基于数字货币的改良发行模型及监督机制的研究

周治垒　张茗淇　陆光亮
西北农林科技大学理学院，中国·陕西 咸阳 712100

【摘　要】数字货币的最大特点是分散化。本节从数字货币的运营、支付、流通、政策、发行和监管等方面对现有的银行和货币模型进行了改良。

本文分析了数字货币的运作、支付、流通、政策、发行和监管。本文提出了一个数字货币发行(DCI)模型，它根据宏观经济变量如产出、消费、投资、失业率和通货膨胀率来调整流通。并且由于数字货币难以监管，本文提出了一个双链监管模型。该模型以联盟链为核心，以公共链为运行基础，保证了货币体系的分散性和匿名性，并提供了监管的可能性。

【关键词】数字货币；货币模型；双链监管结构

1　引言

数字货币安全问题是近年来出现的热门话题之一。关于通用数字货币是否会被普遍接受，众说纷纭。计算和通信协议使技术进步成为可能。一些人认为，数字货币可以加快交易速度，节省支付处理成本，技术进步使它们更加安全。相反，许多由发布的政府警告指出，匿名和缺乏监督为洗钱和恐怖主义等非法活动创造了机会。最大的压力和潜在的挑战之一是数字货币的安全性，因为它的匿名性和在世界各地缺乏监督。由于基于区块链的数字货币的高度加密，监管很困难。前人提出了多链模型[1]试图实现数字货币监管，但链与节点之间的通信更加复杂，并且由于超级链的建立，该模型失去了监管特征的分散性和交易隐私性。

2　改良的银行和货币模型

2.1 经营方式的转变

操作从离线转为在线。商业银行的实体网点要重新布局，在方便客户的前提下，合理减少网点数量。更加注重网上交易，重点观察客户行为习惯和交易形式的变化发展，并对其服务模式进行相应调整，如移动客户端的设计、清算系统的建设等。

2.2 支付模式的管理

首先，加大监管力度，重复建设金融基础设施。因为每个级别的账户支付系统都属于不同的部门，它们之间相互独立，很容易产生数据缺口和信息孤岛。

第二，增加对私营部门的价值保障，减少道德风险。由于数字货币交易的实时支付结算，需要进行欺诈等欺诈活动，因此需要增加私营部门的价值保障。

2.3 分配方法

中央银行或商业银行以纸币和硬币的形式发行替代货币或纸币。与此同时，发行人承诺以固定汇率兑换等值的区块链货币。对于日常生活中的小额交易，可以使用替代货币或钞票进行支付。这样可以减轻区块链货币系统的交易确认压力，缓解区块链货币的交易延迟问题，解决电子通讯网络不存在时的交易困境。

替代货币或纸币可以由中央银行发行，类似于目前的纸币发行系统。一些商业银行也有可能同时发行替代货币或银行券。通过发行银行之间的相互竞争和优胜劣汰，货币市场自发地决定了替代货币或纸币的发行者；政府和中央银行只规定了银行券的发行准备金要求。并且在极端情况下提供一定的区块链货币流动性支持。

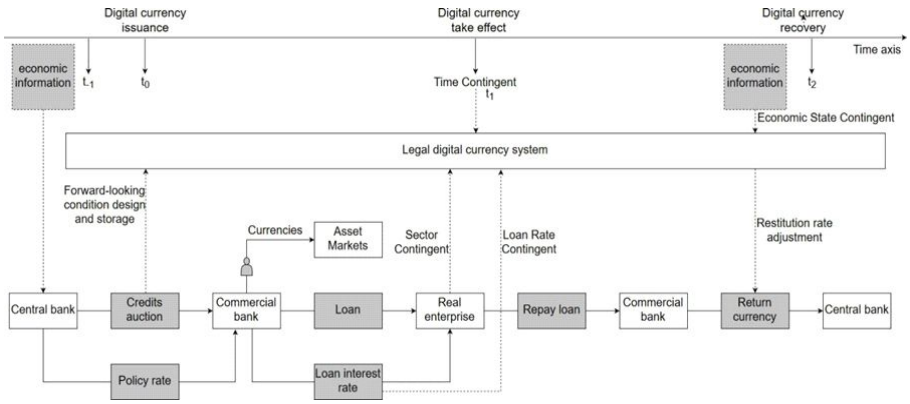

图1　数字货币发行设计

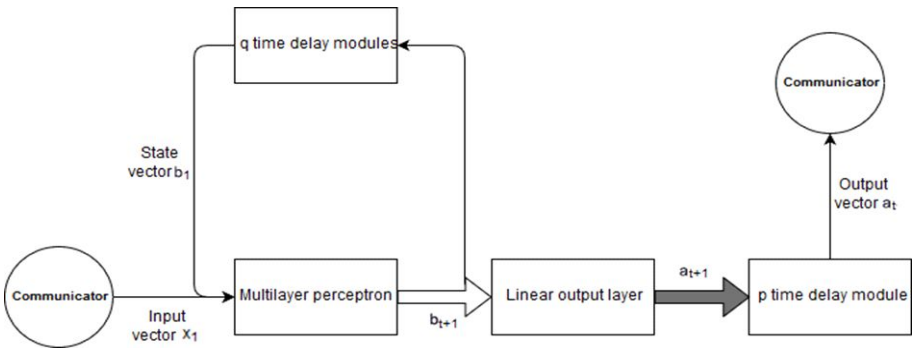

图2　数字货币发行流程

货币形态的数字化在提高货币政策的有效绩效方面发挥着关键作用。货币的“远期或有”设计，即:“时间或有”、“部门或有”、“贷款利率或有”、“经济国家或有”设计。解决传统货币政策传导机制不畅、反周期调控困难、货币“去现实化”、政策沟通不足等困境。

数字货币的发行设计分为四个部分:数字货币发行、生效、回收、流通模式。下图为数字货币发行设计:

2.3.1 数字货币发行

在数字货币发行时(图1中的时间t0)。中央银行预先设定四个前瞻性条件:“时间点条件”、“流向部门条件”。“信贷利率条件”和“经济状况条件”。这些条件是在货币发行时设置的，但在货币投放后触发，因此称为前瞻性条件。

央行在设计了前瞻性条件后，通过信用拍卖机制向商业银行发行了合法的数字货币。央行设定的前瞻性条件，以及拍卖后确定的政策利率，未来商业银行信贷利率和基准利率的依据，由数字货币系统编程存储。

2.3.2 数字货币生效

数字货币发行后，商业银行在 t1 向外放贷。

商业银行将贷款信息发送到合法的数字货币系统，并请求数字货币生效。数字货币系统根据贷款信息判断是否触发了“时点条件”、“流通部门条件”、“信贷利率条件”等前瞻性条件。如果触发，数字货币生效，否则不生效。

2.3.3 数字货币回收

当商业银行恢复信用时(图1中的时间t2)，合法数字货币被回收于中央银行。利率返还央行的情况有两种。一是利率不变，政策利率不变，由货币发行时间 t0 的拍卖确定。另一个是利率改变。数字货币系统根据t2时刻的经济信息自动确定是否触发。如果触发，则调整利率。否则，利率由 t0 时的拍卖决定。

基于状态空间模型递归神经网络,我们初步给出了数字货币发行模型。结合状态空间模型的度量思想和神经网络的建模思想，利用状态空间模型递归神经网络建立数字货币发行模型。

如图所示，数字货币发行模型由三层构成：第一层是输入层。包括反馈节点和源节点，并且多层感知器执行捕获，并且多层感知器可以包括多个隐藏层。源节点连接到外部，并输入可观察向量 xt。第二层是隐藏层。隐藏的神经元定义了不可观察的状态bt。隐藏层的输出通过q单位时间延迟模块反馈到输入。延迟单元将隐藏层的输出反馈到输入层的顺序决定了模型的顺序。第三层是输出层。隐藏的神经元bt通过线性输出层给出网络响应，然后通过 p 个单位时延模块获得 at 的输出矢量。

3 改良的监督机制

3.1 联盟链结构设计

3.1.1 系统初始化

在系统初始化阶段，根据系统安全参数、椭圆曲线密钥生成基本参数、联盟链参与节点总数和秘密恢复阈值，利用椭圆曲线密码算法获取块信息加密密钥。秘密份额将被共享给系统中的n个节点并销毁；然后，每个节点生成一个身份认证签名。节点交换签名密钥，防止假冒联盟链成员传递信息，节点间相互协商信息传递的密钥建立加密通道，防止交易信息泄露。参数初始化完成后，系统建立联盟块。

3.1.2 交易验证和转发

系统通过完整的交易信息验证节点验证用户发送的交易或其他节点转发的交易格式是否符合规范，内容是否正确；用户发送的交易是否已根据交易号收到。并根据交易有效性协议的结果共同决定是否保存转发，

3.1.3 共识协议

本文使用 CPBFT 一致性协议，通过基于投票的机制来验证块信息的正确性。

3.1.4 交易混淆

保护系统数据和用户信息隐私的重要阶段。一个完整的交易由多个出站交易和至少两个转移交易组成。联盟链在确认完整交易正确无误并收到后，将完整交易分割成货币。转账交易和货币转账交易每个交易由多个子交易组成。子交易的编号可以作为其所属完整交易的证明，但不能用于获取子交易的完整交易。子交易号与完整交易一起写入跟踪块，分割交易丢失货币转账，联系转账地址保护用户隐私。

3.1.5 交易可追溯性

该系统通过交易的可追溯性和参与者身份的披露来实现监督的目的。交易被追溯后，监管机构会销毁解密密钥等相关信息。联盟链内部节点之间的通信使用加密通道。

3.2 公共链结构设计

3.2.1 用户身份认证阶段

用户向身份认证服务器提交身份信息。身份验证服务器检查用户的身份，如果有问题，拒绝身份申请。如果用户请求，使用私钥对用户提供的信息进行签名生成证书，并存档发送给用户。

3.2.2 交易生成阶段

交易付款人获取收款人新生成的付款地址，付款人生成交易变更地址。将支付及其解锁密钥和支付地址添加到交易中，然后统计交易中包含的地址数量，验证交易金额是否平衡，生成交易号，并签署交易。

3.2.3 公共区块链生成阶段

公共链节点接收联盟链发送的混淆交易的广播，包括大量的支付交易和收款交易。支付交易对应于现有的未用交易输出(UTXO)，包括 UTXO 号和解锁密钥。收集事务生成一个新的UTXO。在验证消息发送方的身份签名和消息签名后，确定验证后的支付交易的正确性，以及对应的支付交易是否为 UTXO 交易，提供的支付密钥是否正确。最后，将正确的事务打包到块中，以生成 Merkle(其中每个叶节点用数据块哈希，每个非叶节点用其子节点的加密标记哈希)根和块头。

3.2.4 区块验证阶段

接收块确定是否符合正确，包括验证块发送者当前是主节点，验证块的完整性，验证块的数据结构，块头的新信息是否正确，根据商标对照块存储在每个事务中的密文的正确性，最后计算每一层的 Merkle 树的正确性。验证过程中发现块错误或不符合要求的任何步骤都会直接返回错误。

3.2.5 公共区块链共识阶段

采用 DPOS 共识协议，包括见证节点选举和见证节点完成块生成。由于公链节点的规模较大，选择见证节点的间隔时间可以设置得更长，以降低通信成本。公共链节点可以申请做见证节点，但是如果出现块延迟甚至产生错误块，在后续的选举过程中会被其他节点代替。

4 结论

基于数字货币的特点，本文提出了改良的发行模型的监管机制。

对于数字货币的发行、有效性、回收和流通，本文提出了一系列的流通模式和建议。此外，本文还对基于真实货币组合的数字货币在市场上的流通模式提出了混合流通的建议。

本文提出的监管数字货币模型采用双链结构。现有的双链模式只是简单的将用户排除在联盟链之外，只搭建了一个清算平台。虽然它有利于监督，但它不能利用区块链的权力下放。由于基于公共链的数字货币可以掌握每个节点上所有用户的交易信息，如果交易双方没有被很好地隐藏，现有的分析技术可以很容易地找到交易之间的联系，从而获得用户的行为、习惯甚至真实身份[2][3]。

在本文的模型中，联盟链参与者通过秘密共享保证用户交易数据的隐私性，也可以通过投票解密交易内容，从而实现可控匿名，既保持了数字货币的分散性和匿名性。也实现了监督的可能性。

参考文献：

[1]Sun He, Mao Hongliang, Bai Xiaoming, et al. Multi-blockchain model for central bank digital currency [C]//Proc of the 18th Int Conf on Parallel and Distributed Computing,Applications and Technologies (PDCAT). Piscataway, NJ: IEEE, 2017: 360-367.

[2]https://www.msra.cn/zh-cn/news/features/blockchain-20161213.

[3]Xie Ping, Shi Wuguang. Research on digital cryptocurrencies: a literature review[J].Financial research,2015(01):1-15.

作者简介：

周治垒（2000. 8 - ），男，汉，重庆市永川区，在校本科生。