

# 论比特币法律监管

姜宇

(华东政法大学 经济法学院,上海 200042)

**[摘要]** 比特币是基于互联网和密码学所生成的数字代码,虽满足货币五大功能,但由于其易致通货紧缩、替代品丛生,以及币值极不稳定三大因素现无法成为货币,故将之认定为投资品较为恰当。基于保护投资者、防范系统性风险以及反洗钱、反避税三大监管目标,比特币应纳入监管框架,实施以去匿名化和经验制度安排为核心的监管进路。

**[关键词]** 比特币; 金融监管; 去匿名化; 经验制度

**[中图分类号]** D9222.28 **[文献标识码]** A **[文章编号]** 1673-0755(2014)05-0099-05

比特币异常火爆的交易引发了全世界的大讨论,其中各国政府对之态度不一。泰国政府是全球首个禁止使用和交易比特币的国家;德国政府是首个承认比特币合法地位的国家;而美国政府持谨慎观望态度。我国央行等五部委亦试图以《关于防范比特币风险的通知》(以下简称《防范通知》)规制比特币的使用和流转。《防范通知》的发布表明了比特币已引起我国政府的关注,而且国家在面对此等金融创新时并非简单禁止,而是以谨慎态度为之预留了部分发展空间,此值肯定,但单以“通知”调整比特币相关行为是否太过简单?面对比特币的诞生,我们应如何界定其性质?是否将之纳入监管?更为重要的是若纳入监管应如何进行监管?

## 一 比特币之性质探究

比特币是什么?笔者力图避开专业而复杂的术语描述之:首先,比特币与传统货币不同,其没有具体的物质形态,在本质上比特币是一组代码,虚拟化地存在于互联网空间内。其次,比特币与Q币等虚拟代币不同,其没有发行机构。比特币缔造者设计了一套密码程序,为比特币的产生确定了规则;用户则运用计算机高速运算这套密码程序来获取比特币,这被形象地称为“挖矿”。此即所谓比特币的“去中心化”发行,一言以蔽之,乃是在一定规则下,用户公平获得比特币的过程,而这一规则一经确定即不依附于任何机构。再次,比特币与纸质货币不同,其基于一个客观的密码规则存在,它的总量固定于2100万枚,不存在超发的可能。再次,比特币与

一般动产不同,对其所有权的保持或控制非以占有形式为之,流转亦非以交付形式为之。比特币设计者利用电子签名的方式实现对比特币所有权的保持和流转。具体而言,用户通过一个算法程序得到两组相对应的代码,这对代码犹如钥匙和锁关系,一把钥匙开一把锁,用“锁”将比特币锁住,用户则自己保留“钥匙”,此即保障了比特币的所有权;当比特币需要流转时,用户用“钥匙”将“锁”打开,再换上交易对手方的“锁”,交易对手方即获得了比特币。在此,“锁”被称为“公钥”;“钥匙”则被称为“私钥”或“密钥”,“公钥”和“私钥”的区别在于“解锁”前,“公钥”是公开的,而“私钥”如同密码一般由所有人秘密保有。如此,进一步论之,“上锁”的本质即指将作为“公钥”的代码添加于作为比特币的代码之后;而“解锁”则是指作为“私钥”的代码公开并添加于比特币代码和“公钥”代码之后。无论“开锁”,还是“解锁”皆是对比特币复杂签名过程的简单比喻,比特币的持有和流转从根本上讲是一个电子签名层层背书的过程,这种电子签名方式既保障了比特币的所有权,又实现了比特币的可流通性。又次,比特币与一般的电子数据不同,其不易被取消或篡改。如前所述,比特币及其持有和流转皆以代码形式公开呈现于互联网之上,这些代码数据得到了互联网上众多比特币用户的确认。其并非以静态形式保存于某一载体,而是动态地覆盖于整个网络,故取消或篡改比特币数据意味着要将互联网上所有确认比特币信息的用户数据进行取消或篡改,以目前科技水平,此不可能为之。此不仅防止了比特币的伪造,确

保了比特币支付系统的安全性,还限制了包括国家在内任何主体的干预,即任何主体都无法在技术层面上对比特币施以禁令或限制令。最后,比特币与银行支付系统中的电子货币不同,其具有匿名性。比特币所有人通过“私钥”和“公钥”的对应性实现比特币的持有和流转,而“私钥”和“公钥”只是特定算法所生成的两组代码,其并不能指明所有者的身份。总之,比特币是依赖于密码学和互联网技术生成并存在的2100万组代码,其通过电子签名方式确保了所有人的所有权和比特币的可流通性。基于比特币设计所实现的去中心化发行、总量固定、不易取消或篡改以及匿名性的特点充分地体现了比特币缔造者的意旨,即其希冀人类通过比特币的广泛应用摆脱国家通过“铸币税”减少货币持有方财富的行为。

那么,比特币是否可如设计者之意,成为一种货币呢?笔者认为,货币的五大功能是解答这一设问的重要标准。其一,价值尺度功能。以目前情形观之,其不仅可在世界各大比特币交易平台上与传统货币互彰价格,甚至某些虚拟和实体商品以比特币标价亦不为鲜闻,比特币之价值尺度功能自不待言。其二,贮藏手段功能和流通手段功能。比特币依赖于密码学和互联网技术,电子签名方式可保障所有人持有和自由流转。其三,支付手段功能。以比特币支付相应商品和服务价款之情形虽未有形成常态,但世界范围内的广泛尝试却常有发生。据2013年11月20日的《华尔街日报》报道,美国夫妇仅靠比特币竟可环游世界三大洲,比特币的支付手段功能由此可见。其四,世界货币功能。基于互联网,比特币可在全世界范围内自由流通,并且由于其去中心化的独特设计,世界各国的调控和监管部门对之的干预皆极其有限,故比特币相较于传统货币,其世界货币功能更加突显。

基于上述分析,比特币具有了货币的五大功能,成为货币似乎无可厚非。但据笔者考察,比特币欲至货币地位,至少存在三方面的障碍:其一,虽然比特币之设计目的在于反对主权货币当局滥发货币所致的通货膨胀问题,但此设计亦具有较大的负外部性,即通货紧缩——2100万枚比特币的总量是否可以满足全球经济发展的货币需求呢?似乎比特币只是使我们回到了金本位时代。其二,传统货币是以国家信用作为支持,而比特币则是以密码学代替任何第三方的信用支持,由此,密码学的设计似乎可以给比特币标以如黄金般的稀缺性,并通过各交易方的广泛认同,取得所谓的“价值”属性。然而我们亦

必须注意,比特币的算法虽然使其具有了稀缺性,但密码学算法本身并不唯一,事实上,类似于比特币的数字产品已经层出不穷,甚至其交易规模大有追赶比特币之势,如莱特币、质数币、比奥币、点点币、阿依币等等。这种“多币丛生”的现象是否一定程度上减弱了比特币的稀缺性,阻碍了比特币成为货币,甚至超主权货币的道路?其三,由于比特币“挖采”尚在进行,2100万枚比特币并未完全进入流通领域,加之政府态度、替代产品、交易范围等不确定因素的影响,比特币币值极不稳定,故目前比特币绝无可能成为一般等价物。那么,退而求其次,比特币是否可成为一种投资品呢?笔者认为,比特币基于其货币潜质,具有投资属性自不待言,此于实践中亦可得到证明:比特币交易情形异常火爆,世界各大交易平台全天不休几乎至疯狂,在温哥华甚至出现了比特币ATM机。故《防范通知》之观点笔者殊为赞同:“比特币应当是一种特定的虚拟商品。”

## 二 比特币之监管理据

比特币作为投资品,尤其是新生投资品,国家应予以其充分发展之空间,此为保障金融自由、鼓励金融创新理念应有之义,自不待言;然当前之关键乃是比特币是否应纳入金融监管的框架内?依据“双峰”理论,金融监管的逻辑发轫于两处:一者为保护投资者,二者为防范系统性风险<sup>[1]</sup>。除此之外,金融作为现代经济乃至社会之核心驱动力,金融监管还承担着反洗钱、反避税等社会职责。故,比特币是否应纳入监管框架取决于其与上述三大目标关系的考量,详言如下:

第一,保护投资者的目标。比特币之匿名性不同于传统虚拟代币的匿名性:后者的匿名性实质上是账户的匿名性,若账户实名化则其中资产亦显名;但比特币的匿名性并不依赖于匿名账户,用户通过随机生成无数对“公钥”和“私钥”来实现比特币的本身匿名,即以目前科技水平,通过公开于互联网上的比特币代码、“公钥”,甚至“私钥”代码难以识别比特币交易方或所有人身份。如此,比特币的交易安全即无法得以保障,交易双方皆可利用比特币的匿名性拒绝履行支付相应价款或比特币的义务,而此时交易对手却难以举证证明比特币的交易行为或交易状况。更甚之,于某些平台化的交易领域,交易双方甚至不知晓交易对手的身份。

不仅于交易安全,财产安全亦受威胁。如前所述,比特币的持有和流转是通过所有权人独有的“私钥”与在互联网公布的“公钥”相对应来实现的,

而“私钥”则是以数据形式进行保存。如此,黑客即可窃取“私钥”数据,并以比特币所有人的名义转让比特币,获得相应对价。在此,由于比特币的匿名性,不仅黑客身份无法查明,甚至所有权人亦难以证明此非为本人交易或授权交易。据2013年4月18日《国际金融报》报道称:“今年3月,一家比特币中介公司就曾遭黑客袭击,被盗走价值12480美元(约7.7万元)的比特币。由于比特币的特殊性,被盗后基本无法找回,所有损失只能由该中介自行承担。”除此,游离于监管之外的比特币交易平台或中介机构卷款而逃的事件亦不为鲜闻,如轰动一时的“比特币交易平台 GBL 诈骗案”。

第二,防范系统性风险的目标。系统性风险之源无外乎两处:一者源自某一金融机构的崩溃;一者源于某一具体市场或某类具体资产的崩溃<sup>[2]</sup>。有时两种情形同进共生,彼此相长,如2007年美国金融危机中的CDO、CDS与雷曼兄弟。落实于本文,比特币做为一种新兴投资品种,价格波动巨大,若不采取必要监管措施,即会随着世界范围内各大金融机构的参与,以及比特币衍生品的出现,引发系统性风险。而事实上,某些金融机构已对比特币表现出了极大兴趣,比特币衍生品亦如雨后春笋般相继诞生。据2013年12月6日的《华尔街见闻》报道,美银美林宣布正式将比特币纳入研究范围。而比特币的衍生品比特股、比特美元等亦相继出现,爱尔兰某个交易平台甚至推出了比特币价差期权。

第三,反洗钱、反避税等其他社会目标。如前所述,比特币之匿名性可以有效掩盖交易方的真实身份。那么,洗钱与避税即可能通过比特币的匿名交易实现。2013年6月21日,全球最大的比特币交易所 Mt. Gox 宣布暂停美元提款服务,并接受美国国土安全部的反洗钱调查。2013年10月2日,比特币贩毒网站“丝绸之路”被关闭,创始人罗斯·乌尔布莱特被逮捕。此类事件可能会随着比特币的使用和交易深入而逐渐增多。

总之,基于三大金融监管目标之考量,国家应当以更为积极的行动去监管比特币的使用和交易,否则比特币之负外部性足已危及金融业,乃至整个经济与社会,这亦为《防范通知》所内涵之精神。

### 三 比特币之监管进路

面对三大监管目标,比特币症结有二:其一为比特币之匿名性;其二为比特币之监管体系尚未构建。《防范通知》对比特币虽有调整之意,但终觉不足以有效监管比特币。笔者认为监管进路应以去匿名化

和经验制度安排为核心。所谓去匿名化即指通过特殊制度安排使比特币显名化,减少由匿名性所带来的风险;而所谓经验制度安排即指通过借鉴现有证券、期货以及其他投资品市场之经验制度,建构比特币监管体系。

#### (一) 建构比特币去匿名化制度。

如前所述,比特币之匿名性极大威胁了交易安全和财产安全,这种威胁源于对比特币进行电子签名的行为无法产生公示之法律后果。根据物权理论,公示行为乃物权变动之必要条件,其旨在向外界展现物权变动的后物上的权利性质与权利归属<sup>[3]</sup>,而电子签名行为具有匿名性,不能有效地向外界展现权利人的身份。虽然比特币设计者意图以“私钥”作为所有权象征,但“私钥”同“公钥”随机生成,与权利人身份毫无关联,其只能在事实上保证私钥持有者之占有,却无法达至所有权公示之目的,如此,对比特币进行电子签名无法取得如物权理论中交付或登记的公示效力。故,笔者认为应以去匿名化措施,弥补电子签名行为之公示瑕疵,即建立比特币公钥登记体系,并规定以“公钥”的预备登记和比特币电子签名行为之结合作为法定公示行为。比特币账户应实名开立,并由登记机构管理。拟使用的比特币“公钥”,应于使用前登记于比特币实名账户中(当然,在法律颁行前已使用但未解除的“公钥”应在法定过渡期内尽快登记,以实现物权生效)。严禁比特币交易者故意向比特币签署未经登记的“公钥”,否则此行为在民法上视为比特币抛弃,所有权归国家所有。

需说明的是,依据物权理论,向比特币签署未经登记的“公钥”的行为不符合法定的公示要求,应被认定为不产生物权变动的效力,该比特币应恢复至签名前的状态,但笔者却将此行为拟制为抛弃行为,其因有二:其一,如前所述,比特币具有不可篡改性,比特币一经电子签名即在整个互联网上得到确认,“公钥”代码无法撤销,此被称为比特币交易的不可逆性。其二,比特币登记制度不仅是基于交易安全和财产安全之考量,亦为反洗钱、反避税之前置关键举措,故交易者故意违背禁令理当承担不利之法律后果。当然,若交易者可证明其向比特币签署未经登记的“公钥”的行为非系故意,则应将比特币还原至签名前的状态,但基于比特币交易的不可逆性,国家须以替代方式为之,即或以比特币对应价款(按市价)返还发送者,或以原转让者为受让者,向比特币签署他所控制的其他合法“公钥”(变相返还比特币)。

在此可能会引发一个悖论,即既然有“替代方式”,为何还要将“故意向比特币签署未经登记的‘公钥’的行为”拟制为“抛弃行为”呢?前述不可逆性的理据仿佛站不住脚。笔者认为,虽有替代方式,但替代方式若广泛为之成本巨大,实不可及于“故意向比特币签署未经登记的‘公钥’的行为”,而且鉴于交易者违反禁令之过错为故意,理应以不利之法律后果。

除此之外,基于防范黑客窃取数据而进行非本人交易的风险之考虑,可在比特币登记平台之上建立安全交易通道,各个比特币账户之间的比特币交易可通过此安全交易通道完成。具体而言,凡参加安全通道交易的账户应绑定安全密码,持币人进行比特币交易时不仅须进行正确的“私钥”签名,还需输入其账户之安全密码,交易方能完成,笔者命之“双密码保护”。鉴于现有的网上银行支付技术十分成熟,比特币账户安全密码可充分借鉴引进之,如优盾、动态验证码、防钓鱼插件等技术。当然,安全通道交易并不是公示要素,不应强制性规定,只是出于防范黑客风险而设计,由比特币所有者自愿参与。

比特币去匿名化制度除了有保护投资者的功能外,还有一项重要功能,即反洗钱和反避税功能。比特币账户去匿名化后,则与现有的反洗钱体系和征税体系相宜,此自不待言。唯须考虑的是实名账户之外的比特币流转,此公然违背法律的强制性规定,可谓洗钱、逃税嫌疑巨大,应当课以反洗钱和税务调查。如此,去匿名化制度在反洗钱、反避税层面上不仅实现了实名账户的透明监管,其还可迅速锁定可疑交易,为进一步稽查带来便利。当然,对匿名交易的稽查还应当有赖于反洗钱、反避税技术的进一步研究和发展。

## (二)规范比特币集中交易和建构风险防控体系

目前,比特币交易平台未纳入监管,交易规则亦不统一,各个平台的投资者保护和风险防范措施良莠不齐。笔者认为此可借鉴现有证券市场、期货市场以及其他投资品市场之经验制度,建构比特币集中交易规范以及风险防控体系。因为去匿名化后的比特币与一般金融投资品差异甚微,引入正规金融的经验制度可有利于比特币市场的迅速正规化和法治化,有利于投资者保护和风险防范。具体制度安排如下:

第一,设置比特币交易平台的许可制度、比特币经纪业务许可制度,通过强化对交易平台和经纪会员的监管达至防控整个比特币市场风险的目的。

第二,设置规范的集中竞价或做市商制度,限定开市时间、涨跌幅度,减少比特币价格的非理性波动。

第三,设置分级结算制度和共同对手方制度,化解信用风险。

第四,设置货银对付制度。

第五,强化投资者风险教育,建立投资者适当性制度,完善信息披露制度。

第六,设置银行存管制度,保障客户账户资金安全。

第七,设置风险基金制度、交易风险准备金制度、结算备付金制度、结算风险基金制度、结算互保金制度、投资者保护基金制度。

第八,设置金融机构比特币自营业务许可制度,建立比特币业务与其他业务之间的防火墙。

第九,宏观审慎与微观审慎相结合,防范系统性金融风险。等等。

以上皆为经验制度,具体内容不予赘述,未列经验亦不一一详尽。通过借鉴经验制度,比特币市场达至法治化、规范化。此不仅于保护投资者、防范系统性风险有利,还可以增强投资者信心,活跃比特币市场,吸引全世界的投资者,进而使比特金融健康发展。

虽然《防范通知》规定:“现阶段,各金融机构和支付机构不得以比特币为产品或服务定价,不得买卖或作为中央对手买卖比特币,不得承保与比特币相关的保险业务或将比特币纳入保险责任范围,不得直接或间接为客户提供其他与比特币相关的服务……。”但从其中“现阶段”之用语可臆推五部委之态度颇为谨慎,其应已认识到比特币市场正规化乃未来之大势。

总之,比特币监管进路是以去匿名化和经验制度安排为核心的进路,是比特币由地下到地上,由无序到规范,由野蛮生长到风险可控的过程。这个过程可实现比特币市场的法治化和规范化,实现保护投资者、防范系统性风险以及反洗钱反避税的监管目标,从而促进比特金融的健康发展。

## 四 余论

互联网正悄然改变着人们的生活,金融自不例外。2013年被喻为“互联网金融元年”,从余额宝到微信支付,从阿里小贷到P2P网贷,互联网金融予人们以全新的体验和便利的同时,亦带来了挑战。比特币即是互联网时代中的一次金融创新,无论言之为“货币创新”,还是“投资品种创新”,其皆是在

互联网普惠精神下的一次尝试,至于这次尝试是有益、无益,还是有害,当观其日后发展,故政府应予以其发展机会和发展空间,此不仅为金融自由应有之义,更是增进社会福利所必经之途;然其所带来的挑战亦不得小视,国家须谨慎监管以保护投资者权益,防范系统性风险以及实现反洗钱、反避税等其他社会目标。总之,在互联网深入发展的时代中,金融创新必如雨后春笋不断涌现,我们应谨持“予其发展,并纳其监管”的理念对待包括比特币在内的互联网金融创新。

## [参考文献]

- [1] Michael Taylor, Twin Peaks. A Regulatory Structure for the New Century[J]. Center for the study of Financial Innovation, 1995:(12):3-12.
- [2] 韩龙,彭秀坤,包勇恩. 金融风险防范的法律制度研究——以我国金融业对外开放为重心[M]. 北京:中国政法大学出版社,2012:4.
- [3] 王利明,杨立新,王轶,程啸. 民法学[M]. 3版. 北京:法律出版社,2011:251.

## On the Legal Supervision on Bitcoins

JIANG Yu

(East China University of Political Science and Law, Shanghai 200042, China)

**Abstract:** Bitcoins are several sets of code by cryptology on the internet. Bitcoins have the five functions of money, but they couldn't become money, because they may result in deflation, some other coins may take the place of Bitcoins, and their value is not stable, so Bitcoins are investments. The authorities should supervise Bitcoins by deanonymization and referring to the mature rules and regulations, because of protection of investors, guarding against systematic risks, anti-money laundering and anti-tax avoidance.

**Key words:** Bitcoins; financial supervision; deanonymization; the mature rules and regulations

## 建立金砖货币体系

龚刚在《中国金融家》2014年第5期撰文认为,所谓金砖货币体系是一种双重货币体系,“金砖”货币中的“金”并不指黄金,而是代表现有的金砖五国集团。其中,“金砖”称之为上币,体系中的其他主权货币可称之为下币。双重货币体制的基本运行规则如下:下币用于国内交易,上币用于兑换主权货币。这意味着当金砖国家间发生交易时,下币之间不能直接兑换,必须用下币和上币进行兑换。当金砖国家与金砖外国家发生兑换需求时,禁止使用其主权货币进行兑换,而需使用“金砖”货币与金砖外国家的主权货币(如美元)进行兑换。这一规则意味着金砖国家无需积累他国货币,而只需积累“金砖”。与此同时,就那些经常需要与金砖国家进行交易的商家而言,积累“金砖”也不失为一项有意义的选择。在金砖体系下,现有金砖五国共同发起成立发行“金砖”的超主权中央银行——金砖银行。原则上,“金砖”与各主权货币之间的牌价应该由各主权国自行决定。这一货币体系的好处在于:既能兼顾主权货币在对内促进本国经济发展、调控本国经济中的功能,同时在对对外货币战略上又可聚五国之力,联合抗衡美元、欧元等超级货币。由于禁止使用本国主权货币与他国主权货币直接兑换,金砖国家无需积累美元等强势货币,而只需积累“金砖”。