·专题一:区块链技术及应用·

我国区块链发展趋势与思考

郑志明* 邱望洁

(北京航空航天大学,北京 100191)

[摘 要] 区块链是人类历史上首次构建的可信系统,其核心功能是提升各个纬度的治理能力。近日中央将区块链定位为核心技术自主创新的重要突破口以及推进国家治理能力现代化的有效工具。本文将概述国内外区块链技术的发展历史,分析我国区块链发展面临的核心风险以及应对策略,并对我国区块链技术的发展提出一些建议。

[关键词] 自主创新;可信系统;国家治理体系;分布式系统

1 区块链发展概述

区块链作为点对点网络、密码学、共识机制、智能合约等多种技术的集成系统,提供了一种在不可信网络中进行信息与价值传递交换的可信通道,凭借其独有的信任建立机制,与云计算、大数据、人工智能等新技术、新应用交叉创新,融合演进成为新一代网络基础设施,重构数字经济产业生态。2019 年 10 月 24 日,习近平总书记在中央政治局第十八次集体学习时强调“我们要把区块链作为核心技术自主创新的重要突破口,明确主攻方向,加大投入力度,着力攻克一批关键核心技术,加快推动区块链技术和产业创新发展。”区块链是人类历史上首次构建的可信系统,其核心功能是提升各个纬度的治理能力,这也是需要我们深刻理解和准确把握总书记在十九届四中全会之前组织中共中央政治局集体学习区块链的重大意义。

探寻区块链技术的起源,比特币是无法回避的话题。区块链作为一种底层技术,它的出现最早可以追溯到比特币系统中。2008 年一个笔名为中本聪的学者(或团队)发布了名为《比特币——一种点对点的电子现金系统》[1]的文章,比特币作为一种基于分布式可信系统建立的数字资产就此诞生。与大多数货币不同,比特币并非依靠特定机构发行,而是依据特定算法,通过大量的计算产生。比特币经济使用整个对等网络中众多节点构成的分布式数据库来确认并记录所有的交易行为,并使用密码学技术来确保数字资产流通过程中各个环节的安全性。2009 年“区块链本征技术—分布式可信系统”研讨会在北京召开,会议通过《软件可信性动力学特征及其演化复杂性》[2]一文揭示了分布式可信软件系统的动态复杂性,探讨了构建分布式可信系统的基本科学问题和建立系统可信性的度量理论等。

郑志明 北京航空航天大学教授,中国科学院院士,国家新一代人工智能群体智能专题组长,软件开发环境国家重点实验室主任和数学、信息与行为教育部重点实验室主任。在我国最早提出区块链分布式可信系统模型,提出了区块链三元优化平衡策略。曾获国家技术发明奖一等奖、何梁何利科技进步奖、教育部自然科学一等奖和国防技术发明一等奖等。

从 2008 年比特币问世至今,区块链的发展大体可以分为三个时期,其应用范畴已经从最初的数字货币或资产扩展至现今社会经济生活的方方面面。其中 1.0 阶段以比特币等数字资产为典型代表,2.0 阶段以智能合约的应用为典型特征,而 3.0 阶段以可编程社会为核心特征,当前正处于 2.0 高级阶段,区块链仍主要以小规模局部应用为主,真正的行业级和生态级落地还很少。等达到 3.0 阶段,区块链将成为社会治理工具,以基于规则的可信智能社会治理体系为典型特征,将实现社会治理模式从基于

收稿日期:2020-01-10;修回日期:2020-01-14

* 通信作者,Email:zzheng@pku.edu.cn

传统信息化技术辅助的阶段进入基于区块链秩序的法治阶段。

当前区块链技术现状是，国外以区块链基础技术平台或操作系统的研发为主，国内以区块链的应用开发为主。我国企业应用开发主要依赖国外开源社区的成果，尚未出现自主可控的区块链底层架构。根据中国信息通信研究院于 2018 年 10 月发布的《可信区块链标准测试情况通报》，有一半的测试厂商使用了 IBM 主导的超级账本（Hyperledger）区块链底层平台。同以往的信息技术不同，以规则治理为特征的区块链技术具有很强的扩张性。因此，推动我国区块链技术和产业健康发展的核心目标首先是亟需超前布局自主可控的底层平台和基础技术的自主创新。

2　区块链技术与理论解析

区块链技术本质上是一种分布式可信系统，下一代区块链核心技术研究包括共识算法优化平衡、安全与隐私保护、合约可信性、可扩展性和跨链技术等五个方向，分别对应分布式计算理论、密码学理论、软件可信性理论、异构系统交互理论和运筹和并行理论体系。只有从基础理论开始原始创新我国自主安全可控的区块链平台，我们才能掌握全球范围内区块链技术和标准的话语权，实现理论—技术—工程—平台—标准一体化的区块链分布式可信主权体系。

2.1　共识优化平衡

区块链共识机制的目标是使所有的诚实节点保存一致的区块链视图，同时满足两个性质：一是一致性，所有诚实节点保存的区块链的存量部分完全相同；二是有效性，由某诚实节点发布的增量信息终将被其他所有诚实节点记录在自己的区块链中。区块链上采用不同的共识机制，在满足一致性和有效性的同时会对系统整体性能产生不同影响。我们可以从以下 3 个维度来评价各共识机制的技术水平：（1）安全性，是否有能力抵御住来自于拥有一定资源和影响力的参与者的攻击；（2）可扩展性，即节点越多，整个系统处理事务的能力越大；（3）分布式程度，即节点的接入门槛和权利。共识机制存在三元悖论，即：在一个区块链系统中，可扩展性、分布式程度和安全性三者不可兼得，最多得其二。因此，如何在三元问题中找到平衡是设计下一代共识机制的关键。

2.2　安全与隐私保护

在公有链中，需要对交易数据、地址、身份等敏感信息进行保护，同时又能让记账节点验证交易的合法性；对于联盟链，在构建隐私保护方案的同时，需考虑可监管性/授权追踪。我们可以通过采用高效的零知识证明、承诺、证据不可区分等密码学原语与方案来实现交易身份及内容隐私保护；基于环签名、群签名等密码学方案的隐私保护机制、基于分级证书机制的隐私保护机制也是可选方案；也可通过采用高效的同态加密方案或安全多方计算方案来实现交易内容的隐私保护；还可采用混币机制实现简单的隐私保护[3]。

2.3　合约可信性

智能合约是区块链描述业务场景核心逻辑的预言，合约可信性已成为区块链技术发展和应用的重要趋势和必然选择，而合约可信性建模已成为构造可信区块链的先决条件和必要手段。为了探讨和阐明合约可信性的基本科学问题、建立合约可信性度量的理论基础，可以结合动力系统的基本思想探讨合约可信性及其演化规律，研究在各种内部和外部因素作用下合约可信性演化的动力学机制，并建立相应的动力学模型，从而可以认为智能合约系统的可信性是区块链在动态开放环境下其行为的统计特性。通过建模分析，可以说明合约可信属性的极限演化行为与动力系统特征的对应关系，从而诠释智能合约的动力学特征及其演化复杂性。另一方面，我们可以利用动力学统计分析方法给出合约可信性统计指标的不变测度评测方法和合约不可信的动力学判据[4]。

2.4　可扩展性

区块链（特别是公链）想要真正做到深度的应用和普及，关键要解决交易的吞吐率和交易速率问题，我们称之为“可扩展性”。可扩展性旨在分布式账本协议的基础上，对整体进行性能效率的提升、扩容或功能性上的扩充，主要包括分片扩展和分层扩展技术：（1）分片扩展。区块链网络由主链和分片链组成，分片链上交易处于自身的独立空间中，其核心思路是每个节点只需要处理片区内的交易，而不是全网交易；（2）分层扩展。状态通道是一种分层技术，其核心思想是：允许执行脱链交易，在一个状态通道内发生的事情仍然保持着非常高的安全性和最终性，如果出现任何问题，仍然可以选择回溯到主链上进行仲裁。

2.5　跨链技术

区块链是一类分布式总账。一条区块链就是一个独立的账本，两条不同的链如同两个账本没有关联，

因此本质上价值没有办法在账本间转移，但是对于具体的某个用户，用户在一条区块链上存储的价值，要求能够转移为另一条链上的价值，这就是跨链资产流通。跨链资产流通能让价值跨越链与链之间的障碍，进行直接的流通。跨链本质上和货币兑换是一样的，跨链并没有改变每条链上的价值总额，只是在不同的持有人之间进行了一个兑换而已。进一步地，跨链分布式事务是指，事务的多个步骤分散在不同的区块链上执行且要求保证事务的一致性。这是对跨链资产流通的一种扩展，将资产交换的行为扩展成任意行为。而跨链分布式事务使得跨链智能合约成为了可能，一个智能合约可以在多个不同的区块链上执行，或者全部执行完毕，或者全部退回执行前的状态。跨链智能合约将打破链之间的信息孤岛效应，大幅扩张区块链的应用场景。

3 区块链发展的风险与应对

目前，我国区块链技术发展现状是专利多论文代码少，没有自主安全可控底层平台，没有软硬件一体化平台，将直接导致区块链核心技术受制于人的技术风险、国外开源平台抢占金融市场的金融风险以及国外开源平台渗透我国实体和虚拟经济的经济风险。这里我们以 Libra 平台为例进行分析，同时给出相应的应对策略。

全球社交巨头 Facebook 的加密货币项目 Libra 于 2019 年 6 月 18 日发布白皮书。Libra 的使命是：一方面构建一种简单且无国界的数字货币，另一方面构建一套为数十亿人服务的金融基础设施。Libra 所构建的普惠金融体系可以总结为三大要素：(1) Libra 建立在安全、可扩展和可靠的区块链基础上，从技术层面上看，Libra 沿用了区块链发展至今较为成熟的现有技术；(2) Libra 不同于没有内在价值的比特币等数字货币，其内在价值依托于一揽子储备金融资产，具有低波动性的特点；(3) Libra 由独立的 Libra 协会治理，该协会的任务是区块链平台的运营、储备管理以及 Libra 金融生态系统的推广，目前 Libra 是一个多中心化的许可性网络平台，并且按照其发展规划未来将过渡为去中心化的非许可性网络平台。归根到底，Libra 的最终目标可以归结为“一条链，一种币和一个智能合约平台”，链作为基础操作系统，币作为支付手段，而智能合约平台用于构建生态应用。

目前，绝大部分业内人士将 Libra 解读为一个开放、即时和低成本的全球性货币体系。对于我国而言，Libra 因其成本低、时间短、效率高、覆盖面更广的特点，可能会挑战我国现行货币政策：(1) 在我国外汇管理的一个基础要求是强调外汇交易要有真实的交易背景，而 Libra 平台不能给出真实性判断；(2) 非法跨境资本流动可能增加；(3) Libra 锚定美元等主权货币，Libra 的推广将同时为美元附能，强化美元的统治地位；(4) 挤压人民币国际化的空间；(5) 可能会扩展美国长臂管辖的范围，Libra 具有 50%的美元储备，美元的长臂管辖将跟随 Libra 大幅扩展；(6) 挤占全球跨境小额汇款业务。

目前，大家对于 Libra 的担忧主要集中在对我国的货币政策的挑战，而我们还有一些更深层次的担忧。我们注意到 Libra 不但构建了一种数字货币，而且构建了一套智能合约平台，而一个图灵完备的智能合约平台意味着 Libra 平台能够像 windows 系统、安卓系统一样构建任意的应用，覆盖任何的行业及业务。现阶段互联网在我国发展较快，我国的信息化程度较高，几乎所有行业都离不开信息系统，如果这些行业的信息系统被 Libra 平台所替代，那么后果将不堪设想。因此，我们认为不能简单地将 Libra 解读为一种支付和清算结算工具，而应该看到 Libra 未来足以支持任何形式的跨国跨境、跨行业跨领域、多类型(B2B、B2C、C2C)的经济活动。我们要警惕的是，近乎所有的虚拟经济都有可能迁入 Libra 平台，同时实体经济的相当一部业务流程亦有可能借助于 Libra 平台部署业务系统。经济是我国发展的首要任务，Libra 平台可能抢占我国经济发展的信息化与支付业务，从而使我国的经济运行在一个不受监管和控制的平台之上。

如果说 Libra 是美国和美元意志的全球延伸，那么自主可控安全的区块链则是我国国家意志的全球延伸。互联网经历了信息互联、人人互联和万物互联几个阶段，互联网发展初期，美国推出因特网并使之成为了国际标准，以此掌握了互联网世界的话语权，至今全球均在因特网的标准体系之上发展新一代信息产业。现阶段全球正处于价值互联时代初期，区块链构建的是服务于实体经济和虚拟经济的价值互联网，在这一轮竞争中，我国应尽早推出自主可控安全的区块链，并以此作为主链，同时推出区块链国际和国内的技术标准、接口标准、应用标准等系列标准，体现国家意志和治理规则，通过技术标准和应用标准规范和约束国内区块链的开发和应用，通过接口标准实现主链与各应用平台之间的无缝连接，最终实现“以链融链、以链治链”目标。在推出主链的同时，我们也需要考虑推出服务于“一带一路”战略的国家之间的联盟链，国家联盟链旨在从技术角度得到“一带一路”沿线国家的信任，基于共商共

建共享的模式，从技术维度上实现人类命运共同体，实现国际权力观、共同利益观、可持续发展观和全球治理观的国家共识。

4　区块链与国家治理能力现代化

总书记强调“要推动区块链和实体经济深度融合”等七个“要”，为我国如何发展和应用区块链技术指明了方向，对区块链与各种实际应用场景深度融合作出了部署，我们可以将区块链的应用价值归结为促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系五项共性作用。从地方省市来讲，可以结合七个“要”和省市实际情况，以某一个生态或产业作为切入点，带动和促进其他领域生态应用的良性发展。

我们必须看到，中央之所以高度重视区块链技术，是因为看重了它在实体经济、民生领域以及国家治理方面的应用前景。这也为各级政府部门在结合“区块链”进行区域产业转型、民生服务提升、政府治理升级等方面规划了具体目标。各级政府部门应对照七个“要”，让市场的“无形之手”发挥决定性作用，更好地发挥政府“有形之手”作用，推动相关资源流向技术研发和实际应用，引导人才、资金、项目、数据等流向能够实际提升生产效率、加快新旧动能接续转换的领域，流向切实改善民生服务和公共服务水平、提高人民群众获得感的领域，流向真正促进智慧城市建设、推动政府数据共享的领域。

我们要努力利用区块链提升社会治理水平。区块链中的共识机制、智能合约，能够打造透明可信任、高效低成本的应用场景，构建实时互联、数据共享、联动协同的智能化机制，从而优化政务服务、城市管理、应急保障的流程，提升治理效能。例如，依托区块链建立跨地区、跨层级、跨部门的监管机制，有助于降低监管成本，打通不同行业、地域监管机构间的信息壁垒。当审计部门、税务部门与金融机构、会计机构之间通过区块链技术实现审计数据、报税数据、资金数据、账务数据的共享，数据造假、逃避监管等问题将得到有效解决。

5　我国区块链发展展望

总书记已经给我们指明了区块链技术在我国的发展方向。总书记提出要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展，而要实现两个发展，关键在于两点：

一是区块链技术核心技术突破。区块链技术是目前我国和欧美差距最小的技术，所以总书记特别强调在这个新兴领域我国要走在理论最前沿、占据创新制高点、取得产业新优势。要推动协同攻关，加快推进核心技术突破，为区块链应用发展提供安全可控的技术支撑。目前区块链技术大多数停留在概念炒作阶段，很多业务场景单纯为了区块链而区块链。目前为止我国还没有人能在全球范围内解决三元悖论等核心技术困境，因此我们必须回归基础理论和核心技术，通过长期潜心研究，才能取得重大突破。事实上，总书记对区块链技术理论技术和后续的应用发展提出了非常高的要求，做好区块链基础理论研究，着力攻克一批关键核心技术，真正把技术研发的担子挑起来，是当前区块链发展的关键。

二是提升国际话语权和规则制定权。从上文中我们可以看到，不同于以往的信息技术，区块链技术具有很强的扩张性，或者叫侵略性，它的规则或者话语权决定了它的影响范围，因为每一个上链开展业务的个体或机构必须服从区块链所定的规则，无论中外均是如此。举个例子，大家使用 windows 系统时必须要服从 windows 的规则，但是 windows 只是为用户规定了信息交互的规则，这对我们来说是可以接受的，而区块链则规定了产业治理规则，区块链的治理规则凭借其分布式特征，其影响力可迅速超越国界和地域限制。

为了实现上述两点，我们要加强人才队伍建设，建立完善人才培养体系，打造多种形式的高层次人才培养平台，培育一批领军人物和高水平创新团队。区块链作为架构性创新技术，对复合型人才需求巨大，要求从事者掌握涉及密码学、信息科学、基础数学等多种专业技术知识。发展区块链，必须加强学科深度交叉融合的人才队伍建设，从基础研究、应用研发、产业融合等方面前瞻和系统性地建立人才培育体系。

参　考　文　献

[1] Nakamoto S. Bitcoin：a peer-to-peer electronic cash system. Consulted，2008.

[2] 郑志明，马世龙，李未等. 软件可信性动力学特征及其演化复杂性. 中国科学 信息科学：中国科学，2009，39(9)：946—950.

[3] 姚前. 区块链研究进展综述. 中国信息安全，2018(3)：92—95.

[4] 郑志明，马世龙，李未等. 软件可信复杂性及其动力学统计分析方法. 中国科学 信息科学：中国科学，2009，39(10)：1050—1054.

Development Trend and Thinking of China's Blockchain

Zheng Zhiming Qiu Wangjie
(*Beihang University*, *Beijing* 100191)

Abstract Blockchain is a trusted system built for the first time in human history, and its core function is to improve the governance capabilities of various latitudes. Recently, the central government has positioned the blockchain as an important breakthrough in independent innovation of core technologies and an effective tool to promote the modernization of national governance capabilities. This article will outline the history of the development of blockchain technology at home and abroad, analyze the core risks faced by China's blockchain development and coping strategies, propose a method of blockchain as a tool for national and social governance, and will make some suggestions for the development of China's blockchain technology.

Keywords independent innovation; trusted system; national governance system; distributed systems

(责任编辑 齐昆鹏)

·资料信息·

我国学者揭示大脑皮层环路调控的新机制

在国家自然科学基金项目(批准号:31430038,31630029,31661143037)资助下,北京师范大学认知神经科学与学习国家重点实验室舒友生教授团队在皮层环路调控领域取得重要进展,揭示了谷氨酸非同步化释放(asynchronous release,AR)对皮层抑制性微环路的功能具有重要调控作用。研究成果以"Regulation of Recurrent Inhibition by Asynchronous Glutamate Release in Neocortex"(非同步化谷氨酸释放对皮层交互抑制的调控)为题,于 2019 年 12 月 2 日在 *Neuron*(《神经元》)上在线发表。论文链接:https://www.cell.com/neuron/pdf/S0896-6273(19)30933-X.pdf。

大脑皮层中数目众多的兴奋性神经元与抑制性中间神经元通过突触相互连接,构建成复杂的神经网络来执行感觉、运动、学习、决策等功能。其中,兴奋性神经元提供的兴奋和抑制性神经元所提供的抑制,共同维持神经网络的平衡。一旦平衡被打破,皮层环路功能受损,可引发各种神经/精神疾病,如焦虑、癫痫和精神分裂症等。因此,抑制性信号的发生时刻和强度,对神经网络中兴奋—抑制平衡的维持及皮层信号处理十分重要,然而该信号的调控机制尚不清楚。

舒友生课题组用双通道膜片钳电生理技术,对急性分离的皮层脑片上两个邻近的细胞进行同时记录。发现皮层锥体神经元(pyramid cell, PC)的输出突触中存在谷氨酸的 AR 模式,且该模式的强度具有靶向细胞种类特异性,即在 PC 靶向中间神经元 Martinotti 细胞(MC)的突触中 AR 最强。在 PC 高频发放动作电位时,突触后 MC 接受的大量谷氨酸 AR 导致细胞去极化和兴奋性提高,从而促进更多且更长时程的动作电位发放,并且降低其发放精确性,继而在邻近的 PC 上引起持久且不精确的抑制性反应。进一步实验发现,慢钙感受器突触结合蛋白 7(Syt7)的缺失降低 AR 强度,导致 MC 所介导的慢相交互抑制起始时间的推迟和强度的减弱。该研究首次揭示了 AR 释放模式对神经环路功能的重要调节作用,即调控皮层网络中慢相交互抑制的发生时刻及强度。这些发现对深入了解皮层网络中兴奋—抑制平衡的维持机制和皮层信息加工机制具有重要意义。

(供稿:生命科学部 张洪亮 冯雪莲)