Doi:10.11835/j.issn.1008-5831.fx.2021.06.001

欢迎按以下格式引用:马永强. 区块链金融的刑法风险与规则之治[J]. 重庆大学学报(社会科学版),2022(5):249-262. Doi:10.11835/j.issn.1008-5831.fx.2021.06.001.

**Citation Format**: MA Yongqiang. Criminal law risks and rules of governance in blockchain finance[J]. Journal of Chongqing University (Social Science Edition),2022(5):249-262. Doi:10.11835/ j.issn.1008-5831.fx.2021.06.001.

# 区块链金融的刑法风险与规则之治

马永强

(大连海事大学 法学院,辽宁 大连 116026)

**摘要**:区块链技术的特征,一方面奠定了其在金融这一文明社会重要基石中的应用可能性,另一方面也为区块链金融活动中的不法风险埋下了线索。基于区块链技术的实际金融应用场景,区块链技术在金融领域之应用的不法风险,首要体现为以加密货币为基础的区块链金融生态对于骗购外汇类犯罪与洗钱犯罪的助推。区块链ICO等中心化金融活动,更是带来了诸如内幕交易类犯罪、金融诈骗犯罪等扰乱金融秩序的不法风险。区块链技术的进一步发展和应用,还催生出基于智能合约的去中心化场景下的犯罪形态。思考区块链金融犯罪的规则之治,现行法规范的缺乏与区块链技术的风险内生性,共同导致了相关犯罪的认定困难。因此,为了更好地应对区块链金融领域的刑法风险,需要遵循内外有别的原则来对相关风险加以规制。就外部视角而言,为了将区块链金融犯罪纳入刑事法治的轨道,首先必须重新评估加密货币的刑法定性。对此,应当区分不同加密货币的性质来分情况讨论。同时,还需对区块链技术发展主体的法律地位予以明确,合理界定相关区块链企业的平台责任及监管方式。应当反思当前"一刀切"的监管方式,采用带有包容性特征的监管沙盒模式,允许相关企业在可控的范围内开展颠覆式创新,并基于包容审慎的监管方式合理设置平台责任。就内部视角而言,区块链领域的规则之治还要求区块链企业整合刑事合规要求作为内部控制手段。具体而言,涉及区块链信息服务的相关境内企业应当切实履行国内监管要求;涉及区块链金融服务的相关企业应当切实履行反洗钱义务,整合FATF和各国的反洗钱国内法规做好合规工作;涉及区块链金融交易的相关企业则应密切关注金融交易类的犯罪风险,建立和完善金融证券犯罪风险的刑事合规;涉及区块链智能合约研发的相关境内外企业则应积极推动企业刑事合规与区块链代码的整合。以内外兼修的方式完善区块链的监管方式与规则之治,促使刑事法治对区块链金融犯罪做出积极回应,将有助于更好地推动区块链金融领域的创新,助力我国数字经济行稳致远。

**关键词**:区块链;加密货币;虚拟货币;智能合约;刑法风险;刑事合规

**中图分类号**:D924.33 **文献标志码**:A **文章编号**:1008-5831(2022)05-0249-14

**基金项目**:中央高校基本科研业务费专项资金资助项目"弱人工智能时代的刑事风险规制"(3132021292)

**作者简介**:马永强,大连海事大学法学,Email:pony@ pku.edu.cn。

作为互联网技术演化的最新成果,区块链技术正在为人类社会带来新的愿景和想象,同时也带来了新的风险。不同于传统互联网仅仅致力于信息的传输和多样化呈现,区块链技术集中解决的是无需中心化验证的信任问题,自其产生的母体开始,就与金融这一现代社会的重要制度基石密切关联[1]。甚至可以明确地说,对于去中心化和不可篡改的信息验证机制而言,其至为重要的应用领域就在于金融领域,比特币及其他加密货币是区块链技术的金融面向中不可分割的重要组成部分。这些技术实践和金融创新实践,既在无政府主义的旗帜之下,上演着对既有金融秩序的突围和挑战[2],也在这个过程中衍生出许多不法风险。例如,比特币等基于区块链技术的支付系统,正在成为外汇犯罪或洗钱类犯罪的技术支持手段;更有行为人以区块链技术为噱头,虚构区块链的应用场景,以区块链技术创新为名,实施各种类型的"割韭菜"行为,其中许多行为样态已经逾越了刑事法秩序的界限①。

在这一背景下,基于区块链金融的犯罪问题不再是遥远的想象,而是一个正在发生的现实风险。相应地,在数字化生存的时代命题之下[3],如何对这些行为予以评价,不仅是一个金融监管议题,同时也是一个亟待讨论的法律问题乃至刑法学课题。在相关讨论尚处于起步阶段的背景下,本研究旨在标定进阶讨论的准确坐标。具体而言,本文首先试图探讨区块链技术的特征及其在金融领域的应用,进而在观念和行为类型上梳理区块链金融领域之犯罪的若干行为类型,最后对区块链金融领域的相关犯罪行为的刑法规制争点和刑事合规等内外部监管方面的应对措施予以研讨,从而内外兼修地明确区块链金融领域的规则之治。

## 一、区块链技术的金融应用及其不法风险

区块链技术的特殊属性,一方面奠定了其在金融领域的重要应用,另一方面也助推了区块链金融活动中的诸多不法风险。对于这些不法风险的理解,既需要准确把握当前区块链技术的主要金融应用场景,也需要对区块链技术的相关特征及特殊属性有明确认知。区块链技术在金融应用中的不法风险,集中表现为区块链技术本身的去中心化特征与金融的中心化管制之间的张力。妄置文明社会管控要求于不顾的去中心化实践,必将带来逾越法秩序的后果。

### (一)区块链技术的特征及其金融应用场景

区块链技术并非原创性的技术,而是基于密码学知识对互联网领域的多个既有技术的整合,并集中体现于比特币等应用实践。简言之,区块链是一种点对点的分布式账本[4]16。自2009年产生以来,区块链技术在发展愿景和路线图层面被业内人士概括为三个重要的发展阶段[5],这三个阶段均与加密货币这一应用场景相关。第一阶段以比特币为中心,此时的区块链尚不支持应用开发,仅仅作为不可篡改的匿名账本系统而存在,且PoW共识机制存在能耗问题;第二阶段以Ethereum为核心,区块链平台开始支持智能合约和应用开发,但囿于PoW共识机制等技术方面的局限,存在可拓展性问题;第三阶段以Ethereum 2.0、Cardano、Polkadot等基于PoS共识机制的第三代区块链技术为代表,致力于打造区块链3.0时代可拓展的公链平台,将区块链技术推向包括Web3应用、人工智能技术整合等更为广泛的应用场景。从现实的技术演进角度看,第三代区块链技术的发展尚不成熟,目前的区块链技术整体上仍处于2.0时代。甚至,以Ethereum为核心的第二代区块链技术,也很难说已经产生革命性的区

①我国的相关判例,如"赵运等非法吸收公众存款案",参见北京市东城区人民法院(2016)京0101刑初144号刑事判决书;又如"郝铃声、杨放犯集资诈骗案",参见广东省高级人民法院(2020)粤刑终624号刑事判决书。

块链应用[6]。区块链技术的应用整体上仍然处在探索期,并形成了区块链行业与实体产业相融合的展望。而在诸多区块链技术的应用落地方向中,金融呼声甚高。

众所周知,区块链技术具有三大重要特征,分别是去中心化、数据的不可篡改性和非对称加密算法。这三大特征的核心是通过去中心化实现信任问题的解决。如果说基于记账技术的数目字管理是早期资本主义的核心技术之一[7],那么融合了数字化时代诸多技术成果的区块链技术则在结果上带来了对传统数目字管理方式的颠覆式创新。这既引领了金融领域在数字时代的巨大变革,也倒逼传统金融机构学习和采纳区块链技术,开展区块链领域的创新和应用。

我们可将区块链金融界定为区块链技术在金融领域的应用。当前引起广泛讨论的区块链金融形态体现为“区块链+货币”“区块链+银行”以及“区块链+证券”[8]。在这三大领域的应用中,“区块链+货币”和“区块链+证券”是当前的主要应用场景。这里的“区块链+货币”集中体现为当前加密货币的应用,其法律地位尚存争议;“区块链+证券”则集中体现为基于加密货币所开展的 ICO 等融资活动。此外值得注意的是,近年来,依托于 Ethereum 等公链平台,兴起了一系列去中心化金融应用(DeFi),其虽尚处在发展早期,但却标志着新兴区块链金融科技领域的去中心化交易平台(如 Uniswap、Compound)以及去中心化金融活动的落地生根。与此同时,非同质化代币(NFT)的出现,也为知识产权、金融票据、身份证明、资产流通等领域的代币化实践奠定了基础。在传统金融领域,以我国的央行数字货币(CBDC)为代表的由国家信用作为背书的区块链应用尝试,也在积极实验之中。概言之,当前主流的区块链金融实践是围绕加密货币展开的,并在 DeFi 的发展中日渐壮大,这是区块链技术冲击传统金融秩序的体现;传统金融领域基于智能合约对区块链技术的探索和开发,则是仍处在探索期的创新活动。

首先,由于技术创新的困难性,有必要理性审视当前区块链技术的发展阶段,并准确识别当前以加密货币为核心的区块链金融实践和应用场景。虽然在产业政策层面,我国政府积极推动区块链技术的产业落地,特别是积极提倡区块链与当前各行业之间的应用场景对接,但由于技术创新的隔时性与困难性,相关尝试仍处在探索期。而从世界范围来看,当前区块链技术的实际应用场景则仍与加密货币相关联,在“万币齐飞”的热闹景象背后,真正成熟的技术创新凤毛麟角[9],且对日常生活的改善极为有限,其发展阶段类似于 20 世纪 90 年代的早期互联网。当然,区块链技术之所以能够在短短数年内成为世界瞩目的创新焦点,其背后的代币开发、购买支付、投资变现等较为完整的产业链是不容被忽视的过程,正是在这种便利融资的创新机制的催化中,各种区块链的新尝试才如雨后春笋般迸发[10]。区块链团队可以通过各类(去)中心化金融活动获得技术创新所需的发展资金,相关技术创新具有充分的资本保障。然而,由于共识形成和技术创新的困难性,即便存在这一不同于传统技术创新过程的新型融资手段,当前区块链技术的发展和落地仍无法一蹴而就。虽然人们已经在普遍展望区块链技术在各个社会领域中的应用,但区块链的技术开发过程仍然存在大量需要解决的难题。因此,研究者必须认识到当前的区块链实际应用场景仍然是以加密货币为核心的,并对这一现实持一种理解的态度。

其次,在区块链金融的发展过程中,智能合约将是一个极具想象空间的重要应用场景。智能合约是第二代区块链技术的产物,使得区块链不再仅仅是一个数据库,同时也具备了应用于具体现实的可能。智能合约可以排除合约履行过程中的人为影响,不依靠第三方权威机构的信用即可建立充分信任的交易方式[4]262-264。但是,值得注意的是,智能合约本质上是基于技术逻辑建构起来的,这就意味着,编程活动起到了与立法相类似的作用,甚至代码即是法律[11],这必然带来对既有法律制度的冲击。原

因在于,在智能合约的美好蓝图中,我们假定代码是完美的,但这却并非现实生活中的常态。不仅代码本身可能会存在瑕疵而被犯罪人利用,代码也可能成为犯罪人直接参与缔造的工具。例如,一系列基于DeFi平台的"空气币"骗局,已经让这一问题显露端倪。当然,这并不构成对于区块链技术的全然否定,而是说除了代码本身的规则设定以外,依靠法律的区块链治理是必要的。

综上所述,纵览全世界范围内区块链技术的发展现状,当前区块链技术的主要金融应用场景仍然以依托于加密货币的(去)中心化代币发行、交易、借贷等金融活动为核心。虽然可能会有观点认为,对于区块链之价值的探讨不应局限于加密货币层面,但是不可否认,当前区块链技术的普遍性应用场景仍然依托于加密货币这一生态链,区块链技术在支付结算领域的金融应用,也集中体现为加密货币的交易过程。正是加密货币这一区块链技术的主要金融应用场景,对既有制度安排形成了重大挑战,进而产生监管上的迫切制度需求。因此,在当前的监管和规制需求的语境下,必须准确识别上述区块链技术的特征及其金融应用,以明确区块链金融犯罪的现实背景,并基于这一现实有针对性地展开理论思考与实践规制。

**(二)区块链技术的去中心化属性及其不法风险**

区块链是一种数据存储机制,其重大意义在于形成一种虚拟世界中的共识机制,共识的核心建立在区块链技术的去中心化特征基础上。甚至可以说,去中心化是区块链的本质属性。亦即,正是因为任一个体无法控制或篡改区块链上的信息,才摆脱了传统情形下由于中介机构的存在而导致的各类运作成本和寻租问题,使得区块链是可信赖的。基于对区块链技术的信任,人们取得了信任和共识[12]。当然,这也导致了一个重大问题:由于区块链的去中心化特征,必然导致其与监管之间存在张力。

原生的区块链技术与监管之间的张力,已经在实践中得到了充分证明。虽然自由至上主义的意识形态为加密货币的应用提供了理论根据[13],但实践中现实的一面表明:一旦某种完全不受限制的基于自发秩序的技术实践脱离了现代社会制度的制约,就很容易陷入一种古老而熟悉的人与人之间的自然状态,例如加密货币与"丝绸之路"暗网的结合,以及The DAO被盗事件所呈现出的混乱,均表明了绝对去中心化理想的幻灭。马斯克曾在推特上频繁"带货"狗狗币,并因其言论的反复无常加剧了比特币价格的大幅波动,致使大量使用杠杆的非理性投机者爆仓,此类事件更是加重了大众对区块链金融风险的担忧和疑虑。

事实上,为了解决区块链技术的应用与监管之间的张力,银行等传统金融服务机构也在尝试对区块链技术进行取舍。在这种探索中,形成了公有链、私有链和联盟链的区分,其中,带有中心化和封闭性特征的私有链被认为是较为理想的区块链尝试[14]。但问题是,中心化的私有链将更加无法避免以内部人和中介寻租为特征的金融领域犯罪。甚至,由于区块链的本质特征体现为去中心化的信任机器,其所欲解决的正是中心化金融可能存在的顽瘴痼疾,若完全地抛弃了去中心化的特征,则区块链技术本身也会丧失其意义。

总之,相较于未来的技术发展趋势,法学研究者更为关心当下具有法律评价意义的行动或事件。相应地,必须认识到区块链技术的去中心化特征是不可避免的,从这一视角出发,研究者必须正视当前区块链技术的主要金融应用场景及不法风险集中体现于去中心化的加密货币,未来区块链的重要金融应用场景在于智能合约,从而针对性地对相关场景下的监管问题有的放矢地展开研究。在当前区块链的多数应用仍停留于观念想象,对比特币等加密货币和加密货币平台等现实性事物的规范认知尚未建立的语境下,应当将思考和关注的中心,集中于对区块链加密货币相关金融实践中的刑事不法问题的

界定和审查。

## 二、区块链金融的刑法风险之类型化界说

区块链领域的刑法风险集中体现为新兴领域的犯罪风险是切实存在的,但如果严格从定罪角度予以推敲,在现行法秩序下却很难被认定为相应犯罪。从该领域实际发生的不法行为出发,可以识别出骗购外汇类犯罪与洗钱犯罪风险、区块链 ICO 等中心化金融活动的金融犯罪风险,以及基于智能合约技术的去中心化金融活动的金融犯罪风险等具备实质不法属性的刑法风险②。然而,虽然这些行为已经具有侵害法益的风险,但由于现行刑法并非为数字时代量身定做,在根据罪刑法定原则对区块链金融等虚拟世界的行为进行调整时,实定刑法规则"就仿佛在甲板上吧嗒吧嗒挣扎的鱼一样",存在规范上的诸多缺位和不适应[15],这进一步增加了相关领域的刑法风险。

### (一)骗购外汇类犯罪与洗钱犯罪风险

由于加密货币与主流法币之间的双重兑换性,加密货币不仅可以在二级市场上进行交易,也可以作为交易中介在不同的币种之间相互转换,实现本外币之间的兑换和跨境流通。这就对国家管制货币和外汇市场的秩序带来了冲击。以人民币购买比特币,再以比特币兑换外币的行为,若超出法定的限额,则可能成立我国刑法中的骗购外汇罪。

不仅如此,加密货币带来的更大风险在于其对于洗钱类犯罪的助推作用。不同于此前的各类线上或线下的洗钱活动,由于加密货币本身就是一种基于去中心化的支付手段创新产物,因此,基于加密货币的洗钱活动具有不同于传统洗钱行为的特征,为相关的监管带来了重大难题。如果说互联网金融环境下的洗钱活动,已经极大地增加了犯罪风险和治理难度,那么加密货币这一工具的使用,则更是对洗钱活动起到与虎添翼的作用。

加密货币的洗钱风险之所以难以防范,除了其可以借助跨国互联网,迅捷且广泛地支付结算,实现与法币之间的双向兑换等原因以外,也源于加密货币的去中心化特征。因为加密货币的去中心化特征,难以识别通过加密货币实施的转账和交易过程中相关账户的主体身份。因此,以比特币为代表的加密货币,很容易成为犯罪人用以实现反侦察目标的可靠工具。更有许多极端主义者采用比特币作为支付手段,以从事具有高度危险性的恐怖活动。

当然,洗钱行为在本质上属于掩饰与隐瞒犯罪所得、收益来源和性质的行为,其在性质上是将来路不正的黑钱洗白,因此其中必然涉及掩饰资金的非法来源的混合过程。除《刑法修正案(十一)》在洗钱罪中新增的"自洗钱"行为以外,在这中间往往涉及各种中介或平台的参与[16]。因此,虽然加密货币增加了洗钱犯罪在查处方面的难度,但也并非完全无迹可寻。这里的刑法认定争议在于如何妥当解释"自洗钱"行为的入罪边界,并创新监管方式,对相关犯罪链条予以更完整精准的规制。这将涉及对加密货币交易平台的责任确定与规制。

### (二)区块链 ICO 等中心化金融活动的金融犯罪风险

如上所述,虽然加密货币的交易可以脱离第三方平台直接进行,但在现实生活中,无论是骗购外汇,还是利用加密货币洗钱,均可以依托特定的中介平台来进行。这种金融平台的形成,是区块链技术

②值得注意的是,区块链金融信息服务提供者还可能触犯非法经营罪以及网络服务提供者的相关犯罪,限于篇幅,此处不展开讨论。将在后文的企业合规部分简要论及。

在发展过程中区别于传统互联网的重大特点。与传统的证券交易市场类似,加密货币也拥有相对完备的融资平台和融资机制。类似于IPO(首次公开发行股票)的概念,在区块链领域,基于区块链平台发行通证类的虚拟记账凭证(代币发行),以募集项目发展所需要的资本的行为,被称为ICO[17]。借助Coinbase、Binance等"场内"区块链交易平台,区块链开发的项目方可以向不特定的对象募集加密货币,以支持项目发展。投资人则可以通过对该代币的金融交易获得更多的加密货币,从而产生经济回报。

从表面上看,这种运作方式带有互联网金融的特征。但问题在于,由于缺乏正式的监管,此种依托于中心化加密货币交易所的发行代币的融资方式很容易产生金融风险。甚至,传统的金融犯罪领域关于金融市场场内交易的诸多刑法风险,均可能在区块链交易平台上复现。从实践层面看,事实也确实如此。在ICO的生态系统中,面临的主要治理挑战是ICO的支持者和代币持有者之间的权力不平衡[18],这带来了巨大的内幕交易、庄家操控的可操作空间。虽然当前对于加密货币及其交易平台的法律性质尚无明确定论,但在实践层面,ICO活动中潜藏着许多操纵证券、期货市场的内幕交易,以及利用未公开信息交易等与构成证券期货类犯罪类似的风险举动[19]。不仅如此,由于融资使用的白皮书可能是缺乏事实根据的包装,融资后的资金使用用途也缺乏监管途径,因此ICO还为包括传销在内的非法集资以及其他金融诈骗犯罪提供了生存土壤。例如,有许多初创的区块链企业,并不以实际开发和经营为目的,仅仅是通过发行毫无价值的"空气币"或"传销币"来聚敛财富。又如,在"PlusToken"网络传销案中,陈波、丁赞清等行为人成立PlusToken加密货币交易平台,以提供加密货币增值服务为名,组织、领导传销活动。该案系公安机关侦破的首起以加密货币为交易媒介的网络传销案,涉及参与人员200余万人,层级关系多达3 000余层,涉案加密货币总值逾400亿元③。

为了防范上述区块链ICO带来的金融风险,2017年9月4日,中国人民银行、中央网信办、工业和信息化部、工商总局、银监会、证监会和保监会联合发布了《关于防范代币发行融资风险的公告》(以下简称七部委《公告》),全面禁止了此类融资活动。实际上,早在2013年12月3日,中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会联合发布了《关于防范比特币风险的通知》(以下简称五部委《通知》),禁止金融机构和支付机构为比特币交易等活动提供相关服务。但问题在于,这种禁止仅仅是在实践层面遏制了相关行为的公开运作,但由于从业者受到利益的驱动,很难杜绝此类行为。笔者以"区块链"为全文关键词,检索了截至2022年7月10日前中国裁判文书网上的所有刑事裁判文书共计350篇,其中绝大多数案件的犯罪时间为2018年以后④。同时,相关新兴的科技创新也会因为"一刀切"的禁令受到不利影响。自七部委《公告》发布以后,中心化交易所及区块链初创企业被迫出海,这虽然有效防范了相关金融风险,体现了保障和维护投资者权益的"家长主义情怀",但也在一定程度上限制了国内区块链技术创新生态的发展。2021年5月18日,中国互联网金融协会、中国银行业协会、中国支付清算协会联合发布《关于防范虚拟货币交易炒作风险的公告》(以下简称三协会《公告》),重申了此前针对加密货币炒作的一贯立场。5月21日,国务院金融稳定发展委员会召开的第五十一次会议中强调,要强化平台企业金融活动监管,打击比特币挖矿和交易行为,坚决防范个体风险向社会领域传递。2021年9月24日,中国人民银行等十部委发

③参见江苏省盐城市中级人民法院(2020)苏09刑终488号刑事裁定书。

④近期被立案调查的典型案例,如"神奇商城非法集资案"以及"花漾医美传销案"。

布的《关于进一步防范和处置虚拟货币交易炒作风险的通知》(以下简称十部委《通知》)则进一步重申了上述定性以及加密货币可能涉嫌的洗钱、非法经营、金融诈骗等犯罪活动。在此背景下,如何准确解读政策精神的禁止性要求,探索未来我国区块链交易平台的可能合规路径,以服务和促进区块链领域的创新活动,并实事求是地从刑法层面对此类行为所涉及的刑事法律风险给出妥当的规范定性,均是值得研讨的重要议题。

结合金融消费者利益的刑法保护需求,需要考虑行为人未经审核公开发行代币的行为是否涉嫌擅自发行股票及公司、企业债券罪,但这里的争议问题是,代币发行能否等同于股票或债券发行?显然,从我国现行金融实践对此类行为普遍禁止的举措之中,我们很难将代币发行或加密货币的交易认定为证券的发行和交易[20]。五部委《通知》、七部委《公告》、三协会《公告》以及十部委《通知》在规范层级上尚不足以准确界定相关活动的性质。不仅如此,结合加密货币的自身特点,可能仅有少部分去中心化特征不够鲜明的代币能够被理解为证券⑤。因此,就此类问题的研究而言,对区块链技术的理解不足以及作为刑法保护前提的前置法根据的匮乏,均增加了对相关行为的刑法定性难度。

**(三)基于智能合约的去中心化金融活动的金融犯罪风险**

除了上述在中心化金融领域发生的犯罪行为以外,另一刑法层面的重大风险在于基于智能合约的去中心化金融活动的区块链犯罪。如前所述,智能合约是一个正在进行中的金融创新探索,并在 2020 年以来的 DeFi 实践中得到进一步发展。可以将相关犯罪区分为两种典型的智能合约金融犯罪形态:一种是利用智能合约实施的犯罪,即犯罪人针对智能合约的代码局限性或利用智能合约的便利性所采取的犯罪举措,从而危及智能合约或区块链账户的安全;另一种是基于智能合约的金融犯罪,是指智能合约的技术提供者直接把智能合约作为犯罪工具,通过开发有瑕疵的智能合约系统来达成自己的犯罪目标,智能合约的推广只是实施犯罪行为的幌子。

首先,智能合约本身的技术特性,为利用智能合约实施的犯罪提供了土壤。智能合约的执行必须依赖事前编写的代码,且为了确保智能合约的不可篡改性,相关交易的回滚十分繁琐,因此一旦代码的瑕疵在上线前的代码审计过程中没有被发现,其固有瑕疵就可能被犯罪人利用,并且撤销、中止交易和恢复原初状态的难度极高。例如,2018 年发生的 The DAO 智能合约被攻击事件,就是由智能合约本身代码漏洞所引起的犯罪。由于区块链本身的匿名性,在技术上只能锁定被盗加密货币的交易记录,却无法识别黑客的身份[21]。2021 年 5 月,第二大 DeFi 项目 BELT 也发生重大被盗事件。这些事件标志着基于智能合约的犯罪从纯粹的理论设想,演变为一个现实问题。若智能合约的技术提供者存在疏失,则专业黑客可以通过识别和利用智能合约漏洞,非法获取他人智能合约私钥或修改智能合约内容,实施金融诈骗、洗钱等多种破坏金融管理秩序的犯罪行为。不仅如此,智能合约本身是一项中性的工具,还可以被犯罪人用来执行犯罪计划,特别是利用区块链网络的匿名性特征,征召金融机构内部人实施共同犯罪,从而降低线下金融犯罪的组织协调和事后分赃被查证的风险。

其次,区别于利用智能合约实施的金融犯罪,基于智能合约的金融犯罪是相关技术提供者主动设计的犯罪。智能合约的生成要求将传统的线下缔约行为代码化,其编码过程并不为普通人乃至监管者所理解,因此智能合约的信用高度依赖其背后松散或有组织的开发者团队。为了确保信用不受质疑,开放源代码是一个重要举措。例如,在以 Linux 和 Github 为代表的全球开源技术生态中,代码安全问

⑤例如,瑞波币(XRP)能否被理解为证券,至今仍在 SEC 与瑞波公司的诉讼进程中反复拉锯。

题可以在技术共同体内部快速被发现并修复,这极大减少了相关犯罪的产生。开源同样是区块链安全的重要支撑[22]。“绝对的权力导致绝对的腐败”,若智能合约的设计者拒绝将智能合约纳入开源社区的审查,其代码很可能被用来作恶。在此种情形下,如果缺乏外部监管机制,将会带来平台方作恶甚至直接实施金融领域犯罪的风险。然而,出于保密需要,在许多涉及金融应用的场景下,平台方可能会拒绝开源。同时,由于我国的区块链创新具有极强的本土性特征,许多智能合约实践并未或无法向产业界开放源码,因此平台方实施金融违法犯罪的风险不容忽视。近来,在火热的DeFi实践中,就出现了大量“只能买不能卖”的假币,如鼎鼎大名的百倍币TRTC,投资者在追涨买入后,才发现在这些代币的后台代码中即写明了代币只能由项目方卖出,这意味着代币发行方自始至终是在实施诈骗犯罪[23]。

当然,由于区块链技术发展和普及的阶段性以及我国对各类加密货币交易平台的普遍禁止所形成的隔离效应,就我国的刑事法治实践而言,目前在大多数情形下,智能合约犯罪仍是一个未来想象。因此,如何对智能合约的设计进行事前性的法律干预,从而防范和追踪区块链平台上涉及刑事犯罪的相关交易,是当前需要思考的重心。虽然这是一个在区块链应用的研发设计中可以被部分预防的问题,其现实风险相对较小,但也对相关立法及合规计划的建立提出了迫切要求。

## 三、规则之治:刑法规制争点及刑事合规

由于现行法律的不完备性以及区块链技术本身的风险内生性,对于区块链金融领域的刑事风险的治理,需要遵循内外有别的原则,双管齐下。就外部视角而言,若要将区块链领域的若干犯罪问题纳入刑事法治的轨道,则刑事法治本身必须明确地对区块链特别是作为当前区块链金融之主要应用的加密货币予以准确的法律定性。同时,立法者还必须对区块链技术公司等区块链技术发展主体的法律地位予以明确,从而对区块链技术形成更为明确且公正的监管。这主要涉及对中立帮助行为的定性问题。就内部视角而言,区块链领域的规则之治还与区块链公司的内部合规问题息息相关。刑事合规作为内部控制手段,是区块链金融领域的内部监管和规则之治得以实现的关键环节。

### (一)加密货币的刑法定性之重新评估

如前所述,当前区块链在金融领域的主要应用场景仍然是加密货币及相关产业链。但是,由于加密货币的法律地位特别是刑法上的定性尚未得到准确的定位,这就为具体犯罪的认定带来了许多争议和困扰。因此,从具体定罪量刑的规范角度考量,明确加密货币的刑法定性,具有重要的规制意义。

关于加密货币的刑法定性,涉及的核心争议在于,能否将加密货币定义为货币?或者是否可以将加密货币定位为证券等金融工具?根据前述七部委《公告》的规定,ICO中使用的代币或加密货币不具有与货币等同的法律地位,代币发行融资被定义为未经批准非法公开融资等行为。亦即,加密货币既不属于货币,也不属于合法的金融工具。在司法实践中,比特币亦仅仅作为虚拟商品得到保护。值得注意的是,我国司法机关曾以“违反社会公共利益”为由撤销了首例支持以等值美元/人民币赔偿比特币财产损失的仲裁案⑥,但该裁定并不意味着比特币系不受法律保护的违禁品,我国现行监管规则并未禁止普通民众交易和持有加密货币等区块链资产,禁令指向的对象是ICO活动以及金融支付机构和网络平台的服务提供。

质言之,当前高层级的前置法制度供给严重不足。基于现行法律对于比特币等加密货币的规定,

⑥参见广东省深圳市中级人民法院(2018)粤03民特719号民事裁定书。

加密货币并未取得作为货币或金融产品的合法地位。这意味着,对于加密货币的监管缺乏现行刑事法意义上的强有力手段[24]。首先,对加密货币禁止性的规范定位意味着加密货币无法获得与股票、证券类似的法律地位,因此比特币等加密货币的投资者在遭遇内幕交易等事件时,无法获得刑法上的保护。其次,若无法将比特币等加密货币定义为货币,则按照现行刑法对于非法集资类犯罪的规定,非法集币行为将无法成立非法集资类犯罪。原因在于,我国刑法规定的非法集资行为指向的对象是法定货币,包括本币和外币。加密货币交易虽然经历了将法定货币兑换为加密货币的过程,但是基于加密货币展开的集币行为,却并不能被等同于集资行为。基于加密货币的技术潜力,当前讨论中也有论者认为,有必要在立法中确认加密货币作为准货币的法律地位,以此作为逻辑起点建构其作为准货币的系列法律制度[25]。笔者认为,由于当前不同类型的加密货币性质差距极大,应当区分不同加密货币的性质来分情况讨论,如区分比特币与竞争币、代币与稳定币、功能型代币(Utility Tokens)与证券型代币(Security Tokens)的不同刑法属性[26]。

总之,为了防范非法集资类犯罪的发生,增强对加密货币投资者的刑法保护,有必要正视加密货币的法律属性[27]。在现行刑法安排未作出修正的情况下,有必要通过教义学的技术性手段对集资类犯罪的成立进行合理的扩张解释。更重要的是,基于监管加密货币以及完善对投资者的法律保护之迫切需要,有必要在立法层面重新评估加密货币的属性,反思我国现行政策采取的较为保守的定性策略。

**(二)监管方式与平台责任的合理界定**

为了鼓励区块链领域的创新,如何舒缓区块链的匿名性与法律监管之间的张力成为一个重要问题,这涉及应当采用何种方式对自发秩序予以监管。同时,在监管方式的确定过程中,必然涉及平台责任的合理界定。而平台责任的确定,又是刑事合规的重要前提和根据。

在协调区块链创新需求的基础上,需要基于对加密货币的准确定位,对相关平台形成类似于金融机构的监管方式,以防范相关的刑法风险。我国当前对区块链特别是加密货币领域的金融创新,采取的是一种较为严厉的监管方式。而与此同时,我国的现行法律规定却又对相关问题缺乏明确的规定,这就带来了监管方面的怠惰与迟滞。在这种现状下,一个值得提倡的带有试错和探索性质的监管方式是监管沙盒模式。根据这种模式,监管者与被监管者之间形成一种沟通性的关系:在政府可控的范围内,相关企业被允许开展关涉新标准和新模式的测试,从而使新兴领域和初创企业的颠覆式创新可以得到支持和培育[28]。考虑到我国的实际情况,在确定采用新型监管方式的对象时,有必要设置前置性的许可或准入机制,以明确相关企业的资质审查。此外,我国当前方兴未艾的自贸试验区,为监管沙盒模式的探索和实践提供了平台依托。

之所以有必要采用包容性的监管方式,也与区块链平台的特殊性质密切相关。在互联网领域关于平台责任的定位中,区块链平台与传统互联网平台之间存在较大的差异性。在传统互联网中虽然也有关于技术中立论的讨论,但一般还是认为,由于互联网平台在事实上具备对平台用户的监管能力,因而需要对其施加特定的义务。然而就区块链平台而言,问题却更为复杂。原因在于,不同于传统互联网平台,区块链平台的设计更加类似于一种自发秩序[29]。由于区块链技术和应用的去中心化特征,严格遵循去中心化构想的区块链企业实际上没有能力对平台上的活动开展实质性审查,因而需研究如何对自发秩序进行包容性监管。

对此,一个重要的平台责任确定原则是,必须结合履行能力来确定平台义务。这意味着,对于区块链平台无法履行的行为,不能为其施加义务。而区块链平台有能力实施的行为,则应基于包容审慎的

监管方式合理地设置义务。例如,就用户注册时的信息审核问题,应该提高区块链平台在用户身份审核方面的义务要求,确保用户采用真实身份予以注册。同时,在平台开发和运营过程中,也应根据其能力,适度地对用户身份进行识别。这一平台责任的赋予思路也在实践中得到肯定。2019年2月生效的《区块链信息服务管理规定》(以下简称《管理规定》),是我国在国家层面针对区块链领域的监管颁布的第一份规范性文件。该《管理规定》明确规定了区块链行业的监管主体,明确要求了区块链使用者的身份实名制以及区块链服务提供者的备案程序。如何在该规定的基础上,区分不同平台的性质并确立监管模式[30],对于相关具体问题予以细化,并在监管需求与创新实践的沟通过程中进一步做好利益平衡,明确行业规范与合作治理机制,细化不同平台的义务,是当前值得进一步研究的重大问题[31]。

除了上述基于实践情况的义务形成方式以外,还应结合区块链金融这一新兴场景,完善《中华人民共和国反洗钱法》(以下简称《反洗钱法》)以及其他金融市场监管的相关立法,认真研究如何更好地将区块链平台的监管纳入其中。刑法是保护法和第二次法,其适用建立在前置法效力受损的基础上。基于法秩序统一性原理,刑法解释也不能同前置法存在严重抵触。因此,明确区块链应用及区块链平台的义务及监管方式,亦将有助于为刑法层面的规制提供更为准确的解释标准。

**(三)相关企业的刑事合规制度之完备**

第一,涉及区块链信息服务(包括金融类信息服务)的相关境内企业应当切实履行前述《管理规定》要求的各项合规义务。根据该规定,区块链信息服务提供者对于信息内容负有安全管理责任和技术合规义务,应当建立健全用户注册、信息审核、应急处置、安全防护等管理制度,应当对用户真实身份予以认证并对内容予以审查,并具备与其服务相适应的技术条件,对法律、行政法规禁止的信息内容具备即时和应急处理能力⑦。在开始提供服务时,应通过国家网信办办理备案手续,并在日常服务过程中保存六个月内发布的内容信息日志;在开发新产品、应用和功能时,应当报网信部门进行安全评估⑧。对于上述规定的违反,如果达到情节严重的,将会触犯非法经营罪、拒不履行网络安全管理义务罪、帮助网络犯罪活动罪等。因此,相关企业应当梳理整合上述规范要求,建立完备的企业内部管理制度体系。

第二,涉及区块链金融服务的相关企业应当切实履行反洗钱义务,结合FATF和各国的反洗钱国内法规,做好反洗钱犯罪的刑事合规。如前所述,由于加密货币在我国现行法律框架中并未取得货币的法律地位,因此与代币发行及交易相关的金融服务一旦在境内运营即可能触犯刑法。但是,这并不意味着加密货币的货币属性在国际范围内没有获得任何承认。相反,已经有国家开始认可加密货币的货币属性[32]。自2017年9月以来,大量此前在国内运营的区块链公司为规避刑事风险选择了跨国经营和出海经营的战略。在此背景下,相关企业在跨国经营时,仍应积极开展反洗钱内控规则的制定,建立完善的反洗钱合规制度。在这方面,反洗钱金融行动特别工作组FATF制定的一系列规范体系,以及相关服务注册地与区块链金融相关的法律法规,均可作为区块链企业内部合规制度建立的规范参照。此外,获得国内区块链金融服务准入资格,当前正处于探索期的国内区块链创新企业,也应遵循相关国际反洗钱规则和国内相关规定,以免触犯刑法中洗钱犯罪的规定。在这方面,在国内对相关企业的法律地位做出明确之前,相关企业可以具体参考《反洗钱法》《非金融机构支付服务管理办法》以及

⑦参见《区块链信息服务管理规定》第5-10条、第16条。

⑧参见《区块链信息服务管理规定》第11条、第17条、第9条。

《支付机构反洗钱和反恐怖融资管理办法》等法律法规，并与相关监管部门就反洗钱合规问题加强沟通协商。在具体项目涉及金融数据出境时，国内相关企业还需密切关注《中华人民共和国网络安全法》第37条的限制性规定。

第三，涉及区块链金融交易的相关企业应当密切关注金融交易类的犯罪风险，建立和完善金融证券类犯罪的刑事合规。虽然由于我国对ICO行为的全面禁止，加密货币在规范定性层面的属性存疑，因而如何认定涉罪罪名存在较大争议，但是相关交易类服务在我国境内当然地存在逾越刑法规范的风险。同时，虽然加密货币在我国金融法律的框架下，尚未取得金融产品的地位，但在国际语境下，关于加密货币的性质存在不同的理解方式。因此，为了降低相关的犯罪风险，相关出海企业有必要整合内部资源，积极做好针对相关犯罪的预防性举措。根据企业所处区域以及在区块链产业链分工中的位置，针对性地制定符合企业情况的合规计划，争取在STO框架下达成合法合规的代币公开发行⑨。一般而言，加密货币交易平台及区块链交易平台应建立可疑交易和大额交易的信息上报机制以及内部存证制度。这是基于各国的区块链金融监管规定，相关企业所应满足的最为基本的合规要求。

第四，涉及区块链智能合约研发的相关境内外企业应当积极推动企业的刑事合规和区块链代码之间的融合，将法律合规贯彻到智能合约的开发过程中。依托区块链企业本身的开发团队和技术优势，若相关企业可以积极推动代码世界的规则与刑事合规的要求之间的融合，将会形成区块链与法律互补的局面，从而有效地解决法律系统信任崩溃或公信力不足的情形，扩展现有的信任结构[33]。为履行证据留存义务，相关企业应当为智能合约的源码和关键操作设置存证机制，通过时间戳来固定相关敏感操作的证据[34]。企业还应当加强技术研发和创新，在其开发的智能合约中兼顾平台的合规需求以及法律的监管需求，设计出更具兼容性的智能合约条款，采用技术手段将合规要求融合到产品设计和代码编写过程中，以防范智能合约被犯罪人利用。通过合规义务的代码化，不仅可以有效防范刑事法律风险，还将有助于推动区块链技术的颠覆式创新和实际落地。

与区块链企业平台责任的刑法认定标准相对应，完善企业刑事合规制度的法律意义在于，在英美法系国家，刑事合规是一项重要的企业责任减免事由[35]；在大陆法系刑法理论及实践的语境下，企业合规义务的履行，亦可在涉及刑法中的中立帮助行为的场合，尽可能地降低甚至免除企业的相关刑事责任。中立帮助行为是在共同犯罪认定中备受关注的现象，其所涉及的问题是，若特定的主体在实施其日常生活行为或业务行为的过程中，在结果上对特定犯罪行为起到了帮助作用，是否应当将这些行为认定为犯罪[36]？例如，区块链企业在客观上为犯罪集团的洗钱活动提供了便利。对此，从举止规范违反的角度看，能否排除犯罪行为成立的核心判断标准在于企业是否违反了其应当履行的法律义务。在这一义务的判断中，区块链领域的行业规范和合规计划的落实情况是判断涉事企业是否构成犯罪的重要根据。

当然，值得注意的是，企业的刑事合规制度的建立及其完备，并不意味着企业的经营自由应当受到严格的控制，合规制度与经营自由之间并不相悖。不应将合规制度作为强制性的标准要求企业执行。质言之，企业积极地开展和落实合规计划，可以作为犯罪发生时减轻或免除责任的根据[37]。但是在企业基于经营考量，未能全部落实合规计划时，在其正常开展经营活动的过程中，也不能给予其消极的法

⑨STO(Security Token Offerings)即证券化代币发行，是指在确定的监管框架下，按照所在国法律法规的要求，进行合法合规的代币公开发行。See YANO M, DAI C, MASUDA K, et al. Blockchain and crypto currency: Building a high quality marketplace for crypto data[M]. Singapore: SpringerOpen, 2020: 115.

律评价,更不能无底线地将行政法意义上的义务直接置换为刑法层面的义务。

综上所述,由于区块链行业的特殊属性,无论是相关企业单方面拒绝监管,还是政府单方面限制和整顿,都会损害数字时代的金融创新及区块链行业的发展前景,因此合理的方式是双方增进合作与沟通,在这一过程中同步完善相关规则和企业内部合规。借助企业的内部合规,可以尊重区块链企业的自主创新需求,在发生风险时减免刑事责任,同时满足刑事犯罪预防和治理的需要,通过企业的内控和基于区块链技术的自发秩序,形成代码法律化的区块链融合监管成效。这一刑法风险的防范思路,相较于纯粹自上而下的监管思路,不仅具有独特的优势和可行性,更是夯实区块链金融领域的规则之治的"最后一公里"的必由之路。

## 四、结语

总之,本文结合区块链技术的金融应用,基于实体刑法的视角,对区块链金融活动中可能蕴含的刑法风险展开了类型化研讨,揭示出现行法律体系对区块链和加密货币的定位中所蕴含的刑法规制争点,并在此基础上提出完善加密货币的立法定性、明确区块链平台的监管框架以及建立刑事合规制度等应对方案。在此过程中,可以得出的明确结论是:根据十部委《通知》等规范性文件,我国并未禁止普通民众在自担风险的前提下参与加密货币交易的自由,为顺应区块链技术的演化和应用规律留下了适宜的战略空间,同时通过家长主义的禁令有效防止了投资者非理性地涌向交易平台,沦为血本无归的投机者或相关犯罪的被害人等重大风险,但即便如此,我国当前对于区块链金融活动的监管政策,整体上仍处于较为保守的位置。"一刀切"的监管策略不仅会带来区块链创新方面的阻滞与国际合作的困难,还产生了诸多刑法风险,为相关不法乱象的刑法定性以及区块链企业刑事合规制度的完善带来了诸多困惑。

习近平总书记在主持中央政治局关于区块链技术的集体学习时曾强调,"要把区块链作为核心技术自主创新的重要突破口","加快推动区块链技术和产业创新发展"[38]。要跨越当下监管层面过于保守的现况与我国新时代经济高质量发展的目标之间的鸿沟,亟需在社会系统的意义上充分展开对区块链技术之利弊得失的研究,在时机适当时调整监管政策,理性避免因过度惧怕区块链技术的可能风险而导致的因噎废食后果。为了在以区块链为底层技术的"硅基时代"占据创新制高点,刑事法治应当对区块链金融犯罪做出积极回应:一方面,法律工作者特别是刑法学研究者必须做好刑法解释工作,在既有框架下结合前置法规定做好解释论层面的适配,从而尽可能地对相关不法行为展开刑法层面的规制,并为产业发展和相关企业的创新攻坚提出有针对性的合规建议;另一方面,就刑事立法的完善而言,还必须关注和研究如何与时俱进地对洗钱类犯罪以及集资类犯罪的构成要件作出修正,从而使现行刑法的规定足以应对区块链技术及其应用的犯罪风险。

**参考文献:**

[1]NAKAMOTO S. Bitcoin:A peer-to-peer electronic cash system[EB/OL]. (2008-10-31)[2021-06-01]. https://bitcoin.org/bitcoin.pdf.

[2]TAPSCOTT A,TAPSCOTT D. How blockchain is changing finance[EB/OL]. (2017-03-01)[2021-06-01]. https://hbr.org/2017/03/how-blockchain-is-changing-finance.

[3]尼葛洛庞帝. 数字化生存[M]. 胡泳,范海燕,译. 北京:电子工业出版社,2017:228-232.

[4]BASHIR I. Mastering blockchain[M]. Birmingham:Packt Publishing,2018.
[5]SWAN M. Blockchain:Blueprint for a new economy[M]. Sebastopol:O'Reilly Media,2015:preface ix.
[6]BATRA G,OLSON R,PATHAK S,et al. Blockchain 2.0: What's in store for the two ends—semiconductors (suppliers) and industrials (consumers)? [EB/OL]. (2019-01-18)[2021-06-01]. https://www.mckinsey.com/industries/advanced-electronics/our-insights/blockchain-2-0-whats-in-store-for-the-two-ends-semiconductors-suppliers-and-industrials-consumers.
[7]WEBER M. Economy and society[M]. Berkeley:University of California Press,1978:91-92.
[8]朱娟.我国区块链金融的法律规制:基于智慧监管的视角[J].法学,2018(11):129-138.
[9]吴云,朱玮.虚拟货币的国际监管:以反洗钱为起点走出自发秩序[J].财经法学,2021(2):79-97.
[10]SRINIVASAN B S. Thoughts on tokens[EB/OL]. (2017-05-27)[2021-06-01]. https://news.earn.com/thoughts-on-tokens-436109aabcbe.
[11]LESSIG L. Code:Version 2.0[M]. New York:Basic Books,2006:1-8.
[12]郑戈.区块链与未来法治[J].东方法学,2018(3):75-86.
[13]HAYEK F A. Toward free market money[N]. Wall Street Journal,1977-08-19.
[14]崔志伟.区块链金融:创新、风险及其法律规制[J].东方法学,2019(3):87-98.
[15]马永强.正向刷单炒信行为的刑法定性与行刑衔接[J].法律适用,2020(24):63-78.
[16]时延安,王熠珏.比特币洗钱犯罪的刑事治理[J].国家检察官学院学报,2019(2):47-62.
[17]HAHN C,WONS A. Einleitung[M]//Initial coin offering (ICO). Wiesbaden:Springer Fachmedien Wiesbaden,2018:1-8.
[18]HACIOGLU U. Blockchain economics and financial market innovation[M]. Cham:Springer Nature Switzerland AG,2019:68.
[19]朱娴.代币发行交易中的犯罪风险[J].国家检察官学院学报,2018(6):101-117.
[20]王冠.基于区块链技术ICO行为之刑法规制[J].东方法学,2019(3):137-148.
[21]王延川.智能合约的构造与风险防治[J].法学杂志,2019(2):43-51.
[22]SHEALY M. How open source underpins blockchain technology[EB/OL]. (2020-10-01)[2021-06-02]. https://opensource.com/article/20/10/open-source-blockchain.
[23]I bought a hundred times currency, but I can't sell it[EB/OL]. (2020-11-13)[2021-06-03]. https://blockcast.cc/news/i-bought-a-hundred-times-currency-but-i-cant-sell-it/.
[24]谢杰,张建."去中心化"数字支付时代经济刑法的选择:基于比特币的法律与经济分析[J].法学,2014(8):87-97.
[25]杨延超.论数字货币的法律属性[J].中国社会科学,2020(1):84-106.
[26]马永强.论区块链加密货币的刑法定性[J].苏州大学学报(法学版),2022(2):105-120.
[27]杨玉晓.区块链金融衍生品刑法规制研究[J].重庆大学学报(社会科学版),2020(6):127-137.
[28]Regulatory sandbox[R/OL]. (2016-11-09)[2021-06-02]. https://www.fca.org.uk/publications/documents/regulatory-sandbox.
[29]The trust machine:The technology behind bitcoin could transform how the economy works[EB/OL]. (2015-10-31)[2021-06-03]. https://www.economist.com/leaders/2015/10/31/the-trust-machine.
[30]苏宇.数字代币监管的模式、架构与机制[J].东方法学,2021(3):77-94.
[31]马永强,姜宏达.区块链信息服务监管路径初探[N].民主与法制时报,2022-06-08(03).
[32]漆彤,卓峻帆.加密货币的法律属性与监管框架:以比较研究为视角[J].财经法学,2019(4):126-141.
[33]陈吉栋.播撒信任的技术幽灵:区块链法律研究述评[J].探索与争鸣,2019(12):84-94.
[34]刘品新.论区块链存证的制度价值[J].档案学通讯,2020(1):21-30.
[35]菲利普·韦勒.有效的合规计划与企业刑事诉讼[J].万方,译.财经法学,2018(3):141-160.
[36]曹波.中立帮助行为刑事可罚性研究[J].国家检察官学院学报,2016(6):107-121.
[37]陈瑞华.合规视野下的企业刑事责任问题[J].环球法律评论,2020(1):23-40.
[38]李挺.区块链换道超车的突破口(人民时评)[N].人民日报,2019-11-04(05).

# Criminal law risks and rules of governance in blockchain finance

MA Yongqiang

(*Law School*, *Dalian Maritime University*, *Dalian 116026*, *P. R. China*)

**Abstract:** The characteristics of blockchain technology, on the one hand, lay the possibility of its application in finance, which is an important cornerstone of civilized society, and on the other hand, lay the clues for the illegal risks in blockchain financial activities. Based on the actual financial application scenario of blockchain technology, the risk of illegal application of blockchain technology in the financial field is firstly reflected in the promotion of cryptocurrency-based blockchain financial ecology for fraudulent purchase of foreign exchange crimes and money laundering crimes. Blockchain ICO and other centralized financial activities have brought about the risk of disrupting the financial order, such as insider trading crimes and financial fraud crimes. The further development and application of blockchain technology has also given rise to crime forms in decentralized scenarios based on smart contracts. Thinking about the rule of blockchain financial crimes, the lack of current law norms and the risk endogenous nature of blockchain technology have jointly led to the difficulty of identifying related crimes. Therefore, to better cope with the criminal law risks in blockchain finance, it is necessary to follow the principle of internal and external distinction to regulate the relevant risks. From an external perspective, to bring blockchain financial crimes into the rule of criminal law, the criminal law characterization of cryptocurrencies must first be re-evaluated. In this regard, the nature of different cryptocurrencies should be discussed on a case-by-case basis. At the same time, it is also necessary to clarify the legal status of the subjects of blockchain technology development, and reasonably define the platform responsibilities of relevant blockchain enterprises and the way of supervision. The current one-size-fits-all regulatory approach should be rethought, and a regulatory sandbox model with inclusive features should be adopted to allow relevant enterprises to carry out disruptive innovations within a controlled scope, and to reasonably set platform responsibilities based on an inclusive and prudent regulatory approach. As far as the internal perspective is concerned, the rules of governance in the blockchain field also require blockchain enterprises to integrate criminal compliance requirements as internal control means. Specifically, domestic enterprises involved in blockchain information services should effectively fulfill domestic regulatory requirements; enterprises involved in blockchain financial services should effectively fulfill their anti-money laundering obligations and integrate FATF and domestic regulations of various countries to do their compliance work; enterprises involved in blockchain financial transactions should pay close attention to the criminal risks of financial transactions, establish and improve criminal compliance for financial and securities crimes; domestic and foreign enterprises involved in the development of blockchain smart contracts should actively promote the integration of corporate criminal compliance and blockchain code. By improving the regulation and rules of blockchain both internally and externally, and prompting the criminal law to respond positively to blockchain financial crimes, it will help to better promote innovation in the field of blockchain finance and help China's digital economy to move steadily and far.

**Key words:** blockchain; cryptocurrency; virtual currency; smart contract; criminal law risk; criminal compliance

(责任编辑 胡志平)