基于区块链的数字货币发展现状与展望

李娟娟[1, 2] 袁 勇[3] 王飞跃[2]

摘 要 数字货币 (Digital currency) 作为区块链技术迄今为止最典型也最成功的应用, 得益于区块链分布式共识与去中心化信任的技术优势, 也促使了区块链技术与经济活动的深度融合, 并由此改变了数字社会的组织方式. 近年来, 无论是在基础理论研究方面, 还是在实践应用发展方面, 数字货币均呈现出了蓬勃向上的态势. 本文从技术创新、机制设计以及风险监管三个角度梳理了数字货币的主要研究问题, 详细阐述了基础支撑技术、隐私保护技术、共识机制、激励机制、币值机制、发行机制、风险分析、监管考量等方面的研究进展、存在问题及应用现状, 并展望了未来重点研究方向, 致力于为数字货币领域的研究提供有益借鉴.

关键词 区块链, 数字货币, 技术创新, 机制设计, 风险监管

引用格式 李娟娟, 袁勇, 王飞跃. 基于区块链的数字货币发展现状与展望. 自动化学报, 2021, **47**(4): 715−729

DOI 10.16383/j.aas.c210018

Blockchain-based Digital Currency: The State of the Art and Future Trends

LI Juan-Juan[1, 2] YUAN Yong[3] WANG Fei-Yue[2]

Abstract As the most representative and successful application of blockchain technology, digital currency benefits from the technical advantages of distributed consensus and decentralized trust in blockchain, and also promotes the deep integration of blockchain technology and economic activities, thus changing the organization mode of digital society. Recently, digital currency has shown a booming trend both in theoretical researches and practical applications. In view of this, our paper discusses the main research issues of digital currency from three perspectives, including technological innovation, mechanism design and risk regulation, and elaborates the research progress, existing problems and application status of basic technology, privacy protection technology, consensus mechanism, incentive mechanism, value mechanism, issuance mechanism, risk analysis, regulatory considerations, etc., and puts forward the main emphasis of the future researches. Our work is devoted to providing useful reference and good support for the future research in the field of digital currency.

Key words Blockchain, digital currency, technological innovation, mechanism design, risk regulation

Citation Li Juan-Juan, Yuan Yong, Wang Fei-Yue. Blockchain-based digital currency: The state of the art and future trends. *Acta Automatica Sinica*, 2021, **47**(4): 715−729

随着银行在 17 世纪诞生, 货币作为一种重要的媒介工具, 逐步进化成为经济金融体系的核心, 维系社会协作关系[1]. 19 世纪中叶, 马克思主义政治经济学创立, 指出货币就是固定地充当一般等价物的商品, 认为 “金银天然不是货币, 但货币天然是金银”. 在货币发展历史中, 金银在很长一段时间内确实充当了货币, 直到因为携带和交易方便需求被票据和纸币所替代. 20 世纪 30 年代, “金本位”制度崩溃后, 货币开始进入 “法定货币”时代, 世界各国普遍实行以国家信用作为担保的货币体系. 1977 年奥地利经济学派著名的自由主义经济学家哈耶克在《货币的非国家化》一书中提出了非国家化货币的构想, 指出可由私营银行发行竞争性货币[2], 但这一构想在法定货币发行体制下是难以实现的.

20 世纪末, 互联网兴起促进了数字化社会和无现金社会的发展, 也为私营竞争性货币实践提供了新的技术与方法, 形成了数字货币诞生的土壤. Chaum 在其 1983 年发表的论文 “Blind signatures for untraceable payments”中提出了数字货币 (Digital currency) 的概念[3], 并于 1992 年基于

收稿日期 2021-01-07 录用日期 2021-02-26
Manuscript received January 7, 2021; accepted February 26, 2021
国家重点研发计划专项 (2018AAA0101401), 国家自然科学基金 (61533019), 澳门科学技术发展基金 (0050/2020/A1) 资助
Supported by National Key Research and Development Program of China (2018AAA0101401), National Natural Science Foundation of China (61533019), The Science and Technology Development Fund of Macau SAR (0050/2020/A1)
本文责任编委 魏庆来
Recommended by Associate Editor WEI Qing-Lai
1. 北京理工大学自动化学院 北京 100081 2. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室 北京 100190 3. 中国人民大学数学学院 北京 100872
1. School of Automation, Beijing Institute of Technology, Beijing 100081 2. The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 3. School of Mathematics, Renmin University of China, Beijing 100872

盲签名合约创立了具有匿名性的数字货币实体eCash. 1997 年, Adam Back 在密码朋克邮件列表发送了一封主题为 “A partial hash collision based postage scheme”的邮件, 其中提到了工作量证明(Proof of work, PoW) 技术. Stuart Haber 以及Scott Stornetta 则提出了时间戳 (Timestamp) 和Merkle 树的想法. 1998 年, 戴伟发明了 B-money, 强调了点对点交易以及分布式存储问题; Nick Szabo 发明了比特金 (BitGold), 使用了工作量证明机制. 在这些技术探索的基础上, 中本聪于 2008 年发明了比特币, 它是一种点对点的电子现金系统[4], 依托区块链这一底层技术, 实现了去中心化和去中介化的两方交易模式. 它的诞生在一定程度上实现了哈耶克的货币竞争性和中立性设想, 引发了一场 “多元货币竞争理论”的社会大探讨[5].

目前, 数字货币还没有统一的标准化定义. 国际清算银行认为数字货币是基于分布式账本技术, 采用去中心化支付机制的虚拟货币; 国际货币基金组织将数字货币称为价值的数字表达; 我国央行发行的数字货币是指数字化的人民币, 其本身是货币而不仅仅是支付工具. 一般地, 以比特币为代表的数字货币采用了密码学原理来实现货币的发行与交易确认, 可以将此类基于区块链及相关技术支撑的数字货币称为加密货币[6−7].

近年来, 加密货币发展势头迅猛. 截止到 2020 年底, 全球共有超过 8 000 种加密货币, 总市值超过 8 600 亿美元, 能够在世界各国 2019 年 GDP 排名中占据第 18 位. 其中, 市场份额排名第一的比特币供应量 (即已经挖出的比特币数量) 已经超过 1 800 万枚, 总市值已突破 5 000 亿美元. 尽管频繁波动的币值为数字货币投资者带来了获取更高收益的机会, 但也导致它们的价值尺度职能无法有效发挥, 影响了市场对其的认可度和接受度. 在此背景下, 基于特定的机制设计以保持币值稳定的数字货币(即稳定币) 应运而生[7]. 2019 年 6 月, 以 Facebook 为首的全球 28 家金融支付巨头共同研发的 Libra (2020 年底更名为 Diem) 白皮书发布. Libra 作为一种基于区块链的追求实际购买力相对稳定的数字货币, 是在世界货币体系及金融资源匹配结构性失衡的背景下提出的非主权国家货币, 它的出现再一次引发了人们对于数字货币和稳定币的热烈讨论[8].

与此同时, 由中央银行发行的、以国家主权信用背书的、具有法定地位的数字货币也备受关注. 不少国家已经开展央行数字货币 (Central bank digital currency, CBDC) 的发行实验工作, 而其中大多数都是基于区块链技术的[1]. 中国早在 2014 年就开始推动央行数字货币发行, 并将其提升至国家级战略高度, 目前已经进入公开测试阶段. 尽管目前其没有采用区块链技术, 而仅仅借鉴了区块链的分布式存储理念, 但是无论从技术角度还是从业务角度, 如何运用区块链技术更好地服务于中心化管理下的分布式运营, 是 CBDC 需要重点探索的方向.

基于区块链的数字货币是应用创新驱动的新型智能系统和去中心化商业模式, 目前已经发展至稳定币及法定数字货币阶段, 正逐步成为现代经济体系中不可排斥的因素以及数字社会的重要基础, 将为金融、经济、社会等各个领域带来重要的变革. 基于区块链的数字货币的出现催生了新的研究问题、新的管理视角和新的实践需求. 该领域目前仍然处于发展的初期阶段, 存在诸多问题亟待解决, 对其展开系统性的分析具有非常重要的意义. 1) 基于区块链的数字货币是密码学、经济学、管理学和计算机科学等多个学科交叉融合的产物, 其在安全性、稳定性及持续性方面的设计需求对各学科提出了更高的技术要求, 必将加速相关学科的创新发展. 2) 尽管数字货币理论研究与应用实践都呈现出蓬勃发展的态势, 但仍旧存在理论发展不完备、研究滞后于实践的现状. 本文对技术、机制及监管等方面的逐一梳理将有助于推动重点方向的发展, 以对数字货币更深入更广泛的应用提供积极而有效的支撑. 3) 数字货币是区块链技术最典型的应用, 其得益于区块链的技术优势, 又反过来促进了区块链的技术发展. 因此, 对数字货币的研究不仅推动数字货币应用问题的解决, 还将促进区块链技术的创新升级. 鉴于此, 本文着眼于数字货币的核心科学问题, 从技术创新、机制设计、风险监管等三个方面梳理数字货币的理论发展与应用现状, 讨论已有成果、现存问题以及未来重点发展方向, 以期为数字货币发展提供有益参考.

本文的结构安排如图 1 所示. 其中, 第 1 节从基础支撑技术和隐私保护技术两方面讨论数字货币技术创新; 第 2 节梳理了数字货币系统的关键机制设计问题, 主要包括共识机制、激励机制、币值机制以及发行机制; 第 3 节在风险分析的基础上, 从技术理论发展与政策措施实践的角度介绍了数字货币监管问题; 第 4 节总结了本文内容, 并提出了基于区块链的数字货币未来重点发展方向.

1 技术创新

技术创新是驱动数字货币发展的源动力, 该方向已有的研究主要集中在基础支撑技术以及隐私保护技术两方面.

[1] 姚前: 区块链与央行数字货币, 第一财经, 2020 年 4 月 2 日

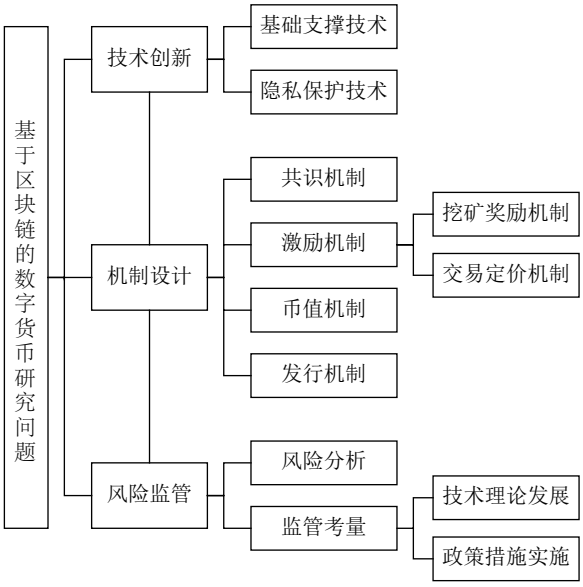

图 1　本文研究框架

Fig. 1　The research framework

1.1　基础支撑技术

尽管目前区块链技术还存在并发量受限及可扩展性不足的问题, 但是目前市场上的私营数字货币几乎均采用区块链作为底层技术, 并基于比特币的代码思想, 进行了不同维度的衍生以提升数字货币的某项性能, 包括提升可扩展性、提高安全与隐私保护、增强可编程性、保证价格稳定性、创新共识算法以及适应特定应用场景等[9]. 同时, 也已经有不少国家开展了基于区块链的法定数字货币研发与实验工作, 例如加拿大推出基于区块链技术的大额支付系统 Jasper; 新加坡实施 Ubin 项目以评估在分布式账本技术 (Distributed ledger technology, DLT) 上以数字新元的代币形式进行支付结算的效果; 欧洲央行和日本央行则通过 Stella 项目研究 DLT 在金融市场基础设施中的应用, 评估现有支付体系的特定功能是否能够在 DLT 环境下安全高效地运转等.

在私营数字货币领域, 区块链技术作为基础技术, 具有不可比拟的优势. 区块链技术通过去中心化自治的共识机制, 构建了新的信任体系, 提升了数字货币系统价值传递的可信性[10−12]. 区块链作为分布式记账数据库, 通过账本查询机制、溯源机制、验证机制、加密机制等的创新, 保证了数字货币系统价值传递的安全性[13−15]. 区块链技术基于点对点的分布式网络, 实现了数据的不可篡改与可追溯, 增强了数字货币系统价值传递的可靠性[16−21].

在法定数字货币领域, 区块链技术的应用也是颇有益处[22]. 利用区块链技术实现数字货币防伪以及交易追溯等, 有利于增强法定数字货币的安全性[23]. 将区块链的分布式网络节点验证功能与可授权的中心化机构运行结合起来, 实现基于联盟链的多中心运行体系, 将有助于提升数字货币系统的安全稳定运行[24]. 区块链技术能够对数据的所有者确权, 有助于央行在法定数字货币的发行与流通体系中实现金融大数据的搜集与管控, 提高法定数字货币的可控性[25]. 基于现有的中央银行与商业银行的二元支付清算体系, 在中心化货币管理模式中融合区块链的 DLT 与加密技术, 实现中心化的货币供应与分布式的交易账本维护的解耦, 能够降低交易成本, 提高效率[26]. 区块链技术为法定数字货币发行提供平台基础, 帮助央行改善支付清算操作, 提升数字货币在全球流通的效率[23, 27]. 结合区块链技术的去中心化特性, 建立国家主权背书下的数字货币交易信用, 通过大量而频繁的交易增强信用基础, 有助于构建全球通用的支付信用体系[28].

1.2　隐私保护技术

在基于区块链的数字货币系统中, 隐私保护技术是安全应用的重要基础. 一方面, 数字货币的匿名性要求在分布式节点共识达成与交易记录全网公开的同时不会暴露用户的合法信息, 主要包括身份、位置以及余额等; 另一方面, 数字货币的匿名性不能脱离安全运营与合法监管的需求, 以避免其成为不法分子的犯罪工具[29].

目前, 主流的数字货币隐私保护技术包括: 点对点混合协议 (Peer-to-peer mixing protocols), 分布式混合网络 (Distributed mixing networks) 以及比特币扩展 (Bitcoin extensions)[30].

1) 点对点混合协议通过混合协议来混淆交易的溯源, 使得用户与交易之间的关联被打破, 是一种去中心化的混合方法. Maxwell 于 2013 年首先提出了 CoinJoin 协议以打破比特币输入输出地址之间的关联, 该协议后来被运用于达世币 (DASH)[31]. Ruffing 等设计了 CoinShuffle 协议, 运用比特币地址混合方案实现内部不可关联性[32]. Ziegeldorf 等在 CoinShuffle 协议的基础上, 基于解密混合网络和阈值签名方案, 提出了 CoinParty 协议, 实现匿名的比特币混合[33]. Ibrahim 受 CoinParty 协议启发提出了 SecureCoin 协议, 该协议不涉及任何单独的混合节点, 因此可以免除它们可能发起的破坏性攻击, 能够实现安全的不可链接匿名交易[34]. 另外, 一种新的基于环签名算法的交易混淆方案被提出, 其可以确保任何用户的输入和输出地址之间的对应关系无法被获取[35].

2) 分布式混合网络本质上是一种依赖第三方的中心化混合方法, 主要包括混币服务平台以及混币协议. 混币服务平台 (例如 Bitcoin Fog, BitLaundry, Blockchain.info 等) 利用可信第三方来完成数字货币用户的资金收集和分配任务. Bonneau 等提出了 MixCoin 混币协议, 其使用基于声誉的加密问责机制以防止混合中的协议破坏与货币窃取[36]. Valenta 等设计了 BlindCoin, 通过盲签名技术对 MixCoin 协议进行扩展, 以实现混合过程中的内部不可链接性[37]. Heilman 等提出了 TumbleBit, 其类似于 eCash 协议, 通过第三方平台 Tumble 实现匿名的离线快速支付[38]. 包子健等使用公平盲签名算法, 并引入可信第三方, 提出了一种可监管的比特币隐私保护混淆方案 RBmix[39].

3) 比特币扩展是基于比特币底层技术, 并采用零知识证明和同态加密等主流密码学算法技术, 对匿名性和隐私保护性进行提升. 目前市场上主要的比特币扩展包括 ZeroCash, CryptoNote, MimbleWimble, ByzCoin, Etherum, MasterCoin, LiteCoin, Monero 以及 Counterparty 等数字货币[30].

2 机制设计

机制设计是数字货币系统架构设计的重要组成部分, 主要包括共识机制、激励机制、币值机制以及发行机制等. 其中, 共识机制是维护系统一致性和安全性的基础, 激励机制是保障系统可持续性和活跃度的核心, 币值机制是实现系统稳定性和实用性的关键, 而发行机制决定了数字货币的固有属性、信用基础及流通方式.

2.1 共识机制

共识机制是数字货币系统的基础设计, 主要指通过特定的规则设计实现矿工利用其掌控的算力或者权益对影响区块链发展的提案进行 “投票”, 实现分布式场景下的一致性达成. 如何在权力分散的去中心化网络中使得矿工高效而安全地达成一致性共识, 是共识机制设计的主要目标.

2008 年, 中本聪在比特币白皮书中提出使用 PoW 机制来实现共识[4]. PoW 的核心思想是各节点 (即矿工) 基于各自的算力相互竞争来共同解决一个求解复杂但是验证容易的 SHA-256 数学难题 (即挖矿). 最快解决该难题的节点将获得下一区块的记账权和系统自动生成的比特币奖励. PoW 共识机制是最早、最可靠、最流行的公有链共识算法[40]. PoW 共识在比特币系统的应用具有重要意义, 其近乎完美地整合了比特币系统的代币发行、流通和市场交易等功能. 然而, PoW 共识也存在着明显的缺陷, 其强大算力造成的资源浪费 (主要是电力消耗) 以及较长的交易确认时间导致的效率低下历来为人们所诟病.

为了改进 PoW 共识, 一系列新的拜占庭容错类共识算法逐步被提出[41−42]. 2011 年数字货币爱好者论坛 Bitcointalk 上署名为 “Quantum Mechanic” 的作者提出了权益证明 (Proof of stake, PoS) 机制, 其基本思路是由系统中具有最高权益而非最高算力的节点获得记账权, 其中权益体现为节点对特定数量代币的所有权. PoS 机制在一定程度上解决了 PoW 机制的算力浪费问题. 2013 年比特股 Bitshares 提出了授权股份证明 (Delegate proof of stake, DPoS) 机制. DPoS 共识机制的基本思路类似于 “董事会决策”, 即系统中每个节点可以将其持有的股份权益作为选票授予一个代表, 获得票数最多且愿意成为代表的前 N 个节点将进入 “ 董事会”, 按照既定的时间表轮流对交易进行打包结算并签署 (即生产) 新区块. DPoS 机制缩短了交易确认时间, 在一定程度上解决了 PoW 机制效率不高的问题.

基于 PoW、PoS 共识机制, 已有不少工作从共识机制的合规监管、性能提升、资源节约以及容错性提升等角度展开研究, 并提出一些改进的新型共识机制如图 2 所示. 具体可分为如下三类:

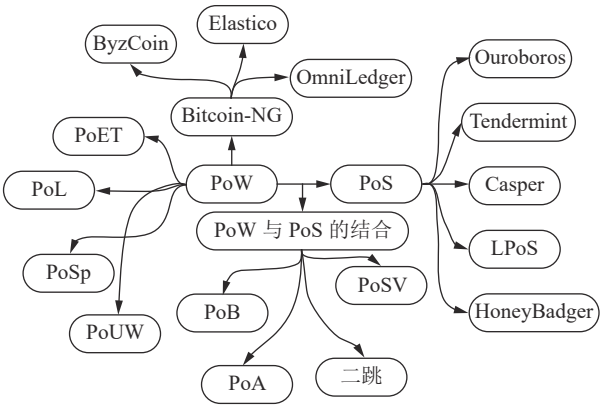

图 2 基于 PoW 与 PoS 的共识机制改进

Fig. 2 The improved blockchain consensus algorithms based on PoW and PoS

1) PoW 与 PoS 机制的有机结合: 解决这两类机制存在的能源消耗与安全风险问题. a) 权益–速度证明 (Proof of stake velocity, PoSV) 机制[43], 在保证所有者权益的基础上鼓励数字货币流通, 以降低系统因囤币行为带来的风险. 为此, 该机制在前期使用 PoW 机制, 后期使用 PoSV 机制, 其将 PoS 机制中的币龄与时间的衰减函数修正为指数非线性

函数. b) 燃烧证明 (Proof of burn, PoB) 机制[44], 利用 PoW 产生初始的代币供应, 但是运用 PoB 和 PoS 来共同实现后期维护; 在该机制下, 矿工通过燃烧代币 (发送代币至无法找回的地址) 来竞争记账权. c) 行动证明 (Proof of activity, PoA) 机制[45], 也是利用 PoW 产生代币, 而采用 PoS 机制分发代币. d) 二跳 (2-hop) 机制[46], 结合 PoW 与 PoS 机制, 使得系统攻击必须同时控制 51% 以上的算力和 51% 以上的权益才能成功, 这无疑提升了数字货币系统的安全性.

2) 对 PoS 机制进行改进: 解决该机制固有的 "无利害关系 (Nothing at stake)" 问题. a) Tendermint 共识[47], 是基于实用拜占庭容错 (Practical byzantine fault tolerance, PBFT) 算法的 PoS 机制, 要求节点缴纳保证金以约束作恶行为, 增强了系统抵御攻击的鲁棒性. b) Casper 机制[48], 是基于链的 PoS 机制. Casper 还有另外一个版本是基于链与基于 PBFT 结合的 PoS 机制. c) Honey-Badger 机制[49], 是首个实用的异步拜占庭容错共识协议, 基于一种可实现渐近有效性的原子广播协议实现每秒上万笔交易的处理. d) Ouroboros 机制[50], 该机制通过奖励机制推动 PoS 共识的实现, 能有效避免矿工的策略性行为导致的安全攻击. e) LPoS 机制[51], 在 PoS 的基础上引入了流动性, 即区块生产者的数量不固定; 还设计了带押金的惩罚机制, 且通过引入背书人的角色来检查区块有效性. 这些改进使得系统在抵御安全风险方面的能力得到一定的提升.

3) 对 PoW 机制的改进: 实现比特币扩容或者降低其能耗. a) 为解决扩容问题, 康奈尔大学提出了 Bitcoin-NG 机制[52]. 该机制设计了用于选举负责生成区块与打包交易的领导者的关键区块、包含交易数据的微区块两种不同的区块, 使得可以在不改变区块容量的情况下通过选举领导者生成更多的区块, 从而辅助解决扩容问题. 后来在此基础上衍生出 ByzCoin[53]、Elastico[54]、OmniLedger[55] 等新型共识机制. 其中, ByzCoin 机制是一种可扩展拜占庭容错算法; Elastico 机制是第一个拜占庭容错的安全分片协议; OmniLedger 机制通过并行跨分片交易处理优化区块链性能. 这三种共识机制通过不同的方式实现了高吞吐量和低确认延迟. b) 为解决能耗问题, 研究者相继提出了消逝时间证明 (Proof of elapsed time, PoET)[56]、运气证明 (Proof of luck, PoL)[57]、空间证明 (Proof of space, PoSp)[58] 以及有益工作证明 (Proof of useful work, PoUW)[59] 等新机制. PoET 机制使得区块链系统不必消耗昂贵的算力来挖矿而提高了效率; PoL 机制采用随机数生成器来选择每一轮共识的记账人, 从而实现可忽略的能源消耗; PoSp 机制不要求矿工通过算力来挖矿; PoUW 机制则将哈希运算转化为面向实际场景的有意义的运算.

除此之外, 其他新型共识机制也被提出. 例如, 结合传统分布式一致性算法而提出的 Tangaroa[60]、ScalableBFT 共识机制, 它们能在拜占庭错误环境下仍然维持安全性、容错性和活性; 由 Ripple 共识机制演化而来的 Stellar 机制改进了 PoW 和 PoS 缺乏最终一致性的问题; 由 MIT 提出的 Algorand 机制[61] 利用密码抽签技术选择共识过程的验证者和领导者, 通过快速拜占庭容错算法达成共识, 优点是计算量极小且分叉极少.

2.2　激励机制

激励机制是数字货币系统的核心设计, 对于系统的可持续稳定发展、参与者的收益优化乃至数字货币的实践应用都有十分重要的意义. 激励机制通过经济利益的分配, 激励矿工在既定的规则框架下, 在挖矿的同时进行交易验证工作 (具体的流程如图 3 所示). 现有研究主要聚焦于挖矿奖励机制以及交易定价机制两方面.

2.2.1　挖矿奖励机制

挖矿奖励机制仅在有挖矿行为的数字货币系统中讨论, 而绝大多数挖矿行为都是以矿池团体形式进行的, 因此需要有特定的机制设计对挖矿收益进行分配.

目前, 已有的奖励分配机制主要包括按比例分配机制、PPS (Pay-Per-Share) 机制、PPLNS (Pay-Per-Last-N-Shares) 机制、Slushes 方法、Geometric 方法、Triplemining 机制等. 在实践中, 按比例分配、PPS 和 PPLNS 是最常用的三种机制[62], 但它们均存在一定的缺陷. 按比例分配机制下矿工的收益不稳定, 他们有动机采取跳矿等策略性行为来获取高于其自身算力比例的收益. PPS 通过将风险转移给矿池从而在一定程度上确保了矿工收益的稳定性, 但其仍旧无法避免矿工的策略性行为带来的损失[7]. PPLNS 从更长的一个时间段 (如一天) 来对收益进行延迟分配, 而不是将每一个新区块的收益进行实时分配, 这种方式的好处在于能够更合理地按照算力进行收益分配, 但是矿工还是可以通过混合汇报策略来获取更高收益[63]. 可以看出, 以上策略都不是激励相容的, 无法促使矿工个体的收益优化行为与矿池整体的收益优化目标保持一致, 不利于系统的稳定性.

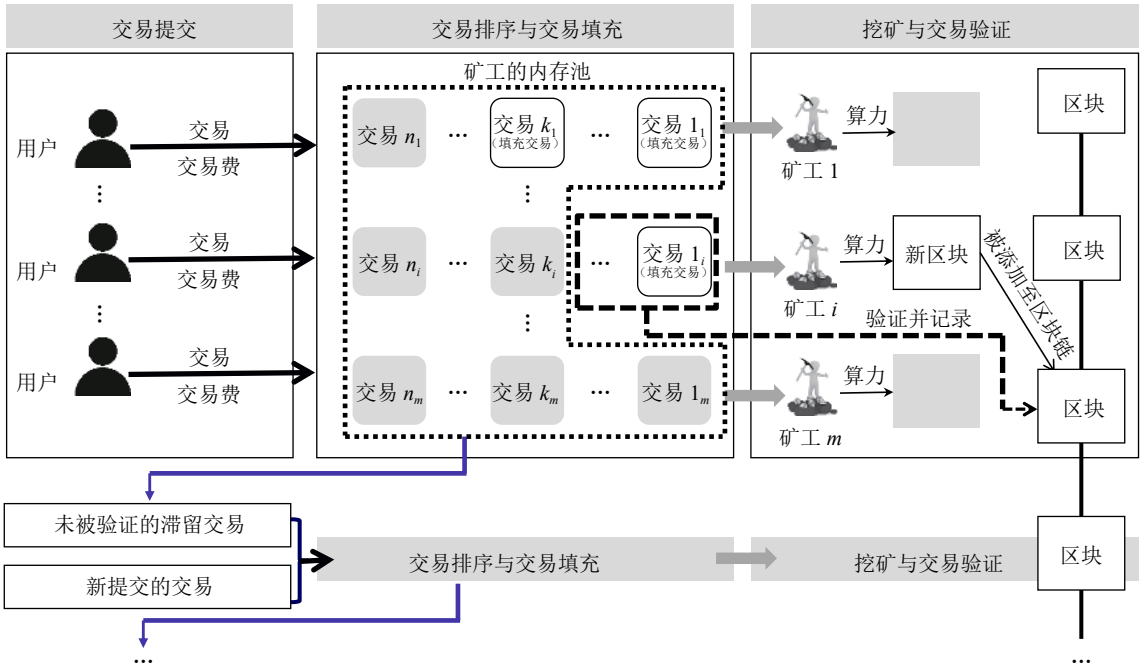

图 3 矿工挖矿与交易验证流程

Fig. 3 The mining and transaction confirmation process

鉴于此, 已有不少研究从挖矿奖励机制的激励相容性出发设计新型分配机制. Schrijvers 等针对一个比特币矿池的情况提出了矿池奖励函数的博弈论模型, 并给出了奖励函数满足激励相容性所需的条件[64]. 他们指出在目前已有的条件下, 按比例分配的奖励函数不是激励相容的. Zolotavkin 等也研究了 PPLNS 机制下奖励函数的激励相容性, 并提出一个延迟的通用博弈论模型来应对矿工通过延迟向矿池汇报所发现的部分解来增加收益的情况[65]. 此外, 他们还讨论了激励相容奖励函数所满足的条件, 并提出了一个算法来寻找纳什均衡. Zhang 等提出了一种后向兼容的防御机制来防止自私挖矿, 并指出该机制是最接近激励相容性的防御机制[66].

2.2.2 交易定价机制

数字货币系统中的交易定价是指对矿工提供的交易验证服务进行定价, 其主要通过用户与矿工参与群体性的多重交易费竞价博弈来实现[67−69]. 因此, 交易定价机制本质上是指交易费竞价机制.

目前, 大部分数字货币系统的交易验证博弈, 包括比特币、以太坊等, 本质上都是采用的广义一价 (Generalized first price, GFP) 机制. 这是一种易于理解和实施的最高费用拍卖模式, 但其在实际应用中存在着不少问题: 1) 用户为维持期望的交易确认等候时间支付了不必要的高价[70], 尤其当内存池存在交易拥堵时, 用户更需要支付额外的高价[67]. 2) GFP 机制已经被证明在动态场景中是不稳定的, 会鼓励无效率的策略性行为. 在一定的条件下, 用户会进行周期性的策略调整, 使得均衡表现出价格上升阶段和价格崩溃阶段交错显现的剧烈波动现象[71], 不利于维护交易验证博弈的稳定性与效率性. 另外, 由于每个区块的交易费收益极有可能是属于不同矿工, GFP 机制下矿工的收益不稳定且不公平, 导致交易费的激励作用无法有效发挥. 3) 比特币等典型数字货币系统一般采用双通道机制将付费与非付费交易分别排队, 并在分开的区块空间中进行验证. 这种模式设计需要耗费更多的资源, 带来额外的效率损失[72].

为了解决现行机制面临的问题, 已有工作针对数字货币交易验证博弈的独有特性, 根据机制设计的优化目标, 提出了更为优良的替代性机制. 已有交易定价机制的关键性质分析如表 1 所示.

1) 垄断价格机制 (Monopolistic price, MP): 该机制由 Lavi 等提出, 矿工筛选出能够带来最大收益的可填充交易数量, 而每个被填充交易只需支付它们中的最低交易费出价即可[73]. 该机制在用户足够多的情况下是近乎激励相容的, 能够帮助矿工更好地获取交易费收益[74]. 因此, 采用 MP 机制就不再需要交易费预测机制, 也不需要诉诸于出价隐匿策略, 且当内存池增长时也无需调整交易费.

2) 广义二价 (Generalized second price, GSP)

表 1　已有交易定价机制的比较
Table 1　The comparison of pricing mechanisms

机制	动态稳定性	激励相容性	计算复杂度
GFP	不具备	不具备	不复杂
MP	具备	在用户数量足够多的情况下具备	不复杂
GSP	具备	不具备	不复杂
VCG	具备	具备	复杂
RSOP	具备	未知	较复杂

机制: 在该机制下, 交易获得验证的用户无需按交易费出价进行支付, 而只需要支付比其排名靠后一位的用户的交易费. 该机制在静态完全信息博弈和动态不完全信息博弈环境中均存在稳定均衡, 能够显著地帮助用户减少交易费支出, 并能够在用户数量增加的情况下有效地应对策略性行为[69, 72, 75]. 已有研究表明 GSP 机制能够有效缓解交易费通胀, 稳定参与者收益, 提高数字货币系统的交易效率, 并且不会增加均衡计算的复杂度, 因此显著优于 GFP 机制.

3) 其他机制: Lavi 等还提出了随机采样最优价格 (Random sampling optimal price, RSOP) 机制, 但是该机制被证明不如 MP 机制性能优越[73]. Huberman 等认为区块链系统的用户交易费竞价具有 VCG (Vickrey-Clark-Groves) 性质, 即用户根据他们施加的外生性进行出价. 在此基础上, 他们证明了用户的均衡交易费与 VCG 机制下售卖交易验证优先级的均衡结果保持一致[76]. Iyidogan 构建了包含外生给定的挖矿难度的区块链经济模型来研究交易费结构, 并采用一个双边激励机制来决定最优交易费与最优挖矿成本[77].

在实践中, 也有数字货币系统尝试设计和使用新的交易定价机制. 如以太坊设计了提案 EIP-1559, 基本理念是要求用户支付一笔称为 BASE FEE 的最低交易费, 其可以根据网络的拥堵情况进行调整. 另外, 用户不仅需要设置一笔固定的 Tip (小费) 以激励矿工打包自己的交易, 还需要设置一个 FEE CAP 以表示其愿意支付的最高费用. 当网络较为拥堵时, Tip 可以设置得高于 BASE FEE 以确保交易被尽快确认; 当网络较为通畅或者用户时间成本较低时, 可以设置一个相对较低的 FEE CAP, 以等到 BASE FEE 低于 FEE CAP 时再进行交易确认. 在这个过程中, 矿工只能获得 Tip, 而 BASE FEE 会被协议销毁. 这种设计将有效阻止矿工操纵交易以获取更多交易费, 并使得他们的收入更具可预测性. 比特币重要分叉 BSV (Bitcoin satoshi vision) 允许矿工为 Mining 和 Relay 这两类交易设置不同的保留交易费率, 并允许免费合并一些小微金额的交易, 同时还引入商户用 API (Application programming interface) 以允许交易通过中间商进行提交, 这些机制设计均可以保证小微支付交易能够成功地被及时确认.

2.3　币值机制

一般地, 法定数字货币是由央行提供的一种数字化支付工具, 用以取代现金、降低交易成本和货币发行成本、提升支付效率. 法定数字货币本质上属于流通中的现金, 沿用既有法定货币的计价单位, 其币值与现钞货币相等同, 通常情况下币值较为稳定[78]. 因此, 币值机制研究适用于由私营主体发行的没有国家公信力背书的数字货币, 主要是指对数字货币价格进行合理评估, 并通过特定的机制设计维持数字货币的币值稳定.

虽然从理论上讲, 基于区块链的数字货币可以为任何拥有互联网设备的人提供货币服务, 但目前数字货币只能在有限的范围内为相对较少的人提供货币服务, 很难发展成为国际通用货币[79−81]. 在实践中, 私营数字货币由于币值的剧烈波动性, 导致其在更大程度上是扮演了 “投资品”的角色, 本质上是一种金融资产, 而不是作为公允的 “一般等价物”[82−83]. 只有解决价格波动性问题才能使得数字货币成为真正的货币, 并为其找到作为价格投资品之外更合理、更具有价值的应用. 因此, 对数字货币的价值基础以及价格形成机制的研究显得尤为重要[84−85]. Glaser 等提出了一个经济计量模型对比特币进行估值, 该模型包含了当前数字货币汇率价格发现过程的基本组成部分, 并基于实证分析表明比特币的价格波动受到媒体报道和积极情绪的显著影响[86]. Ciaian 等以比特币为代表, 研究了数字货币的价格形成机制, 基于 Barro 模型, 利用 2009 年 ~ 2015 年的实际数据, 考虑了货币价格的传统决定因素以及数字货币的特定因素, 对比特币价格进行预测, 指出市场力量、用户兴趣以及金融发展等共同推动了比特币价格上涨[87]. 陈享光等分析了数字货币的锚定物, 认为货币价格的维护取决于有效的货币锚定机制的建立[88].

在数字货币价格影响因素与形成机制分析的基础上, 通过有效的币值机制设计来稳定数字货币价格成为了新的研究焦点. 2013 年, Willet 在万事达币 (Master Coin, 后更名为 Omni) 白皮书中提出的锚定资产的稳定币的想法[89], 开启了基于区块链的数字货币价格稳定机制的研究. 目前, 已有三种类型的价格稳定机制设计, 即链下抵押机制、链上抵押机制和算法式稳定机制.

1) 链下抵押机制: 通常是通过锚定法定货币或者一揽子资产 (包括国家债券、大宗商品、黄金等) 来维护数字货币的价格稳定. 其基本原理类似于货币局制度, 由中心化机构采用足额信用较好的货币或资产作为抵押物保证价格稳定. 该类型的价格稳定机制要求有足够的抵押物储备, 才能维持价格稳定. 2015 年, Tether 公司基于比特币发行的锚定美元的泰达币 (USDT), 最早启用了法币抵押机制. 2018 年, Lipton 等基于区块链技术, 利用套期保值机制, 建立了一种面向交易的数字货币, 它在价格稳定机制设计方面是通过实际资产背书实现的[90]; 同年, 纽约信托公司 Gemini 和初创公司 Paxos 相继基于以太坊推出锚定美元的数字货币 GUSD (Gemini Dollar) 和 Pax (Paxos Standard); 2019 年, Facebook 则推出了新的数字货币 Libra, 通过一揽子银行存款和法币政府债券的储备来实现人们对其价格的认定, 后又改进为也提供锚定单一法币的稳定币.

2) 链上抵押机制: 一般是以主流数字货币做背书并进行超额抵押来维持价格稳定, 通过写入智能合约的算法来自动管理抵押资产的清算. 该类价格稳定机制最大的缺陷在于价格会随抵押物价格的波动而波动, 不够稳定. 2017 年, MakerDAO 发行了 Dai, 其采用锚定以太币的去中心化抵押机制; 2018 年 Havven 公司发行了 nUSD, 在价格稳定机制方面也是锚定以太币.

3) 算法式稳定机制: 摆脱了对其他资产的依赖, 通过去中心化的算法设计来主动调整供求关系, 自动增发或者回收数字货币, 以实现市场供求平衡和价格稳定. 这种价格稳定机制的缺陷在于去中心化的设计, 使得数字货币价格在面临瞬时大幅变动时, 很难及时有效地恢复稳定状态. 2014 年, BASIS 发行, 它的智能合约中内置的算法被用来衡量需求变动以触发新币的铸造或者旧币的销毁, 直到价格回到预设值为止; Al-Naji 等也提出了基于算法设计实现数字货币价格稳定的机制[91].

2.4 发行机制

在私营数字货币系统中, 发行机制受发行方式、发行总量、产出速度、发行币种等影响而有所不同. 根据发行方式不同分为挖矿机制和非挖矿机制两类. 其中, 挖矿机制通过矿工的算力投入寻找特定随机数产生新区块的同时挖出新的数字货币, 如比特币、莱特币等; 非挖矿机制则无需挖矿而直接在网络中发行货币, 如 Libra、USDT 等. 根据发行总量是否有上限可以分为有限发行机制、无限发行机制以及有限与无限混合发行机制, 如比特币的发行总量限制在 2 100 万枚; 以太币则无总量限制; 点点币的代币分为有限和无限两种, 有限的部分随着区块高度增加不断减少, 而无限的部分每年有 1% 的通胀率. 根据产出速度不同可以分为定量发行机制和增量发行机制, 如瑞波币自上线开始就一次性定量发行 1 000 亿枚货币, 但总量会随着使用逐渐减少; 而比特币按照预先设定的产出速度进行增量发行 (约每 4 年减半一次). 按照发行币种可以分为单币发行机制与双币发行机制, 如大部分非稳定币值的数字货币采用单币发行机制; 而稳定币一般采取双币发行机制, 以保证系统内运行的币种具有价格稳定的特性.

由国家公信力背书的法定数字货币在设计过程中, 发行机制受货币政策、金融体系等的影响要复杂得多. 在区块链的技术背景下, 数字货币的支付与流通方式发生了巨大的变化, 对发行管理方式提出了新的要求. 尽管现行的基于区块链的私营数字货币发行机制能够提供一定的参考, 但显然完全去中心化的发行机制并不能完全适用于法定数字货币, 因为其需要更低的成本、更快的速度、更可控的发行量与更完善的管理方式来保障法定数字货币的信用基石. 在法定数字货币发行机制研究方面, 重点解决数字货币的货币层次与发行数量、发行方式与发行主体、流通与回笼机制等设计问题.

1) 货币层次与发行数量. 如中国的央行数字货币是具有无限法偿特性的货币, 其功能和属性与纸币相似, 只是形式是数字化的, 在一定程度上取代了流通中的现金 (即 M0), 可以直接用于零售消费. 因此, 法定数字货币的发行数量也需要根据社会价格水平、社会总产出、货币流通速度、货币乘数等传统货币发行理论指标, 并基于其对货币政策、货币体系与金融稳定等的影响分析来综合考虑决定[92−93].

2) 发行方式与发行主体. 可以有两种模式选择: 由中央银行直接面向公众发行数字货币或遵循传统的中央银行–商业银行二元模式[22, 94]. 目前已有的法定数字货币设计与实践大多采用第二种方式. 如英国的 RSCoin 原型、加拿大的电子加元等, 均是由中央银行作为法定数字货币的发行主体, 并通过商业银行间接向公众提供法定数字货币的存取等服务, 两类主体共同维护数字货币发行与流通体系的正常运行[95].

3) 流通与回笼机制. 流通机制主要研究数字货币如何从中央银行产生并发送至商业银行, 最终进入流通环节, 在用户之间进行转移支付[96]; 回笼机制主要研究商业银行如何将数字货币缴存至中央银

行. 在这个过程中重点分析商业银行存款准备金, 兑换机制以及存储机制等问题[22, 94]. 尤其是基于区块链的体系设计中, 法定数字货币在中央银行以及商业银行的存储格式、存储位置、存储方法以及转移方式等不仅需要考虑到传统发行流通机制中涉及的管理问题, 还需考虑区块链技术背景下的运行安全性问题[97].

3 风险监管

基于区块链的数字货币在发展过程中, 应用场景与范围逐步扩大, 影响能力也日益增强. 现有的监管体系与数字货币 (尤其是私营数字货币) 发展实践不匹配, 很难防范其对金融体系与经济运行带来的不确定性影响及衍生风险. 因此, 需要从理论与实践两方面创新数字货币监管, 以促进数字货币生态与应用的健康发展.

3.1 风险分析

尽管币值不稳定的私营数字货币并不完全具备货币属性, 但是它们作为新的金融信息技术与支付工具, 由于发行成本低、防伪性能高、保管成本低、便捷性高、去中心化管理等优点对传统货币具有一定的替代性, 在一定程度上丰富了支付渠道, 降低了支付成本并提升了支付清算效率[98]. 随着私营数字货币向稳定币进化, 发展出了 Libra 这样的数字货币, 其以区块链技术构建基础金融设施, 以一揽子货币作为储备资产, 具备全球流通性、币值稳定性以及一定的供需均衡性, 本质上是超主权数字货币 (尽管在其 2.0 版本的白皮书中不再宣称成为超主权数字货币), 已经具备了货币的主要功能, 可成为支付手段、储值工具以及记账单位, 由此与现有的经济生活与金融生态产生了更为紧密的关联. 可以看出, 数字货币在不断进化与发展的过程中所能产生的影响越来越广泛而深远, 进而也会对现行支付体系运行、货币政策执行、金融稳定维护以及国际货币体系构建等带来一定的风险[99−101].

1) 支付体系: 私营数字货币的流通、交易与支付都是独立于法定支付体系之外, 为洗钱、非法买卖等一系列违法支付活动提供了便利, 对央行和货币当局的监管造成困难[100]. 它们与现行支付体系的支付工具是竞争关系, 具有一定的替代作用, 因此会对商业银行等金融机构的支付功能造成冲击, 并由此对支付体系带来不确定风险[99]. 同时, 它们的发行流通机制以及信用背书能力与法定数字货币大不相同, 导致其在清算量大、价格波动、宏观经济形势变化等特殊情况下很难具备良好的应对能力并发挥好支付结算功能[2].

2) 货币政策: 央行通过支付体系监测货币流动等信息的能力会因为私营数字货币的流通有所削弱. 另外, 私营数字货币还具备投资属性, 导致监管机构很难判断用户是出于何种需求用其来替代现行支付工具, 这就加大了广义货币量的统计难度, 进一步降低了货币指标统计的准确性[100, 102]. 央行货币政策有效调控的前提是垄断货币发行权, 对货币供给数量与价格具备完全的调控能力, 显然这一点对私营数字货币是很难实现的. 私营数字货币的存在还会降低货币需求的稳定性. 因此, 当数字货币达到一定规模, 它们会从货币供需与货币乘数角度削弱货币政策的有效性, 提高货币政策制定的难度[8, 103]. 另外, 私营数字货币的流通也会造成中央银行铸币税损失[102].

3) 金融稳定: 私营数字货币的去中心化属性会引发金融脱媒现象, 对金融系统的储蓄与授信机制产生影响, 削弱国家对于金融系统的调控[103]. 其系统本身就存在的风险, 包括合规风险、隐私暴露风险、信用风险等, 也会随着它们的流通进入金融市场, 影响金融生态的稳定性[99]. 私营数字货币跨境流通比较便利且不受有效监管, 可对经济体的资本流通造成冲击, 造成国内资产价格波动, 进而影响金融稳定性[104]. 私营数字货币与法定货币之间的替代关系还会加大主权国家法定货币的汇率波动, 损害经济体的金融发展与经济增长[100].

4) 国际货币体系: 大部分私营数字货币以美元结算, 而大部分稳定币以美元为主要甚至唯一储备资产, 在一定程度上会强化美元在国际货币体系中的主导地位, 遏制包括人民币在内的其他货币的国际化发展. 数字货币的流通在线上, 法定货币的流通主要在线下, 数字货币锚定法定货币的机制将国际货币竞争格局从线下扩大至线上, 引发法定数字货币领域的战略竞争, 从而对国际货币体系产生冲击[99].

3.2 监管考量

对数字货币的监管需从技术理论发展与政策措施实践两个角度进行考虑, 两个方面相互配合以建设完善的监管体系.

3.2.1 技术理论发展

在数字货币监管理论与技术发展方面, 重点关注可监管模型、用户识别理论以及链上数据分析方法等[105].

[2] 陈雨露. 稳定币可能对一国货币政策产生影响. 2019 中国金融学会学术年会暨中国金融论坛年会, 2019 年 12 月 21 日

可监管数字货币模型是在隐私保护和共识可信的基础上, 将监管机制引入数字货币系统内部, 实现对账户及交易信息的监控、追溯和管理. 监管机制的构建可以通过引入第三方用户身份认证以及改变交易账本结构来实现[106]. 用户身份认证也是用户识别理论的核心, 其关键是保证信息只被合法授权用户获取和访问[107], 目标是将用户与交易进行匹配, 以便实现对其的追踪, 认证的可以是地址[108−109]、公钥[110] 或签名[111]. 改变交易账本结构主要是将账本区分为公共和私有两部分. 其中, 公共部分记录完整的交易信息, 用于在保护用户隐私的前提下进行监管追溯, 这部分账本的维护者比普通用户有更高的权限; 私有部分仅记录存储交易状态信息, 每个普通用户都可以参与其中. 用联盟链记录公共账本, 公有链记录私有账本的双链设计机制可以实现交易账本的分级结构, 以实现可监管的目的[112−113]. 另外, 链上数据分析方法在隐私保护的前提下, 通过大数据分析、信息挖掘、机器学习等技术, 对一些匿名的未经验证的账户及交易进行追踪, 以实现对非法交易的识别与监管.

3.2.2 政策措施实践

首先, 需要对数字货币的金融属性与法律属性达成统一认识, 并依此选择合适的监管模式[114]. 如美国将数字货币认定为非储蓄型的货币, 对参与机构的限制较松, 而对产品和服务的监管相对较严; 欧盟将数字货币定义为一个单独的行业, 侧重于对发行机构的监管, 对其单独颁发专门的牌照; 新加坡对数字货币采用分类监管模式, 资本市场产品类的监管相对严格, 需遵循证券和期货法案, 而工具性通证类的监管则相对自由灵活; 我国将比特币等数字货币定性为虚拟商品而不是真正意义上的货币, 认为这类数字货币的公开发行 (Initial coin offering, ICO) 本质上是一种未经批准的非法融资行为, 对数字货币发行、交易和流通都采取了严格监管.

其次, 根据数字货币市场发展实践, 制定健全且可操作的标准与政策. 如日本是亚洲数字货币交易发展最早也最活跃的国家, 其根据数字货币发展阶段的不同陆续推出了一系列法律与政策措施, 包括数字货币的法定地位认定、数字货币税收征缴、数字货币发行监管、数字货币兑换与交易规范等, 逐步形成了完善的数字货币监管体系.

再次, 在多元主体混合监管模式下, 对监管界限和权责进行清晰的划分. 如美国 “2020 年加密货币法案”将数字货币分为加密商品、加密货币和加密证券三类, 分别由商品期货交易委员会、金融犯罪执法网络以及证券交易委员会进行监管.

最后, 鉴于数字货币的跨境流通属性, 需要构建全球监管的协调机制[99, 115]. 如二十国集团 (G20) 认为数字货币缺乏主权货币的属性, 为金融稳定带来潜在风险, 因此推动在全球范围内实施金融行动特别工作组标准, 以期构建全球数字货币风险监测与管理体系.

4 总结与展望

近年来, 基于区块链的数字货币理论研究和应用实践得到了广泛关注和快速发展. 本文阐述了数字货币技术创新、机制设计以及风险监管三方面的研究与实践进展, 从基础支撑技术、隐私保护技术两个方向分析了数字货币技术创新; 从共识机制、激励机制、币值机制以及发行机制等角度梳理了数字货币核心机制设计; 从风险分析与监管考量两方面讨论了数字货币的风险监管, 以期为未来研究提供有益的启发和参考.

未来, 无论是私营数字货币从 “投资品”发展成为真正的货币工具与支付手段, 还是法定数字货币从研发试验走向应用落地, 都离不开基础理论支撑. 因此, 需要进一步从交易定价、稳定币、可监管数字货币、量子货币、企业货币、平行货币等重点方向对数字货币理论进行深入的探索.

4.1 交易定价

在数字货币系统中, 矿工通过持续性的算力投入在保护数字货币账本一致性的同时为用户提供交易验证服务; 用户通过持久活跃的交易参与, 为矿工提供交易费激励. 矿工的算力投入在一定程度上取决于用户的交易费激励, 而用户的交易费决策则在一定程度上依赖于矿工所能提供的交易验证效率. 优良的交易定价机制设计不仅从微观层面调节用户的交易确认等候时间, 激励诚实矿工确认与记录交易, 还从宏观层面保障数字货币系统运行的安全性、活跃性与持续性 (如遏制参与者的某些有损系统安全的非诚实性策略行为, 包括用户提交大量低值交易、矿工挖空块、分布式拒绝服务攻击等), 并影响数字货币的落地应用 (如交易费通胀阻碍小微交易场景, 交易费波动过于频繁影响数字货币成为可信支付工具).

基于区块链的数字货币定价机制研究面临着巨大的挑战: 受众多耦合的外部环境因素和内部参与者行为因素的综合影响; 参与者的策略行为与交易定价机制存在闭环反馈的影响关系; 交易定价机制与共识机制、币值机制密切关联. 因此, 如何在充分考虑各个因素、各种行为以及各类机制的耦合与关联的基础上, 创新交易定价机制设计研究以匹配数字货币系统运行实践是亟需解决的关键问题.

4.2 稳定币

2019 年, Libra 的出现引发了人们对于稳定币以及数字货币币值的热烈讨论. 尽管从本质上来说, 几乎所有的稳定币最终的锚定物都是美元, 但它们在实现机制上还是有很大区别的. 采用链下抵押机制和链上抵押机制的稳定币均需借助中心化的抵押模式, 实现数字货币与抵押资产的联结. 市场实践表明, 与抵押物脱钩是这两类稳定币面临的最大风险. 算法式机制由于抛弃了抵押模式, 转而借助供需关系调节实现数字货币的货币信用与价格稳定, 从而在一定程度上解决了抵押式稳定币面临的问题.

算法式稳定币是稳定币的主流发展方向. 如何在纪元时间与锁定时间、代币基数调整机制、供需关系判断、货币价值评估、价值信息传递、算法套利等方面进行设计以完善数字货币调节机制, 实现价格偏离程度较小且市场投机程度较低的稳定币是值得关注的重要问题.

4.3 可监管数字货币

对数字货币进行监管以防止其成为非法金融活动的工具, 已经成为政府和业界的共识. 然而在实践中, 由于数字货币越来越强的匿名性, 导致对其监管困难重重. 目前, 已有的监管政策与措施主要着力于数字货币与其他金融系统产生关联的部分, 而缺乏一种深入系统内部的监管方案. 因此, 基于区块链的可监管数字货币研究显得尤为重要.

目前已有研究主要通过引入媒介化的身份认证机制或层级化的双链机制来实现监管功能, 而这两种方案均带来了中心化问题, 在一定程度上削弱了数字货币系统的安全性与效率性. 如何在不破坏去中心化可信共识的前提下, 将监管机制引入数字货币系统内部, 实现匿名性隐私保护与可控监管的平衡共存是可监管数字货币设计中值得探讨的核心问题. 首先, 基于区块链的数字货币发行可以在公有链、联盟链和私有链上实现, 对于这三类运营方式, 监管机制设计与监管技术应用应有不同的针对性, 如联盟链的穿透式监管, 公有链的主动发现与探测技术, 以链制链的体系结构以及标准等. 其次, 监管机制内嵌于数字货币交易业务流程中, 其对节点的追踪与对交易请求、流程、结果等的实时监控应在可控范围之内, 以保证区块链的匿名性与隐私保护优势仍旧得以发挥. 最后, 深入数字货币系统内部的监管部门属性、监管职能权限以及监管规则制定应当具备一定的可调整性, 以适应不同的数字货币应用场景.

4.4 量子货币

近年来, 量子计算与量子通信的快速发展, 已经对基于区块链的数字货币体系产生了切实的威胁和深远的影响. 目前, 绝大多数数字货币的安全性均是建立在传统计算机难以有效求解单向困难数学问题的密码学假设基础之上, 依赖由此设计的 SHA-256、RSA 以及椭圆曲线加密等算法实现数字货币的安全发行、交易与验证. 然而, 量子计算特有的并行计算能力将会使这些密码学算法的攻击难度减半甚至破解, 因而催生了后量子时代的数字货币 (称为量子货币) 研究[116].

实际上, 量子货币研究由来已久, 由哥伦比亚大学 Wiesner 首先提出[117], 其基本思想是利用量子不可克隆原理和测不准原理等量子力学特性来解决传统数字货币的伪造与双花问题, 实现无条件安全的量子货币. 数十年来, 研究者一直致力于量子货币发行权和验证权的去中心化研究, 提出了基于量子密钥分发或量子隐形传态技术的货币发行与支付技术, 以及基于量子数字签名技术的货币验证技术等. 同时, 抗量子数字签名技术也蓬勃发展, 为抵御量子计算威胁奠定了坚实基础. 可以预见, 随着数字货币研究与应用的不断深入, 量子货币必将是未来研究的重点领域和发展趋势.

4.5 企业货币

如果私营数字货币的信用度和流通性强大到用户无需将其兑换成法定货币便可用于交易, 那么私营发行机构将成为用户的 “中央银行”; 而在现行的经济框架与货币体系下, 要实现这一愿景, 必须借助企业货币. 企业货币是继加密货币、稳定币、法定数字货币之后, 数字货币的第四个发展阶段, 其概念由中科院自动化所的王飞跃研究员于 2016 年提出[118]. 企业货币强调的是企业管理模式借助数字货币实现商业流程优化和转型升级, 而非借助 ICO 等手段实现发币募资.

当数字货币发展至企业货币阶段, 任何有需求的企业均可依托自身信用发行专属数字货币, 并将其用于人员绩效、任务分配等内部核心业务管理以及成本支出、业务收入等外部关联业务管理, 使得企业与员工、企业与企业、员工与员工之间的任何交易都有迹可循、有据可依、有法可考. 在理论研究方面, 构建企业货币的生态体系与运行架构, 设计企业货币的应用场景与业务逻辑, 评估企业货币的建设成本与应用价值是支撑企业货币从概念走向实践的关键基础.

4.6 平行货币

区块链技术使得传统的难以流通和商品化的 “注意力”和 “信用力”成为可批量生产的流通商品, 革命性地扩展了经济活动的范围与提高效率的途径. 平行经济是通向智能经济的技术之路, 智能经济是工业经济升级转型的必由之路, 而基于区块链的平行货币则是平行经济的 “血液”[119].

平行货币基于平行智能理论与 ACP 方法 (Artificial systems + Computational experiments + Parallel execution, 人工系统 + 计算实验 + 平行执行), 构建人工数字货币系统及与原生货币对应的人工货币, 面向特定经济场景利用计算实验进行实验优化, 并通过实际数字货币系统与人工数字货币系统的虚实交互与闭环反馈, 来实现原生数字货币与人工数字货币的平行调谐. 平行货币系统将大有可为, 它的存在为非常态情况下的数字货币发行、交易、流通、估值、监管等提供了实时的管理决策优化支持.

References

1 Ferguson N. *The Ascent of Money*: *A Financial History of the World*. London: Allen Lane, 2008.

2 Hayek F A. *Denationalisation of Money*: *The Argument Refined*. New York: Transatlantic Arts, 1977.

3 Chaum D. Blind signatures for untraceable payments. *Advances in Cryptology*. Boston, MA: Springer, 1983. 199−203

4 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [Online], available: https://bitcoin.org/bitcoin.pdf, October 31, 2008

5 Zhu Ge. The concept and controvery of digital currency. *Value Engineering*, 2015, **34**(31): 163−167
(朱阁. 数字货币的概念辨析与问题争议. 价值工程, 2015, **34**(31): 163−167)

6 Yao Qian, Tang Ying-Wei. Some thoughts on central bank-issued digital currency. *Journal of Financial Research*, 2017(7): 78−85
(姚前, 汤莹玮. 关于央行法定数字货币的若干思考. 金融研究, 2017(7): 78−85)

7 Yuan Yong, Wang Fei-Yue. *Blockchain Theory and Method*. Beijing: Tsinghua University Press, 2019.
(袁勇, 王飞跃. 区块链理论与方法. 北京: 清华大学出版社, 2019.)

8 Li Zhen, Liu Ying-Ge, Dai Yi-Cheng. The impact of Libra on China′s monetary policy and its countermeasures. *Journal of Xi'an Jiaotong University (Social Sciences)*, 2020, **40**(3): 55−63
(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. 西安交通大学学报 (社会科学版), 2020, **40**(3): 55−63)

9 Yuan Y, Wang F Y. Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018, **48**(9): 1421−1428

10 Ali R, Barrdear J, Clews R, Southgate J. Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, 2014, **54**(3): 262−275

11 Zarifis A, Cheng X S, Dimitriou S, Efthymiou L. Trust in digital currency enabled transactions model. In: Proceedings of the 9th Mediterranean Conference on Information Systems (MCIS). Samos, Greece: The Association for Information Systems, 2015. 1−8

12 Zhang Ji-Teng. Blockchain, super-sovereign digital currency, and reform of the international monetary system: The case of E-SDR. *Global Review*, 2019(6): 20−45
(张纪腾. 区块链及超主权数字货币视角下的国际货币体系改革—以 E-SDR 的创新与尝试为例. 国际展望, 2019(6): 20−45)

13 Clark J, Essex A. CommitCoin: Carbon dating commitments with Bitcoin. In: Proceeding of the 2012 International Conference on Financial Cryptography and Data Proceedings of the 2012 Security. Berlin, Heidelberg: Springer, 2012. 390−398

14 Xie Kai-Bin. Study on evolution of digital currency based on blockchain. *Application Research of Computers*, 2019, **36**(7): 1935−1939
(谢开斌. 基于区块链的数字货币演化. 计算机应用研究, 2019, **36**(7): 1935−1939)

15 Zhang L C, Mao Y Q. Discussion on the development prospect of digital currency based on blockchain technology. In: Proceedings of the 2018 International Workshop on Advances in Social Sciences (IWASS 2018). Hong Kong, China: Francis Academic Press, 2018. 1249−1252

16 Abboushi S. Global virtual currency-brief overview. *Journal of Applied Business and Economics*, 2017, **19**(6): 10−18

17 Balvers R J, McDonald B. Designing a global digital currency. *Journal of International Money and Finance*, DOI: 10.1016/j.jimonfin.2020.102317

18 Yang Tao. Review on the researches of digital currency based on blockchain technology. *Times Finance*, 2017(4): 305−307
(杨涛. 区块链技术创新发展数字货币的研究综述. 时代金融, 2017(4): 305−307)

19 Zhu Shao-Ping. Thoughts on blockchain and digital currency. *Tsinghua Financial Review*, 2018(4): 83−86
(朱少平. 关于区块链与数字货币的思考. 清华金融评论, 2018(4): 83−86)

20 Si Xue-Ming, Xu Mi-Xue, Yuan Chao. Survey on security of blockchain. *Journal of Cryptologic Research*, 2018, **5**(5): 458−469
(斯雪明, 徐蜜雪, 苑超. 区块链安全研究综述. 密码学报, 2018, **5**(5): 458−469)

21 Huang Ying. Survey on blockchain-based digital currency. *Financial Computer of China*, 2019(6): 78−81
(黄瑛. 基于区块链技术的数字货币发展综述. 中国金融电脑, 2019(6): 78−81)

22 Yao Q. A systematic framework to understand central bank digital currency. *Science China Information Sciences*, 2018, **61**(3): 033101

23 Zhang Wei, Chen Yang. Prospects and challenges of blockchain technology applied in digital currency. *Tsinghua Financial Review*, 2017(4): 34−36
(张伟, 陈旸. 区块链技术在数字货币应用中的前景与挑战. 清华金融评论, 2017(4): 34−36)

24 Xiao Feng. From public chain to private chain: Blockchain returns to reality. *Modern Bankers*, 2016(2): 35−37
(肖风. 从公有链到私有链: 区块链回归现实. 当代金融家, 2016(2): 35−37)

25 Han Feng, Liu Yi-Fang, Sun Xue-Qiang. The central bank′s issuing of digital currency must be based on the public chain. *Tsinghua Financial Review*, 2016(6): 99−102
(韩锋, 刘一方, 孙雪强. 央行发行数字货币必须基于公有链. 清华金融评论, 2016(6): 99−102)

26 Danezis G, Meiklejohn S. Centrally banked cryptocurrencies. arXiv:1505.06895, 2015.

27 Raskin M, Yermack D. Digital currencies, decentralized ledgers and the future of central banking. *Research Handbook on Central Banking*. Cheltenham, UK: Edward Elgar Publishing, 2018. 474−486

28 Cai Zhao. Blockchain technology and its application in financial industry. *Financial Computer of China*, 2016(2): 30−34
(蔡钊. 区块链技术及其在金融行业的应用初探. 中国金融电脑, 2016(2): 30−34)

29 Fu Shuo, Xu Hai-Xia, Li Pei-Li, Ma Tian-Jun. A survey on anonymity of digital currency. *Chinese Journal of Computers*, 2018, **42**(5): 1045−1062
(付烁, 徐海霞, 李佩丽, 马添军. 数字货币的匿名性研究. 计算机学报, 2018, **42**(5): 1045−1062)

30 Conti M, Kumar E S, Lal C, Ruj S. A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 2018, **20**(4): 3416−3452

31 Maxwell G. CoinJoin: Bitcoin privacy for the real world

[Online], available: https://bitcointalk.org/?topic=279249, August 1, 2013

32 Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical decentralized coin mixing for Bitcoin. In: Proceedings of the 2014 European Symposium on Research in Computer Security (ESORICS). Wroclaw, Poland: Springer-Verlag, 2014. 345−364

33 Ziegeldorf J H, Grossmann F, Henze M, Inden N, Wehrle K. CoinParty: Secure multi-party mixing of Bitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. San Antonio, Texas, USA: ACM, 2015. 75−86

34 Ibrahim M H. SecureCoin: A robust secure and efficient protocol for anonymous Bitcoin ecosystem. *International Journal of Network Security*, 2017, **19**(2): 295−312

35 Peng Yu-Xing, Wei Bo. Enhancing anonymity of Cryptocurrency based on ring signature algorithm. *Cyberspace Security*, 2019, **10**(3): 99−104
(彭育兴, 魏波. 基于环签名的数字货币隐私保护技术. 网络空间安全, 2019, **10**(3): 99−104)

36 Bonneau J, Narayanan A, Miller A, Clark J, Kroll J A, Felten E W. Mixcoin: Anonymity for Bitcoin with accountable mixes. In: Proceedings of the 2014 International Conference on Financial Cryptography and Data Security. Christ Church, Barbados: Springer, 2014. 486−504

37 Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for Bitcoin. In: Proceedings of the 2015 International Conference on Financial Cryptography and Data Security. San Juan, Puerto Rico: Springer, 2015. 112−126

38 Heilman E, Alshenibr L, Baldimtsi F, Scafuro A, Goldberg S. TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub. Network & Distributed System Security Symposium. San Diego, California, USA: Internet Society, 2017. 1−15

39 Bao Zi-Jian, Wang Qing-Hao, Zhang Yong-Xin, Wang Bin, Lu Ning, Shi Wen-Bo. Regulatory Bitcoin privacy-preserving mixing service. *Chinese Journal of Network and Information Security*, 2019, **5**(4): 40−51
(包子健, 王庆豪, 张永欣, 王斌, 鲁宁, 史闻博. 可监管的比特币隐私保护混淆服务. 网络与信息安全学报, 2019, **5**(4): 40−51)

40 Tang Chang-Bing, Yang Zhen, Zheng Zhong-Long, Chen Zhong-Yu, Li Xiang. Game dilemma analysis and optimization of PoW consensus algorithm. *Acta Automatica Sinica*, 2017, **43**(9): 1520−1531
(唐长兵, 杨珍, 郑忠龙, 陈中育, 李翔. PoW 共识算法中的博弈困境分析与优化. 自动化学报, 2017, **43**(9): 1520−1531)

41 Xia Qing, Zhang Feng-Jun, Zuo Chun. Review for consensus mechanism of cryptocurrency system. *Computer Systems and Applications*, 2017, **26**(4): 1−8
(夏清, 张凤军, 左春. 加密数字货币系统共识机制综述. 计算机系统应用, 2017, **26**(4): 1−8)

42 Yuan Yong, Ni Xiao-Chun, Zeng Shuai, Wang Fei-Yue. Blockchain consensus algorithms: The state of the art and future trends. *Acta Automatica Sinica*, 2018, **44**(11): 2011−2022
(袁勇, 倪晓春, 曾帅, 王飞跃. 区块链共识算法的发展现状与展望. 自动化学报, 2018, **44**(11): 2011−2022)

43 Ren L. Proof of stake velocity: Building the social currency of the digital age [Online], available: https://assets.coss.io/documents/whitepapers/reddcoin.pdf, April 10, 2018

44 Stewart I. Iain Stewart′ s version of proof of burn [Online], available: https://en.bitcoin.it/wiki/Proof_of_burn, January 15, 2018

45 Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: Extending Bitcoin′s proof of work via proof of stake. *ACM SIGMETRICS Performance Evaluation Review*, 2014, **42**(3): 34−37

46 Gunduz D, Devillers B. Two-hop communication with energy harvesting. In: Proceedings of the 4th IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing. San Juan, PR, USA: IEEE, 2011. 201−204

47 Kwon J. Tendermint: Consensus without mining [Online], available: http://tendermint.com/static/docs/tendermint.pdf, April 18, 2016

48 Zamfir V. Introducing Casper “the friendly ghost” [Online], available: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost, August 1, 2015

49 Miller A, Xia Y, Croman K, Shi E, Song D. The honey badger of BFT protocols. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016. 31−42

50 Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Proceedings of the 2017 Annual International Cryptology Conference. Santa Barbara, USA: Springer, 2017. 357−388

51 Goodman L M. Tezos-a self-amending crypto-ledger White paper [Online], available: https://www.tezos.com/static/papers/white_paper.pdf, September 2, 2014

52 Eyal I, Gencer A E, Sirer E G, Van Renesse R. Bitcoin-NG: A scalable blockchain protocol. arXiv:1510.02037, 2015.

53 Kokoris-Kogias E, Jovanovic P, Gailly N, Khoffi I, Gasser L, Ford B. Enhancing bitcoin security and performance with strong consistency via collective signing. In: Proceedings of the 25th USENIX Conference on Security Symposium. Berkeley, CA, United States: USENIX Association, 2016. 279−296

54 Luu L, Narayanan V, Zheng C D, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer & Communications Security. Vienna, Austria: ACM, 2016. 17−30

55 Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. OmniLedger: A secure, scale-out, decentralized ledger via sharding. In: Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA: IEEE, 2018. 583-598

56 Chen L, Xu L, Shah N, Gao Z M, Lu Y, Shi W D. On security analysis of proof-of-elapsed-time (PoET). In: Proceedings of the 2017 International Symposium on Stabilization, Safety, and Security of Distributed Systems. Boston, MA, USA: Springer, 2017. 282−297

57 Milutinovic M, He W, Wu H, Kanwal M. Proof of luck: An efficient blockchain consensus protocol. arXiv: 1703.05435, 2017.

58 Abusalah H, Alwen J, Cohen B, Khilko D, Pietrzak K, Reyzin L. Beyond Hellman′s time-memory trade-offs with applications to proofs of space. In: Proceedings of the 2017 International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China: Springer, 2017. 357−379

59 Dong Z L, Lee Y C, Zomaya A Y. Proofware: Proof of useful work blockchain consensus protocol for decentralized applications. arXiv: 1903.09276, 2019.

60 Copeland C, Zhong H X. Tangaroa: A byzantine fault tolerant raft [Online], available: http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf, December 30, 2014

61 Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: Scaling byzantine agreements for cryptocurrencies. In: Proceedings of the 26th Symposium on Operating Systems Principles. Shanghai, China: ACM, 2017. 51−68

62 Rosenfeld M. Analysis of Bitcoin pooled mining reward systems. arXiv:1112.4980, 2011.

63 Qin R, Yuan Y, Wang F Y. A novel hybrid share reporting strategy for blockchain miners in PPLNS pools. *Decision Support Systems*, 2019, **118**: 91−101

64 Schrijvers O, Bonneau J, Boneh D, Roughgarden T. Incentive compatibility of Bitcoin mining pool reward functions. In: Proceedings of the 2016 International Conference on Financial Cryptography and Data Security. Christ Church, Barbados: Springer, 2016. 477−498

65 Zolotavkin Y, Garcia J, Rudolph C. Incentive compatibility of pay per last N shares in Bitcoin mining pools. In: Proceedings of the 2017 International Conference on Decision and Game Theory for Security. Vienna, Austria: Springer, 2017. 21−39

66 Zhang R, Preneel B. Publish or perish: A backward-compatible defense against selfish mining in Bitcoin. In: Proceedings of the 2017 Cryptographers′ Track at the RSA Conference. San Francisco, USA: Springer, 2017. 277−292

67 Moser M, Bohme R. Trends, tips, tolls: A longitudinal study of Bitcoin transaction fees. In: Proceedings of the 2015 International Conference on Financial Cryptography and Data Security. San Juan, Puerto Rico: Springer, 2015. 19−33

68 Jiao Y T, Wang P, Niyato D, Xiong Z H. Social welfare maximization auction in edge computing resource allocation for mobile blockchain. In: Proceedings of the 2018 IEEE International Conference on Communications (ICC). Kansas City, MO, USA: IEEE, 2018. 1–6

69 Basu S, Easley D, O'Hara M, Sirer E G. Towards a functional fee market for cryptocurrencies. arXiv: 1901.06830, 2019.

70 Edelman B, Ostrovsky M, Schwarz M. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *The American Economic Review*, 2007, **97**(1): 242–259

71 Zhang X, Feng J. Cyclical bid adjustments in search-engine advertising. *Management Science*, 2011, **57**(9): 1703–1719

72 Li J J, Yuan Y, Wang F Y. A novel GSP auction mechanism for ranking Bitcoin transactions in blockchain mining. *Decision Support Systems*, 2019, **124**: 113094

73 Lavi R, Sattath O, Zohar A. Redesigning Bitcoin's fee market. arXiv: 1709.08881, 2017.

74 Yao A C C. An incentive analysis of some Bitcoin fee design. arXiv: 1811.02351, 2018.

75 Li J J, Ni X C, Yuan Y, Wang F Y. A novel GSP auction mechanism for dynamic confirmation games on Bitcoin transactions. *IEEE Transactions on Services Computing*, DOI: 10.1109/TSC.2020.2994582

76 Huberman G, Leshno J, Moallemi C. Monopoly without a monopolist: An economic analysis of the Bitcoin payment system [Online], available: http://dx.doi.org/10.2139/ssrn.3025604, August 28, 2017

77 Iyidogan E. An equilibrium model of blockchain-based cryptocurrencies [Online], available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3152803, April 11, 2018

78 Yang Dong, Chen Zhe-Li. Research on the positioning and characteristics of fiat digital currency. *Journal of the Renmin University of China*, 2020, **34**(3): 108–121
(杨东, 陈哲立. 法定数字货币的定位与性质研究. 中国人民大学学报, 2020, **34**(3): 108–121)

79 Yermack D. Is Bitcoin a real currency? An economic appraisal. *Handbook of Digital Currency*. San Diego, CA: Academic Press, 2015. 31–43

80 Glaser F, Zimmermann K, Haferkorn M, Weber M C, Siering M. Bitcoin-asset or currency? Revealing users' hidden intentions. In: Proceedings of the 22nd European Conference on Information Systems (ECIS 2014). Tel Aviv, Israel: The Association for Information Systems, 2014. 1-14

81 Ali R, Barrdear J, Clews R, Southgate J. The economics of digital currencies. *Bank of England Quarterly Bulletin*, 2014, **54**(3): 276–286

82 Hao Peng-Peng, Wang Yan-Bo. Analysis on the value source of non-legal digital currency based on the perspective of currency duality. *Tsinghua Financial Review*, 2018(4): 94–96
(郝鹏鹏, 王彦博. 基于货币二象性视角的非法定数字货币价值源泉探析. 清华金融评论, 2018(4): 94–96)

83 Ciaian P, Rajcaniova M, Kancs D. The digital agenda of virtual currencies: Can BitCoin become a global currency? *Information Systems and e-Business Management*, 2016, **14**(4): 883–919

84 Chen Hao. The Economic Analysis of Bitcoin [Master dissertation], Zhejiang University, China, 2015
(陈豪. 比特币的经济学分析 [硕士学位论文], 浙江大学, 中国, 2015)

85 Wu Jing. The Study on the Price Forming Mechanism of Virtual Currency Under the Background of the Internet Economy: Exemplify Bitcoin [Master dissertation], Ocean University of China, China, 2015
(吴静. 互联网经济背景下虚拟货币价格形成机制研究—以比特币为例 [硕士学位论文], 中国海洋大学, 中国, 2015)

86 Glaser F, Haferkorn M, Weber M C, Zimmermann K. How to price a digital currency? Empirical insights on the influence of media coverage on the Bitcoin bubble [Online], available: https://ssrn.com/abstract=2430653, April 29, 2014

87 Ciaian P, Rajcaniova M, Kancs D. The economics of BitCoin price formation. *Applied Economics*, 2016, **48**(19): 1799–1815

88 Chen Xiang-Guang, Huang Ze-Qing. The formation mechanism of currency anchors and the maintenance of currency quality: Collaterally study on the anchor of digital currency. *Journal of the Renmin University of China*, 2018, **32**(4): 86–94
(陈享光, 黄泽清. 货币锚定物的形成机制及其对货币品质的维护—兼论数字货币的锚. 中国人民大学学报, 2018, **32**(4): 86–94)

89 Willet J R. MasterCoin: New protocol layer starting from "the exodus address" [Online], available: http://bitcointalk.org/index.php?topic=265488.0, June 10, 2013

90 Lipton A, Hardjono T, Pentland A. Digital trade coin: Towards a more stable digital currency. *Royal Society Open Science*, 2018, **5**(7): 180155

91 Al-Naji N, Chen J, Diao L. Basis: A price-stable cryptocurrency with an algorithmic central bank [Online], available: http://www.basis.io/basis_whitepaper_en.pdf, June 20, 2017

92 Engert W, Fung B. Central bank digital currency: Motivations and implications [Online], available: https://ssrn.com/abstract=3081001, December 7, 2017

93 Wang Xiao-Dong. The distribution mechanism and institutional guarantee of digital money. *Special Zone Economy*, 2019(2): 80–82
(王晓东. 数字货币的发行机制及其制度保障. 特区经济, 2019(2): 80–82)

94 Yao Qian. Experimental study on prototype system of central bank digital currency. *Journal of Software*, 2018, **29**(9): 2716–2732
(姚前. 中央银行数字货币原型系统实验研究. 软件学报, 2018, **29**(9): 2716–2732)

95 Qiu Xun. The issue of China's central bank digital currency: Path, problems and Countermeasures. *Southwest Finance*, 2017(3): 14–20
(邱勋. 中国央行发行数字货币: 路径、问题及其应对策略. 西南金融, 2017(3): 14–20)

96 Li Li. Discussion and suggestions on the issue and circulation of digital currency in China. *Heilongjiang Finance*, 2017(5): 30–32
(李莉. 我国数字货币发行流通问题探讨及建议. 黑龙江金融, 2017(5): 30–32)

97 Li Bo, Li Jing-Yue. Research of fiat digital currency based on blockchain technology. *Heilongjiang Finance*, 2018(1): 57–59
(李博, 李景跃. 基于区块链技术的法定数字货币研究. 黑龙江金融, 2018(1): 57–59)

98 Zhang Xin-Jian. The influence of digital currency on payment system. *Modern Marketing*, 2018(12): 171
(张新建. 数字货币对支付体系影响的几点思考. 现代营销, 2018(12): 171)

99 Jing Zhong-Bo. Analysis on the mechanism, influence and issue obstacles of Libra. *Guizhou Social Sciences*, 2019(11): 116–126
(荆中博. 数字货币 Libra 的机制、影响与落地障碍探析. 贵州社会科学, 2019(11): 116–126)

100 Chen Bo-Wen, Zhu Yuan-Qian. Viewing the rebalancing of the global monetary system from the perspective of super-sovereign stable coins: Based on the perspective of Libra 2.0. *Journal of Financial Development Research*, 2020(6): 40–46
(陈博闻, 朱元倩. 从超主权稳定币看全球货币体系的再平衡—基于 Libra 2.0 的视角. 金融发展研究, 2020(6): 40–46)

101 Zhao Hong, Fu Jun-Wen. Analysis on the impact of Libra on the international monetary system: From the perspective of digital currency. *Forum of World Economic & Politics*, 2020(1): 114–127
(赵红, 付俊文. 浅析 Libra 对国际货币体系的可能冲击—基于数字货币视角. 世界经济与政治论坛, 2020(1): 114–127)

102 Wen Xin-Xiang, Zhang Bei. The influence of digital currency on monetary policy. *China Finance*, 2016(17): 24–26
(温信祥, 张蓓. 数字货币对货币政策的影响. 中国金融, 2016(17): 24–26)

103 Li Zhi-Wen, Zhuang Lei, Zhao Cheng-Guo. Research on the influence mechanism of digital currency on traditional monetary and financial system. *China Economist*, 2020(2): 120–122, 126
(李治文, 庄雷, 赵成国. 数字货币对传统货币金融体系的效应影响机制研究. 经济师, 2020(2): 120–122, 126)

104 Zhao Yue-Qiang. Development trend, contingent risks and regulatory considerations of digital currencies in the public and private sectors. *Economist*, 2020(8): 110–119

(赵越强. 公共和私有部门数字货币的发展趋势、或有风险与监管考量. 经济学家, 2020(8): 110−119)

105 Li Jian-Jun, Zhu Ye-Chen. Research progress of digital currency theory and practice. *Economic Perspectives*, 2017(10): 115−127
(李建军, 朱烨辰. 数字货币理论与实践研究进展. 经济学动态, 2017(10): 115−127)

106 Tian Hai-Bo, Lin Hui-Zhi, Luo Fei-Ran, Su Yin-Xue. Scheme for being able to regulate a digital currency with user privacy protection. *Journal of Xidian University*, 2020, **47**(5): 40−47
(田海博, 林会智, 罗裴然, 苏吟雪. 一种用户隐私保护数字货币的可监管方案. 西安电子科技大学学报, 2020, **47**(5): 40−47)

107 Zhang Qing-He. Research on Identification and Access Control in Blockchain [Master dissertation], Beijing Jiaotong University, China, 2018
(张青禾. 区块链中的身份识别和访问控制技术研究 [硕士学位论文], 北京交通大学, 中国, 2018)

108 Ateniese G, Faonio A, Magri B, De Medeiros B. Certified Bitcoins. In: Proceedings of the 2014 International Conference on Applied Cryptography and Network Security. Lausanne, Switzerland: Springer, 2014. 80−96

109 El Defrawy K, Lampkins J. Founding digital currency on secure computation. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, Arizona, USA: ACM, 2014. 1−14

110 Lin Qi-Ping. An Anonymous Digital Currency Transaction Supervision Method, CN Patent 109727031A, May 2019
(林齐平. 一种中心隐匿的匿名数字货币交易监管方法, CN 109727031A, 2019 年 5 月)

111 Wu Y B, Fan H N, Wang X Y, Zou G N. A regulated digital currency. *Science China Information Sciences*, 2019, **62**(3): 32109

112 Zhang Jian-Yi, Wang Zhi-Qiang, Xu Zhi-Li, Ouyang Ya-Fei, Yang Tao. A regulatable digital currency model based on blockchain. *Journal of Computer Research and Development*, 2018, **55**(10): 2219−2232
(张健毅, 王志强, 徐治理, 欧阳雅菲, 杨涛. 基于区块链的可监管数字货币模型. 计算机研究与发展, 2018, **55**(10): 2219−2232)

113 Xu Zhi-Li. A Study of Regulatory Digital Currency Model Based on Blockchain [Master dissertation], Xidian University, China, 2018
(徐治理. 基于区块链的可监管数字货币模型研究 [硕士学位论文], 西安电子科技大学, 中国, 2018)

114 Jiao Jin-Pu, Sun Tian-Qi, Huang Ting-Ting, Wang Tian-Du. Digital currency and fiancial services: Theoretical framework, international practice and regulation systems. *Financial Regulation Research*, 2015(7): 19−35
(焦瑾璞, 孙天琦, 黄亭亭, 汪天都. 数字货币与普惠金融发展—理论框架、国际实践与监管体系. 金融监管研究, 2015(7): 19−35)

115 Yang Yan-Chao. On the legal attributes of digital currency. *Social Sciences in China*, 2020(1): 84−106, 206
(杨延超. 论数字货币的法律属性. 中国社会科学, 2020(1): 84−106, 206)

116 Jia Heng-Yue, Wu Xia, Zhu Jian-Ming. Survey of quantum crypto currency. *Chinese Journal of Network and Information Security*, 2017, **3**(2): 5−12
(贾恒越, 武霞, 朱建明. 量子加密货币研究进展概述. 网络与信息安全学报, 2017, **3**(2): 5−12)

117 Wiesner S. Conjugate coding. *ACM SIGACT News*, 1983, **15**(1): 78−88

118 Wang Fei-Yue. Enterprise Money: A Digital Currency for Real-time Coordination and Incentivation in Management, Technical Report No.06-27-2016, Qingdao Academy of Intelligent Industries, China, 2016
(王飞跃. 企业币: 企业管理的一种实时协调与激励的数字货币机制, 技术报告 No.06-27-2016, 青岛智能产业技术研究院, 中国, 2016)

119 Wang Fei-Yue. Parallel Currency: An Economic Mechanism for Coordination and Integration of Real-virtual Interaction in Parallel Management, Technical Report No.11-02-2018, Alfred North Whitehead College, China, 2018
(王飞跃. 平行币: 平行管理中虚实一体化的一种经济机制, 技术报告 No.11-02-2018, 怀德海学院, 北京, 中国, 2018)

李娟娟 北京理工大学自动化学院博士, 中国科学院自动化研究所复杂系统管理与控制国家重点实验室助理研究员. 2010 年获中国人民大学经济学硕士学位. 主要研究方向为区块链, 计算经济学. 本文通信作者.
E-mail: juanjuan.li@ia.ac.cn
(**LI Juan-Juan** Ph. D. candidate at School of Automation, Beijing Institute of Technology, and assistant professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. She received her master degree in economics from Renmin University of China in 2010. Her research interest covers blockchain, and computational economics. Corresponding author of this paper.)

袁 勇 中国人民大学数学学院教授, 中国自动化学会区块链专委会主任. 2008 年获得山东科技大学计算机软件与理论专业博士学位. 主要研究方向为区块链, 计算经济学.
E-mail: yong.yuan@ruc.edu.cn
(**YUAN Yong** Professor at the School of Mathematics, Renmin University of China. He is also the director of Technical Committee on Blockchain, Chinese Association of Automation. He received his Ph. D. degree in computer software and theory from Shandong University of Science and Technology in 2008. His research interest covers blockchain, and computational economics.)

王飞跃 中国科学院自动化研究所复杂系统管理与控制国家重点实验室主任, 国防科技大学军事计算实验与平行系统技术研究中心主任, 中国科学院大学中国经济与社会安全研究中心主任, 青岛智能产业技术研究院院长. 主要研究方向为平行系统的方法与应用, 社会计算, 平行智能和知识自动化.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** Director of the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. Director of the Research Center for Computational Experiments and Parallel Systems Technology, National University of Defense Technology. Director of China Economic and Social Security Research Center in University of Chinese Academy of Sciences. Dean of Qingdao Academy of Intelligent Industries. His research interest covers methods and applications for parallel systems, social computing, parallel intelligence, and knowledge automation.)