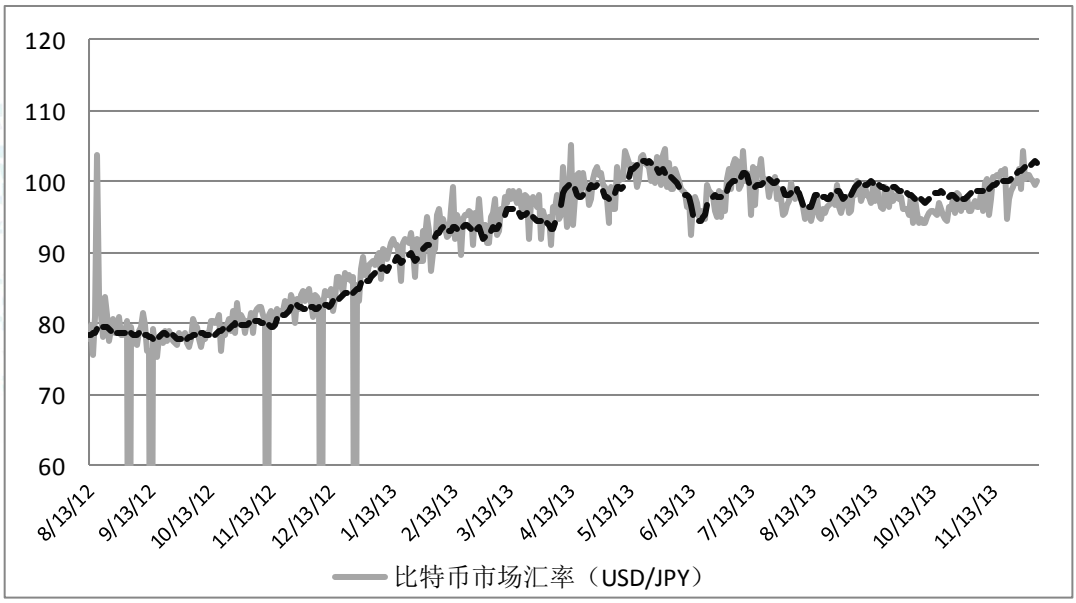
**图 9 人民币兑美元汇率**




数据来源：国家外汇管理局、Bitcoin Charts。

我们在图10中比较了美元兑日元的比特币市场汇率与外汇市场汇率。可以发现，两者走势的吻合程度要显著超过图 9 中人民币兑美元两种汇率走势的吻合程度。考虑到美日之间的资本账户已经全面开放，这也说明了通过比特币市场推算出来的汇率，可以用来近似地估计资本账户开放条件下的汇率走势。

**图 10 美元兑日元汇率**




数据来源：Quandl、BitCoin Charts。

## 四、比特币的前景展望

### 1、比特币长期发展面临的主要限制

货币产生的背景是社会分工背景下物物交换的发展，而比特币产生的背景则是全球经济一体化和互联网全球化。比特币天生具有全球化和去中心化特征，这是与互联网经济的发展相适应的。然而，货币的使用具有很强的制度依赖与网络外部性特征，因此一种新的货币要想取代传统货币的地位，必须在某些方面具有明显优势，而在其他方面也不能显著弱于现有货币。从这一角度来看，比特币的长期发展显著受制于如下缺陷：

**（1）安全风险**

如前所述，比特币采用了一套严密的密码学体系，除非相关数学领域出现重大突破，否则其自身的安全性是值得信任的。但随着比特币的市场价格不断走高，相关交易网站被攻击和账号被盗等事件时有发生。理论上非常安全的比特币为何安全事故频出呢？

由于比特币账户只是一个地址，账户拥有者标识自己所有权的唯一证明就是私钥，因此，盗取比特币的黑客没有能力也没有必要去攻击比特币系统本身，而只需盗取用户的私钥就可以获得比特币。迄今为止，黑客盗取比特币的途径主要有以下几种：第一，通过木马程序盗取保存在用户主机里的私钥文件，并回传给黑客；第二，利用软件和操作系统的漏洞来截获相关信息，经过分析后得到完整的私钥。通常而言，与私钥有关的信息在网络上传播时应该采用随机方式严格加密，但部分应用程序在设计时存在漏洞，始终采用固定方式加密或是加密等级不够，以至于黑客在截获相关信息后，经过分析比对就可推算出私钥的完整内容，从而实现盗窃；第三，使用 DDOS（分布式拒绝服务，这是一种通过极大数量虚假的网络请求来占用攻击目标的计算和网络资源，从而使其无法处理正常用户请求的攻击方式）攻击网络钱包服务器，使服务器瘫痪。在工作人员进行诊断修复的过程中，利用临时出现的系统漏洞入侵服务器，盗取密钥；第四，由于部分网络钱包网站的认证过程存在漏洞，因此一旦黑客侵入用户电子邮件账号，取得相关信息后，就可以通过重新设定网络钱包认证信息来绕开认证过程，从而非法进入用户账号并窃取私钥。

事实上，比特币面临的上述威胁，在现有银行的网银体系中也都会遇到，但考虑到比特币的匿名性，警方即使查到被盗比特币的去向，也很难锁定犯罪分子。更重要的是，由于没有相应仲裁机构，受害用户无法进行申诉。而即便可以申诉，由于犯罪

分子已经掌握了私钥，导致受害用户没有别的途径可以证明自己对账户的所有权，造成取证裁决相当困难。吊诡的是，比特币在安全方面的缺陷，恰好是其匿名性和去中心化的典型特征所导致的。这说明比特币在创新的同时，也为自身发展留下了隐患。

**（2）政策风险**

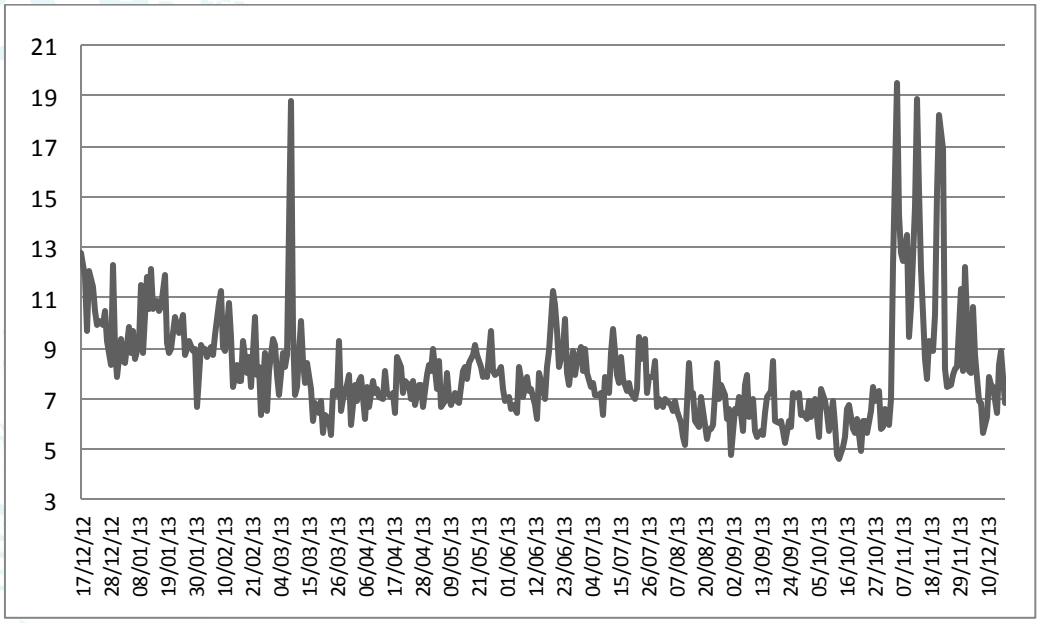
迄今为止，各国政府在面对比特币这一新生事物时，采取了截然不同的态度。以美国和德国为代表的一些国家对比特币给予了充分肯定，而且正在着手修订相关法律法规，以适应比特币可能带来的变化。印度等国家对比特币始终持观望态度，既不明确支持也不明确反对比特币相关产业发展，而是准备等到时机成熟后再采取相应措施。中国、泰国和韩国等国家则是比特币的反对者，都在公开场合明确表示反对，也都要求国内金融机构停止比特币相关服务。

各国对比特币态度迥异的主要原因包括：首先，各国对本国金融体系的监管能力不同。尽管电子货币有助于促进新兴市场国家的经济增长，但同时也显著增加了监管难度，并对央行掌控货币政策的能力提出了新的挑战。发达国家的金融市场发展程度较高，在金融监管方面经验丰富、手段多样，且各项制度相对完善，因此对金融创新所造成冲击的消化能力更强。相反，新兴市场经济体的金融市场发展较为落后，政府金融监管能力较为薄弱，对金融创新所造成冲击的防御能力较弱。这就可以说明为何发达国家总体上对比特币更为欢迎；其次，各国接触比特币的时间和程度不同，在比特币方面按的既得利益也存在较大差异。比特币的匿名性使得我们无从得知各国已取得比特币的具体数额和分布。但鉴于美德等发达国家起步较早，从比特币诞生时起就有大量人员从事比特币的研究和挖矿工作，而且至今有增无减。因此有理由相信，美德等发达国家在比特币的已开采总量中已经持有相当份额，形成了各自的既得利益，甚至有可能已经具备操纵市场的能力；再次，比特币在控制犯罪方面向政府提出了新的挑战。对匿名交易的比特币犯罪来说，只有美国等少数国家才具备追缉罪犯的技术能力，它们也已经为此投入了巨额资金。例如，2013 年 10 月，美国联邦调查局（FBI）宣布彻底捣毁著名的地下交易网站“丝绸之路”（Silk Road）。这一网站 70%的交易集中于毒品，该网站利用比特币的匿名性隐藏了交易双方的真实信息，为破案带来了巨大麻烦。即便是 FBI 这样全球顶尖的情报部门，也是在进行了漫长的数据分析之后，借助 Google 公司的帮助，才从多种渠道锁定犯罪嫌疑人。之后，FBI 还出动了多名探员，通过长期的卧底工作才掌握了大量证据，从而成功将案件破获。对新兴市场国家来说，如此庞大的技术和资金投入都是难以接受的。

**（3）社会接受程度**

与传统货币相比，比特币在使用的便利性还面临如下问题：其一，如前所述，每笔比特币交易都要等待后续若干个区块被加入主区块链后才能最终确认，这是个相当耗时的过程。图 11 显示了近年来比特币交易的确认时间分布。如图所示，一笔比特币交易的确认时间最少需要 5 分钟，最多接近 20 分钟，这与目前传统银行的交易确认通常只需要数秒形成了鲜明对比；其二，比特币市场价值的大起大落也限制了其使用。很少人会愿意接受一种一天之内涨跌幅度超过 50%的货币，这一波幅已经超出了绝大多数人的风险承受能力。正如 Yermack（2013）所言，由于比特币汇率的变动规模与波动性远远超过其他常用货币，这破坏了比特币作为一种计价单位与储藏手段的有效性；其三，比特币的设计理念中隐含了风险自担的思想，例如没有中心节点、缺乏中央监管和仲裁机制、除私钥之外没有其他身份核实机制、交易验证只涉及有效性而不验证合法性等。一旦出现问题，几乎不能给用户提供任何保障。然而，目前大多数人在使用货币时还是习惯于受到某种保护，而且为了获得保护，甚至可以牺牲部分隐私权。这是长期以来社会演化形成的固有思维，短时间内很难发生实质性改变。

**图 11 平均交易确认时间（分钟）**




数据来源：BlockChain。

## 2、比特币未来发展的可能路径

比特币要想继续发展壮大，就必须克服上述限制条件。由于比特币是密码学发展

的产物，要对其进行改进，需要从原理入手重新进行设计，而对相关技术的深入讨论明显超出了本文的范围。因此，我们尝试从其他角度来为比特币寻求几种可行的发展路径。

**（1）基于比特币的创新生态系统**

如果我们不把比特币视为一种潜在的全球货币，而是将比特币系统作为一种点对点的安全交易平台，那么其设计还是非常严谨的。因此，不妨将比特币系统作为一种底层支撑平台，利用它能提供的服务来构建更上层的应用。就像目前互联网采用的五层协议一样，每一层协议都不是完美的，都有自己的独特优势和致命问题。但各协议层之间相互配合，互为补充，就构成了一套切实可行的解决方案。我们也可借鉴这种思路，即并不要求比特币本身十全十美，而是将其视为一个更大系统中的重要部件，通过构建与之相匹配的上层应用或底层支撑，来构建更宏大的系统。

在 2013 年召开的几次全球比特币大会上，一些比特币社区的领导者已经介绍了他们在这方面的积极尝试。目前有代表性的项目包括：一是 SmartCoins，这是一种基于比特币的股票和债券流通系统，对一些在场内市场交易不活跃、或者根本不存在场内市场的金融产品提供了一种更加安全可靠的流通方式；二是 NameCoin，这是一种使用现有货币和比特币来合并挖矿的系统。该系统的基本原理，是利用现有比特币网络超强的散列算力，在现有主区块链的基础上重新构建一个附属区块链，而这个附属区块链背后对应的可能是人民币或美元等现有货币。从本质上来看，这是利用比特币的优势来对现有货币体系进行改造，但该方案的具体运作模式还在停留在讨论中；三是“开放交易系统”，这是一种位于区块链外的交易系统。该系统尝试在局部网络内建立一个有中心节点的交易环境。该系统能够与比特币网络连接起来，从而形成一个全局无中心、局部有中心的分层次网络结构。这种结构一方面可以避免比特币系统相对繁琐的交易确认过程，另一方面又可以继承比特币系统的其他优势。目前我们还无法预知上述创新应用能在未来走多远，但它们的确为比特币提供了一些更加务实和可行的思路。比特币在这些全新的生态系统中将不会扮演基础货币的角色。总之，如何跳出固有的思维框架，对比特币系统进行重新审视和再利用，或许是未来比特币的一条发展之路。

**（2）借鉴比特币思想改造现有货币**

过去几十年来，国际金融危机频发，证明当前的国际货币体系并非一个最优体系，对其进行改革可谓势在必行。当前全球范围内各种货币面临的诸多问题，都直接或间

接地与币值不稳定有关。Shiller（2004）对未来的货币形式做出了大胆预测。他认为货币的交易媒介属性和记账单位属性并不一定要在同一种介质上共存。换句话说，可以在未来创造一种货币，它仅仅承担交易媒介的功能，代表商品或服务所有权的转移，而货币本身的价值无关紧要，因为商品和服务的价格不会以该货币的数量作为衡量标准。Shiller 特别提到了智利目前所采用的“发展单位”概念，认为以“发展单位”为代表的指数型会计单位是解决目前币值不稳定的有效途径。

我们认为，如果 Shiller 描述的未来货币发展趋势是正确的，那么如果对比特币进行改造，使之作为交易媒介，与此同时再创造出一种适合的指数型会计单位进行计价的话，就可能给现有货币体系带来重大变革。作为交易媒介，比特币的去中心化、安全性、透明性、可追溯性、全球性、便利性是值得肯定的，但其总量固定、交易确认时间太长等缺陷也非常突出。因此，我们可以借鉴比特币的发明思路，对其缺点进行改进后，重新创造一种新的货币形式（不妨称之为新比特币），使其能够更好地满足交易媒介的重要特质。交易媒介的作用是标记商品、服务或其他经济利益的转移，其本身发行多少与价值几何，可以完全不影响商品或服务的相对价格。作为记账用的会计单位，我们可以像智利“发展单位”一样使用一种指数型会计单位，所有商品价格都用该单位来衡量。而这种指数型会计单位与比特币的挂钩可以采用松散的方式，即根据比特币总量的变化来适时调整两者之间的兑换关系，以避免币值波动影响经济增长。

当然，这种全新组合的可行性和实施细节都需要进一步的探讨，本文在此只是提出一种思路，还需经过严格论证。

## 五、结论

本文通过对比特币运行原理的阐述，剖析了比特币的典型特征，并展望了比特币的可能前景。主要结论包括：首先，作为货币发展史上的重大革新，比特币在设计中使用的一系列创新思想和方式是值得借鉴的。它的出现是解决当前世界各国货币所面临问题的一种积极尝试，因此受到了全世界的广泛关注；其次，由于比特币在寻求以创新途径解决问题的同时，引入了一些难以调和且致命的新问题，导致市场对以目前形式存在的比特币能否取得长远发展报以怀疑态度；再次，比特币的发展前景取决于其能否顺利完成转型。无论是在其上建立其他应用层级，还是将其作为全球货币改革的一个组件，都需要对它进行重新审视和设计。我们认为，如果设计更为合理，且在

实施过程中能更好地协调各方利益，比特币的发展前景虽然路途遥远，但值得世人期待。

## 参考文献


米什金（2011）：《货币金融学》，中国人民大学出版社，2011 年。

姚勇（2013）：“易懂的比特币工作机理详解”，www.btc123.com/data/docs/easy_understood_bitcoin_mechanism.pdf。

周光友（2010）：“电子货币对货币流动性影响的实证研究”，《财贸经济》，第 7 期。

Bassey, C. (2008): “Digital Money in a Digitally Divided World: Nature, Challenges and Prospects of ePayment Systems in Africa”, scott.mainzone.com/bassey-digitally-divided-world.pdf.

Cassoni, A. and Ramada C. (2013): “Digital Money and its Impact on Local Economic Variables: The Case of Uruguay”，*Document of Investigation*, No. 92, University ORT Uruguay, May.

Grinberg R. (2012): “Bitcoin: An Innovative Alternative Digital Currency”, *Hastings Science & Technologies Law Journal*, Vol 4, pp.160.

Jack, W., Suri, T. and Townsend R. (2010). “Monetary Theory and Electronic Money: Reflections on the Kenyan Experience”, *Economic Quarterly*, Vol.96, No.1, pp.83–122.

Jacobs E. (2011): “Bitcoin: A Bit Too Far ?” *Journal of Internet Banking and Commerce*, Vol.16, No.2.

Lots, S. and Vasselin F. (2013): “Electronic Purse Versus Fiat Money: A Harsh Competition”, *Working paper of GDRE*, June.

Marimon，R., Nicolini，J. and Teles P. (2003): “Inside–Outside Money Competition”，*Journal of Monetary Economics*, Vol.50, pp. 1701-1718.

Nakamoto, S (2008): “Bitcoin: A Peer-to-Peer Electronic Cash System”, bitcoin.org/bitcoin.pdf.

Shiller R. (2004): *The New Financial Order: Risk in the 21st Century*, Princeton University Press.

Šurda, P. (2012): “Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold”, *Diploma Thesis*, WU Vienna University of Economics and Business.

Woo, D., Gordon, I., and Laralov, V. (2013): “Bitcoin: a first assessment”, *FX and Rates*, Research Report from Merrill Lynch , December.

Yermack, D. (2013). “Is Bitcoin a Real Currency”, *NBER Working Paper*, No.19747, December.