

当前主流数字货币交易模式分析及发展趋势研究

课题组

摘 要:基于密码学和现代网络技术的数字货币近几年来发展异常迅速,数字货币的种类持续增多,以比特币为代表的数字货币交易活跃,日本等部分国家也承认了数字货币的合法性。中国人民银行早在 2014 年就开始数字货币的研究,基于区块链和数字货币的数字票据交易平台于 2017 年成功测试运行,并正式挂牌成立了数字货币研究所。从趋势来看数字货币发展前景广阔,但就目前而言尚存在着线下交易应用不畅、存在隐私泄露风险,易成为洗钱、诈骗等犯罪工具,影响金融稳定与安全等诸多问题与缺陷。本文通过研究以上问题的解决对策,对我国发展数字货币进行展望。

关键词:数字货币;交易模式

DOI:10.16395/j.cnki.61-1462/f.2018.03.012

中图分类号:F832.35

文献标识码:B

文章编号:1674-0017-2018(3)-0050-05

数字货币是基于密码学和现代网络技术,利用复杂的数学算法所产生的网络货币的总称,它是特殊的电子化、数字化的虚拟货币。目前,数字货币的种类已突破 100 多种。由于其去中心化、分布式记账的特点,成为继虚拟货币、电子货币之后发展非常迅猛的价值认定形式。在最新的理论研究中,越来越多的学者认为相较于传统货币,数字货币发行与交易具有低成本、高效率的特点。随着商业化创新和监管的完善,数字货币作为一种新的现象势必进一步发展,同时也将丰富传统的货币和支付理论。

一、数字货币的概念

数字货币是电子货币形式的替代货币,数字金币和密码货币都属于数字货币。数字货币属于非实物货币范畴,是区别于实物货币的一个概念,是指不存在于现实世界、不以物理介质为载体的货币形式。目前数字货币是基于密码学和网络技术,通过算法所产生的非实物货币,其关键底层技术为区块链。它不能完全等同于虚拟世界中的虚拟货币,因为它经常被用于真实的商品和服务交易,而不仅仅局限在网络游戏等虚拟空间中。

电子货币是电子化的“法定货币”,常见于以磁卡或账号的形式存储在金融信息系统内,以方便储藏和支付,其价值等价于法定货币,主要有两种。一种是基于 Internet 网络环境使用的且将代表货币价值的二进制数据保管在微机终端硬盘内的电子现金;一种是将货币价值保存在 IC 卡内并可脱离银行支付系统流通的电子钱包。

表 1 电子货币、虚拟货币、数字货币的对比

名称	电子货币	虚拟货币	数字货币
发行方	中央银行	网络运营商	无
使用范围	一般不限	网络企业内部	不限
发行数量	法币决定	发行主体决定	数量一定
储存形式	磁卡或账号	账号	数字
流通方式	双向流通	单向流通	双向流通
货币价值	与法币对等	与法币不对等	与法币不对等
信用保障	政府信用	企业信用	网民信念
交易安全性	较高	较低	较高
交易成本	较高	较低	较低
运行环境	内联网、外联网	企业服务器与互联网	开源软件以及 P2P 网络
典型代表	支付宝、银行卡等	腾讯 Q 币以及其他游戏币等	比特币、莱特币等

收稿日期:2018-1

课题组组长:张 驰(1983.3-),男,现供职于重庆银行延安分行。

课题组成员:贺 岩(1988.1-),男,现供职于重庆银行延安分行。

呼延雅妮(1991.9-),女,现供职于重庆银行延安分行。

董 琦(1984.5-),女,现供职于重庆银行西安分行。

柴旃嫻(1981.6-),女,现供职于中国人民银行延安市中心支行。

虚拟货币是指没有实物形态的货币、非真实的货币,是基于网络的虚拟性,由网络运营商提供并应用于网络虚拟空间,又被称为网络货币。

二、数字货币的发展现状

(一)数字货币的发展历程

数字货币的关键底层技术是区块链。最早的区块链雏形形成于 1991 年,是哈勃(Haber)与斯托尔内塔(Stornetta)提出的一种对数字文件进行时间戳记录的加密方法。在随后的研究中,戴伟(Wei Dai)提出类似于比特币的 B 币,在点对点网络中每个节点维护一个数据库账本。而真正让数字货币进入大众视野的则是比特币,中本聪(Satoshi)在 2009 年发布《比特币:一种点对点的电子现金系统》中,正式引入区块链概念。随着比特币为代表的数字货币发展,由此也引发了一系列社会问题,尤其其去中心化、不易追踪等特点,容易引发道德风险及监管风险,越来越受到监管当局的重视。2013 年以后的研究者也从其是否具备法定货币基础、易被非法组织利用的应用于洗钱等领域进行研究,也有学者提出,数字货币实际已逐渐脱离作为货币的本质,正在演变为投机工具,应予限制。

在最新的理论研究中,越来越多的学者认为相较传统货币,数字货币发行与交易具有低成本、高效率的特点,随着商业化创新和监管的完善,数字加密货币作为一种新的现象势必进一步发展,同时也将丰富传统的货币和支付理论。

(二)数字货币在全球大发展

数字货币发行是大势所趋,只是目前还处于技术准备层面,对于数字货币的发行模式尚无定论。从官方的态度来看,世界各国对于数字货币的保持了积极的乐观态度,例如 2012 年 12 月 6 日,首家在欧盟法律框架下进行运作的比特币交易所——法国比特币中央交易所诞生,这是世界首家官方认可的比特币交易所。2013 年 6 月底德国议会决定,持有比特币一年以上将予以免税后,比特币被德国财政部认定为“记账单位”,这意味着比特币在德国已被视为合法货币,并且可以用来交税和从事贸易活动。8 月 19 日,德国政府认可了比特币的法律和税收地位,成为全球第一个正式认可比特币合法身份的国家。2013 年 10 月 29 日,全球第一部比特币自动提款机于加拿大温哥华激活。2015 年 3 月 5 日,英格兰银行宣布计划发行一种数字货币。2015 年 7 月 10 日,花旗银行承认正在开发自己的数字货币——花旗币(CitiCoin)。2015 年 9 月 8 日,瑞士银行宣布利用比特币技术开发数字货币。2017 年 4 月 1 日,日本内阁签署的《支付服务修正法案》正式生效,承认了比特币等数字货币的合法性,允许比特币作为支付工具。2017 年 6 月 15 日,中国人民银行在发布风险提示中明确,中国尚未发行法定数字货币,市场上所谓“数字货币”均非法定数字货币。

三、当前主流数字货币形式

按照目前数字货币依赖的底层技术、依靠分布式记账解决信任问题、去中心化的特点,当前主流的数字货币均为民间发行。截至 2017 年 9 月 17 日,共存在 1000 多种数字货币,总市值超过 1200 多亿美元。其中,排名位居前列的数字货币市值分别是比特币、以太坊、瑞波币和莱特币等。

表 2 数字货币市值一览表

名称	简称	市值	价格	货币供应量	过去 24 小时交易量
Bitcoin 比特币	BTC	\$58,410,835,219	\$3,554.33	16,571,625	\$1,277,930,000
Ethereum 以太坊	ETH	\$22,923,734,144	\$242.14	94,672,188	\$422,521,000
Bitcoin Cash 比特币现金	BCH	\$6,736,415,681	\$406.13	16,587,050	\$248,144,000
Ripple 瑞波币	XRP	\$6,732,986,915	\$0.18	38,343,841,883	\$49,103,100
Litecoin 莱特币	LTC	\$2,514,590,975	\$47.47	52,971,432	\$277,340,000
Dash 达世币	DASH	\$2,229,064,850	\$294.74	7,562,843	\$37,994,100

数据来源:2017 年 9 月 17 日 www.coinmarketcap.com 实时监测数据。

(一)比特币

比特币的前身是密码朋克。2008 年中本聪发表题为“比特币:一种点对点的电子现金系统”的白皮书,宣告了比特币的诞生。比特币特点是去中心化,比特币是一种 P2P 形式的数字货币,比特币的出现被视为电子货币划时代的标志,它依据特定算法产生,不依靠特定机构发行,可以用来兑换成大多数国家的货币。它依托于互联网进行交易,拥有数量无限的分布式节点,存在终极数量 2100 万枚。在某些国家,比特币已逐步实现了与现实法定货币的自由兑换,并涉足现实商品和服务的购买。

(二)以太坊

以太坊是开源平台数字货币和区块链平台,它为开发者提供在区块链上搭建和发布应用。以太坊

(ETH)是以太坊(Ethereum)的一种数字代币,开发者们需要支付以太币(ETH)来支撑应用的运行。以太币和其他数字货币一样,可以在交易平台上进行买卖。以太币通过挖矿的形式每年以不变的数量发行。每年发行的数量是预售以太币总量的0.3倍。作为比特币的竞争对手,以太币正在获得越来越多加密货币支持者的青睐。

(三)瑞波币

Ripple是一个开放支付网络,XRP是该网络中的基础货币。XRP由Ripple的运行公司OpenCoin集中发行,XRP的总量是1000亿枚,OpenCoin将这些XRP赠送给投资人和普通用户,通过赠送的速率来控制XRP的价格。XRP与比特币相比的一大优点是建立了共识机制,把交易确认速度缩短至3~5秒,大大加快了转账的便捷程度。

(四)莱特币

莱特币与比特币在技术上具有相同的实现原理。莱特币旨在改进比特币,与其相比,莱特币具有三种显著差异:第一,莱特币网络每2.5分钟可以处理一个区块,因此可以提供更快的交易确认;第二,莱特币最终总量8400万个,是比特币的四倍;第三,莱特币在其工作量证明算法中使用了scrypt加密算法,相比于比特币,在普通计算机上进行莱特币挖掘更为容易。

(五)达世币

达世币(DASH)是一款支持即时交易、以保护用户隐私为目的的数字货币。它基于比特币,特有的双层网络使其能够更加全面地进行测试和更新。如同使用现金一样,达世币可以有效保护交易过程中的隐私。当使用比特币时,交易都会被写到数据块链中,可以查询到接收和发送双方。然而达世币通过独创的去中心化网络服务器“主节点”混淆交易,实现匿名,使得交易无法被追踪查询。

四、数字货币发展中存在的问题

当前主流的数字货币形式中,其存储及交易模式核心依托区块链技术,区块链的优势在于网络中各个区块共同记账来解决信任问题。而凡是货币,必须要能够易于使用,可根据需要随时随地向对方进行支付。如果发生区块节点被恶意攻击,或者在网络连接故障时,则存在数字货币无法被其他区块进行记录与验证。即尽管拥有数字货币的形式,但无法支付给对方,或支付给对方但对方无法验证收到的数字货币是存在且合法的,这会对线下应用形成很大的困扰。目前的网络普及度虽然大幅增加,但是依然有很多区域尚未完全覆盖,而货币的普惠性也是其基本要求。

(一)强化交易安全的同时,存在隐私泄露风险

为了确保数字货币交易易于确认,往往需要进行验证,尽管从理论上讲区块链技术具有匿名性,传输或交易的只是有限的信息,或者剔除了拥有者身份的信息,最典型的代表就是比特币的发明者中本聪先生,到目前为止依然保持着神秘身份。但是每个个体,其支付往往具有一定的倾向,例如集中在一定的区域,或者与固定的对象发生频繁的交易,通过大数据比对也可对其数字货币的拥有者进行追踪,对交易过程中相同的发送方、接收方进行统计分析,可以判断出其在现实生活中的真实身份,从而破坏了其匿名性的特点。同时,由于基于区块链技术的数字货币发生交易时,必须通过分布式记账的方式进行确认,共识机制决定了发生交易时必须将金额(或称为数量)向链中的每个人进行广播,因而造成了交易金额的公开。当个人的交易习惯或支付行为失去匿名的特性,就容易被不法分子收集利用,存在很大的安全隐患。

(二)去中心化记账模式下,易成为洗钱、诈骗等犯罪工具

按照当前以区块链技术为基础的数字货币表现形式,其去中心化、分布式记账的特点,使得数字货币交易与支付变得较为隐秘,通过网络进行交易又使得其便于进行跨境流通,未经实名登记存在身份识别的缺陷,难以进行有效追踪与堵截,这些特点极易成为洗钱、诈骗等犯罪工具。

(三)价格机制不完善,影响金融稳定与安全

当前主流的数字货币形式普遍价格不稳定,其价格机制与法定货币缺乏对应机制,价格取决于用户期望,波动性较大。例如,比特币价格指数级增长,成交价近3万元人民币,一度成为投资、投机对象。价格机制存在的缺陷,数量与价格形成机制也不能反映经济活动,无法真实反映货币供应总量,也不能利用货币政策进行经济调节。

五、促进数字货币良性发展的对策建议

基于区块链的数字货币分布式记账模式仅仅解决了信任及安全问题,但存在着对区块链网络的高度依赖,线下交易在脱离网络的情况下应用具有局限性。为了提高交易的便利性,真正达到类货币的作用,需要对现有的网络连接技术进行革新,使得数字货币的交易与验证不依赖于单一的网络连接。同时,利用密码学技术,将区块链中的数字货币进行加密,转化为数字钱包形式后支付,接收方在交易确认过程中通过密码学中的公钥进行解密,从而验证其真实存在且合法性,存入数字钱包后,再进行加密并入区块链网络。

(一)降低资源消耗的同时,提高匿名化加密技术

数字货币的匿名性受到挑战后,技术人员尝试利用其它加密技术隐藏交易身份或信息,多重加密技术的嵌入需要消耗更多的算力,对资源提出了更高的要求。Greg Maxwell 提出的“机密交易”概念,是实现交易金额(数量)隐藏的较好方案,通过对交易数据的盲化处理,同时运用零知识证明来对交易情况进行模糊验证,既能达到确认与验证交易行为,又无须公开身份信息或交易金额等情况,从而实现隐私保护。但与此同时,盲化、零知识证明等也存在着破解漏洞,需要引用更加可靠的密码学技术进行处理。因此,数字货币需要在降低资源消耗与实现隐私保护方面寻求平衡。

(二)开放追踪端口,打击洗钱犯罪

数字货币多利用区块链进行分布式记账,为了保护用户的隐私,往往不具有使用者真实信息的可追溯性。从监管层面而言,以公共方式进行记账的数字货币不利于监管,也常被不法分子用于洗钱等犯罪。一旦数字货币沦为洗钱工具,将会对社会造成极大危害,也将成为各国监管当局打击的重点,其存在或普及性将大打折扣。因此,数字货币必须具备可追溯性,这就需要技术专家对可追溯信息进行加密,并将追踪端口向监管部门开放,以便于监管部门打击洗钱犯罪。实现反洗钱目的,不仅要开放追踪端口,使得监管部门对数字货币用户身份进行有效识别,同时对其交易记录及交易去向能够有效监测,即实现端口开发可追踪,同时也要满足交易隐秘,不泄露用户隐私。

(三)强化主权货币功能,控制发行主体

去中心化的数字货币发展模式,如若参与个体可自行创造与发行货币,就会削弱货币政策的有效性和控制力,没有发行主体进行管制,数字货币价格也容易产生较大波动,容易引发金融风险。数字货币应用涉及面广,区域辐射大,任何组织或平台开发的数字货币天然缺乏普惠性,不管是基础电信终端建设还是移动网络建设,都存在难以覆盖到偏远地区的情况,地域投放的差异也将对数字货币本身的价值产生影响,造成相同的数字货币由于交易环境的不平衡形成价格差,从而演变为投机工具。因此,由中央银行发行数字货币,可从主权层面实现数字货币的权威性,保持价值稳定,有利于进行货币政策调节。发行层面由央行主导,在保持实物现金发行的同时,发行以加密算法为基础的数字货币,数字货币纳入 M0 的一部分,构成货币供应的主要形式,通过运行逐步增加数字货币在货币供应中的占比,在保持货币供应平稳的情况下切实发挥货币调节功能,维护金融稳定。

随着信息科技的发展以及移动互联网、区块链等技术的演进,全球范围内支付方式发生了巨大的变化,数字货币的发展正在对中央银行的货币发行和货币政策带来新机遇和挑战。我国应在做好关键技术攻关,解决数字货币目前存在的主要问题情况下,加快推进数字货币的发行工作,发挥分布式记账优势,提高支付效率,同时必须明确央行主导作用,强化央行主权货币发行权,维护法定货币权威,鼓励科技企业共同投入技术研究,革新存储载体与连接技术,扩展更多的应用场景,丰富数字货币的支付、流通形式,提高实际生活中使用数字货币的便利度。

参考文献

- [1]杜小玲,聂昌腾,陈永良.数字货币及其货币金融理论影响初探[J].电子商务,2018,(1):46-47,91。
[2]黄震.数字货币交易市场亟待监管介入[J].中国党政干部论坛,2017,(7):79-83。
[3]王晓峰.数字货币环境下电子商务平台交易模式研究[J].商业经济研究,2017,(17):76-78。
[4]习辉.数字货币:理论基础和前景[J].新华月报,2018,(1):34-40。
[5]周金黄.民间数字货币与法定数字货币[J].中国金融,2017,(18):83-84。

The Analysis on the Current Mainstream Digital Currency Trading Modes and the Research on Their Development Trend

Research Group

Abstract: The digital currency which is based on cryptography and modern network technology has developed rapidly in recent years, the types of the digital currency have continued to increase, the transactions of the digital currency represented by bitcoin have been active, and Japan and some other countries have admitted the legitimacy of the digital currency. The People's Bank of China began to carry out the research on the digital currency as early as 2014, the digital notes trading platform based on the block chain and the digital currency was successful tested and run in 2017, and the Institute of Digital Currency was formally founded. In the light of the trend, the development prospects of the digital currency is wide, but for now, there exist a number of problems and defects such as unsmooth offline transaction application, privacy leakage risk, easily being used as criminal tools such as money laundering and fraud, easily causing the failure of monetary policies, influencing the financial stability and security and so on. By studying the solutions to the above problems, the paper forecasts the development of the digital currency in China.

Keywords: digital currency ;Trading Modes ;

责任编辑、校对:陈参军

(上接第 14 页)

The Research on the Path of the Equilibrium between Business Development and Risk Management and Control of Commercial Banks

WANG Wei ZHANG Zhaodi WANG Bofeng

(Shanxi Branch ABC, Xi'an Shanxi 710002)

Abstract: The business development and risk management and control are two eternal themes of commercial banks, and it is a major task to explore the balanced development path of the business development and risk management and control under the new normal of the economic development which commercial banks need to carefully think about and study at present and in the future. From the perspectives of macroscopic economic structural reform, the transformation of commercial banks and risk management and control innovation etc., the paper analyzes the economic situation faced by commercial banks. Centered on the balance between the development and the risk management and control and using the panel data method, the paper quantitatively analyzes the relationship between the business development and the risk management and control. Finally, the paper draws lessons from foreign management modes, and puts forward the ideas, principles, and the path of balancing the business development and risk management and control, which is the reference to the sustainable development of the commercial banks.

Keywords: commercial bank; business development; risk management and control; equilibrium path

责任编辑、校对:党海丽