区块链式法定货币体系研究

□王 晟

（浙江大学 经济学院，浙江 杭州 310058）

进入21世纪以来，随着P2P通讯技术与区块链技术的成熟，哈耶克所预言的“非国家化货币”有了技术可行性，某种类似于黄金本位的区块链式法定货币体系可能在未来出现。本文在总结现行区块链货币技术特点基础上，分析了区块链式法定货币体系的制度优势，探讨了承担法定货币职能时区块链货币的技术形态，研究了区块链式法定货币体系下支付体系、货币政策、金融监管的可能变化。

关键词：区块链；法定货币；比特币；黄金本位

中图分类号：F820.2 文献标识码：A 文章编号：1003—5656（2016）09—0077—09

DOI:10.16158/j.cnki.51-1312/f.2016.09.009

一、背 景

（一）现行货币体系的脆弱性

1930年代全球金本位制崩溃以来，各国间汇率大幅波动，有些国家频繁面临恶性通货膨胀威胁。在信用货币体系下，除美国外的几乎所有国家，为保持本国货币币值稳定，不得不持有大量的美元储备和黄金储备，并为获得与维持美元、黄金储备付出巨大代价。2014年底，俄罗斯坐拥近4000亿美元外汇储备，仍无法消除卢布对外贬值预期与国内通货膨胀预期。截止至2016年5月末，中国拥有3万多亿美元的外汇储备，但仍需对信用货币体系的脆弱性保持高度警惕。

值得注意的是，货币贬值与通货膨胀并非人类历史的常态。在17世纪至20世纪30年代初，各国货币与黄金保持固定兑换比率，主要国家基本上保持了物价的稳定。但是，黄金的开采量具有严重的不确定性，且黄金开采量长期落后于全球经济增长与货币需求，全球经济经常性地面临流动性不足与通货紧缩的压力。1929年开始的经济危机，以银行大量倒闭、货币流动性（黄金）极端匮乏、物价和产出大幅下跌为标志，彻底摧毁了全球的金本位制。

早在1976年，作为坚定的自由主义者，哈耶克在《货币的非国家化》一书中，分析了基于政府信用的法定货币体系的脆弱性，论述了由不同发行主体（银行）发行竞争性货币的制度优势，探讨了货币发行权独立于主权国家的前景[1]。21世纪以来，随着计算机与互联网通讯技术进步，出现了去中心化的P2P通讯技术与区块链技术，比特币、莱特币、Ripple XRP等区块链货币纷纷出现，哈耶克所预言的非国家化货币在技术上有了现实可行性。

（二）全球竞争下的区块链货币

随着区块链技术的成熟，随着现有货币币值与金融系统的剧烈动荡，随着各国对铸币收益、金融体系主导权的剧烈争夺，各国可能会竞相发行某种基于区块链技术的电子货币，对全球货币金融体系产生深远影响[2]。可能这样做的主要是以下这几类国家。

第一，中小规模国家。为维持本国货币体系稳定、削减美元储备、防止铸币收益外流，某些中小规模国家，有可能在现行法定货币体系中引入某种形式的区块链货币[3]。例如，据中国驻厄瓜多尔大使馆的报道，2014年，厄瓜多尔政府禁止了比特币在本国的流通，同时宣布建立由本国控制的电子货币体系，作为现行货币支付体系的一部分，减轻本国货币对美元储备的依赖[4]。

第二，币值不稳定国家。一些币值不稳定、长期遭受通货膨胀威胁、外汇储备严重缺乏的国家（例如俄罗斯、巴西、阿根廷），有可能在某次货币危机中突然转向基于区块链货币的法定货币体系。此外，国际货币基金组织为了应对滥发货币的威胁，在未来也可能要求资金受助国采用某种具有发行总量控制的区块链货币作为法定货币。

第三，美国。当前全球货币体系中，美元是主要的国际贸易货币与国际储备货币，美国是铸币收益的主要获得者、全球金融体系的主导者，目前采用区块链货币的可能性不大[5]。但是，人民币汇率与美元紧密联系，若美国采用某种形式的区块链货币，将使人民币与此种区块链货币间接挂钩，将对中国的货币体系产生重大影响。

第四，欧盟与其他发达国家。若欧元债务危机频繁出现，或欧盟国家内部对货币政策产生争执，欧盟可能会将欧元转为某种恒定比率增长的区块链货币。其他发达国家，有可能基于争夺货币金融体系主导权（例如：英国、日本），也有可能基于国内政治压力（例如，在瑞士，全民投票可改变本国货币体系），而采用某种形式的区块链货币，并在全球范围内产生示范效应[6]。

第五，中国。在严格监管现有区块链货币的同时，中国人民银行正在密切关注区块链技术的最新进展与可能的应用前景[7]。2016年初，中国人民银行行长周小川曾在专访中表示，数字货币作为法定货币，应由央行来发行；数字货币的发行、流通和交易，都应当遵循传统货币与数字货币一体化的思路，实施同样原则的管理[8]。

二、区块链货币的技术特点

（一）区块链货币的技术原理

区块链（Block Chain）是一种由多个独立节点分散记录的分布式数据库，在2009年由化名中本聪的开发者在比特币（Bitcoin）系统中提出与实现，其他开发者随之在一些新货币系统（如莱特币、Ripple XRP）中进行了借鉴与改造。

以比特币为例，比特币系统的区块链由一连串加密的数据块（block）构成，每个数据块中包含一定个数的比特币，并记录了每一单位比特币的当前所有者（公匙）与历史交易记录（比特币最小单位是0.00000001比特币）。比特币系统的区块链类似于一个无所不包的分布式账本，由对等的P2P网络节点共同保存。为节省存储空间，每个节点也可选择不保存区块链中的早期数据。在比特币系统中，每10分钟内发生的所有有效交易，被统一记录在一个新增数据块中，随之被链接到整条区块链的尾部。在新数据块的生成过程中，所有参与比特币系统计算的网络节点，有一定概率获得新数据块中比特币的初始所有权（这一过程被称为“挖矿”）[9]。

在比特币系统中，每个账户由一对公匙、私匙构成，有私匙的人就是账户的拥有者，拥有公匙及其对应比特币的所有权。如果A要给B转一笔钱，A就把钱的数量加上B的公匙，用自己的钥匙签名，然后把签过名的交易单尽量广播到比特币系统中，最终让每个节点进行记录。当B看到A的公匙时，可以得知是A转给了他一定数额的比特币。B从比特币系统中不断收到其他节点的确认信息，当B收到足够多的确认信息后，就可以认为A的支付是有效的。

（二）交易延时性

区块链记录在所有节点中，因此，区块链货币的交易，依赖区块链货币系统中所有节点对交易的确认。以比特币系统为例，每隔10分钟，每个比特币系统网络节点对收到的交易账单汇总一次，制造新的数据块。由于比特币系统网络节点很多，交易账单不可能迅速广播到全网络。因为每个小群体都可能认为他们看见的那部分更长更有效，多个全局账单的分支可能同时共存。但是，若有节点发现另一条分支更长，它就会转换阵营。所以，有一定的可能性，一份账单被一个小群体接受，但在一段时间后，被更大的阵营抛弃。在数学上可证明，一份账单经过6次确认后（生成6个数据块后），被滚回和撤销的概率即可忽略不计。因此，若要保证交易的不可逆转，一般要等待6个数据块完全确认，这大概需要1个小时时间。

如果要缩短交易确认时间，则需要减少数据块的生成时间。但是，数据块生成时间缩短（例如从10分钟缩短至1分钟），全局账单的分支就越多。为了确保交易不被滚回、降低交易被撤销的风险，就需要提高数据块的确认次数，这就延长了交易时间。例如，莱特币生成数据块的时间较比特币短，但是为了保证交易的不可逆性，莱特币交易一般需要24次确认，总耗时与比特币接近。

（三）交易安全性

区块链货币依赖独立、对等的P2P网络节点来保存所有的交易记录，因而，从理论上来说，若有人能控制所有网络节点的半数以上，则可以修改现有区块链货币的交易记录，这就是所谓的“51%攻击”问题。以比特币为例，如果某机构掌握了比特币全网半数以上的计算力，就可以运用手中的计算力，从自己对外付款交易之前的数据块开始，忽略自己所有对外的付款交易，重新构造后面的数据块，利用计算力优势与比特币系统剩余部分赛跑。若本系统最终创建的数据块长度超过原主分支，则成为新的主分支。这样，可以修改最近的任意交易记录，抹去最近的任意一笔交易。

从统计上来看，区块链货币系统中的网络节点越多、计算力越强，半数以上网络节点被单一主体控制的概率就越低。截止至2016年6月底，比特币全网计算力每秒超过1200P（1P=1024T，1T=1024G），只有几大矿池联合，才具有发动51%攻击的实力，普通个人或机构实施51%攻击的可能性越来越小。但是，矿池持有大量比特币，51%攻击会严重伤害人们对比特币系统的信任度，会导致比特币价格暴跌，矿池持有的比特币会变得一文不值。正常情况下，矿池出于自身的利益，不会用51%攻击收回自身交易出去的比特币，反而会主动规避持有比特币比例过大的情况[10]。

（四）货币系统的控制权

现行大多数区块链货币，货币的生产、转移支付，都由相互独立、对等、去中心化的P2P网络节点共同完成，没有一个明确的发行、结算、控制中心。比特币是一种典型的去中心化的区块链货币。除非取得半数以上节点支持，没有一个节点（包括比特币系统的创造者中本聪在内），可以独自修改比特币的生产总量、货币分配与交易规则。在货币供应量方面，根据比特币系统算法，在比特币创建的最初4年里，会有1050万个比特币被制造出来；每隔4年，每个新增数据块包含的比特币减少一半。因此，在第5到第8年中，会有525万个比特币被制造，在第9到第12年中，会生产262.5万个比特币，依此类推。因此，比特币的累积总量，在数学上是一个递减等比数列的累加。到2140年，比特币的累积总量会趋近于2100万个[11]。这使得比特币具有与黄金类似的特征，任何机构都无法控制比特币的生产总量，杜绝了滥发货币的可能性，有利于公众形成稳定的货币供给预期与货币币值预期[12]。

由商业公司OpenCoin基于区块链技术构造的Ripple货币系统，就具有一个传统意义上的支付结算中心。Ripple货币系统创立时，OpenCoin公司发行了1000亿Ripple XRP币，且承诺总额不再增加，并在2013年9月公开了源代码。但是，中心化的电子货币意味着货币总量可以被中心节点修改，OpenCoin公司仍有独自修改Ripple系统代码的能力，且不需要其他货币持有人加以确认。

（五）铸币收益的分配

现行区块链货币的铸币收益分配与信用货币体系有很大不同。现行区块链货币的铸币收益，主要

被用来吸引、奖励本货币的早期使用者，推广本货币的使用与交易，维持本货币运转的系统开销。以比特币为例，比特币系统由自愿参与的网络节点共同维护，没有一个官方机构来维持比特币系统的运转。如果没有人挖矿、参与交易，比特币的交易活动就无法处理；因此，所有新增的比特币，按照一定算法随机分配给所有比特币系统的参与节点。在比特币创建初期，为了吸引足够的网络节点来处理数据块、维持计算力，早期用户获得比特币的成本十分之低。而在2016年，即使比特币价格已大幅度上涨，但由于新增比特币渐次减半，且比特币系统的参与节点爆炸性增长，获得比特币的概率与收益已经很小。因此，随着比特币成为重要的交易媒介与价值贮藏手段，由此产生的铸币收益将主要被早期使用者、投资者获得。

三、区块链式法定货币的技术形态设计

现行的区块链货币（如比特币、莱特币），皆由非官方机构推出，并无政府信用背书，大都具有去中心化、通货紧缩、交易延时较长、交易安全性较低、早期参与者获利较多等共同特点。若某国政府拟用区块链技术生成自己的法定货币，其技术形态必然与现行区块链货币有较大不同。

（一）区块链式法定货币的控制权

政府对本位货币的控制权是一把双刃剑。一方面，这种控制权赋予了政府极强的货币金融调控能力；另一方面，这种控制权对货币币值稳定构成威胁。而区块链技术为法定货币的控制权在政府与民众之间的重新分配提供了技术基础。

若发行某种去中心化的区块链货币作为法定货币，区块链货币发行总量（或者发行总量的增长规则），将在货币发行之初被确定。对于去中心化的区块链货币，政府基本上无法独自修改区块链货币的发行总量与增长规则。这与黄金类似，一方面构成了货币发行总量的可信承诺，有利于消除通货膨胀、货币贬值预期；另一方面则削弱了政府的货币政策调控能力。尤其是经常性遭受恶性通货膨胀的国家（例如巴西、阿根廷、津巴布韦），公众已经形成强烈的通货膨胀预期，政治结构上缺乏对政府滥发货币的约束，本国货币也缺乏外汇储备支撑，此时，可以考虑发行某种去中心化的区块链货币作为法定货币，在技术上杜绝滥发货币的可能性，消除公众的通货膨胀预期[13]。

若发行某种中心化的区块链货币作为法定货币，则新货币体系将由政府来控制，与现行信用货币体系类似。中心化的电子货币意味着货币总量可以被中心节点修改，且不需要电子货币持有人加以确认。这时，就会碰到现行货币体系中的类似问题：中心节点（政府）有滥发货币的倾向，非中心节点（公众）会形成通货膨胀预期。因此，币值较为稳定的国家，可以发行某种中心化的区块链货币作为法定货币，确保政府对区块链货币的最终控制权。

除上述两种极端情况外，也可构造处于上述两者之间的区块链货币，对区块链式法定货币的控制权进行细致分配。政府作为中心节点，对区块链货币具有一定程度的控制权，同时也赋予非中心节点一定的投票权。例如，可以在区块链货币系统创设时约定，政府作为中心节点有权对区块链式法定货币系统进行修改；同时，半数以上的非中心节点即可否决中心节点对货币系统控制权的修改，三分之二以上的非中心节点即可否决中心节点对货币供应量的修改。

（二）区块链式法定货币的发行规模

现行的大多数区块链货币，为了在货币发行早期尽可能地吸引使用者、提高货币贮藏价值，被设计成发行增量逐渐下降的生产模式，并存在发行总量的最高上限。以比特币为例，比特币的前期供应量很大，后期供应量逐渐减少，在2140年时接近于停止，比特币的累积总量会趋近于2100万个。对于主权国家而言，考虑到经济总量与交易总量的增长率通常大于零，在创制区块链货币作为法定货币时，若选择

类似比特币的货币发行机制，这一电子货币体系会面临与黄金本位制下的类似问题：货币需求超出货币供应量的增长，整个经济体系陷入通货紧缩的状态。在极端情况下，对流动性的恐慌性需求，可能造成1929年大萧条中流动性极度稀缺的境况，引发严重的经济危机。

不过，若政府使用某种形式的区块链货币作为法定货币，并以法定货币形态进入流通领域，则毋需以币值上升为诱饵来吸引早期交易者与投资者。政府可以选择某种算法，以恒定增长率生产区块链货币。例如，以上年度区块链货币存量为基数，每年生产上年度货币存量的5%，作为新增的区块链货币量。由此，一方面，区块链货币的生产总量不存在上限，并可以规避黄金产量的不稳定性和黄金供应成本较高的问题，满足由经济增长带来的流动性需求；另一方面，区块链货币发行总量符合弗里德曼倡导的“单一规则”，有利于公众形成稳定的通货膨胀预期。

（三）区块链式法定货币的铸币收益分配

传统的信用货币体系中，铸币收益主要发行现钞的主权政府获取。同时，这些铸币收益通过外汇储备的形式，在各国间重新分配。除美国外，大多数国家都持有外汇储备，来维持本国货币币值的稳定。各国外汇储备中，美元是主要的储备资产。这意味着，要维持本国货币稳定，需要向美国让渡很大一部分的铸币收益。而选择区块链货币作为法定货币，不需依赖外汇、黄金作为发行储备，即可获得币值稳定的预期，可大量增加本国的铸币收益。

此外，现行的各种区块链货币，需要向使用者让渡铸币收益来尽可能地吸引与推广本货币系统。由此不可避免地带来铸币收益分配不公与计算机资源浪费。若政府创制某种形式的区块链货币作为法定货币，并以政府信用让此区块链货币进入流通领域，铸币收益将主要为政府获得，可以较好解决现行区块链货币存在的铸币收益分配不公问题。

对于去中心化、无中心控制权的区块链货币，政府可以在区块链货币发行之初，声明一个庞大的货币数量为政府所有，尔后增加的区块链货币则可按照一定规则，在政府节点与公共节点间进行分配，以吸引和维持区块链货币系统的运作。对于中心化的区块链货币，其发行与现钞发行类似，政府可以直接创设一定数量的区块链货币为政府所有，且可节省现钞的印制、流通与防伪成本。

尤其应该重视的是，一旦区块链技术的应用价值得到确认，各国间可能会进行剧烈的铸币收益的争夺。在现行的货币体系下，纸币是主要的法定货币，本国可以限制外国纸币在国内的流通，也可通过对银行业的监管限制外国存款货币的流通。但是，若其它主要国家使用区块链货币（例如欧元、卢布），由于现代电子通讯技术的特点，本国很难像封锁纸币一样，封锁外国区块链货币在本国的流通。铸币收益可能会被其它强势货币国家获取，全球货币支付体系和金融体系可能会被重新洗牌。

四、基于区块链式法定货币的支付体系设计

（一）区块链式法定货币支付及其应用场景缺陷

现行的区块链货币，可以作为交易媒介在用户之间进行转移。若政府发行中心化的区块链货币作为法定货币，政府作为中心节点，同时承担清算职能，则区块链货币的支付确认将十分迅捷，这与现行中央银行清算类似，也与存在中心节点的Ripple XRP货币系统类似。若政府发行某种形式的去中心化的区块链货币，赋予所有节点一定的控制权限，依赖P2P网络节点来确认、记录交易，则将带来较长交易延时问题。比如，比特币确认一笔交易需要10分钟至1小时不等；莱特币缩短了交易确认时间，但这在一定程度上又影响到交易安全性。最终，现行的大多数区块链货币，若进行大额交易，可能需要等待数小时，来确认交易不被撤销和逆转。如此高的交易延时，是难以满足日常交易场景需求的。

因此，在区块链式法定货币体系中，尤其是在去中心化的区块链式法定货币体系中，区块链货币本

身将可能主要作为货币储备，只用于大额的、机构间的、非实时性的交易（类似于金本位下的黄金交易、清算）。而日常交易则应考虑使用基于区块链货币的其他支付方式，来克服区块链货币的交易延时性问题，来确保新货币体系与现有支付体系的兼容性。

（二）基于区块链式法定货币的代用货币与银行券

去中心化的区块链货币体系，与现有的现钞流通体系有较大差异，每笔交易需要全网络节点进行确认。即使是在中心化的区块链货币体系下，区块链货币的交换需要依赖电子网络，可能不符合很多居民的交易支付习惯；在有些交易场景下，可能不存在电子通讯网络，无法及时完成区块链货币的交换、确认。

为此，可以由中央银行或商业银行发行纸币、铸币形式的代用货币或银行券，并由发行者承诺，按照固定比率兑换等值的区块链货币。对于日常生活中的小额交易，可用代用货币或银行券支付来替代，减轻区块链货币系统的交易确认压力，缓解区块链货币交易延时性问题，解决电子通讯网络不存在时的交易困境。

代用货币或银行券可由中央银行垄断发行，这种情况与现行纸币发行体系类似。也可由多家商业银行同时发行代用货币或银行券，通过发行银行间的相互竞争、优胜劣汰，由货币市场自发确定代用货币或银行券的发行主体；政府与中央银行只规定银行券的发行储备要求，并在极端情况下提供一定的区块链货币流动性支持。

（三）基于区块链式法定货币的存款货币

2013年，在美国圣何塞召开的比特币大会上，与会者提出了很多方法来解决交易延时性问题。其中最重要的一项为链外交易，即不在区块链内进行交易确认。例如，若有中介公司能以其信誉赢得用户的信任，从而推出自己的钱包软件，那么只要交易双方注册该公司的账户，便可以把自己的部分比特币存入该公司账户，并通过在线钱包将比特币从自己的账户汇入另一账户。由于这种交易实际上只是在该公司的系统内部进行金额转移，不涉及区块链的确认，所以交易几乎是在瞬间完成的。

事实上，上述交易方式，正是现代货币系统中基于商业银行存款货币的交易方式。若政府构建区块链式法定货币体系，可以预计，大多数区块链货币将直接存入商业银行（或与银行类似的储蓄机构）。大量交易将直接使用存款货币进行转账支付，并不需要使用区块链货币自身的交易确认机制，可以完美解决区块链货币交易延时性问题。在此基础上，可以完美兼容、延续现有的金融支付方式。例如，使用基于区块链货币的信用卡、商业票据、信用证进行支付，使用支付宝、PayPal等第三方支付平台进行支付。

基于区块链货币的代用货币、银行券、存款货币支付体系，将与人类历史上存在过的基于黄金的代用货币、银行券、存款货币支付体系类似，并不改变大多数场景下的交易支付习惯，并可加强货币系统的稳健性。在现代信用货币体系下，一旦某国货币体系崩溃（如2016年的委内瑞拉），那么，本国经济很可能退回到物物交换模式下，交易效率大幅度降低，货币经济几近崩溃；或者，外国货币在本国大量流通，滋生大量黑市交易。而基于区块链货币的银行券、存款货币交易体系，即使政府信用丧失、银行体系崩溃，还可用区块链货币的直接交换作为替代交易媒介（虽然其交易延时增长、交易效率降低），避免货币金融体系的彻底崩溃。

五、区块链式法定货币体系下的货币政策与金融监管

（一）区块链式法定货币体系下的货币政策目标

若一国的货币政策目标主要为稳定物价，那么，创制去中心化的、固定增长的区块链货币作为法定货币，本身即可限制政府超发货币的冲动，消除公众形成通货膨胀预期。即使出现货币供给超过货币需

求的情况，也只会出现暂时性的货币贬值和通货膨胀；不会形成轮番性的通货膨胀。创制区块链货币作为法定货币，可以遵循弗里德曼提倡的单一规则，以恒定比率生产区块链货币，可以起到“自动稳定器”的效果[14]。例如，以上年度货币存量为基数，每年生产上年度货币存量的5%，作为新增的区块链货币量。当经济过热时，经济增长率超过5%，则具有紧缩性货币政策的效果；当经济萧条时，经济增长率低于5%，则具有扩张性货币政策效果。这限制了政府对货币政策的相机抉择，但可以起到反经济周期的效果，可达到自动稳定器的效果[15]。

若一国的货币政策目标为货币宽松、刺激经济增长，那么，以去中心化的区块链货币作为法定货币，在中央银行区块链货币储备不足的情况下，可能会限制宽松性货币政策的实施，影响到部分货币政策目标的实现。

（二）区块链式法定货币体系下的货币政策工具

使用区块链货币作为法定货币，则中央银行的货币政策工具控制力，取决于创制区块链货币时约定的控制权分配。若构建一种完全由政府控制的区块链货币作为法定货币，中央银行的货币政策工具与现行信用货币体系一致。若政府放弃对区块链货币的控制权，创设去中心化的区块链货币作为法定货币，则可能使得中央银行货币政策工具效力回归到金本位制时代，这会削弱中央银行的货币政策工具效力，但不会使得主要的货币政策工具全部失效[16]。

目前，中央银行常用的货币政策工具，包括存款准备金率政策、再贴现政策、公开市场操作。存款准备金率政策，并不依赖采用何种货币形态作为法定货币。即使创制某种形式的区块链货币作为法定货币，主要的支付工具仍将是基于此种区块链货币的银行券与存款货币。因此，与现行的货币体系类似，以区块链货币作为法定货币，政府仍然可通过调整银行的存款准备金率，来影响货币乘数和货币供应量。对于再贴现政策和公开市场操作，在进行紧缩流动性操作时，在区块链式法定货币体系下不会面临障碍；在进行扩张流动性操作时，则可能要求中央银行提供等值的区块链货币来注入流动性。由此，与持有外汇储备和黄金储备类似，中央银行需要保持一定的区块链货币储备来实施再贴现政策和公开市场操作[17]。

表1　区块链式法定货币体系下的中央银行资产负债表

资产	负债和权益
区块链货币储备	流通中的银行券
外汇、黄金储备	金融机构在央行的存款
贴现和放款	公共机构（国库）在央行的存款
政府债券和财政借款	央行发行的债券和票据
其他资产	其他负债和资本项目

（三）区块链式法定货币体系下的金融监管

现行区块链货币存在较为严重的非法交易问题。一方面，现有的区块链货币被有意设计为匿名的、难以追溯的P2P式交易网络，以争取更多的使用量（如洗钱、毒品交易），促进这种货币的广泛使用；另一方面，区块链货币依靠通讯网络进行交易，相对于面对面的现钞交易场景，本身就具有一定的隐蔽性[18]。

若由政府设计某种区块链货币作为法定货币，则可以在技术设定上加入区块链货币的交易监管机制，区块链货币交易可以被回溯、阻断，其交易监管成本与便利程度要远优于现行的现钞交易体系。例如，区块链货币可以被设计为实名账户体系，只有进行实名验证的交易账户，才能进入区块链货币的确认网络，可确保每笔交易都可以追溯到最终的真实交易者，防止在纸币交易体系下的洗钱、地下交易与其他金融犯罪[19]。而基于区块链货币的银行券、存款货币的交易监管，则可直接沿用现有的交易监管机制。同时，相对于纸币而言，可随时被监控区块链货币的发行总量、流通总量，可准确统计区块链货币的流通频次，货币流通速度将成为可精确监控的变量。

在区块链式法定货币体系下，现代金融机构仍然会影响货币与代用支付手段的创造与流通，从而影响货币体系的安全。这种情况将与金本位货币体系类似，影响到现行的金融监管。例如，竞争性商业

银行发行的银行券，可能缺乏对应的100%区块链货币储备；现实中流通的银行券，有可能从足值的代用货币逐渐演变成不足值代用货币；商业银行基于区块链式法定货币的存款货币，可能面临储户挤兑为区块链货币的风险。在信用货币体系下，作为最后贷款人的中央银行，可以向商业银行提供无限流动性支持；而在区块链式法定货币体系下，中央银行提供的流动性将取决于其自身的区块链货币储备[20]。

即使采用去中心化的区块链货币作为法定货币，即使中央银行无法再控制区块链货币的发行总量与增长规则，政府与立法机构仍然对法定货币体系拥有最终控制权限。在极端情况下，政府与立法机构也可以将现实中流通的银行券、存款货币与区块链货币脱钩，再次将与区块链货币挂钩的等值银行券、存款货币转变成信用货币。

六、研究结论

21世纪以来，随着P2P通讯技术与区块链技术的成熟，比特币、莱特币、Ripple XRP币等区块链货币纷纷出现，哈耶克所预言的“非国家化货币”在技术上有了现实可行性，货币发行权可能再次从各国政府手中部分转移，某种类似于黄金本位的区块链式法定货币体系可能在未来出现，货币技术形态、支付体系、货币政策与金融监管，都可能在未来出现重大变化。

现行的区块链货币，其货币创设与交易维护主要基于区块链技术，由对等的P2P网络节点合作完成，一般不存在中心节点，货币交易需要较长确认时间，并有可能遭到51%攻击，而铸币收益一般为货币系统的创造者和早期使用者获得。自行创设某种区块链货币作为法定货币，有利于构造货币不被滥发的可信承诺，消除公众的通货膨胀预期；有利于为本国争取铸币收益，降低外汇储备持有量；也有利于本国货币经济的自动稳定与金融监管。

若某国拟用区块链技术生成自己的法定货币，其技术形态必然与现行区块链货币有较大不同。作为法定货币的区块链货币，可以选择遵循弗里德曼倡导的“单一规则”，可以规避黄金、现行各种区块链货币面临的通货紧缩问题。同时，铸币收益将主要为政府获得，可以较好地解决现行各种区块链货币带来的铸币收益分配不公问题。某些小国或经常遭受恶性通货膨胀的国家，可能会发行去中心化的区块链货币（类似于比特币），放弃对区块链货币的控制权，以换取货币币值稳定；某些国家可能会发行中心化的区块链货币，确保政府对区块链货币的最终控制权；某些国家可能会发行处于上述两者之间的区块链货币，政府作为中心节点，对区块链货币具有一定程度的控制权，同时也赋予非中心节点一定的投票权。

若某国拟用区块链技术生成自己的法定货币，那么，区块链式法定货币体系下的支付体系、货币政策、金融监管将出现某些变化。在支付体系方面，基于区块链货币的银行券、存款货币将是日常交易的主要形式，区块链货币将主要作为货币储备，只用于大额的、机构间的、非实时性的交易。在货币政策方面，若使用去中心化的区块链货币作为法定货币，政府放弃对区块链货币的修改权，则可能使得政府对货币体系的影响退回到金本位制时代，影响到中央银行的再贴现政策、公开市场操作，但不会影响存款准备金率政策。在金融监管方面，由政府创制的区块链货币可以建立实名账户认证体系，可以确保每笔交易能够追溯到真实交易者，可以规避非法交易问题。

参考文献：

[1]哈耶克. 货币的非国家化[M]. 北京：新星出版社，2007.

[2]TURPIN J B. Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework[J]. Indiana Journal of Global Legal Studies, 2013,21(1):335-368.

[3]JACK W, SURI T, TOWNSEND R. Monetary Theory and Electronic Money: Reflections on the Kenyan Experience[J].

Economic Quarterly, 2010,96(1):83-122.

[4]经济商务参赞处. 厄瓜多尔公布电子货币使用规定[EB/OL]. 中华人民共和国驻厄瓜多尔大使馆, 2014-10-16. http://ec.mofcom.gov.cn/article/jmxw/201410/20141000760901.shtml.

[5]SHY O. Account-to-Account Electronic Money Transfers: Recent Developments in the United States[J].Research Review, 2011(16):21-24.

[6]FUJIKI H, TANAKA M. Currency Demand, New Technology, and the Adoption of Electronic Money: Micro Evidence from Japan[J].Economics Letters, 2014,125(1):5-8.

[7]李东荣. 我国电子现金发展相关问题研究[J].金融研究, 2014,(3):1-10.

[8]郑昊宁. 周小川提到的"数字货币"意味着什么?[EB/OL].新华网, 2016-02-16. http://news.xinhuanet.com/world/2016-02/16/c_128724364.htm.

[9]王 燕, 周光友. 比特币的货币属性分析[J].金融教育研究, 2014,(3):3-7.

[10]叶 佳. 比特币的优势——基于比特币与其他虚拟货币的对比[J].科技情报开发与经济, 2014,(12):150-152.

[11]WENKER N. On line currencies, real-world chaos: the struggle to regulate the rise of Bitcoin[J].Texas Review of Law & Politics, 2014,19(1):145-197.

[12]王 谦, 戚增艳. 网络货币的产生与应对策略研究[J].经济学家, 2015,(9):86-95.

[13]SUGIURA N. Electronic Money and the Law: Legal Realities and Future Challenges[J].Pacific Rim Law & Policy Journal, 2009,18(3):511-524.

[14]FREEDMAN C. Monetary Policy Implementation: Past, Present and Future-Will Electronic Money Lead to the Eventual Demise of Central Banking?[J]. International Finance, 2000,3(2):211-227.

[15]SINGH S. Electronic Money: Mnderstanding its Use to Increase the Effectiveness of Policy[J].Telecommunications Policy, 1999,23(10-11):753-773.

[16]BRITO J, CASTILLO A. Bitcoin: a Primer for Policymakers[J].Policy, 2013,29(4):3-12.

[17]AL-LAHAM M, AL-TARAWNEH H, ABDALLAT N. Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy[J].Issues in Informing Science & Information Technology, 2009,6:339-349.

[18]LY M K. Coining Bitcoin's "Legal-bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies[J]. Harvard Journal of Law & Technology, 2014,27(2):587-608.

[19]SLATTERY T. Taking a Bit Out of Crime: Bitcoin and Cross-border Tax Evasion[J].Brooklyn Journal of International Law, 2014,39(2):829-873.

[20]HALPIN R, MOORE R. Developments in Electronic Money Regulation-the Electronic Money Directive: A Better Deal for E-money Issuers?[J].Computer Law & Security Review, 2009,25(6):563-568.

(收稿日期:2016—07—02 责任编辑:赵爱清)

Research on Blockchain of Legal Tender System

Wang Sheng

(Department of Economics,Zhejiang University, Hangzhou,Zhejiang, 310058)

Abstract: Since entering the 21st century, "Denationalization of Currency" predicted by Hayek has gotten technical feasibility along with the aging of P2P communication technology and blockchain technology. Some legal tender systems with blockchain like gold standard may come to earth in the future. After summarizing characteristics of current blockchain technology of currency, this paper analyzed advantages of legal tender system with blockchain and discussed the technical form of blockchain currency when acting as legal tender. Besides, this paper also explored the possible changes of paying system, monetary policy and financial supervision under the blockchain of legal tender system.

Key Words: Blockchain; Legal Tender; Bitcoin; Gold Standard