

区块链技术驱动下私人数字货币的发展风险与系统治理

程雪军^{1,2}

(1.同济大学法学院,上海 200092;2.中国社会科学院金融研究所,北京 100710)

摘要:在区块链技术驱动下,私人数字货币登上历史舞台并蓬勃发展。从演进历史来看,货币历经了“商品货币—金属货币—法定货币—数字货币”的发展阶段。其中,从法定货币到数字货币是一次“惊险跳跃”。作为数字货币的重要构成,私人数字货币具有超越非数字货币的优势,即它以区块链技术为架构核心、以分布式账本为交易前提、有利于推进货币的国际化。虽然私人数字货币的发展极大地刺激了金融创新,但是其衍生的金融风险、技术风险与法律风险等难题也应当引起重视。域外国家私人数字货币的风险治理经验为我国加强私人数字货币的系统治理、促进私人数字货币稳健发展提供了参考。具体而言,应加强私人数字货币的金融治理,防范货币政策风险;统一金融监管机构,夯实私人数字货币的关键基础设施;警惕“技术中心化”,强化私人数字货币风险防范;加大反逃税监管力度,积极参与国际数字货币反逃税协作;健全私人数字货币的反洗钱与反恐怖融资法律机制,严防私人数字货币犯罪。

关键词:区块链技术;数字货币;私人数字货币;金融风险;系统治理;金融稳定法

中图分类号:DF 832.5;D 922.294

文献标识码:A

文章编号:1000-260X(2022)03-0062-12

“次贷危机”暴发之后,为防范系统性金融风险以及保护金融消费者权益,国际社会开始积极探索创新型金融,以中本聪为代表的“赛博朋克主义者”提出了基于区块链技术的比特币理念。此后,在区块链技术的驱动下,数字货币日益成为一种重要的金融创新产物。基于内在的技术特性,数字货币有效提高了支付效率,降低了货币流通成本。伴随着持续的技术创新与应用深化,数字货币在某种程度上可能成为现有支付体系的有益补充。

数字货币的形式多种多样。根据信用基础与承载主体不同,可以将其分为私人数字货币、机构

数字货币与法定数字货币。伴随着区块链技术的不断成熟,私人数字货币从区块链技术 1.0 时代的比特币(Bitcoin)快速发展至区块链技术 2.0 时代的以太币(Ether)。然而,私人数字货币在底层技术、金融以及法律层面上仍然存在一定风险难题。私人数字货币具有较强的匿名属性,这导致其越来越多地被用于洗钱、恐怖融资、逃税等经济犯罪活动中,成为犯罪分子逃脱法律制裁的帮手。尽管在现有的国家法律体系中,已经有相关法律政策对私人数字货币犯罪问题进行规范,但由于私人货币的技术创新属性难以理解,有关私人货币的本质仍处于争

收稿日期:2022-02-20

基金项目:国家社科基金一般项目“我国互联网金融市场准入与监管法制重大理论与实践问题研究”(16BFX098);中国社会科学院国情调研重大项目“关于互联网金融风险治理调研”(GQZD2020006)

作者简介:程雪军,法学博士,经济学博士,同济大学法学院助理教授、上海市人工智能社会治理协同创新中心副研究员,中国社会科学院金融研究所特邀研究员,主要从事法律与金融科技研究。

论之中,导致相关的风险认定及治理具有较大难度。基于此,有必要对私人数字货币的发展本质与潜在风险进行系统研究,以有效应对私人数字货币在发展过程中遇到的风险治理难题。

一、从历史演进探究私人数字货币的本质特征

(一)从商品货币到法定货币的历史演进

货币的演变与人类社会及经济发展息息相关,并在很大程度上塑造了我们今天的社会。在货币出现以前,人们采取物物交换的手段交易商品,然而物物交换存在流通效率低、交换范围窄等明显问题。商品经济发展促使人们提高了交易需求,客观上需要一种被广泛接受的、有长期时效性的一般等价物作为交易媒介。目前已知最早的称量货币是苏美尔人使用的大麦。由于人们对于粮食有刚性需求,并且其物理特性能够以体积、数量等计量方式进行精确计算,因此,大麦较好地承担了一般等价物的流通手段职能,具有原始货币属性。然而,大麦作为可流通的货币,存在着单位价值低、储存期限短等缺陷,因此逐步被贝壳等货币取代,世界上许多地方都曾使用过贝壳作为货币,比如我国三星堆遗址便出土了大量海贝货币^[1]。不过,贝壳亦具有来源不稳定、易损耗等问题,随着商品经济的进一步发展,贝币被金属货币取代^[2]。

最初的金属货币主要为贵金属货币,由于具有高度可分割、不易损耗、易于辨认的特性,金属货币迅速成为新的流通货币。不过,该阶段货币仍然停留于称量货币阶段,在交换时具有非便利性。随着铸币技术的发展,民间自发地开始进行铸币活动,金属铸币进入流通领域,货币由此迈入数量货币阶段。在我国古代,随着秦始皇统一了度量衡,货币统一为半两钱,货币信用由民间私人信用转入主权信用,主权货币更多地被市场青睐。回顾中国货币发展历史,每当国家财政不足以维持铸币权之时,民间铸币就会大量产生。宋元时期存在官方与民间货币并行的局面,双方分别通过发楮印钞、使用白银、短陌支付等方式应对铜钱危机。时至明朝时期,资本主义开始萌芽,货币需求攀升。在主权货

币贬值情况下,民间私钱盛行,共同支持了市场的发展^[3]。商品交换需求的日益增加推动纸币应运而生,最初的纸币并非由国家印发,而是由私人机构发行。纸币凭借其轻便、快捷等属性,迅速取代金属货币成为新的流通货币。然而,纸币作为信用货币,相较于金属货币,本身已不具有价值,而主要承担价值尺度的职能。同时,现代国家为了促进社会经济的统一发展与货币信用的稳定,将发行法定货币权(铸币权)作为货币主权而归国家行使。法定货币具有可轻易印发的特性,为防止类似于“一战”后德国魏玛政府由于货币超发而引起的恶性通货膨胀事件,同时稳定纸币价值,维护货币秩序,防止币值震荡导致经济秩序紊乱,各国开始以相对应量的贵金属作为支撑,实行贵金属本位制。由于主权信用一般高于私人信用,且以贵金属作为支撑,法定货币作为主权货币的地位就此稳定。

综上所述,市场对货币有着天然的需求,由于市场会自发地选择信用更高、交易能力更强、市场化程度更高的货币,所以民间私人货币与主权货币天然存在竞争关系。

(二)从法定货币到数字货币的惊险跳跃

马克思在《资本论》中曾说:“从商品到货币是一次惊险的跳跃”。实际上,从传统法定货币到数字货币,同样是一次“惊险的跳跃”。与传统的法定货币(纸币、硬币)不同,数字货币是一种电子化货币。由于数字货币是区块链技术驱动下的创新金融产品,各国尚未对其概念的内涵和外延形成统一认识。一般认为,数字货币有狭义与广义之分,狭义的数字货币专指不需要物理形式载体、数字化形式的货币;而广义的数字货币则涵盖了一切电子形式的货币,是电子货币的同义概念^[4]。根据发行主体的差别,可以将数字货币分为法定数字货币与非法定数字货币两类。

其一,法定数字货币。法定数字货币主要包括央行数字货币(CBDC)与央行数字账户(CBDA)两类,其中前者按照应用场景又可以分为零售型央行数字货币(如E-CNY)与批发型央行数字货币(如Jasper)。以数字人民币(E-CNY)为例,数字人民币是由中国人民银行发行的数字形式的法定货币,由

指定运营机构(主要为商业银行)参与运营并向公众兑换,秉承技术中性原则,以广义账户体系为基础,支持银行账户松耦合以及可控匿名功能,具有法定数字货币地位。一方面,数字人民币由人民银行做信用担保,仍然为主权信用货币,具有无限法偿性^[5]。数字人民币与传统法定货币(纸币、硬币)相同,都代表了中央银行对公众的负债,双方保持了传统货币形态中的债务债权关系;另一方面,由于数字人民币仍然采取中心化管理模式,即人民银行在数字人民币的发行流通中居于中心地位,所以我国数字人民币仍旧遵循传统法定人民币模式下货币政策的调控原则^[6]。

其二,非法定数字货币。非法定数字货币又称约定数字货币。根据是否具有稳定价值,可以将其划分为私人数字货币与机构数字货币。其中,常见的私人数字货币有比特币、以太币、EOS 币等,其本质不再是法定货币。私人数字货币并不锚定法定货币,其发行摆脱了中央信任机构(如中央银行),由民间发行与流通。以比特币为代表,私人数字货币基于哈希算法等技术保证其具有不可伪造性,通过点对点(P2P)网络进行全球范围内的发行与流通,并基于区块链技术保障交易清算时的完整度与信任问题。由于无中央信任机构介入,使用私人数字货币进行交易时,不再需要传统银行业务中本质为债权转移的清算结算,而是实现了资产端到端的转移。同时,货币总量基于哈希算法而保持有限性(如比特币上限为 2100 万枚),导致货币政策难以对私人数字货币进行有效的宏观调节^[7],私人数字货币面临着币值频繁震荡的风险。与此形成对照,机构数字货币(如 Facebook 发行的稳定币 Libra)则通过“锚定”某一链下资产,实现币值与该资产的价值相同,成功获得了币值的稳定属性。在具体的金融实践中,机构数字货币可进一步分为锚定链下资产的抵押稳定数字货币,以及通过高度精密的算法进行即时供求关系调节的算法稳定数字货币两类。基于是否存在中心化的发行机构,又可分为中心化与去中心化稳定数字货币。当发行机构为中心化的,且币值与特定资产锚定时,该数字货币被称为中心化的稳定数字货币。由此可见,中心化稳定数字货币具有稳定的数字货币币值与中心化的发行

机构,因此与中心化的中央发行机构(如中央银行)发行的法定数字货币具有一定的相似性,但二者在发行主体、法律地位以及法律影响等层面仍旧有所不同。

二、私人数字货币的发展动因:具有超越非数字货币的优势

(一)私人数字货币以区块链技术为架构核心

1. 通过全程数字化,助力数字货币交易综合效率提升

私人数字货币并非真正意义上的货币,而是基于密码学加密的数据信息,其交易类型主要是无须信任中介参与的 P2P 交易。在区块链技术的驱动下,私人数字货币并没有对接中央信任机构,且不依赖网络以外的任何实体,因而可以削减交易成本,免除传统金融机构的深度介入,基于全程数字化方式以最大限度地降低金融中介费用,只需支付少量的私人数字货币给挖出区块链的“矿工”作为激励。此外,区块链技术驱动私人数字货币基于 P2P 网络方式进行交易,这意味着它不需经过传统中介金融机构的响应与审核,只需将数据信息传递给全球的账本终端即可完成交易,相较于传统中介金融机构的长周期审核,私人数字货币可以在数分钟内甚至数秒内完成交易,有效降低了时间成本。

2. 具有高度技术依赖性,推动区块链技术与数字技术进步

私人数字货币依靠哈希加密算法以实现防伪与去中心化,其交易过程高度依赖于互联网信息平台。对于私人数字货币的广泛研究,势必频繁涉及区块链技术以及哈希加密算法,从而推动区块链及数字技术进步。如今,发行私人数字货币的公司大量出现,在推动数字金融不断创新的同时,间接发展了密码学与区块链技术,不断改进哈希加密算法,提高了碰撞阻力。不仅如此,对区块链技术的创新推动了区块链技术与新业态的融合,催生出私人数字货币以外的新兴产品,如非同质化代币(NFT)。NFT 具有不可分、唯一性等特点,较好地解决了比特币等私人数字货币可分性的问题。通过与艺术品行业高度结合,它可以生成基于区块链技术的新的

型资产模式,创造出具有高保值性的数字资产。

(二)私人数字货币以分布式账本为交易前提

1. 交易中介扁平化,有利于提升治理能效

私人数字货币大多采取分布式账本的去中心化发行模式,其相关交易信息储存于不同的区块上。由于私人数字货币采取分布式账本,交易时无需经过中央机构,交易过程在公链记录,数据信息可达性强,且真实性有高度保障,从底层技术层面有效避免了通过修改数据进行的经济犯罪。通过实施自下而上的技术变革,可以助力交易中介的扁平化,提高信息数据的利用效率与质量,为市场监管提供数字支撑,有效实现及时准确的数据收集。相较于立体复杂的交易中介架构,中心化的货币政策调控措施通过扁平化的作用路径,可以直接高效地作用于私人数字货币领域,增强政策实效性,降低政策制定与执行的滞后性缺陷。私人数字货币交易架构简洁,有利于货币调控政策直达痛点,提高私人数字货币领域的治理能效。

2. 私人数字货币可以实现可控匿名性

对于去中心化的私人数字货币系统,往往引入P2P网络架构,该网络具有高度的开放性特点,任何人都可以随时加入。同时,私人数字货币基于公钥与私钥签名和验证实现交易,且可以不实名地创建任意数量的地址,因而能够满足假名性的需要。使用去中心化的私人数字货币系统进行交易时,公开信息只有交易面额、输出与输入地址,因而隐私信息可以被较好地保护。不过,由于基于P2P网络架构达成的所有交易都被公开,通过分析找零地址与服务商,并结合不具有假名性的互联网信息,可以分析并找到地址间的联系,进而还原用户的真实信息^[9]。这一过程虽然相当繁琐且颇具难度,但可以发挥链接用户信息的作用。因而,去中心化的私人数字货币系统仅具有假名性而非完全匿名性,监管机构可通过链接相关信息数据对用户进行追查,从而达到有效的金融监管,实现可控匿名。

(三)私人数字货币有利于推进货币国际化

私人数字货币通常基于P2P全球网络架构,用户可以在全球范围使用私人数字货币进行交易,

物理空间限制被打破,使其客观上具有跨国使用潜力。比如,在爆发于2022年2月底的“俄罗斯—乌克兰冲突”中,美国对俄罗斯封锁了国际资金清算系统(SWIFT),但是俄罗斯可通过连接私人数字货币系统(如比特币),在全球范围内实现货币流通。这也是为何两国冲突发生后,俄罗斯本国的法定货币(卢布)出现大幅度下跌,而私人数字货币(如比特币)却出现价格上扬的原因,这也在一定程度上帮助俄罗斯“突围”了SWIFT的金融制裁。

一方面,去中心化的私人货币系统有利于促进传统货币跳出国际政治力量的博弈,摆脱国别限制,成为国际货币。同时,由于私人数字货币并无中央发行机构,天然具有反货币霸权(比如,美元霸权)的特征,符合部分国家对于公平公正的国际货币体系的诉求,具有较好的需求基础。随着跨国私人数字货币的兴起,国际货币的理念将深入人心,一定程度上为货币的国际化奠定了市场基础。

另一方面,发行主体、网络架构、加密手段的多元化有利于推动私人数字货币走向国际化与体系化,并以新兴优势强势抢夺传统货币的话语权,这有利于打破布雷顿森林体系后的美元霸权体系^[9],减少国际金融体系下导致全球经济失衡的不稳定因素^[10]。具言之,私人数字货币的公开性、去中心化以及总量固定属性,能够有效应对围绕“货币权力”的国家之争^[11],规避中心化的发行机构为敛财而进行的货币超印与超发,保护国家的金融主权安全,防止世界货币的主权国将本国经济失衡的风险通过货币政策转嫁给其他国家,最终避免国际金融危机与经济失衡。私人数字货币的存在将成为促使各国进行货币体系改革的重要推手,推动其向着更加公平、公正、公开的方向不断发展。

三、私人数字货币在发展中面临的主要风险

区块链技术被称为价值互联网时代的革新技术,它对传统的货币体系发挥了建设性作用,助推了私人数字货币的快速发展。但是,区块链技术同样具有破坏性。从私人数字货币的损害性以及(使用)可能性来看,它具有高损害性、较高的(使用)可

能性,其总体风险远远超过其他数字货币以及传统法定货币(见图1)。总体来说,私人数字货币深度利用区块链技术,创新金融产品与服务,突破了传统法律规范的制约,具有较高的技术深化性、金融创新性以及法律突破性,而这些特性可能衍生相关的金融风险、技术风险以及法律风险。

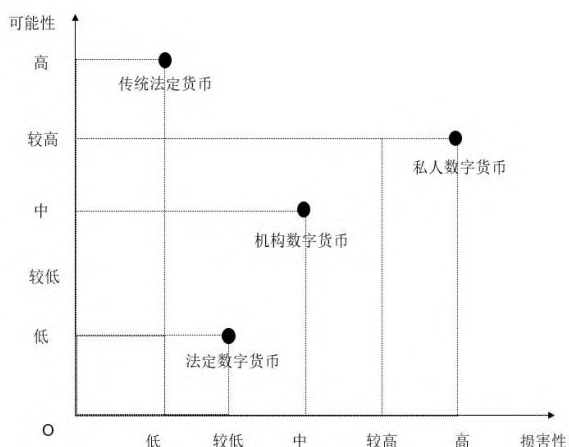


图1 私人数字货币的风险矩阵

资料来源:同济大学经济法治研究中心绘制

(一)金融风险:私人数字货币引发的金融风险与监管漏洞

1. 影响法定货币发行量的确定,引发货币政策风险

自从比特币于2009年初发行以来,私人数字货币的全球化进程加快,使用可能性日益提高。就私人数字货币发行而言,要么采用去中心化的公有链发行结构,要么采用弱中心化的联盟链发行结构,而无论选择哪一种,其发行与流通都具有繁杂性和较大的监管难度。

从国内层面看,我国无法完全限制私人数字货币利用区块链技术进行的“超主权”发行,且难以通过现有金融监管体系确定其在我国的使用情况。从国际层面看,私人数字货币的发行不与某个国家或地区的经济总量挂钩,其发行量不断“膨胀”且难以准确估计。各主权国家在增发法定货币时,对于私人数字货币一定时期的发行量无法考量也不应当考量,否则法定货币增发的收益将由私人占有。个人用来购买私人数字货币的法定货币不会被“冷却”,而是从私人数字货币生产者、原持有者一方流

入社会。同时,买家购买的私人数字货币也会流入社会,用来兑换与其所“认定”的交换价值相当的商品。实际上,私人数字货币的“铸造”并未消耗相应的社会生产力。因此,社会中的货币总量总体大于整个社会的生产能力,从而可能导致通货膨胀。

从私人数字货币的兑换动因来讲,在主权法定货币面临弱势或是币值不够稳定时,私人数字货币的持有率、使用率仍可能在严格管控下逆势增长。不法分子出于转移赃款等因素,也有将资产转移到国外的需求。然而,私人数字货币可以不经第三方完成匿名兑换,兑换隐蔽且便捷,亦可大量控制。从私人数字货币的获取来讲,买方既可利用虚假身份直接在线上从不规范的国外私人数字货币交易所购买,也可无须提供任何身份证明直接从本地“挖矿者”或外来游客中购买。比如,到中国旅行和工作的人有可能将其持有的私人数字货币带入我国并与相关需求方完成交易,待交易完成后,私人数字货币可直接被带到国外兑换为外币或者用于消费,这给现有外汇管理制度带来巨大挑战,不排除会出现资本外逃、货币汇率波动的可能性,并削弱国家对私人数字货币投资炒作的抵御能力。

综上所述,现阶段由于对私人数字货币发行缺乏有效治理,出现了私人数字货币野蛮生长的乱象。而且,私人数字货币可能会从货币供应量、基础货币、货币流通速度、利率政策、货币政策传导机制等方面影响我国中央银行货币政策的制定和运行^[12]。我国现有的监管体系不足以监测与协调应对私人数字货币带来的金融风险,原有数字货币政策或将导致宏观调控偏差。基于此,我国亟待出台应对私人数字货币发展新形势的相关货币政策。

2. 冲击金融监管体制,带来金融监管套利风险

对于私人数字货币的金融监管,各监管部门的具体监管职责划分尚不明确,而职责不清的“分业监管”会产生监管空隙,为私人数字货币的不良发展预留空间。私人数字货币使用与流通不受地域限制的属性,以及某些国家对私人数字货币采取合法化甚至大力支持的政策态度,很可能导致私人数字货币转为“地下货币”,成为各类经济犯罪甚至暴力犯罪的“基础设施”,各主权国家将为此承受巨大的金融监管压力。从当前各个国家私人数字货币

的监管政策来看,我国的监管理念有其独特性。具体来说,我国采取“一刀切”政策否决私人数字货币的发行与交易。诚然,这种金融监管理念在短期监管上具有相当程度的有效性,它使得过热过乱的私人数字货币市场实现了短暂的冷却,有效遏制了首次币发行(ICO)及私人数字货币交易带来的金融乱象,也为我国私人数字货币治理路径设计争取到了时间及借鉴他国治理经验的余地。然而,倘若考虑将“一刀切”否决私人数字货币的政策作为长期治理方式,那么就需要金融监管机构相机对此抉择并适当调整治理政策。

现阶段,我国已经形成了以国有控股金融企业为主,银行、证券、保险和其他非银行金融机构相结合的金融体系,并构建了以机构监管为特征、以合规监管为重点的“分业监管”体制。然而,长期以来,中国人民银行与银保监会、证监会之间监管职责不清,且存在协调合作、资源共享、信息交流不足的突出问题。随着大数据、区块链与人工智能技术的突飞猛进^[13],尤其是在私人数字货币快速繁荣的大环境下,传统金融环境呈现出新的特点:一是各种传统金融业务随着区块链技术的发展相互渗透,金融机构经营业务日益综合化、多元化,金融衍生产品不断创新,产品结构体系越来越复杂,金融服务边界日渐模糊;二是金融市场全球化加快,全球贸易、投资、货币、资本流动格局发生重大变化,金融机构活动日益国际化。这些新特点、新形势要求国家对现行金融监管体制进行适当改革,以更好地适应区块链技术驱动下私人数字货币以及货币金融行业的创新发展。

(二)技术风险:私人数字货币发展时间短,技术成熟度低

私人数字货币作为区块链技术深化应用的产物,高度依赖于计算机技术与网络。由于计算机硬件与软件基础具有不完备性,私人数字货币面临着硬件与软件层面的风险。私人数字货币要求用户记忆私钥,而私钥的高度复杂性、不可找回性驱使用户往往依赖于数字货币钱包软件存储私钥,难以在物理层面留存使用。私人数字货币的假名性导致私钥成为唯一的使用数字货币钱包的手段,除此

之外没有其他身份验证工具。任何持有私钥的人都可以使用对应账户下的私人数字货币,这会带来很大的风险。当出现计算机病毒或硬件故障时,用户有极大概率陷入私钥难以找回的困境,就会导致资产损失。同时,网络黑客可以利用软件的程序故障进行攻击,窃取用户私钥,轻而易举地转移资产并逃脱惩罚。私人数字货币的交易高度依赖网络,基于全网所有账本的对比要求使得交易无法离开网络。尽管私人数字货币的产生与发行比较安全,交易时也能够较好地防止“双花(Double Spending)”问题,但是其需要在中间交易所进行交易的特点,使得黑客可针对中间交易所进行网络攻击,从而影响交易的安全性。申言之,中间交易所系统的稳定性与网络安全程度,同样影响了私人数字货币的交易安全性。由于私人数字货币的不可找回性,中间交易所成为私人数字货币链条中风险较大的一环。

尽管私人数字货币的唯一性识别技术是基于哈希算法下的加密技术,但哈希算法内部同样会发生迭代,针对哈希算法的碰撞破译仍然存在。哈希算法(MD5)具有“数字指纹”特性,是目前应用最广泛的一种文件完整性校验和(checksum)算法^[14]。然而,哈希算法在技术底层无法避免碰撞的产生,且现阶段针对哈希算法的碰撞攻击已经发生。私人数字货币广泛使用的“安全哈希”只能保证较低的碰撞概率。尽管社会层面对哈希算法的迭代正在进行^[15],但是随着计算机性能的发展以及区块链、量子计算技术带来的算力增长,私人数字货币底层技术(如加密算法等)的安全性仍旧面临挑战。

(三)法律风险:针对私人数字货币的法律规范不足

1. 缺乏相应的税收政策,存在偷税漏税风险

从私人数字货币的技术原理看,它具有排除中心化机构发行与流通、采取点对点匿名交易等特性,从而降低了贸易监管和协调成本,加快了交易速度,常常被用来进行跨境贸易。然而,正是由于私人数字货币具备这些内在特性,给执法部门监测交易记录、识别交易方、探寻课税对象等方面的工作带来较大困难,导致私人数字货币成为了国际偷税漏税的金融工具。与此同时,我国对于私人数字货币缺

乏相应的税收政策,致使偷税漏税风险较为严重。一方面,我国在私人数字货币的取得、兑换、增值等层面没有进行相应的征税规定。具体而言,无论是对于通过“挖矿”或其他权益证明取得私人数字货币的行为,还是对于利用私人数字货币兑换商品以及用商品来兑换私人数字货币的行为,亦或是对于企业及个人通过经营或者其他方式使得私人数字货币资产增加的行为,我国都没有相应的征税规定。另一方面,尽管我国与其他国家订立了关于关税以及打击偷逃税的协定,但是各国对于私人数字货币的征税规定以及治理态度具有显著区别,难以达成明显共识,这便导致对私人数字货币的国家征税存在税收监管“缝隙”。我国需要重新梳理、填补因缺乏其他国家的协助而产生的税收监管“缝隙”。

2. 私人数字货币交易中洗钱、恐怖融资活动层出不穷

以比特币为代表的私人数字货币具有匿名交易、超主权国家支付兑换等特点,对于洗钱、恐怖主义融资活动形成天然的技术支撑。私人数字货币加剧了监管之于犯罪难度的不对称。面对私人数字货币交易中层出不穷的洗钱、恐怖主义融资等破坏金融秩序的犯罪行为,我国目前尚缺乏明确的法律层面的规定,使得犯罪愈加方便,监管愈加困难。

首先,私人数字货币所具有的匿名性、难追溯性符合犯罪分子藏匿以及筹集犯罪资金的需要,很可能被犯罪分子用来隐瞒和转移犯罪所得或进行恐怖主义融资。私人数字货币不需要验证用户的身份信息,仅需要交易双方的付款、收款地址即可完成资金的转移。即使交易双方需要在实名认证的中心化的数字货币交易机构进行交易,但是由于这些交易机构本身就是营利性质的,因此可能疏于实质审查,并纵容不法分子冒用他人身份进行注册。

其次,私人数字货币的法律性质和法律责任尚不明确。如我国相关法律政策将私人数字货币定义为“虚拟货币”,但虚拟货币并不是明确的法律概念,具有较强的模糊性,容易与传统互联网阶段的社区“虚拟货币”(如 QQ 币)发生混淆,不利于对洗钱犯罪、恐怖融资犯罪的法律追诉。当前,我国制定的《关于防范比特币风险的通知》《关于防范代币发行融资风险的公告》等规范性文件的法律位阶普

遍较低,且相关规定不够细致,导致在具体的反洗钱、反恐怖融资犯罪等活动中操作性不强。

最后,洗钱、恐怖主义融资活动呈现国际化趋势,而国际社会缺乏对于防范利用私人数字货币进行洗钱的国际协定。私人数字货币的各种“基础设施”广泛分布在多个国家,犯罪分子不仅能够将私人数字货币转化为法定货币,而且还能通过“跳跃”位于不同法域的私人数字货币“基础设施”来规避反洗钱和反恐怖主义组织的监管政策,从而达到逃脱法律制裁的目的。

四、我国私人数字货币发展风险的系统治理

著名科学家钱学森面对当代科技的快速发展,提出了现代科技体系的结构问题^[16],并通过吸收 Bertalanffy 的一般系统论、Haken 的协同学理论等,提出了系统工程理念^[17]。对于私人数字货币的风险治理同样是一项系统性工程,与域外发达国家(美国、德国等)对私人数字货币的治理相比,尽管我国在《关于防范比特币风险的通知》《关于进一步防范和处置虚拟货币交易炒作风险的通知》等文件中将私人数字货币定义为“虚拟货币”,并禁止其发行与流通,但这只是从法律层面对其进行限制,还需要配合其他路径展开系统治理(见图 2)。

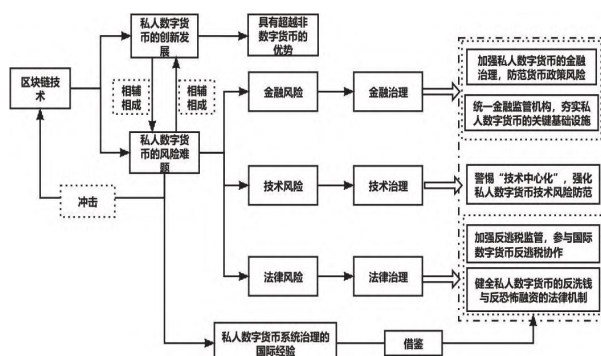


图 2 私人数字货币的系统治理路径

资料来源:同济大学经济法治研究中心绘制

(一) 私人数字货币系统治理的国际经验借鉴

截至 2021 年 6 月底,全球共有约 5460 种私人数字货币在 20445 个交易平台上不间断交易,交易

总额达 1.29 万亿美元^[18]。随着私人数字货币的井喷式增长,各种风险突显,滋生出一系列违法犯罪活动。对此,美国、德国等私人数字货币发展较快的国家从法律定位、金融监管、税收治理、反洗钱反洗钱等方面对私人数字货币进行了系统的治理探索。

首先,在私人数字货币的法律定位方面,不同国家的认定方式有所不同。在美国,金融犯罪执法网络局(FinCEN)将比特币等私人数字货币定义为“可转化虚拟货币”,国家税务局(IRS)认定比特币等可兑换私人数字货币为“应税资产”,商品期货交易委员会(CFTC)则认为其属于“大宗商品”。德国于 2013 年赋予比特币以合法地位,将其列为官方记账单位之一,并且对不同类型的私人数字货币做了法律性质上的区分:一是将私人数字货币认定为支付工具,即支付型数字货币(比如比特币);二是将私人数字货币认定为一种特殊的证券,即证券型数字货币;三是功能型数字货币。其中功能型数字货币不属于金融监管的范围。

其次,在私人数字货币发行以及流通的监管层面,受政治体制的影响,美国采取联邦与州的二元监管模式。根据《证券法》,如果首次币发行(ICO)的公司不满足豁免条件,则须在证券交易委员会(SEC)登记。除此之外,私人数字货币交易服务提供商还须接受州层面的实质审查并申请牌照发放,各个州也分别制定本州的私人数字货币监管规则,各州的监管政策相对独立且监管机构具有多样性。在私人数字货币的监管体系与适用法律方面,德国依照现有的机构设置以及既有法律对私人数字货币进行分类监管,主要由联邦金融监管局(BaFin)对私人数字货币进行统一监管。德国通过《银行法》和《反洗钱法》来对支付型数字货币进行监管;通过《欧盟金融工具市场法》《资本投资法》《证券交易法》来监管证券型数字货币。现阶段,德国尚未针对私人数字货币设立专项监管法规,而是以业务行为作为监管对象,其金融监管领域立法具有全面性和系统性等特征,基本上涵盖了所有金融行为。完善的金融监管体系为德国私人数字货币等金融工具的发展营造了稳健的环境^[19]。另外,德国对私人数字货币交易所以及数字货币钱包管理商实施牌照许可制,任何数字货币交易所或数字资产托管机构

运营都须得到联邦金融监管局批准。其业务开展具体可以分为 3 种形式:一是成立实体公司并申请牌照;二是与有牌照的托管机构合作;第三种是与许可证的提供商协调灵活的营业方案。

再次,在针对私人数字货币的税收政策方面,美国国家税务局(IRS)将私人数字货币与法定货币的兑换、不同私人数字货币之间的兑换、私人数字货币与商品或服务的交易,以及把私人数字货币作为收入的事项都规定为应税事项。IRS 还发布了 2014-21 号、2019-24 号等征税规定。不过,IRS 在实际征税过程中遇到诸多阻碍:私人数字货币的种类和业务繁杂,纳税人对于纳税政策难以准确把握并进行有效申报;私人数字货币交易的隐蔽性及监管的不周延,导致纳税人不想进行有效申报等。在对私人数字货币的课税方面,由于德国将比特币等私人数字货币界定为财产,根据德国当前的税收法律政策,财产的转让需要缴纳增值税,所以德国财政部明确规定比特币交易需要纳税。具体来说,比特币作为商品或财产被购买时,卖方作为比特币的出售者需要缴纳税款;而个人在使用比特币作为支付工具时,则无须纳税。

最后,在对私人数字货币交易中的洗钱等犯罪活动治理方面,美国将私人数字货币交易所等管理服务作为重点监管对象,要求其严格遵守金融犯罪执法网络局(FinCEN)的各项政策规定。管理服务需要对客户做尽职调查,对客户交易记录进行监测、存档,必要时须及时向监管部门汇报。德国则将私人数字货币的使用纳入了反洗钱监管。根据 2018 年《欧盟反洗钱第五号指令(AMLD5)》的规定,私人数字货币被界定为非央行信用的兑换货币,私人数字货币钱包管理服务商与私人数字货币交易所均被纳入反洗钱监管义务主体。德国于 2019 年通过针对《欧盟反洗钱第四号指令(AMLD4)》的修正案,该修正案放宽了私人数字货币的经营和交易,允许金融机构在获得许可证后进行自行管理,而无需再托管第三方机构。通过采用许可证制度并要求相关主体在德国具有法人实体方可开展私人数字货币业务,德国加强了反洗钱与反恐怖组织融资的犯罪治理。

(二)防范我国私人数字货币发展风险的系统治理路径

我们既要正视私人数字货币内在的风险性,也要看到私人数字货币的发展前景。2022年4月初,人民银行联合其他部门共同起草《金融稳定法(草案征求意见稿)》,重点强调防控金融风险、促进金融稳定。基于此,我们应当通过构建系统的私人数字货币治理路径,补齐金融风险防控工作的短板弱项,促进我国私人数字货币的稳健化发展。

1.加强私人数字货币的金融治理,防范货币政策风险

私人数字货币的发行不与社会经济活动总量相对应,尽管从技术原理上说,某些私人数字货币的发行数量具有一定的上限,但是通过类“资产证券化”的方式,比特币被不断细分为更小的份额,其数量上限可能被指数型放大,从而背离了私人数字货币的设计初衷,对传统货币政策造成冲击。在社会经济日益全球化以及私人数字货币超主权国家发行的背景下,现有的单个国家或地区的宏观调控政策初现乏力,致使私人数字货币的金融风险在全球范围内积聚,不排除因其风险蔓延而衍生金融危机的可能性。

为预防私人数字货币引发的货币政策风险,有两种手段可以选择:一种是“硬手段”,国家以极大金融监管代价对私人数字货币的财产信息进行狙击,并通过强化法律手段严厉打击使用甚至持有私人数字货币的个人或组织,以遏制私人数字货币在境内的使用泛化,使其维持在一个相对较低的保有率和使用率;另一种是“软手段”,针对私人数字货币的钱包管理商、中间交易所等中心化运营管理机构,可以通过现有金融机构(如证券公司、商业银行等)对私人数字货币业务进行垄断,增强现有金融机构对于私人数字货币交易市场乃至发行市场的控制力。一旦这种控制力得以形成,我国将垄断第一手私人数字货币的信息交易数据流,为国际反逃汇协作提供筹码,并通过私人数字货币外汇兑换、国际贸易、交易税收政策来影响私人数字货币交易价格。相比较而言,“硬手段”将会在缺乏国家间协作的情况下,使我国承受巨大的金融治理压力,不适宜作为长期手段。基于此,对于私人数字货币对货币

政策的影响,我国应该充分重视并制定相关预案,考虑适当优化当前部分货币政策措施,增强价格型货币政策,相对弱化数量型货币政策,提高利率调控在货币政策中的地位。另外,应积极开展私人数字货币的“封闭实验”以及国际私人数字货币的发展对话,及时了解发展新动向,预判其可能带来的机遇与风险,提前做好货币政策预案,积极参与私人数字货币的全球化金融治理。

2.统一金融监管机构,夯实私人数字货币的关键基础设施

在私人数字货币快速发展的背景下,参照域外的风险治理经验,尤其是德国由联邦金融监管局(BaFin)来进行统一监管的做法,我国可以考虑统一相应的金融监管机构,将中国银保监会与证监会整合到新组建的金融监督管理总局,形成以“中央人民银行—国家金融监督管理总局”为中心的“一行一局”的金融监管结构,从法律层面明确人民银行与金融监管总局之间的职责分配,以适应全球金融一体化、金融业务一体化的趋势和特点。同时,可考虑在统一的金融监管机构层面试点“私人数字货币监管沙盒”,即在“一行一局”的新监管机制下开展“沙盒试点”,明确私人数字货币从业机构等进入“沙盒试点”的测试主体的标准和业务范围,规定私人数字货币交易商、管理商在试点沙盒中需要履行的监管义务和所应担负的法律责任。在监管实践中检验新监管机制的协同性与有效性,权衡私人数字货币的创新性与稳定性,针对“沙盒试点”中出现的各种情况及时调整金融监管措施,合理借鉴英国、美国等国家“监管沙盒”的实践管理经验,探索出符合我国国情的包容审慎的监管范式。

我国应当利用自身的优势技术与信息网络资源推动私人数字货币基础设施建设,包括支持或影响私人数字货币发行,由中央银行或者商业银行等金融机构垄断关键私人数字货币基础设施的建设等。我国可以联合其他国家共同加强私人数字货币基础设施建设,推动注资、交易节点认证实名制,对用户身份信息进行实质审查并录入私人数字货币数据库,监测主流私人数字货币交易所的报价数据。还可以通过监测、抓取、记录、追踪主流私人数字货币交易数据流,建立私人数字货币大数据库,

积极与世界各国围绕私人数字货币开展协同治理,建立信息共享机制,防范由私人数字货币引发的洗钱、逃税、恐怖融资等犯罪风险。

3.警惕“技术中心化”,强化私人数字货币技术风险防范

私人数字货币的去中心化并非完全的去中心化,而是排除国家货币发行垄断的“技术中心化”,这就意味着区块链技术将会取代包含人在内的其他主体而成为唯一责任承担者。届时,社会财富将以数字技术的形式暴露于区块链网络之上。对于掌握了大量数据甚至私钥的私人数字货币交易所或其他私人数字货币从业组织来说,其不仅要面临各种掌握黑客技术的犯罪集团的觊觎,还要面临自身内部的安全问题。私人数字货币发展时间较短,技术成熟度低,而数字技术迭代迅速,各种拥有超级算力的计算机层出不穷。以比特币为例,在巨大的利润诱惑下,众多庞大的算力机器牢牢握在“算力寡头”手里,在比特币开采完毕之后,这些庞大的算力机器有可能会被加以利用转而成为掠夺私人数字货币的犯罪工具。私人数字货币仍处于不成熟的阶段,其底层技术的突破与安全性的及时补强将是一项长期工作。

我国要时刻注意自身私人数字货币技术成熟度低的不足,警惕“技术中心化”的风险,坚持以数据保护为总抓手,以个人与管理服务商两类主体为保护对象,强化私人数字货币的技术风险防范。一是要在智能合约(Smart Contract)录入前进行法律审核与技术代码审核,加强代码之治(The Rule of Code),实现技术代码、金融监管、法律规制等多维治理。二是要警惕自然灾害、战争、公共卫生危机(如 COVID-19)等突发事件,防范突发事件造成的算力塌方,进而引发对私人数字货币的“算力洗劫”。三是要及时更新私人数字货币所应用的底层技术,加强技术层面的治理。四是要加强个人私钥数据保护以及管理服务商数据保护。五是要加大对互联网与区块链网络的巡查力度,及时发现并打击钓鱼网站。六是要利用新型金融监管科技进行追赃,通过利用区块链、大数据挖掘、云计算、人工智能等技术,深化金融监管科技的应用,对区块链的链上交易进行链上追赃,积极应对区块链技术驱动下的

私人数字货币创新发展。

4.加大反逃税监管力度,积极参与国际数字货币反逃税协作

在私人数字货币的税收管理层面,尽管我国早在2008年就发布了《关于个人通过网络销售虚拟货币取得收入计征个人所得税问题的请示》的批复文件(国税函[2008]818号),规定对网络销售虚拟货币转让获利行为进行征税,但是该批复文件发布时间早于比特币等私人数字货币发行时间,而且这里所指的虚拟货币并非私人数字货币,而是网络玩家的虚拟货币,因此对私人数字货币并不适用。税收属于法律的相对保留事项,私人数字货币发行后出台的相关法律政策文件即使将私人数字货币定义为虚拟货币,但是因为其法律位阶低,而且虚拟货币的法律内涵与私人数字货币不同,同样不能成为对私人数字货币征税的法律依据。

私人数字货币具有业务与风险的跨国界性。在幅员辽阔、人口众多、技术深化的资源禀赋下,即使我国对私人数字货币采取“一刀切”的否定政策,但是在区块链技术渗透下我国依然是私人数字货币的重要市场,并且将直接或间接承担私人数字货币所带来的各种风险。在国际反逃税方面,已经出现了一些新的形势:一方面,税收利益争夺和税收竞争已经在国际层面展开,各国要么为私人数字货币征税做长期准备,要么已经对私人数字货币开征各种税目;另一方面,各国正在积极洽谈以凝聚共识,试图通过国际标准制定以及国际协作来破解私人数字货币国际化发展的税收管理难题。

在这种私人数字货币反逃税新形势下,对外我国应当积极参与关于私人数字货币征税标准、征税政策的国际协定,在不弱化我国税收主权的情况下与他国达成一定共识。在新的共识基础上加强私人数字货币反逃税监管的协同力度,建立税收信息共享系统。对内我国应当配套反逃税立法,在法律框架内对私人数字货币逃税行为进行治理:一是在《税收管理法》和《刑法》中明确利用私人数字货币进行偷逃税的行为认定与责任承担。二是最高人民检察院与最高人民法院应尽快出台相应的配套司法解释,发布指导性案例以统一起诉、裁判的标准。三是国家税务和海关部门应在治理逃税事件

的基础上出台典型的行政处罚案例。

5. 健全私人数字货币反洗钱与反恐怖融资的法律机制

在私人数字货币犯罪防范层面,我国尚未出台专门的法律,也未出台相应的司法解释或指导性案例。我国迫切需要健全私人数字货币的反洗钱与反恐怖融资的法律机制。

第一,增强监管力度,遵循国际准则,切实履行反洗钱监管义务。金融行动特别工作组(FATF)分别于2015年和2018年发布了《关于虚拟货币的风险为本方法指引》和《金融行动特别工作组建议》,确立了反洗钱的国际标准以及各国在反洗钱中的国际义务^[20];一是制定切实可行的私人数字货币反洗钱风险防范措施,防患于未然。二是切实履行对于私人数字货币客户的尽职调查。三是切实履行记录与报告可疑交易的义务。遵循国际准则,及时与其他国家制定相应的监管合作计划,推动私人数字货币的反洗钱工作,减少与其他国家间的监管摩擦;增强对私人数字货币的管理商、交易商、金融机构的内部控制和风险管理,密切关注私人数字货币发展的新形势,将私人数字货币纳入反洗钱的监管范围,并对监管主体、监管内容、监管程序、监管对象作出明确规定。

第二,加大反恐怖融资打击力度,加快对《刑法》的修订,对于利用私人数字货币进行恐怖主义融资的行为施以严厉的法律制裁。根据罪刑法定原则,法无明文规定不为罪,法无明文规定不处罚。因此,我国需要加快《刑法》的修订,将利用私人数字货币进行恐怖主义融资的行为规定为犯罪,同时还应规定利用各个法域的监管“缝隙”组成完整恐怖主义融资组织的行为以及各个法域中有关私人数字货币交易商、管理商的协助行为均构成犯罪。在必要的情况下,我国《刑法》可以根据犯罪的形式规定私人数字货币交易商、管理商的过失犯罪。相较于普通金融产品,私人数字货币具有更高的内在风险,它可能会放大恐怖主义融资的风险,对社会造成更大的危害性。根据罪刑相适应原则,我国可以将利用私人数字货币进行恐怖主义融资的行为规定为情节加重犯。

五、结 语

纵观货币发展史,从最初的商品货币(大麦)发展至当今的数字货币,货币伴随人类社会经济发展几经变革,其内在经济价值逐渐退化,由商品货币转向了信用货币,由实物货币转向了信息货币。不仅货币的形式发生巨大变化,在区块链技术的驱动下,国家的货币垄断发行权也受到挑战;以技术背书的去中心化私人数字货币(如Bitcoin)、以私人组织信用背书的机构数字货币(如Libra)、以国家信用背书的法定数字货币(如E-CNY)三者之间展开激烈竞争。私人数字货币以其匿名、难以篡改、不可复制、点对点交易等突出特点深受货币金融市场青睐,并为货币全球化发行与流通提供了一次“社会信用实验”。然而,由于金融监管的滞后性,区块链技术驱动的私人数字货币以及基于区块链技术优点所“锻造”的“社会信用实验”被其内生性风险所“消费”。私人数字货币裹挟着金融风险、技术风险、法律风险,对我国的治理体系形成巨大冲击,再加上区块链技术的内在局限,以及无主权信用背书、无内在经济价值等缺陷,私人数字货币的法律地位饱受质疑。我们既要承认区块链技术驱动下私人数字货币的发展性,也要正视其风险性,并通过采用系统治理路径,全面防范风险,促进我国私人数字货币稳健发展。

参考文献:

- [1] 程雪军.央行数字货币对商业银行的影响与回应[J].当代经济管理,2022,(4):88-96.
- [2] Glyn Davies.A History of Money-From Ancient Times to the Present Day[M].Cardiff: University of Wales Press,2002. 34-65.
- [3] 万志英,王文成.11~18 世纪中国的货币与货币政策[J].思想战线,2012,(6):74-78.
- [4] 姚前,陈华.数字货币经济分析[M].北京:中国金融出版社,2018.3.
- [5] 穆杰.央行推行法定数字货币 DCEP 的机遇、挑战及展望[J].经济学家,2020,(3):95-105.
- [6] 徐忠,汤莹玮,林雪.央行数字货币理论探讨[J].中国金融,2016,(17):33-34.

- [7] 贾丽平. 比特币的理论、实践与影响[J]. 国际金融研究, 2013,(12):14-25.
- [8] 高峰, 毛洪亮, 吴震等. 轻量级比特币交易溯源机制[J]. 计算机学报, 2018,(5):989-1004.
- [9] 李向阳. 布雷顿森林体系的演变与美元霸权[J]. 世界经济与政治, 2005,(10):14-19+4.
- [10] 何帆, 张明. 国际货币体系不稳定中的美元霸权因素[J]. 财经问题研究, 2005,(7):32-37.
- [11] 兰永海, 贾林州, 温铁军. 美元“币权”战略与中国之应对[J]. 世界经济与政治, 2012,(3):121-137+159-160.
- [12] 李真, 刘颖格, 戴祎程. Libra 稳定币对我国货币政策的影响及应对策略[J]. 西安交通大学学报(社会科学版), 2020,(3):55-63.
- [13] 程雪军. 人工智能深度介入消费金融: 动因、风险及防控[J]. 深圳大学学报(人文社会科学版), 2021,(3):67-76.
- [14] Monika Parmar, Harsimran Jit Kaur. Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things[J]. International Journal of Advanced Computer Science and Applications (IJACSA), 2021,12(3):1-11.
- [15] Ammar Mohammed Ali, Alaa Kadhim Farhan. A Novel Improvement With an Effective Expansion to Enhance the MD5 Hash Function for Verification of a Secure E-Document[J]. IEEE Access, 2020,8: 80290-80304.
- [16] 钱学森. 系统科学、思维科学与人体科学[J]. 自然杂志, 1981,(1):3-9+80.
- [17] 钱学森. 再谈系统科学的体系[J]. 系统工程理论与实践, 1981,(1):2-4.
- [18] 陈伟光, 明元鹏. 数字货币: 从国家监管到全球治理[J]. 社会科学, 2021,(9):13-27.
- [19] 高洪民, 李刚. 金融科技、数字货币与全球金融体系重构[J]. 学术论坛, 2020,(2):102-108.
- [20] 兰立宏, 庄海燕. 论虚拟货币反洗钱和反恐怖融资监管的策略[J]. 南方金融, 2019,(7):61-68.

【责任编辑: 龚紫钰】

Risks and Regulation of the Development of Private Digital Currencies Based on Blockchain Technology

CHENG Xue-jun^{1,2}

(1. Law School of Tongji University, Shanghai, 200092;

2. Institute of Finance and Banking, Chinese Academy of Social Sciences, Beijing, 100710)

Abstract: Private digital currencies have entered our life and rapidly developed with blockchain technology. From historical perspective, currencies have gone through four major stages of commodity currencies, metal currencies, legal tenders, and digital currencies, and the transition from legal tenders to digital currencies is a big leap. Being an important part of digital currencies, private digital currencies have advantages over non-digital currencies. They are built upon blockchain technology and take distributed ledgers as the transaction prerequisite, which is conducive to the internationalization of currencies. Although the development of private digital currencies has greatly boosted financial innovation, there are great financial, technical and legal risks in the development of private digital currencies. We can draw on the risk management experience of private digital currencies in foreign countries to formulate systematic measures to regulate private digital currencies and promote the steady development of private digital currencies in China. Firstly, we need to put more efforts in regulating private digital currencies to guard against monetary policy risks. Secondly, we need to unify financial regulations to consolidate the critical infrastructures for private digital currencies. Thirdly, we need to be wary of technocentrism and improve risk management. Fourthly, we need to toughen supervision over tax evasion, and actively participate in the international cooperation against tax evasion with digital currencies. Lastly, we need to improve the anti-money laundering and anti-terrorism financing mechanisms for private digital currencies to prevent crimes with digital currencies.

Key words: blockchain technology; digital currency; private digital currency; financial risks; systematic regulation; Financial Stability Act