平行区块链: 概念、方法与内涵解析

袁 勇 [1,2] 王飞跃 [1,3,4]

摘 要 本文提出了平行区块链的概念框架、基础理论和研究方法体系, 并探讨了平行区块链的内涵. 平行区块链技术是平行智能理论方法与区块链技术的有机结合, 致力于通过实际区块链系统与人工区块链系统的平行互动与协同演化, 为目前的区块链技术增加计算实验与平行决策功能, 实现描述、预测、引导相结合的区块链系统管理与决策. 平行区块链这一新型研究范式可望为下一步区块链研究和未来产业应用提供有益的启发与借鉴.

关键词 区块链, 平行区块链, 平行智能, 计算实验, 知识自动化

引用格式 袁勇, 王飞跃. 平行区块链: 概念、方法与内涵解析. 自动化学报, 2017, **43**(10): 1703−1712

DOI 10.16383/j.aas.2017.c170543

Parallel Blockchain: Concept, Methods and Issues

YUAN Yong[1,2] WANG Fei-Yue[1,3,4]

Abstract In this paper, we propose the conceptual framework, fundamental theory, research methodology and issues of parallel blockchains. As an organic combination of both parallel intelligence theory and blockchain technology, parallel blockchain is aimed to offer the key capabilities including computational experiments and parallel decision-making to blockchains via parallel interactions and co-evolution between real and artificial blockchain systems, thus realizing the effective blockchain management and decision-making with descriptive intelligence, predictive intelligence and prescriptive intelligence. Parallel blockchain can be considered as a novel research paradigm for blockchain, and is expected to offer helpful guidance and reference for future research efforts and industrial applications.

Key words Blockchain, parallel blockchain, parallel intelligence, computational experiment, knowledge automation

Citation Yuan Yong, Wang Fei-Yue. Parallel blockchain: concept, methods and issues. *Acta Automatica Sinica*, 2017, **43**(10): 1703−1712

区块链技术起源于 2008 年末的 "比特币", 一种由化名为 "中本聪" 的学者设计的新型数字加密货币, 是比特币的底层支撑技术[1]. 在比特币的诞生之初, 其关注范围仅局限于少数加密货币研究人员, 2013 年前后随着比特币价格飞涨曾经掀起过短暂的热潮, 引起众多专家学者的研究兴趣. 尽管其后比特币的关注度随着其价格下跌而逐渐回落, 但研究者发现比特币底层的区块链技术具有更为重要、甚至是颠覆性的应用价值. 2015 年起, 区块链技术逐渐走入公众视野, 成为近两年来金融科技和互联网经济领域的新研究热点.

区块链技术具有诸多其他技术不可比拟的优势: 首先, 区块链系统的根本特征是去中心化, 采用点对点 (Peer-to-Peer, P2P) 对等网络, 各节点地位对等且通过分布式共识机制实现相互间的协调与协作, 同时节点基于各自贡献获得经济激励, 这使得区块链系统具有很强的健壮性, 因而也被认为是构建未来去中心化社会的核心技术之一; 其次, 区块链系统通过数学算法形成节点之间的共识, 新数据必须获得全部或者大多数节点的验证方可写入由全体节点共同维护的区块链账本, 因而极难篡改和伪造; 这使得区块链成为依靠共识机制和密码学算法自动产生信任的系统, 可以实现信息流、资金流和物质流等要素的去中介化自由流通; 第三, 区块链系统采取建立在隐私保护基础上的、公开透明的数据读取方式, 区块链账本数据以零成本方式向全体节点公开查询, 从而可以降低节点的信任成本和系统不确定性. 这些显著优势在现代社会系统中有着重要且广泛的应用

收稿日期 2017-06-07 录用日期 2017-07-09
Manuscript received June 7, 2017; accepted July 9, 2017
国家自然科学基金 (71472174, 61533019, 71232006, 61233001), 青岛智能产业智库基金资助
Supported by National Natural Science Foundation of China (71472174, 61533019, 71232006, 61233001), Qingdao Think-tank Foundation on Intelligent Industries
本文责任编委 张俊
Recommended by Associate Editor ZHANG Jun
1. 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 2. 青岛智能产业技术研究院 青岛 266109 3. 国防科学技术大学军事计算实验与平行系统技术中心 长沙 410073 4. 中国科学院大学中国经济与社会安全研究中心 北京 101408
1. The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 2. Qingdao Academy of Intelligent Industries, Qingdao 266109 3. Research Center of Military Computational Experiments and Parallel Systems, National University of Defense Technology, Changsha 410073 4. Center of China Economic and Social Security, The University of Chinese Academy of Sciences, Beijing 101408

前景[2].

然而, 作为一项新兴技术, 区块链相关理论研究与产业实践仍然处于起步阶段, 诸如共识算法、网络结构、智能合约、激励机制等微观层面的核心技术要素尚处于探索、实验和持续优化的状态, 而宏观层面的区块链产业生态及其对社会经济的影响也迫切需要实验、分析、评估和必要的监管.

例如, 技术层面上, 共识机制的切换对于区块链系统通常具有重要影响. 由于缺乏实验和评估的有效手段, 目前主流区块链 (特别是公有链) 通常采用渐进式实验方式. 以太坊计划采用的 "PoW+PoS" (Proof of Work + Proof of Stake, 工作量证明 + 权益证明) 混合共识机制即是典型案例: 由于 PoW 共识直接切换为 PoS 共识可能为以太坊生态系统带来难以估量的潜在风险, 因而不得不采用相对安全的混合机制, 即 99% 的绝大多数交易区块采用传统的比特币挖矿式 PoW 共识, 而仅有 1% 的区块链采用仍处于实验阶段的 Casper 式 PoS 共识. 在此基础上, 根据实验效果决定后续的共识切换策略. 产业生态层面上, 区块链技术与生俱来的颠覆性潜质也为各行各业带来深刻变革, 迫切需要国家和行业的监管和调控. 例如, 基于区块链技术的 ICO (Initial Coin Offering, 首次代币发行) 通过公开发行区块链系统内置的加密货币来筹措资金, 近一两年来已对传统金融和资本市场形成强力冲击. 2014 年, 基于以太坊的区块链项目 The DAO 通过 ICO 在短时间内筹集到 1.5 亿美元, 成为网络众筹历史上的里程碑之一. 然而, ICO 技术的快速发展势必会影响国家经济和金融稳定, 因而涌现出面向 ICO 技术的实验和监管需求的各类 "沙盒" 机制.

从学术研究角度来说, 现有的区块链技术本质上仍然是一种新型的链式数据结构和分布式计算架构, 能够有效实现复杂社会、经济与金融系统的描述性建模和计算, 但是欠缺对于区块链系统在自身不同配置条件下和各类应用场景中的计算实验与预测解析能力, 同时也欠缺虚实结合、以虚拟引导现实、以人工引导实际的引导与决策能力. 这是导致目前区块链技术只能依靠真实系统的 "链上" 增量式试错实验、或者利用沙盒监管等 "摸着石头过河" 的经验性决策方法, 来实现区块链技术发展与产业生态优化的根本原因. 为解决这一问题, 当前迫切需要发展一套面向区块链的建模、实验与决策的新理论与新方法, 旨在为区块链技术和相关产业提供一套可计算、可实现和可比较的描述建模、预测解析与引导决策方法[3].

平行区块链是有效解决区块链建模、实验与决策相关问题的理论方法, 是平行智能这一本世纪初提出的原创性研究范式与新兴区块链技术的深度结合[4−5]. 目前, 平行智能理论已在国防安全[6−7]、平行交通[8]、平行经济[9−10]、平行控制[11]、平行视觉[12]、平行图像[13] 和平行数据[14] 等十余个典型应用领域有了显著的实践效益和初步的理论结果. 平行智能研究主要面向 "人在环路中"、兼具高度社会复杂性和工程复杂性的社会物理信息或人机物三元系统 (Cyber-physical-social systems, CPSS), 通过研究数据驱动的描述智能、实验驱动的预测智能, 以及互动反馈的引导智能, 为不定、多样和复杂问题提供灵捷、聚焦和收敛的解决方案[15]. 平行区块链的首次提出是在 2017 年 4 月美国丹佛大学召开的第一届区块链与知识自动化国际研讨会. 会上, 本文作者之一王飞跃教授作了 "Parallel Blockchain: Concept, Techniques and Applications" 主旨报告, 首次提出并解读了平行区块链的概念、技术及其在金融、交通、健康和农业等领域的初步应用实践[16].

具体说来, 平行区块链基于平行智能理论和 ACP 方法 (Artificial systems + Computational experiments + Parallel execution, 人工系统 + 计算实验 + 平行执行), 其基本思想是通过形式化地描述区块链生态系统核心要素 (例如计算节点、通信网络、共识算法、激励机制等) 的静态特征与动态行为来构建人工区块链系统, 利用计算实验对特定区块链应用场景进行试错实验与优化, 并通过人工区块链系统与实际区块链系统的虚实交互与闭环反馈实现决策寻优与平行调谐. 本质上, 平行区块链系统是以人工区块链系统作为 "计算实验室", 利用常态情况下人工区块链系统中 "以万变应不变" 的离线试错实验与理性慎思, 实现真实区块链系统在非常态情况下 "以不变应万变" 的实时管理与决策.

本文的主要目的是研究、发展和完善平行区块链的理论方法与关键技术体系. 该体系致力于通过充分利用互联网开源情报大数据和新兴的知识自动化手段[17−18], 结合人工智能前沿的 ACP 方法、平行学习和平行动态规划等计算模式[19−21], 以平行智能方法论为基础, 制造面向各类应用场景的、算法和智能合约驱动的 "平行区块链"; 进而基于特定网络结构、交互机制与共识协议实现各类 "平行区块链" 智能系统或平台; 最终实现大规模分布式节点的群集与涌现驱动的 "平行区块链" 智能生态系统, 建立理论、技术、应用和生态的完整链条, 实现区块链与平行智能深度耦合的区块链平行实验与决策模式, 为区块链技术在交通、农业、健康、教育和金融等社会经济领域的重大决策奠定新的理论与方法基础.

本文组织结构如下: 第 1 节阐述平行区块链的概念框架; 第 2 节探讨平行区块链的基础理论、关键问题、研究方法与平台架构; 第 3 节讨论和辨析平行

区块链在三个不同层次上的内涵及其异同之处; 第 4 节总结本文并提出未来的研究方向.

1　平行区块链的概念框架

一般说来, 区块链可以狭义地定义为一种按照时间顺序将数据区块以链条的方式组合成特定数据结构、并以密码学方式保证不可篡改和不可伪造的去中心化共享总账 (Decentralized shared ledger). 该账本可以安全地存储简单的、有先后关系的、能在系统内验证的数据. 相对应地, 广义的区块链则是由数据链路、通信网络、共识算法、激励机制、智能合约和应用场景等要素共同组成的新技术框架、以及由此衍生出的新兴产业和生态系统. 这种新技术框架能够利用加密链式区块结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用自动化脚本代码 (智能合约) 来编程和操作数据, 是一种全新的去中心化基础架构与分布式计算范式[22].

由此可见, 区块 "链" 本身仅仅是数据存取的客观载体和表现形式, 更为本质和复杂的是区块链背后由各节点、各要素深度耦合与相互反馈而构成的复杂生态系统. 因此, 平行区块链不是多条相互独立的区块链的简单叠加与互动, 而是以一种 "人机结合、虚实一体" 的方式、通过人工区块链系统与实际区块链系统的协同演化与平行反馈来实现区块链系统建模、预测与引导的新型研究框架.

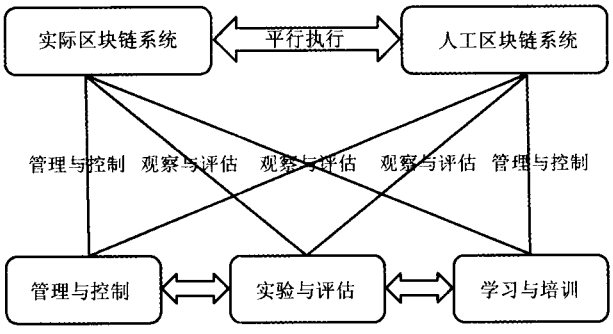

图 1　平行区块链的概念框架

Fig. 1　A conceptual framework of parallel blockchain

平行区块链的概念框架如图 1 所示, 其核心思想是基于 ACP 方法来实现区块链系统的建模、实验与决策, 即: 利用人工系统 (A) 方法建立与实际区块链系统相对应、能够反映实际系统的状态与演化规律的人工区块链系统; 利用计算实验 (C) 方法, 在人工系统中对实际区块链系统进行实验、分析和评估, 从而掌握实际区块链系统在各种可能场景下的演化规律; 利用平行执行 (P) 方法, 通过人工系统和实际系统的平行执行与协同演化, 实现对实际区块链系统的管理和控制.

具体说来, 平行区块链技术通过综合考虑物理、网络和社会三元空间的各种复杂因素, 采用理论建模、经验建模和数据建模有机结合的方法, 建立与实际区块链系统 "伴生" 的一个或多个人工区块链系统. 实际区块链系统中因缺乏有效的建模、实验和评估手段而引发的问题, 可以在人工区块链系统中构建相对应的实验场景, 通过对于区块链系统个体 (如矿工节点或交易节点) 特征与行为的准确建模, 以自底向上的涌现方式实施大量的计算实验, 模拟并 "实播" 区块链系统的各种状态与发展特性, 从而辅助推理和预测实际区块链系统各核心要素在常态和非常态情况下的演化规律与相互作用关系; 实际区块链系统在其整个生命周期内与人工区块链系统协同演化, 二者通过特定的平行交互机制与协议相互连接, 在数据、模型、场景和决策等要素的实时同步基础上, 通过人工系统中 "What-if" 形式的场景推演和实验探索, 实现对各自未来状态的 "预估" 及其相互 "借鉴", 并相应地调节各自的控制与管理方式.

平行区块链的核心优势在于其能够有效实现区块链系统的学习与培训、实验与评估、以及管理与控制.

1) 学习与培训: 新兴的区块链技术已经衍生出巨大的市场培育和技术培训需求. 一般来说, 学习者随着对区块链技术由浅入深的熟悉和掌握, 势必会经历由离线到在线、由链下到链上的演进过程; 而链上的在线操作一方面可能为真实区块链系统带来安全性风险, 另一方面也可能由于执行特定操作 (如执行链上代码) 产生实际成本; 平行区块链则可以安全、灵活和低成本方式实现场景化甚至游戏化的学习与培训过程; 平行区块链可在真实区块链系统的基础上, 根据特定学习目标来实例化一个或多个人工区块链系统, 通过人工与实际系统的适当连接组合, 使得学习者在人工系统中快速掌握区块链系统的各项操作及其可能的效果, 并量化考核学习与培训的实际效果.

2) 实验与评估: 真实区块链系统通常由于成本、安全和法律等原因而无法进行某些重要的破坏性实验和创新性实验, 平行区块链则可以计算实验的方式实施这些实验, 从而为量化评估区块链系统性能、实现区块链要素创新提供决策依据. 例如, 通过在一个模拟真实系统的人工区块链和多个不同配置的人工区块链中同时实施各类 "压力" 实验、"极限" 实验和 "攻击" 实验, 可以在测试评估真实区块链的安全性能的同时, 搜索能够有效抵御此类破坏性攻击的区块链优化配置; 此外, 平行区块链可有效支持类似 "Trading agent competition[23]" 模式的开源实验与创新, 其基本思路是根据特定需求定义合适的实验场景和目标, 构建相应的人工区块链系统环境、

固定某些区块链控制变量的同时向社会公众或科研人员开放若干实验变量 (例如共识机制、激励机制等), 通过竞赛或者众包等形式、汇集集体智慧实现特定实验变量的评估与优化, 从而推动区块链技术的创新和发展.

3) 管理与控制: 平行区块链可以作为政府机构和行业组织实施宏观监管与趋势预测的 "平行沙盒", 以虚实结合的方式实现区块链生态系统的管理与控制. 一方面, 区块链领域涌现出的新技术、新模式和新业态可首先在一个或多个尽可能逼近实际状态的人工区块链系统中实验、测评和完善, 达到特定监管目标和性能要求后方可应用于实际区块链系统, 从而以 "人工逼近实际" 的方式实现平行沙盒的 "孵化" 功能; 另一方面, 实际区块链系统中发现的新问题、新需求和新趋势也可以实时导入人工区块链系统, 通过人工系统中大量的计算实验和搜索寻优, 获得最优化的新解决方案, 并据此引导实际区块链系统的发展和演变, 从而以 "实际逼近人工" 的方式实现平行沙盒的 "创新" 功能.

2 平行区块链的研究框架

简言之, 区块链的核心特点是基于分布式共识和链式数据结构的多智能体系统. 一方面, 区块链共识是多智能体社会网络中的大规模群体协调与协作过程. 受经济激励等因素影响, 共识过程中存在着高度不确定性 (Uncertainty) 的心理与行为 (如自私挖矿、恶意粉尘攻击等)、高度多样化 (Diversity) 的共识机制与策略、以及高度复杂化 (Complexity) 的智能体竞争与合作博弈. 这是由 "人" 参与而为区块链带来的社会复杂性; 另一方面, 区块链的链式数据结构集成了多种特殊技术处理以实现安全可信和不可篡改等特性, 例如时间戳、Hash 运算、密码学算法和去中心化的 P2P 网络等. 这是区块链在技术层面上原生的工程复杂性. 由此可见, 区块链系统是典型的 "人在环路中"、兼具社会复杂性与工程复杂性的复杂系统.

不确定、多样化和复杂性特征 (UDC) 使得基于机理分析的传统理论与方法难以直接应用于区块链系统研究, 必须通过实验方法来解决. 然而, 由于 "人" 的心理、行为和策略性交互博弈等复杂因素的引入, 研究和优化区块链系统的本质困难是在很难甚至无法进行实验的情况下, 如何定量、实时地对区块链系统内部的行为、机制、策略、结构等要素进行建模、分析和评估. 本质上, 这就是应对 "建模不可建模者"、"预测不可预测者" 和 "决策不可决策者" 的矛盾. 平行智能是解决这一本质矛盾的有效理论和方法. 本节将详细阐述平行区块链的基础理论、研究问题、以及研究方法和平台体系.

2.1 基础理论

平行智能理论是复杂自适应系统理论和复杂性科学在新时代 CPSS 复杂环境下的逻辑延展和创新, 是实际与人工相结合、整体与还原相结合、定性与定量相结合的新型研究范式. 基于平行智能理论的平行区块链研究主要解决如下三个关键问题:

研究问题 1. 区块链复杂生态系统的整体建模与还原建模的有机集成与统一

复杂系统的整体建模与还原建模是既对立又统一的两种研究方法, 前者强调宏观系统层面的高层涌现与演变规律, 而后者则注重微观个体层面的特征刻画与行为交互. 平行区块链理论必须将二者有机结合. 一般说来, 区块链 (特别是公有链) 系统通常包含大量的个体参与者, 例如挖矿节点、交易节点、矿池等. 这些参与者通过区块链网络相互连接, 并遵循特定交互协议和共识算法共同维护和更新数据链条. 因而, 必须首先针对大量个体参与者节点进行微观层面的还原建模, 全面、精准地刻画参与者的静态特征、动态行为及其交互机制. 还原建模越精准、粒度越细, 则后续整体建模的复杂度越高, 但获得的高层涌现与演变规律更为准确可信. 因此, 区块链系统建模必须有机地集成两种研究方法, 兼顾还原建模粒度和整体建模复杂度、并寻求二者的最优均衡.

研究问题 2. "人在环路中" 的区块链计算实验与预测解析

受经济成本、技术条件和法律法规等因素的制约, 区块链领域的新思想和新技术很难直接应用于实际区块链系统, 这也是目前许多比特币改进提议 (Bitcoin improvement proposal, BIP) 仍然处于提出和草案状态、无法真正激活和落地的主要原因. 利用计算实验方法来测试其可行性、评估其效率和效果是解决该问题的有效途径, 其关键研究问题在于: 区块链系统并不是由可控制和可预测的简单工程技术构成的 "牛顿系统", 而是 "人在环路中"、人和社会因素深度影响系统行为规律、具有自我实施特征的 "默顿系统"[24−25]. 因此, 区块链实验不能局限于比特币测试网络这类以尽可能 "仿真" 为目的的实验场景与环境, 而是应该基于各类实际或虚拟的计算实验场景、利用自适应演化算法、平行学习等算法来驱动实验, 从而观察和量化评估各类参数配置、新技术方案和体系架构等在不同实验场景下的效果性能, 并预测其演变规律.

研究问题 3. 实际与人工区块链系统的双向引导与协同演化

平行区块链的主要目标并非是狭义地引导人工区块链系统逼近真实区块链系统, 而是更广义地使

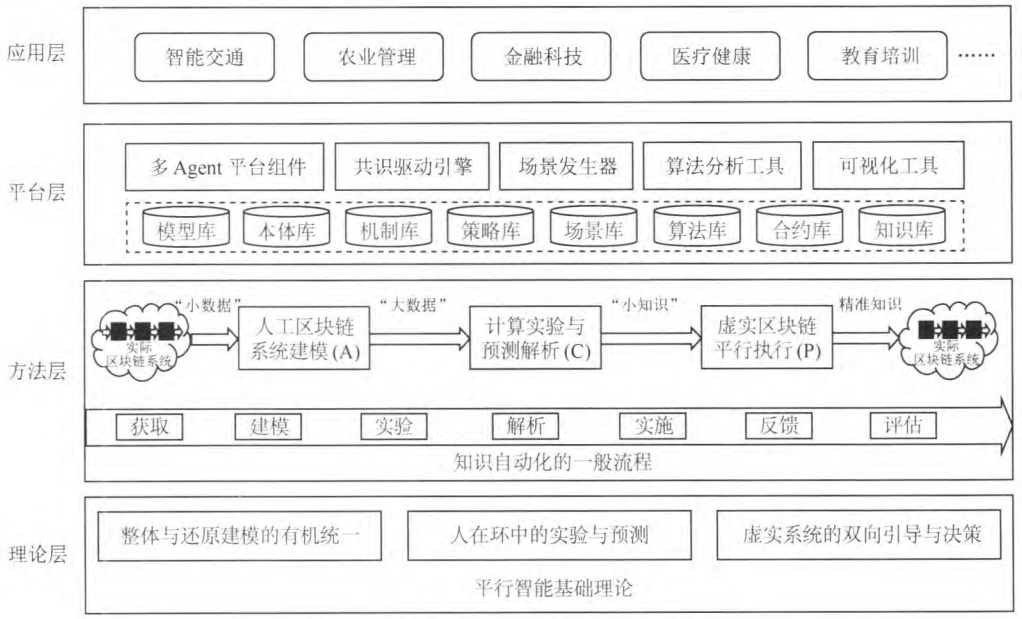

图 2　平行区块链的研究框架

Fig. 2　The research framework of parallel blockchain

得实际与人工区块链系统协同演化、闭环反馈和双向引导, 并以此来实现对实际区块链系统的优化, 促使整个平行区块链系统向设定或涌现的目标收敛. 在此过程中, 虚实区块链系统的交互协议与同步机制是值得深入研究的关键问题. 常态情况下, 人工区块链通过大量虚拟产生的计算实验场景来探索各类新的模型、场景、机制和策略等, 形成体系完备的 "情境 – 应对" 知识库; 非常态情况下 (例如 The DAO 硬分叉事件), 平行区块链应具备自适应切换到与当前情境最优匹配的应对方案的能力, 并通过数据、机制、策略和算法等要素在虚实区块链系统之间的实时同步, 逐步引导实际区块链逼近最优化的人工区块链状态.

这三个研究问题分别对应着平行智能基础理论中的数据驱动的描述智能、实验驱动的预测智能和互动反馈的引导智能. 平行区块链就是利用 "三位一体" 的平行智能理论, 通过实际系统与人工系统的 "链上" 平行互动与协同演化, 为目前以 "描述性" 为主的区块链技术增加预测解析与平行引导功能, 从而更好地服务于未来复杂社会经济系统的建模、实验与决策需求.

2.2　研究方法

区块链系统是典型的分布式多智能体系统. 因此, 平行区块链遵循复杂性科学中自下而上的研究方法, 通过 ACP 方法中基于人工系统的区块链建模、基于计算实验的预测解析和基于平行执行的引导决策, 来实现区块链系统的 "描述 + 预测 + 引导" 平行智能.

2.2.1　思路: ACP 驱动的区块链 BDI 形态演变

平行区块链研究范式中, 区块链系统可视为一个由大规模智能体节点通过社会网络连接组成的虚拟区块链 "智能体". 该智能体可由其 BDI (Belief, desire, intention, 信念、愿望和意图) 模型表述, 其中: 信念是区块链系统对当前世界状态的客观认知, 是系统内部产生的数据和外部环境状态参数的描述性记录; 愿望是区块链系统内部各节点对希望达到的状态的共识, 是区块链整体优化的目标; 意图则是区块链系统为实现愿望 (目标) 而从多个可能的规划和行动集合中选取的最优值, 是系统下一时间节点待实施的动作.

相对应地, 平行区块链系统中, 每一个实际区块链系统都会构建与之共生演化的三类人工形态的区块链系统, 即

1) "记录" 形态的区块链 (对应信念模型): 包括一个通过 "仿真" 手段构建的、与当前实际区块链系统保持一致的人工区块链, 以及一个或者多个根据历史出现过、或者未来可能产生的配置条件或实验参数而虚拟构建的人工区块链.

2) "实验" 形态的区块链 (对应意图模型): 针对常态或非常态情况下任意选定的一组实验场景, 选择与之适用的全部 "记录" 形态区块链, 使其在相同的参数配置和实验场景设置下以时钟同步的方式共同演化, 并实时评估每一个 "实验" 形态的区块链系统的性能指标 (如适应度、安全性、共识速度等).

3) "理想" 形态的区块链 (对应愿望模型): 即针对每种可能的优化目标 (如性能优先、安全优先或效

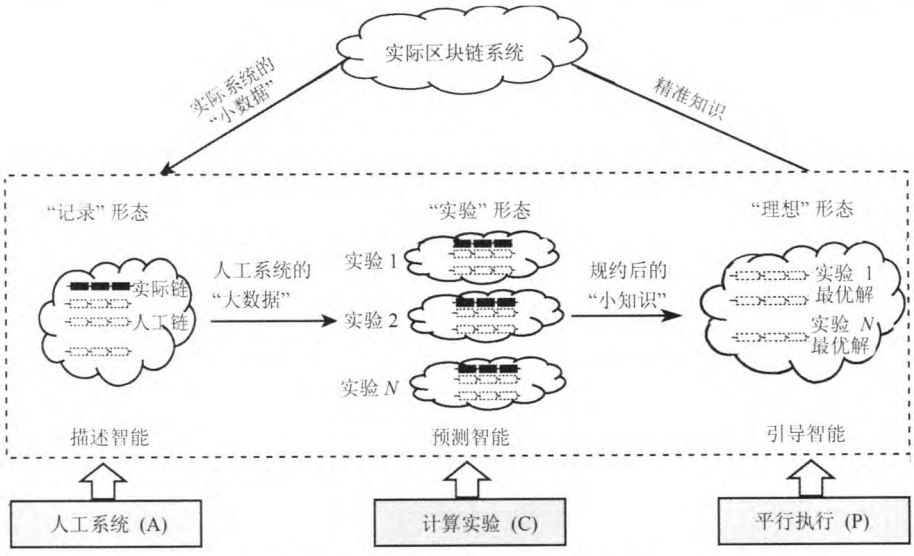

图 3 平行区块链的研究方法与思路

Fig. 3 Research method and issues of parallel blockchain

率优化等), 通过实验试错和搜索寻优后获得的一组最优配置的人工区块链.

作为上述三种形态区块链的混合智能系统, 平行区块链基于 ACP 方法来驱动区块链形态间的自演化, 并通过大量的计算实验场景推演、形成区块链的实际记录状态在虚拟实验场景中所能达到的最优化理想状态的知识库, 进而形成 "情境 – 应对" 规则库, 从而将非常态情况下应急响应规则的生成过程转化为常态情况下基于计算实验的理性慎思过程, 并形成引导实际区块链系统向最优化理想状态的人工区块链主动逼近的规划和行动.

2.2.2 方法: 基于平行学习的区块链知识自动化

如图 2 所示, 平行区块链采用基于 ACP 的平行学习方法实现区块链系统的知识自动化, 即实现面向区块链系统的开源数据获取、人工区块链系统建模、计算实验场景推演、实验解析与预测、管控决策优化与实施、虚实系统的平行反馈、实施效果的实时评估共七个步骤的闭环处理过程.

平行学习是近两年来新兴的机器学习理论框架, 该框架结合了现有多种机器学习理论框架的优点, 其新颖之处在于基于 ACP 方法衍生出的三大特色方法, 即利用软件定义的人工系统进行大数据预处理, 包含预测学习和集成学习的数据学习, 以及基于默顿定律实现数据 – 行动引导的指示学习[20]. 平行学习与传统机器学习方法的本质区别在于: 机器学习方法大多基于实际历史数据, 而平行学习则是基于实际 "小数据"+ 人工 "大数据" 的混合平行数据, 其中人工数据是在可能出现在未来场景中的虚拟数据[14]. 因此, 如果说传统机器学习是 "面向历史的机器学习" 方法, 那么平行学习就是 "面向未来的机器学习" 方法, 是虚实系统相互伴生、协同演化的终生学习方法.

近年来出现的人工智能围棋程序 AlphaGo 是平行学习方法最为成功的应用案例: AlphaGo 首先采集和分析人类棋手真实历史棋局的 "小数据", 然后通过 "左右互搏" 式的计算实验、生成大量的虚拟棋局来实现自博弈、自适应和自演化, 产生虚拟空间的围棋 "大数据"; 再通过算法规约为判断局势和确定落子的价值网络和策略网络等 "小知识", 并通过与人类棋手的不断对弈实现平行进化[26].

相对应地, 平行区块链系统首先基于开源情报与大数据解析方法[27]、实时地采集实际区块链系统产生的节点状态数据、链内交易数据和系统运行数据等. 这些实际系统的 "小数据" 可作为种子数据辅助建立实际区块链的模型, 并通过灵活改变区块链核心要素 (如共识机制、网络结构或数据结构等)、算法 (如难度调整算法、代币产量算法等) 和参数 (如手续费、节点数量等) 来扩展区块链模型, 进而通过实例化生成大量 "记录" 形态的、软件定义的人工区块链系统. 其次, 根据系统优化目标生成若干计算实验场景, 在每种实验场景中同步运行实际和人工区块链系统, 通过类似 AlphaGo 的算法驱动的自博弈、自适应和自演化过程, 生成更大规模的人工区块链 "大数据", 并与实际系统的 "小数据" 相结合, 形成区块链系统的平行数据. 此时, 即可采用传统的机器学习方法, 基于虚实结合的平行数据、学习和预测区块链系统的演变规律与趋势, 将 "大数据" 规约为应用于某些具体场景或任务、适合解决特定问题或实现特定优化目标的 "小知识". 最后, 将获得的小知识应用于实际区块链系统, 通过虚实系统的

平行闭环反馈和协同演化实现对这些知识实施效果的量化评估. 基于由此形成的 "小知识" 库, 当实际区块链系统出现特定场景或问题时, 即可快速查询知识库获得与之相匹配的精准知识并实施到实际系统中.

2.3 平台架构

平行区块链平台的基本要素如图 2 中的平台层所示, 由底层要素库和上层应用组件组成. 需要说明的是, 此处提出的是平行区块链平台的最简参考实现, 实际平台建设过程中可以根据需求灵活增加各类组件.

要素库包括模型库、本体库、机制库、策略库、场景库、算法库、合约库和知识库共八类, 其可通过各类要素的实例化和合理组装形成一个体系完备的平行区块链系统. 其中, 模型库存储区块链的各类显性模型, 例如智能体模型、区块链数据结构模型 (Merkle 树、Patricia 树等), 网络结构模型 (P2P 网络、MeshNet 网络等); 本体库存储潜在应用领域的领域本体 (如农业本体、金融本体等), 以增强平台内部各智能体交互的语义互操作性; 机制库存储智能体的交互协议和各类共识机制; 策略库存储智能体在挖矿、交易等过程中呈现出的典型策略和行为模式; 场景库存储平台预定义、可配置的实验场景与参数; 算法库存储区块链系统内生的算法 (例如难度调整算法) 和外部的算法 (如驱动实验进行的协同进化算法、深度学习算法等); 合约库存储区块链的各类智能合约; 知识库则存储系统优化后获得的管控决策和情境 – 应对规则.

值得一提的是, 平行区块链平台可以借鉴类似 Trading agent competition 的智能体平台, 通过设计特定的标准和规范来方便配置各类要素, 并将要素库向社会公众开放, 通过多智能体竞赛的方式吸引研究与工程人员设计和评测各类新颖的模型、机制、策略等要素, 从而借助集体智慧不断丰富和完善平台、同时促进区块链领域的创新和发展.

上层应用组件包括多智能体平台组件、场景发生器、共识驱动引擎、算法分析工具和大规模可视化工具等. 多智能体平台组件为平台用户提供区块链节点的建模能力、通讯协议和交互机制, 是自底向上建模方法中最重要的组件之一. 多智能体平台组件通常遵循 FIPA (Foundation for intelligent physical agents) 规范, 由智能体管理系统、目录服务器和智能体组件 (Agentware) 构成, 并可统一描述内部消息传输和内容语言的语法与语义[28]. 场景发生器能够从场景库中动态提取和配置真实或虚拟的计算实验场景, 并选择合适的机制、策略或算法等要素加以实例化、形成一个或多个人工区块链系统. 进而, 共识驱动引擎可在人工区块链系统的基础上完成区块链共识过程的计算实验, 并根据计算实验结果更新各个要素库; 共识驱动引擎可以基于多种算法加以实现, 例如离散事件仿真技术可通过推进仿真时钟和处理离散事件来动态模拟智能体 (即区块链节点) 之间及与外部环境的交互、通信与达成共识的过程. 算法分析工具则通过实时采集和分析区块链计算实验过程中产生的数据实现其优化目标, 促使区块链系统由 "实验" 形态演变为 "理想" 形态. 最后, 可视化工具通过动态实时的人机交互界面, 以多种形式全方位地呈现计算实验及区块链共识控制的过程.

2.4 应用领域

平行区块链特别适合 "人在环路中"、具有复杂社会和人的因素的应用场景, 例如智能交通、农业生产、金融科技、医疗健康和教育培训等领域. 2016 年, 中国科学院自动化研究所和青岛智能产业技术研究院提出了 "天链工程" 规划, 旨在利用区块链、大数据和知识自动化等技术, 助力打造去中心化、安全可信、可灵捷编程的智能产业生态系统, 并在智能交通、智慧农业、智慧健康和组织管理等领域进行了若干初步的探索性工作[29−31].

以智能交通领域为例, 平行区块链、平行交通管控系统和 "五交一体" (即城市交通、公共交通、静态交通、物流交通和社会交通) 示范应用共同组成了平行交通系统的核心模块, 其中平行区块链通过提供灵活可配置的底层区块链环境, 为上层平行交通管控决策和示范应用奠定了安全可信的数据和信任基础[29]. 目前, 平行交通区块链的探索性工作主要围绕着重要交通数据的存储与鉴证、去中介化的交通金融小生态、以及基于区块物联网 (Blockchain of things, BoT) 的交通设备监控与溯源等展开.

3 平行区块链的内涵辨析

正如第 2 节概念框架所示, 本文提出的平行区块链是一种新型的区块链系统研究范式, 其特点是通过实际区块链系统与人工区块链系统的平行执行和协同演化, 来为区块链系统提供描述、预测与引导决策服务. 需要说明的是, 目前国内外区块链技术和产业从业人员曾在不同上下文语境中使用过 "平行链" 或 "Parallel blockchain" 的概念, 但其内涵与本文提出的平行区块链有本质区别. 总体说来, 我们认为平行区块链的内涵可以归纳为跨链平行、O2O 平行和本文提出的虚实平行三种模式, 如图 4 所示. 本节将阐明其异同之处.

首先, 随着近年来区块链技术的发展和普及应用, 各类区块链 (特别是联盟链和私有链) 的数量快

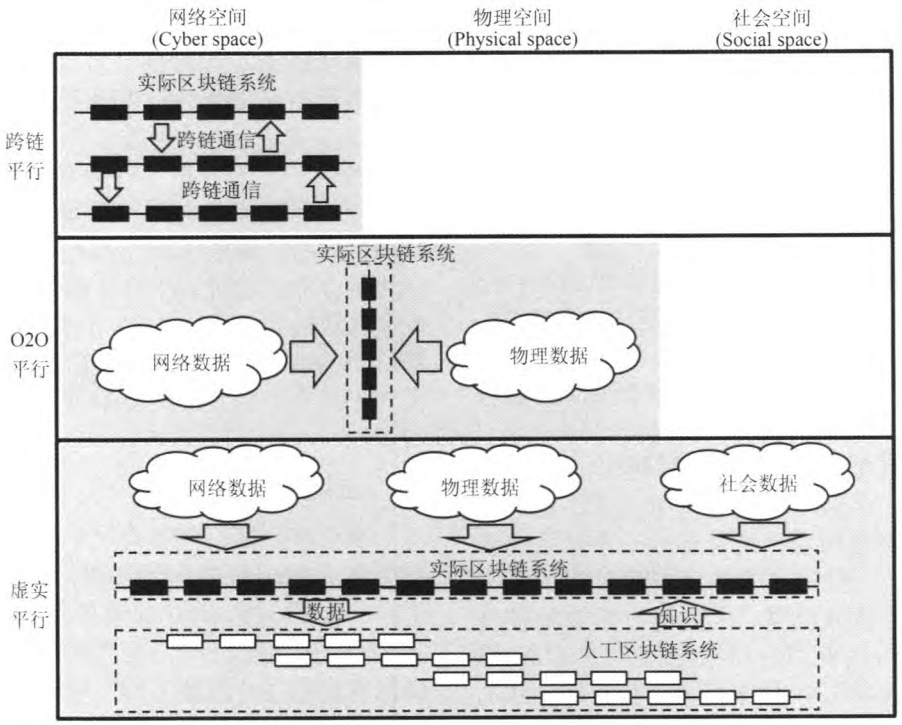

图 4 平行区块链的内涵辨析

Fig. 4 Connotation analysis of parallel blockchain

速增长, 跨链通信和互操作成为区块链未来发展的必然趋势. 因而, "跨链平行" 模式即是指这种形式上 "平行" 运行的多条实际区块链. 该模式的初衷是希望通过特定技术手段连接多条独立运行的区块链, 形成区块链群的 "绳网结构"、以增强区块链间的互操作性和链上资产的兼容互通性, 避免出现区块链 "数据孤岛". 目前提出的跨链互操作技术包括中心化或多重签名的见证人模式 (Centralized or multi-sig notary schemes)、侧链或中继模式 (Sidechains or relays)、哈希锁定模式 (Hash-locking)[32]. 例如, Polkadot 提出的平行链技术即是以中继模式实现公有链 (如以太坊) 与联盟链和私有链的连接[33]. "跨链平行" 是局限于网络空间的区块链平行模式. 值得一提的是, 研究人员亦曾提出以并行执行 (Parallel execution) 为目标的区块链技术[34], 旨在通过设计新区块链模型以便于并行处理区块链内部的交易、数据或者智能合约, 从而提高区块链的运行性能和效率. 此处, parallel 是 "并行" 而不是 "平行" 之意, 二者区别在于前者通过 "大而化小" 的分治法解决问题, 而后者则通过 "以小扩大" 的方式将一个实际系统扩展到虚拟空间的 N 个人工系统, 通过计算实验和平行演化解决问题. 由于这种 "链内并行" 的区块链仅是研究设想, 此处不再赘述.

其次, "O2O 平行" 模式是以实际区块链系统为桥梁, 沟通虚拟网络空间与现实物理空间、形成 O2O (Online to offline 或者 Offline to online, 线上线下连通) 平行社会的模式. 近年来, 现代社会、产业组织和企业形态已经越来越明显地呈现出虚拟网络空间和现实物理世界平行存在的态势, 例如研究人员提出的物理信息系统 (Cyber-physical systems, CPS)[35], 产业公司如西门子提出的数字化工厂、通用提出的数字孪生计划以及 SAP 提出的软件定义的企业等都是未来 O2O 平行趋势的例证. 区块链技术可以作为沟通虚拟和现实社会之间的安全可信、去中心化的分布式账本: 一方面, 线上的网络大数据可以自然地集成到区块链; 另一方面, 区块链技术也可以与物联网技术相结合, 形成目前快速发展的 Blockchain of things 技术, 从而将线下物理空间中的设备设施、实体资产等数字化后集成到区块链. 例如, 智能物联设备将是区块链的典型应用场景, 能够实现以安全可信的方式监控设备生产的整个生命周期、实现设备之间的数据传输和协商交易、以及利用智能合约实现设备的自动化操作等[36].

最后, "虚实平行" 模式的平行区块链与上述两种模式有本质区别, 是存在于物理与网络空间的区块链系统向第三社会空间延展而形成的 CPSS 平行系统[37−38]. 这种模式将分布式区块链系统中蕴含的社会与人的复杂因素纳入研究范畴, 利用实际和人工区块链系统的计算实验与平行优化, 赋予区块链技术以描述、预测和引导三位一体的平行智能. 与前两种模式相比, 平行区块链更多地是一种新型研究范式, 而非一项具体的技术或方法.

4 结论与展望

区块链技术作为信息科学、管理科学和社会科学交叉领域的新生事物, 其在高速发展的同时不可避免地会存在传统理论研究难以有效解决的问题. 目前, 国内外区块链相关研究尚处于起步阶段, 缺乏针对区块链架构、机制、策略等核心要素的深入研究, 导致区块链技术创新和发展缺乏必要的理论研究支撑. 鉴于此, 本文将平行智能理论与区块链技术相结合, 提出了平行区块链的概念框架、基础理论和研究方法体系, 并探讨了平行区块链的内涵, 以期为区块链未来研究和产业应用提供有益的启发与借鉴.

未来研究工作将围绕平行区块链的技术实现和平台建设开展. 技术实现方面, 除正文中介绍的构建与实际区块链平行独立运行的人工区块链方法之外, 我们还拟尝试采用有向无环图作为平行区块链的拓扑结构, 利用主链的硬分叉实现特定场景下的计算实验, 并利用进化算法在线评估各条分叉链的适应度, 引导区块链节点算力向最优链转移, 通过分叉链的 "优胜劣汰" 实现区块链优化. 平台建设方面, 我们拟选择典型区块链评测场景, 建设一组标准化的人工区块链系统, 通过设计接口向社会公众开放、作为 "平行沙箱" 实现各类区块链机制、策略或算法的评估与优化.

References

1 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [online], available: https://bitcoin.org/bitcoin.pdf, 2009.

2 Yuan Yong, Zhou Tao, Zhou Ao-Ying, Duan Yong-Chao, Wang Fei-Yue. Blockchain technology: from data intelligence to knowledge automation. *Acta Automatica Sinica*, 2017, **43**(9): 1485−1490
(袁勇, 周涛, 周傲英, 段永朝, 王飞跃. 区块链技术: 从数据智能到知识自动化. 自动化学报, 2017, **43**(9): 1485−1490)

3 Wang Fei-Yue. Parallel system methods for management and control of complex systems. *Control and Decision*, 2004, **19**(5): 485−489, 514
(王飞跃. 平行系统方法与复杂系统的管理和控制. 控制与决策, 2004, **19**(5): 485−489, 514)

4 Wang F Y, Wang X, Li L X, Li L. Steps toward parallel intelligence. *IEEE/CAA Journal of Automatica Sinica*, 2016, **3**(4): 345−348

5 Wang Fei-Yue. Computational experiments for behavior analysis and decision evaluation of complex systems. *Journal of System Simulation*, 2004, **16**(5): 893−897
(王飞跃. 计算实验方法与复杂系统行为分析和决策评估. 系统仿真学报, 2004, **16**(5): 893−897)

6 Wang Fei-Yue. CC 5.0: intelligent command and control systems in the parallel age. *Journal of Command and Control*, 2015, **1**(1): 107−120
(王飞跃. 指控 5.0: 平行时代的智能指挥与控制体系. 指挥与控制学报, 2015, **1**(1): 107−120)

7 Wang Zhen, Yuan Yong, An Bo, Li Ming-Chu, Wang Fei-Yue. An overview of security games. *Journal of Command and Control*, 2015, **1**(2): 121−149
(王震, 袁勇, 安波, 李明楚, 王飞跃. 安全博弈论研究综述. 指挥与控制学报, 2015, **1**(2): 121−149)

8 Wang F Y. Parallel control and management for intelligent transportation systems: concepts, architectures, and applications. *IEEE Transactions on Intelligent Transportation Systems*, 2010, **11**(3): 630−638

9 Wang Fei-Yue, Zeng Da-Jun, Yuan Yong. An ACP-based approach for complex analysis of E-commerce system. *Complex Systems and Complexity Science*, 2008, **5**(3): 1−8
(王飞跃, 曾大军, 袁勇. 基于 ACP 方法的电子商务系统复杂性研究. 复杂系统与复杂性科学, 2008, **5**(3): 1−8)

10 Yuan Y, Zeng D. Co-evolution-based mechanism design for sponsored search advertising. *Electronic Commerce Research and Applications*, 2012, **11**(6): 537−547

11 Wang Fei-Yue. Parallel control: a method for data-driven and computational control. *Acta Automatica Sinica*, 2013, **39**(4): 293−302
(王飞跃. 平行控制: 数据驱动的计算控制方法. 自动化学报, 2013, **39**(4): 293−302)

12 Wang Kun-Feng, Gou Chao, Wang Fei-Yue. Parallel vision: an ACP-based approach to intelligent vision computing. *Acta Automatica Sinica*, 2016, **42**(10): 1490−1500
(王坤峰, 苟超, 王飞跃. 平行视觉: 基于 ACP 的智能视觉计算方法. 自动化学报, 2016, **42**(10): 1490−1500)

13 Wang Kun-Feng, LU Yue, Wang Yu-Tong, Xiong Zi-Wei, Wang Fei-Yue. Parallel imaging: a new theoretical framework for image generation. *Pattern Recognition and Artificial Intelligence*, 2017, **30**(7): 577−587
(王坤峰, 鲁越, 王雨桐, 熊子威, 王飞跃. 平行图像: 图像生成的一个新型理论框架. 模式识别与人工智能, 2017, **30**(7): 577−587)

14 Liu Xin, Wang Xiao, Zhang Wei-Shan, Wang Jian-Ji, Wang Fei-Yue. Parallel data: from big data to data intelligence, *Pattern Recognition and Artificial Intelligence*, 2017, **30**(8): 673−681
(刘昕, 王晓, 张卫山, 汪建基, 王飞跃. 平行数据: 从大数据到数据智能. 模式识别与人工智能, 2017, **30**(8): 673−681)

15 Wang X, Li L X, Yuan Y, Ye P J, Wang F Y. ACP-based social computing and parallel intelligence: societies 5.0 and beyond. *CAAI Transactions on Intelligence Technology*, 2016, **1**(4): 377−393

16 Wang F Y. Parallel blockchain: concept, techniques and applications. Keynote Speech in the First International Symposium on Blockchain and Knowledge Automation, 2017, Denver, USA

17 Wang F Y. Toward a paradigm shift in social computing: the ACP approach. *IEEE Intelligent Systems*, 2007, **22**(5): 65−67

18 Wang Fei-Yue. The destiny: towards knowledge automation—preface of the special issue for the 50th anniversary of Acta Automatica Sinica. *Acta Automatica Sinica*, 2013, **39**(11): 1741−1743
(王飞跃. 天命唯新: 迈向知识自动化 —《自动化学报》创刊 50 周年专刊序. 自动化学报, 2013, **39**(11): 1741−1743)

19 Wen D, Yuan Y, Li X R. Artificial societies, computational experiments, and parallel systems: an investigation on a computational theory for complex socioeconomic systems. *IEEE Transactions on Services Computing*, 2013, **6**(2): 177−185

20 Li Li, Lin Yi-Lun, Cao Dong-Pu, Zheng Nan-Ning, Wang Fei-Yue. Parallel learning—a new framework for machine learning. *Acta Automatica Sinica*, 2017, **43**(1): 1−8
(李力, 林懿伦, 曹东璞, 郑南宁, 王飞跃. 平行学习 — 机器学习的一个新型理论框架. 自动化学报, 2017, **43**(1): 1−8)

21 Wang F Y, Zhang J, Wei Q L, Zheng X H, Li L. PDP: parallel dynamic programming, *IEEE/CAA Journal of Automatica Sinica*, 2017, **4**(1): 1−5

22 Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481−494)

23 Trading agent competition website [online], available: http://tac.sics.se, October 1, 2017

24 Wang Fei-Yue. Software-defined systems and knowledge automation: a parallel paradigm shift from Newton to Merton. *Acta Automatica Sinica*, 2015, **41**(1): 1−8
(王飞跃. 软件定义的系统与知识自动化: 从牛顿到默顿的平行升华. 自动化学报, 2015, **41**(1): 1−8)

25 Wang Fei-Yue, Wang Xiao, Yuan Yong, Wang Tao, Lin Yi-Lun. Social computing and computational societies: the foundation and consequence of smart societies. *Chinese Science Bulletin*, 2015, **60**(S1): 460−469
(王飞跃, 王晓, 袁勇, 王涛, 林懿伦. 社会计算与计算社会: 智慧社会的基础与必然. 科学通报, 2015, **60**(S1): 460−469)

26 Wang F Y, Zhang J J, Zheng X H, Wang X, Yuan Y, Dai X X, Zhang J, Yang L Q. Where does AlphaGo go: from church-Turing thesis to AlphaGo thesis and beyond. *IEEE/CAA Journal of Automatica Sinica*, 2016, **3**(2): 113−120

27 Zeng Shuai, Wang Shuai, Yuan Yong, Ni Xiao-Chun, Ouyang Yong-Ji. A survey on question answering systems towards knowledge automation. *Acta Automatica Sinica*, 2017, **43**(9): 1491−1508
(曾帅, 王帅, 袁勇, 倪晓春, 欧阳永基. 面向知识自动化的自动问答研究进展. 自动化学报, 2017, **43**(9): 1491−1508)

28 The foundation for intelligent physical agents website [online], available: http://www.fipa.org/, October 1, 2017

29 Yuan Y, Wang F Y. Towards blockchain-based intelligent transportation systems. In: Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). Rio de Janeiro, Brazil: IEEE, 2016. 2663−2668

30 Kang M Z, Wang F Y. From parallel plants to smart plants: intelligent control and management for plant growth. *IEEE/CAA Journal of Automatica Sinica*, 2017, **4**(2): 161−166

31 Ni X C, Zeng S, Qin R, Li J J, Yuan Y, Wang F Y. Behavioral profiling for employees using social media: a case study based on WeChat. In: Proceedings of 2017 Chinese Automation Congress (CAC 2017). Shandong, China, 2017.

32 Buterin V. Chain interoperability. Technical Report [online], available: https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf, September 9, 2016.

33 Wood G. Polkadot: vision for a heterogeneous multi-chain framework. Polkadot White Paper [online], available: https://github.com/w3f/ polkadot-white-paper/raw/ master/PolkaDotPaper.pdf, 2016.

34 Dillenberger D E, Su G. Parallel execution of blockchain transactions, U.S. Patent 0212781, July 2017.

35 Derler P, Lee E A, Vincentelli A S. Modeling cyber-physical systems. *Proceedings of the IEEE*, 2012, **100**(1): 13−28

36 Conoscenti M, Vetró A, De Martin Juan Carlos. Blockchain for the internet of things: a systematic literature review. In: Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). Agadir, Morocco: IEEE, 2016. 1−6

37 Wang Fei-Yue. Artificial societies, computational experiments, and parallel systems: a discussion on computational theory of complex social-economic systems. *Complex Systems and Complexity Science*, 2004, **1**(4): 25−35
(王飞跃. 人工社会、计算实验、平行系统 — 关于复杂社会经济系统计算研究的讨论. 复杂系统与复杂性科学, 2004, **1**(4): 25−35)

38 Wang F Y. The emergence of intelligent enterprises: from CPS to CPSS. *IEEE Intelligent Systems*, 2010, **25**(4): 85−88

袁 勇 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副研究员, 青岛智能产业技术研究院副院长. 2008 年获得山东科技大学计算机软件与理论专业博士学位. 主要研究方向为社会计算, 计算广告学与区块链.
E-mail: yong.yuan@ia.ac.cn
(**YUAN Yong** Associate professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He is also the vice president of Qingdao Academy of Intelligent Industries. He received his Ph. D. degree of computer software and theory from Shandong University of Science and Technology in 2008. His research interest covers social computing, computational advertising, and blockchain.)

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研究员, 国防科技大学军事计算实验与平行系统技术中心教授, 中国科学院大学中国经济与社会安全研究中心主任. 1990 年获美国伦塞利尔理工学院计算机与系统工程博士学位. 主要研究方向为智能系统和复杂系统的建模, 分析与控制.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** Professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He is also a professor at the Research Center of Military Computational Experiments and Parallel System, National University of Defense Technology; and also the director of the Center of China Economic and Social Security, The University of Chinese Academy of Sciences. He received his Ph. D. degree of computer and system engineering from Renselier Institute of Technology in 1990. His research interest covers modeling, analysis, and control of intelligent systems and complex systems.)