区块链技术发展现状与展望

袁 勇 [1, 2] 王飞跃 [1, 3]

摘 要 区块链是随着比特币等数字加密货币的日益普及而逐渐兴起的一种全新的去中心化基础架构与分布式计算范式, 目前已经引起政府部门、金融机构、科技企业和资本市场的高度重视与广泛关注. 区块链技术具有去中心化、时序数据、集体维护、可编程和安全可信等特点, 特别适合构建可编程的货币系统、金融系统乃至宏观社会系统. 本文通过解构区块链的核心要素, 提出了区块链系统的基础架构模型, 详细阐述了区块链及与之相关的比特币的基本原理、技术、方法与应用现状, 讨论了智能合约的理念、应用和意义, 介绍了基于区块链的平行社会发展趋势, 致力于为未来相关研究提供有益的指导与借鉴.

关键词 区块链, 比特币, 共识机制, 智能合约, 平行社会

引用格式 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

DOI 10.16383/j.aas.2016.c160158

Blockchain: The State of the Art and Future Trends

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

Abstract Blockchain is an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, and has recently attracted intensive attention from governments, financial institutions, high-tech enterprises, and the capital markets. Blockchain′s key advantages include decentralization, time-series data, collective maintenance, programmability and security, and thus is particularly suitable for constructing a programmable monetary system, financial system, and even the macroscopic societal system. In this paper, we proposed a basic model of the blockchain system, discussed the principles, technologies, methods and applications of blockchain and the related Bitcoin systems. We also discussed the smart contract and its applications, and presented the future trends of blockchain-enabled paralleled societies. This paper is aimed at providing helpful guidance and reference for future research efforts.

Key words Blockchain, Bitcoin, consensus mechanism, smart contract, paralleled society

Citation Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494

区块链是以比特币为代表的数字加密货币体系的核心支撑技术. 区块链技术的核心优势是去中心化, 能够通过运用数据加密、时间戳、分布式共识和经济激励等手段, 在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作, 从而为解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了解决方案. 随着比特币近年来的快速发展与普及, 区块链技术的研究与应用也呈现出爆发式增长态势, 被认为是继大型机、个人电脑、互联网、移动/社交网络之后计算范式的第五次颠覆式创新, 是人类信用进化史上继血亲信用、贵金属信用、央行纸币信用之后的第四个里程碑[1]. 区块链技术是下一代云计算的雏形, 有望像互联网一样彻底重塑人类社会活动形态, 并实现从目前的信息互联网向价值互联网的转变.

区块链技术的快速发展引起了政府部门、金融机构、科技企业和资本市场的广泛关注. 2016 年 1 月, 英国政府发布区块链专题研究报告[2], 积极推行区块链在金融和政府事务中的应用; 中国人民银行召开数字货币研讨会探讨采用区块链技术发行虚拟货币的可行性, 以提高金融活动的效率、便利性和透明度. 美国纳斯达克于 2015 年 12 月率先推出基于区块链技术的证券交易平台 Linq, 成为金融证券市场去中心化趋势的重要里程碑; 德勤和安永等专业审计服务公司相继组建区块链研发团队, 致力于提升其客户审计服务质量. 截止到 2016 年初, 资本市场已经相继投入 10 亿美元以 加速区块链 领域的 发

收稿日期 2016-02-22 录用日期 2016-03-02
Manuscript received February 22, 2016; accepted March 2, 2016
国家自然科学基金 (71472174, 71102117, 61533019, 71232006, 61233001) 资助
Supported by National Natural Science Foundation of China (71472174, 71102117, 61533019, 71232006, 61233001)
本文责任编委 林宗利
Recommended by Associate Editor LIN Zong-Li
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. 国防科技大学军事计算实验与平行系统技术中心 长沙 410073
1. The State Key Laboratory of Management and Control for 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 System, National University of Defense Technology, Changsha 410073

展. 初创公司 R3CEV 基于微软云服务平台 Azure 推出的 BaaS (Blockchain as a service, 区块链即服务) 服务, 已与美国银行、花旗银行等全球 40 余家大型银行机构签署区块链合作项目, 致力于制定银行业的区块链行业标准与协议.

区块链技术起源于 2008 年由化名为 “中本聪” (Satoshi nakamoto) 的学者在密码学邮件组发表的奠基性论文《比特币: 一种点对点电子现金系统》[3], 目前尚未形成行业公认的区块链定义. 狭义来讲, 区块链是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的不可篡改和不可伪造的去中心化共享总账 (Decentralized shared ledger), 能够安全存储简单的、有先后关系的、能在系统内验证的数据. 广义的区块链技术则是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) 来编程和操作数据的一种全新的去中心化基础架构与分布式计算范式.

区块链具有去中心化、时序数据、集体维护、可编程和安全可信等特点. 首先是去中心化: 区块链数据的验证、记账、存储、维护和传输等过程均是基于分布式系统结构, 采用纯数学方法而不是中心机构来建立分布式节点间的信任关系, 从而形成去中心化的可信任的分布式系统; 其次是时序数据: 区块链采用带有时间戳的链式区块结构存储数据, 从而为数据增加了时间维度, 具有极强的可验证性和可追溯性; 第三是集体维护: 区块链系统采用特定的经济激励机制来保证分布式系统中所有节点均可参与数据区块的验证过程 (如比特币的 “挖矿” 过程), 并通过共识算法来选择特定的节点将新区块添加到区块链; 第四是可编程: 区块链技术可提供灵活的脚本代码系统, 支持用户创建高级的智能合约、货币或其他去中心化应用. 例如, 以太坊 (Ethereum) 平台即提供了图灵完备的脚本语言以供用户来构建任何可以精确定义的智能合约或交易类型[4]; 最后是安全可信: 区块链技术采用非对称密码学原理对数据进行加密, 同时借助分布式系统各节点的工作量证明等共识算法形成的强大算力来抵御外部攻击、保证区块链数据不可篡改和不可伪造, 因而具有较高的安全性.

区块链技术是具有普适性的底层技术框架, 可以为金融、经济、科技甚至政治等各领域带来深刻变革. 按照目前区块链技术的发展脉络, 区块链技术将会经历以可编程数字加密货币体系为主要特征的区块链 1.0 模式、以可编程金融系统为主要特征的区块链 2.0 模式和以可编程社会为主要特征的区块链 3.0 模式[1]. 目前, 一般认为区块链技术正处于 2.0 模式的初期, 股权众筹和 P2P 借贷等各类基于区块链技术的互联网金融应用相继涌现. 然而, 上述模式实际上是平行而非演进式发展的, 区块链 1.0 模式的数字加密货币体系仍然远未成熟, 距离其全球货币一体化的愿景实际上更远、更困难. 目前, 区块链领域已经呈现出明显的技术和产业创新驱动的发展态势, 相关学术研究严重滞后、亟待跟进. 截止到 2016 年 2 月, 以万方数据知识服务平台为中文数据源、以 Web of Science 和 EI Village 为英文数据源的文献检索显示, 目前篇名包含关键词 “区块链/blockchain” 的仅有 2 篇中文[5−6] 和 9 篇英文文献[6−14]. 本文系统性地梳理了区块链的基本原理、核心技术、典型应用和现存问题, 以期为未来研究提供有益的启发与借鉴.

本文组织结构为: 第 1 节概述区块链与比特币的发展史及二者的关系; 第 2 节阐述区块链的基础架构模型及其关键技术; 第 3 节和第 4 节分别概要总结了区块链技术的应用场景与现存的问题; 第 5 节介绍智能合约及其在区块链领域的应用现状; 第 6 节展望了区块链驱动的平行社会发展趋势; 第 7 节总结本文内容.

1 比特币与区块链概述

比特币是迄今为止最为成功的区块链应用场景. 据区块链实时监控网站 Blockchain.info 统计显示, 平均每天有约 7 500 万美元的 120 000 笔交易被写入比特币区块链, 目前已生成超过 40 万个区块[15]. 加密货币市值统计网站 coinmarketcap.com 显示, 截止到 2016 年 2 月, 全球共有 675 种加密货币, 总市值超过 67 亿美元, 其中比特币市值约占 86 %, 瑞波币和以太币分别居二、三位[16]. 目前比特币供应量 (即已经挖出的比特币数量) 已经超过 1 500 万枚, 按照每枚比特币 389.50 美元的现行价格估算其总市值已超过 59 亿美元, 在世界各国 2015 年 GDP 排名中占据第 144 位 (略低于欧洲的摩尔多瓦). 换言之, 在没有政府和中央银行信用背书的情况下, 去中心化的比特币已经依靠算法信用创造出与欧洲小国体量相当的全球性经济体. 预计到 2027 年, 全球 10 % 的 GDP 将会通过区块链技术存储[17].

比特币区块链的第一个区块 (称为创世区块) 诞生于 2009 年 1 月 4 日, 由创始人中本聪持有. 一周后, 中本聪发送了 10 个比特币给密码学专家哈尔芬尼, 形成了比特币史上第一次交易; 2010 年 5 月, 佛罗里达程序员用 1 万比特币购买价值为 25 美元的披萨优惠券, 从而诞生了比特币的第一个公允汇率. 此后, 比特币价格快速上涨, 并在 2013 年 11 月创下每枚比特币兑换 1 242 美元的历史高值, 超过同期每盎司 1 241.98 美元的黄金价格. 据 CoinDesk 估算, 目前全球约有 6 万商家接受比特币交易, 其中中国

是比特币交易增长最为迅速的国家[18].

比特币本质上是由分布式网络系统生成的数字货币, 其发行过程不依赖特定的中心化机构, 而是依赖于分布式网络节点共同参与一种称为工作量证明 (Proof of work, PoW) 的共识过程以完成比特币交易的验证与记录. PoW 共识过程 (俗称挖矿, 每个节点称为矿工) 通常是各节点贡献自己的计算资源来竞争解决一个难度可动态调整的数学问题, 成功解决该数学问题的矿工将获得区块的记账权, 并将当前时间段的所有比特币交易打包记入一个新的区块、按照时间顺序链接到比特币主链上. 比特币系统同时会发行一定数量的比特币以奖励该矿工, 并激励其他矿工继续贡献算力. 比特币的流通过程依靠密码学方法保障安全. 每一次比特币交易都会经过特殊算法处理和全体矿工验证后记入区块链, 同时可以附带具有一定灵活性的脚本代码 (智能合约) 以实现可编程的自动化货币流通. 由此可见, 比特币和区块链系统一般具备如下五个关键要素, 即公共的区块链账本、分布式的点对点网络系统、去中心化的共识算法、适度的经济激励机制以及可编程的脚本代码.

区块链技术为比特币系统解决了数字加密货币领域长期以来所必需面对的两个重要问题, 即双重支付问题和拜占庭将军问题[19]. 双重支付问题又称为 “双花”, 即利用货币的数字特性两次或多次使用 “同一笔钱” 完成支付. 传统金融和货币体系中, 现金 (法币) 因是物理实体, 能够自然地避免双重支付; 其他数字形式的货币则需要可信的第三方中心机构 (如银行) 来保证. 区块链技术的贡献是在没有第三方机构的情况下, 通过分布式节点的验证和共识机制解决了去中心化系统的双重支付问题, 在信息传输的过程同时完成了价值转移. 拜占庭将军问题是分布式系统交互过程普遍面临的难题, 即在缺少可信任的中央节点的情况下, 分布式节点如何达成共识和建立互信[20]. 区块链通过数字加密技术和分布式共识算法, 实现了在无需信任单个节点的情况下构建一个去中心化的可信任系统. 与传统中心机构 (如中央银行) 的信用背书机制不同的是, 比特币区块链形成的是软件定义的信用, 这标志着中心化的国家信用向去中心化的算法信用的根本性变革.

比特币凭借其先发优势, 目前已经形成体系完备的涵盖发行、流通和金融衍生市场的生态圈与产业链 (如图 1 所示), 这也是其长期占据绝大多数数字加密货币市场份额的主要原因. 比特币的开源特性吸引了大量开发者持续性地贡献其创新技术、方法和机制; 比特币各网络节点 (矿工) 提供算力以保证比特币的稳定共识和安全性, 其算力大多来自于设备商销售的专门用于 PoW 共识算法的专业设备 (矿机). 比特币网络为每个新发现的区块发行一定数量的比特币以奖励矿工, 部分矿工可能会相互合作建立收益共享的矿池, 以便汇集算力来提高获得比特币的概率. 比特币经发行进入流通环节后, 持币人可以通过特定的软件平台 (如比特币钱包) 向商家支付比特币来购买商品或服务, 这体现了比特币的货币属性; 同时由于比特币价格的涨跌机制使其完全具备金融衍生品的所有属性, 因此出现了比特币交易平台以方便持币人投资或者投机比特币. 在流通环节和金融市场中, 每一笔比特币交易都会由比特币网络的全体矿工验证并记入区块链.

比特币是区块链技术赋能的第一个 “杀手级” 应用, 迄今为止区块链的核心技术和人才资源仍大多在比特币研发领域. 然而, 区块链作为未来新一代的底层基础技术, 其应用范畴势必会超越数字加密货币而延伸到金融、经济、科技和政治等其他领域.

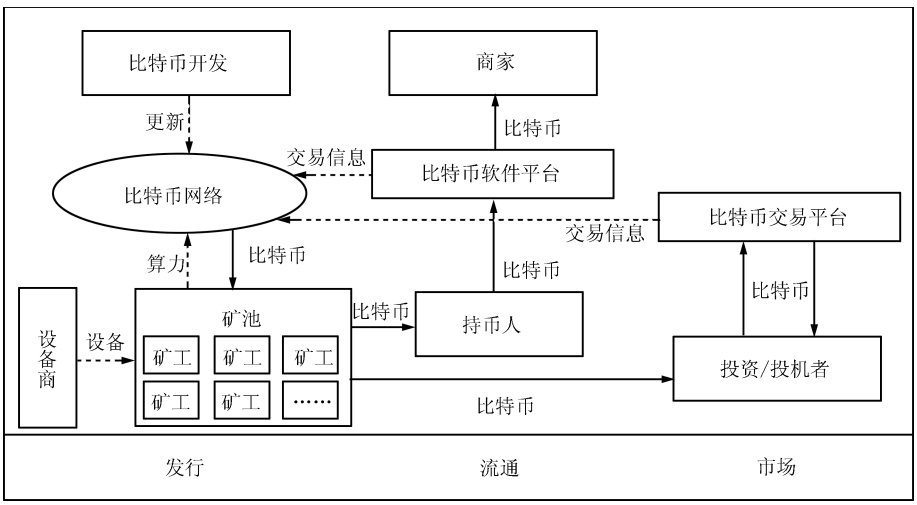


图 1　比特币生态圈

Fig. 1　The Bitcoin ecosystem

比特币的现有技术、模式和机制, 将会对区块链在新应用领域的发展提供有益的借鉴, 而新领域的区块链创新也势必反过来促进解决比特币系统现存的问题. 因此, 比特币和区块链技术存在着协同进化、和谐共生而非相互竞争的良性反馈关系.

2 区块链的基础模型与关键技术

本节将结合比特币系统的技术与应用现状, 阐述区块链技术的基础模型、基本原理和关键技术, 以及区块链在比特币系统之外的若干创新模式. 现存的其他区块链应用大多都与比特币类似, 仅在某些特定的环节或多或少地采用比特币模式的变种.

区块链技术的基础架构模型如图 2 所示. 一般说来, 区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成. 其中, 数据层封装了底层数据区块以及相关的数据加密和时间戳等技术; 网络层则包括分布式组网机制、数据传播机制和数据验证机制等; 共识层主要封装网络节点的各类共识算法; 激励层将经济因素集成到区块链技术体系中来, 主要包括经济激励的发行机制和分配机制等; 合约层主要封装各类脚本、算法和智能合约, 是区块链可编程特性的基础; 应用层则封装了区块链的各种应用场景和案例. 该模型中, 基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点.

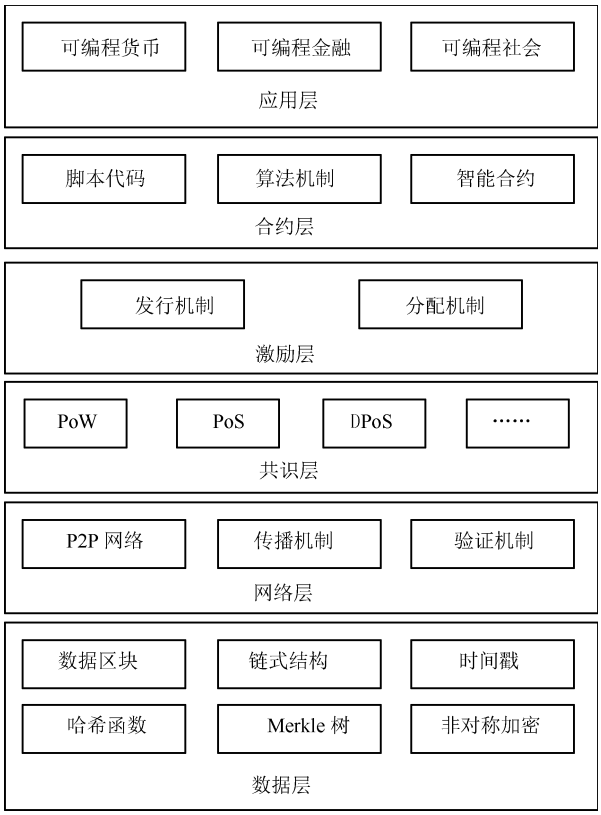


图 2 区块链基础架构模型

Fig. 2 A basic framework of blockchain

2.1 数据层

狭义的区块链即是去中心化系统各节点共享的数据账本. 每个分布式节点都可以通过特定的哈希算法和 Merkle 树数据结构, 将一段时间内接收到的交易数据和代码封装到一个带有时间戳的数据区块中, 并链接到当前最长的主区块链上, 形成最新的区块. 该过程涉及区块、链式结构、哈希算法、Merkle 树和时间戳等技术要素.

数据区块: 如图 3 所示, 每个数据区块一般包含区块头 (Header) 和区块体 (Body) 两部分. 区块头封装了当前版本号 (Version)、前一区块地址 (Prev-block)、当前区块的目标哈希值 (Bits)、当前区块 PoW 共识过程的解随机数 (Nonce)、Merkle 根 (Merkle-root) 以及时间戳 (Timestamp) 等信息[21]. 比特币网络可以动态调整 PoW 共识过程的难度值, 最先找到正确的解随机数 Nonce 并经过全体矿工验证的矿工将会获得当前区块的记账权. 区块体则包括当前区块的交易数量以及经过验证的、区块创建过程中生成的所有交易记录. 这些记录通过 Merkle 树的哈希过程生成唯一的 Merkle 根并记入区块头.

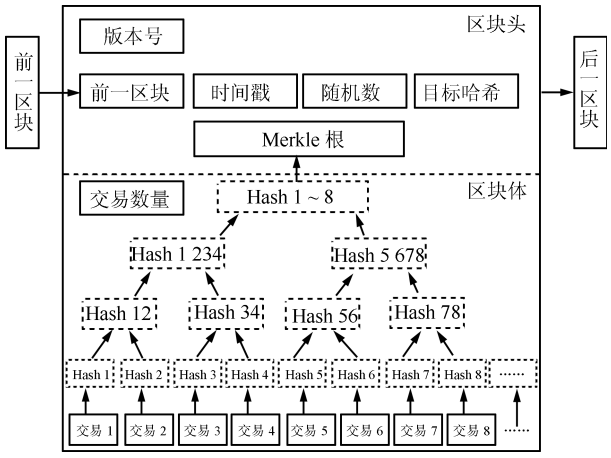


图 3 区块结构

Fig. 3 The structure of blocks

链式结构: 取得记账权的矿工将当前区块链接到前一区块, 形成最新的区块主链. 各个区块依次环环相接, 形成从创世区块到当前区块的一条最长主链, 从而记录了区块链数据的完整历史, 能够提供区块链数据的溯源和定位功能, 任意数据都可以通过此链式结构顺藤摸瓜、追本溯源. 需要说明的是, 如果短时间内有两个矿工同时 “挖出” 两个新的区块加以链接的话, 区块主链可能会出现暂时的 “分叉” 现象, 其解决方法是约定矿工总是选择延长累计工

作量证明最大的区块链. 因此, 当主链分叉后, 后续区块的矿工将通过计算和比较, 将其区块链接到当前累计工作量证明最大化的备选链上, 形成更长的新主链, 从而解决分叉问题[19].

时间戳: 区块链技术要求获得记账权的节点必须在当前数据区块头中加盖时间戳, 表明区块数据的写入时间. 因此, 主链上各区块是按照时间顺序依次排列的. 时间戳技术本身并不复杂, 但其在区块链技术中的应用是具有重要意义的创新. 时间戳可以作为区块数据的存在性证明 (Proof of existence), 有助于形成不可篡改和不可伪造的区块链数据库, 从而为区块链应用于公证、知识产权注册等时间敏感的领域奠定了基础. 更为重要的是, 时间戳为未来基于区块链的互联网和大数据增加了时间维度, 使得通过区块数据和时间戳来重现历史成为可能.

哈希函数: 区块链通常并不直接保存原始数据或交易记录, 而是保存其哈希函数值, 即将原始数据编码为特定长度的由数字和字母组成的字符串后记入区块链. 哈希函数 (也称散列函数) 具有诸多优良特点, 因而特别适合用于存储区块链数据. 例如, 通过哈希输出几乎不能反推输入值 (单向性), 不同长度输入的哈希过程消耗大约相同的时间 (定时性) 且产生固定长度的输出 (定长性), 即使输入仅相差一个字节也会产生显著不同的输出值 (随机性) 等. 比特币区块链通常采用双 SHA256 哈希函数, 即将任意长度的原始数据经过两次 SHA256 哈希运算后转换为长度为 256 位 (32 字节) 的二进制数字来统一存储和识别. 除上述特点外, SHA256 算法还具有巨大的散列空间 (2^{256}) 和抗碰撞 (避免不同输入值产生相同哈希值) 等特性, 可满足比特币的任何相关标记需要而不会出现冲突.

Merkle 树: Merkle 树是区块链的重要数据结构, 其作用是快速归纳和校验区块数据的存在性和完整性. 如图 3 所示, Merkle 树通常包含区块体的底层 (交易) 数据库, 区块头的根哈希值 (即 Merkle 根) 以及所有沿底层区块数据到根哈希的分支. Merkle 树运算过程一般是将区块体的数据进行分组哈希, 并将生成的新哈希值插入到 Merkle 树中, 如此递归直到只剩最后一个根哈希值并记为区块头的 Merkle 根. 最常见的 Merkle 树是比特币采用的二叉 Merkle 树, 其每个哈希节点总是包含两个相邻的数据块或其哈希值[22], 其他变种则包括以太坊的 Merkle patricia tree 等[4]. Merkle 树有诸多优点: 首先是极大地提高了区块链的运行效率和可扩展性, 使得区块头只需包含根哈希值而不必封装所有底层数据, 这使得哈希运算可以高效地运行在智能手机甚至物联网设备上; 其次是 Merkle 树可支持 "简化支付验证" 协议, 即在不运行完整区块链网络节点的情况下, 也能够对 (交易) 数据进行检验[3]. 例如, 为验证图 3 中交易 6, 一个没有下载完整区块链数据的客户端可以通过向其他节点索要包括从交易 6 哈希值沿 Merkle 树上溯至区块头根哈希处的哈希序列 (即哈希节点 6, 5, 56, 78, 5 678, 1 234) 来快速确认交易的存在性和正确性. 一般说来, 在 N 个交易组成的区块体中确认任一交易的算法复杂度仅为 $\log_2 N$. 这将极大地降低区块链运行所需的带宽和验证时间, 并使得仅保存部分相关区块链数据的轻量级客户端成为可能.

非对称加密: 非对称加密是为满足安全性需求和所有权验证需求而集成到区块链中的加密技术, 常见算法包括 RSA、Elgamal、Rabin、D-H、ECC (即椭圆曲线加密算法) 等. 非对称加密通常在加密和解密过程中使用两个非对称的密码, 分别称为公钥和私钥. 非对称密钥对具有两个特点, 首先是用其中一个密钥 (公钥或私钥) 加密信息后, 只有另一个对应的密钥才能解开; 其次是公钥可向其他人公开、私钥则保密, 其他人无法通过该公钥推算出相应的私钥. 非对称加密技术在区块链的应用场景主要包括信息加密、数字签名和登录认证等, 其中信息加密场景主要是由信息发送者 (记为 A) 使用接受者 (记为 B) 的公钥对信息加密后再发送给 B, B 利用自己的私钥对信息解密. 比特币交易的加密即属于此场景; 数字签名场景则是由发送者 A 采用自己的私钥加密信息后发送给 B, B 使用 A 的公钥对信息解密、从而可确保信息是由 A 发送的; 登录认证场景则是由客户端使用私钥加密登录信息后发送给服务器, 后者接收后采用该客户端的公钥解密并认证登录信息.

以比特币系统为例, 其非对称加密机制如图 4 所示: 比特币系统一般通过调用操作系统底层的随机数生成器来生成 256 位随机数作为私钥. 比特币私钥的总量可达 2^{256}, 极难通过遍历全部私钥空间来获得存有比特币的私钥, 因而是密码学安全的. 为便于识别, 256 位二进制形式的比特币私钥将通过 SHA256 哈希算法和 Base58 转换, 形成 50 个字符长度的易识别和书写的私钥提供给用户; 比特币的公钥是由私钥首先经过 Secp256k1 椭圆曲线算法生成 65 字节长度的随机数. 该公钥可用于产生比特币交易时使用的地址, 其生成过程为首先将公钥进行 SHA256 和 RIPEMD160 双哈希运算并生成 20 字节长度的摘要结果 (即 hash160 结果), 再经过 SHA256 哈希算法和 Base58 转换形成 33 字符长度的比特币地址[19]. 公钥生成过程是不可逆的, 即不能通过公钥反推出私钥. 比特币的公钥和私钥通常

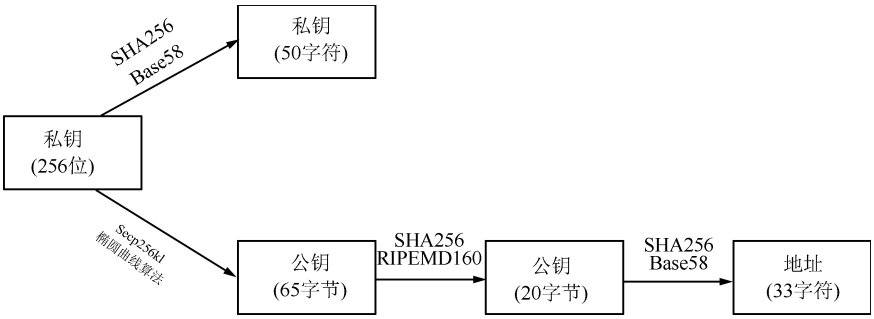


图 4 比特币非对称加密机制

Fig. 4 The asymmetric cryptography of the Bitcoin system

保存于比特币钱包文件, 其中私钥最为重要. 丢失私钥就意味着丢失了对应地址的全部比特币资产. 现有的比特币和区块链系统中, 根据实际应用需求已经衍生出多私钥加密技术, 以满足多重签名等更为灵活和复杂的场景.

2.2 网络层

网络层封装了区块链系统的组网方式、消息传播协议和数据验证机制等要素. 结合实际应用需求, 通过设计特定的传播协议和数据验证机制, 可使得区块链系统中每一个节点都能参与区块数据的校验和记账过程, 仅当区块数据通过全网大部分节点验证后, 才能记入区块链.

组网方式: 区块链系统的节点一般具有分布式、自治性、开放可自由进出等特性, 因而一般采用对等式网络 (Peer-to-peer network, P2P 网络) 来组织散布全球的参与数据验证和记账的节点. P2P 网络中的每个节点均地位对等且以扁平式拓扑结构相互连通和交互, 不存在任何中心化的特殊节点和层级结构, 每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点等功能. 按照节点存储数据量的不同, 可以分为全节点和轻量级节点. 前者保存有从创世区块到当前最新区块为止的完整区块链数据, 并通过实时参与区块数据的校验和记账来动态更新主链. 全节点的优势在于不依赖任何其他节点而能够独立地实现任意区块数据的校验、查询和更新, 劣势则是维护全节点的空间成本较高; 以比特币为例, 截止到 2016 年 2 月, 创世区块至当前区块的数据量已经超过 60 GB. 与之相比, 轻量级节点则仅保存一部分区块链数据, 并通过第 2.1 节提到的简易支付验证方式向其相邻节点请求所需的数据来完成数据校验.

数据传播协议: 任一区块数据生成后, 将由生成该数据的节点广播到全网其他所有的节点来加以验证. 现有的区块链系统一般根据实际应用需求设计比特币传播协议的变种, 例如以太坊区块链集成了所谓的 “幽灵协议” 以解决因区块数据确认速度快而导致的高区块作废率和随之而来的安全性风险[4]. 根据中本聪的设计, 比特币系统的交易数据传播协议包括如下步骤[3]:

1) 比特币交易节点将新生成的交易数据向全网所有节点进行广播;

2) 每个节点都将收集到的交易数据存储到一个区块中;

3) 每个节点基于自身算力在区块中找到一个具有足够难度的工作量证明;

4) 当节点找到区块的工作量证明后, 就向全网所有节点广播此区块;

5) 仅当包含在区块中的所有交易都是有效的且之前未存在过的, 其他节点才认同该区块的有效性;

6) 其他节点接受该数据区块, 并在该区块的末尾制造新的区块以延长该链条, 而将被接受区块的随机哈希值视为先于新区块的随机哈希值.

需要说明的是, 如果交易节点是与其他节点无连接的新节点, 比特币系统通常会将一组长期稳定运行的 “种子节点” 推荐给新节点建立连接, 或者推荐至少一个节点连接到新节点. 此外, 交易数据广播时, 并不需要全部节点均接收到, 而是只要足够多的节点做出响应即可整合进入区块账本中. 未接收到特定交易数据的节点则可向邻近节点请求下载该缺失的交易数据[19].

数据验证机制: P2P 网络中的每个节点都时刻监听比特币网络中广播的数据与新区块. 节点接收到邻近节点发来的数据后, 将首先验证该数据的有效性. 如果数据有效, 则按照接收顺序为新数据建立存储池以暂存尚未记入区块的有效数据, 同时继续向邻近节点转发; 如果数据无效, 则立即废弃该数据, 从而保证无效数据不会在区块链网络继续传播. 以比特币为例, 比特币的矿工节点会收集和验证 P2P 网络中广播的尚未确认的交易数据, 并对照预定义的标准清单, 从数据结构、语法规范性、输入输出和数字签名等各方面校验交易数据的有效性, 并将有效交易数据整合到当前区块中; 同理, 当某矿工

“挖” 到新区块后, 其他矿工节点也会按照预定义标准来校验该区块是否包含足够工作量证明, 时间戳是否有效等; 如确认有效, 其他矿工节点会将该区块链接到主区块链上, 并开始竞争下一个新区块.

由网络层设计机理可见, 区块链是典型的分布式大数据技术. 全网数据同时存储于去中心化系统的所有节点上, 即使部分节点失效, 只要仍存在一个正常运行的节点, 区块链主链数据就可完全恢复而不会影响后续区块数据的记录与更新. 这种高度分散化的区块存储模式与云存储模式的区别在于, 后者是基于中心化结构基础上的多重存储和多重数据备份模式, 即 “多中心化” 模式; 而前者则是完全 “去中心化” 的存储模式, 具有更高的数据安全性.

2.3 共识层

如何在分布式系统中高效地达成共识是分布式计算领域的重要研究问题. 正如社会系统中 “民主” 和 “集中” 的对立关系相似, 决策权越分散的系统达成共识的效率越低、但系统稳定性和满意度越高; 而决策权越集中的系统更易达成共识, 但同时更易出现专制和独裁. 区块链技术的核心优势之一就是能够在决策权高度分散的去中心化系统中使得各节点高效地针对区块数据的有效性达成共识.

早期的比特币区块链采用高度依赖节点算力的工作量证明 (Proof of work, PoW) 机制来保证比特币网络分布式记账的一致性. 随着区块链技术的发展和各种竞争币的相继涌现, 研究者提出多种不依赖算力而能够达成共识的机制, 例如点点币首创的权益证明 (Proof of stake, PoS) 共识[23] 和比特股首创的授权股份证明机制 (Delegated proof of stake, DPOS) 共识机制[24] 等. 区块链共识层即封装了这些共识机制.

PoW 共识: 中本聪在其比特币奠基性论文中设计了 PoW 共识机制, 其核心思想是通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性. 比特币系统中, 各节点 (即矿工) 基于各自的计算机算力相互竞争来共同解决一个求解复杂但验证容易的 SHA256 数学难题 (即挖矿), 最快解决该难题的节点将获得区块记账权和系统自动生成的比特币奖励. 该数学难题可表述为: 根据当前难度值, 通过搜索求解一个合适的随机数 (Nonce) 使得图 3 中区块头各元数据的双 SHA256 哈希值小于或等于目标哈希值. 比特币系统通过灵活调整随机数搜索的难度值来控制区块的平均生成时间为 10 分钟左右. 一般说来, PoW 共识的随机数搜索过程如下 (参照图 3 区块结构)[19]:

步骤 1. 搜集当前时间段的全网未确认交易, 并增加一个用于发行新比特币奖励的 Coinbase 交易, 形成当前区块体的交易集合;

步骤 2. 计算区块体交易集合的 Merkle 根记入区块头, 并填写区块头的其他元数据, 其中随机数 Nonce 置零;

步骤 3. 随机数 Nonce 加 1; 计算当前区块头的双 SHA256 哈希值, 如果小于或等于目标哈希值, 则成功搜索到合适的随机数并获得该区块的记账权; 否则继续步骤 3 直到任一节点搜索到合适的随机数为止;

步骤 4. 如果一定时间内未成功, 则更新时间戳和未确认交易集合、重新计算 Merkle 根后继续搜索.

符合要求的区块头哈希值通常由多个前导零构成, 目标哈希值越小, 区块头哈希值的前导零越多, 成功找到合适的随机数并 “挖” 出新区块的难度越大. 据区块链实时监测网站 Blockchain.info 显示, 截止到 2016 年 2 月, 符合要求的区块头哈希值一般有 17 个前导零, 例如第 398 346 号区块哈希值为 “000000000000000077f754f22f21629a7975cf $\cdots$”. 按照概率计算, 每 16 次随机数搜索将会有找到一个含有一个前导零的区块哈希值, 因而比特币目前 17 位前导零哈希值要求 16^{17} 次随机数搜索才能找到一个合适的随机数并生成一个新的区块. 由此可见, 比特币区块链系统的安全性和不可篡改性是由 PoW 共识机制的强大算力所保证的, 任何对于区块数据的攻击或篡改都必须重新计算该区块以及其后所有区块的 SHA256 难题, 并且计算速度必须使得伪造链长度超过主链, 这种攻击难度导致的成本将远超其收益. 据估计, 截止到 2016 年 1 月, 比特币区块链的算力已经达到 800 000 000 Gh/s, 即每秒进行 8×10^{18} 次运算, 超过全球 Top500 超级计算机的算力总和.

PoW 共识机制是具有重要意义的创新, 其近乎完美地整合了比特币系统的货币发行、交易支付和验证等功能, 并通过算力竞争保障系统的安全性和去中心性; PoW 共识机制同时存在着显著的缺陷, 其强大算力造成的资源浪费 (如电力) 历来为研究者所诟病, 而且长达 10 分钟的交易确认时间使其相对不适合小额交易的商业应用.

PoS 共识机制: PoS 共识是为解决 PoW 共识机制的资源浪费和安全性缺陷而提出的替代方案. 限于篇幅, 本文主要聚焦于 PoS 相对于 PoW 的创新之处. PoS 共识本质上是采用权益证明来代替 PoW 中的基于哈希算力的工作量证明, 是由系统中具有最高权益而非最高算力的节点获得区块记账权. 权益体现为节点对特定数量货币的所有权, 称为币龄或币天数 (Coin days). 币龄是特定数量的币与其最后一次交易的时间长度的乘积, 每次交易都将会消

耗掉特定数量的币龄. 例如, 某人在一笔交易中收到 10 个币后并持有 10 天, 则获得 100 币龄; 而后其花掉 5 个币后, 则消耗掉 50 币龄. 显然, 采用 PoS 共识机制的系统在特定时间点上的币龄总数是有限的, 长期持币者更倾向于拥有更多币龄, 因此币龄可视为其在 PoS 系统中的权益. 此外, PoW 共识过程中各节点挖矿难度相同, 而 PoS 共识过程中的难度与交易输入的币龄成反比, 消耗币龄越多则挖矿难度越低. 节点判断主链的标准也由 PoW 共识的最高累计难度转变为最高消耗币龄, 每个区块的交易都会将其消耗的币龄提交给该区块, 累计消耗币龄最高的区块将被链接到主链. 由此可见, PoS 共识过程仅依靠内部币龄和权益而不需要消耗外部算力和资源, 从根本上解决了 PoW 共识算力浪费的问题, 并且能够在一定程度上缩短达成共识的时间, 因而比特币之后的许多竞争币均采用 PoS 共识机制.

DPoS 共识机制: DPoS 共识机制的基本思路类似于 "董事会决策", 即系统中每个股东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 101 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且签署 (即生产) 一个新区块. 每个区块被签署之前, 必须先验证前一个区块已经被受信任的代表节点所签署. "董事会" 的授权代表节点可以从每笔交易的手续费中获得收入, 同时要成为授权代表节点必须缴纳一定量的保证金, 其金额相当于生产一个区块收入的 100 倍. 授权代表节点必须对其他股东节点负责, 如果其错过签署相对应的区块, 则股东将会收回选票从而将该节点 "投出" 董事会. 因此, 授权代表节点通常必须保证 99 % 以上的在线时间以实现盈利目标[24]. 显然, 与 PoW 共识机制必须信任最高算力节点和 PoS 共识机制必须信任最高权益节点不同的是, DPoS 共识机制中每个节点都能够自主决定其信任的授权节点且由这些节点轮流记账生成新区块, 因而大幅减少了参与验证和记账的节点数量, 可以实现快速共识验证.

除上述三种主流共识机制外, 实际区块链应用中也衍生出了 PoW+PoS、行动证明 (Proof of activity) 等多个变种机制. 这些共识机制各有优劣势, 比特币的 PoW 共识机制依靠其先发优势已经形成成熟的挖矿产业链, 支持者众多, 而 PoS 和 DPoS 等新兴机制则更为安全、环保和高效, 从而使得共识机制的选择问题成为区块链系统研究者最不易达成共识的问题.

2.4 激励层

区块链共识过程通过汇聚大规模共识节点的算力资源来实现共享区块链账本的数据验证和记账工作, 因而其本质上是一种共识节点间的任务众包过程. 去中心化系统中的共识节点本身是自利的, 最大化自身收益是其参与数据验证和记账的根本目标. 因此, 必须设计激励相容的合理众包机制, 使得共识节点最大化自身收益的个体理性行为与保障去中心化区块链系统的安全和有效性的整体目标相吻合. 区块链系统通过设计适度的经济激励机制并与共识过程相集成, 从而汇聚大规模的节点参与并形成了对区块链历史的稳定共识.

以比特币为例, 比特币 PoW 共识中的经济激励由新发行比特币奖励和交易流通过程中的手续费两部分组成, 奖励给 PoW 共识过程中成功搜索到该区块的随机数并记录该区块的节点. 因此, 只有当各节点通过合作共同构建共享和可信的区块链历史记录、并维护比特币系统的有效性, 其获得的比特币奖励和交易手续费才会有价值. 比特币已经形成成熟的挖矿生态圈, 大量配备专业矿机设备的矿工积极参与基于挖矿的 PoW 共识过程, 其根本目的就是通过获取比特币奖励并转换为相应法币来实现盈利.

发行机制: 比特币系统中每个区块发行比特币的数量是随着时间阶梯性递减的. 创世区块起的每个区块将发行 50 个比特币奖励给该区块的记账者, 此后每隔约 4 年 (21 万个区块) 每区块发行比特币的数量降低一半, 依此类推, 一直到比特币的数量稳定在上限 2 100 万为止[19]. 比特币交易过程中会产生手续费, 目前默认手续费是万分之一个比特币, 这部分费用也会记入区块并奖励给记账者. 这两部分费用将会封装在每个区块的第一个交易 (称为 Coinbase 交易) 中. 虽然现在每个区块的总手续费相对于新发行比特币来说规模很小 (通常不会超过 1 个比特币), 但随着未来比特币发行数量的逐步减少甚至停止发行, 手续费将逐渐成为驱动节点共识和记账的主要动力. 同时, 手续费还可以防止大量微额交易对比特币网络发起的 "粉尘" 攻击, 起到保障安全的作用.

分配机制: 比特币系统中, 大量的小算力节点通常会选择加入矿池, 通过相互合作汇集算力来提高 "挖" 到新区块的概率, 并共享该区块的比特币和手续费奖励. 据 Bitcoinmining.com 统计, 目前已经存在 13 种不同的分配机制[25]. 主流矿池通常采用 PPLNS (Pay per last N shares)、PPS (Pay per share) 和 PROP (PROPortionately) 等机制. 矿池将各节点贡献的算力按比例划分成不同的股份 (Share), 其中 PPLNS 机制是指发现区块后, 各合作节点根据其在最后 N 个股份内贡献的实际股份比例来分配区块中的比特币; PPS 则直接根据股份比例为各节点估算和支付一个固定的理论收益, 采用此方式的矿池将会适度收取手续费来弥补其为各

节点承担的收益不确定性风险; PROP 机制则根据节点贡献的股份按比例地分配比特币. 矿池的出现是对比特币和区块链去中心化趋势的潜在威胁, 如何设计合理的分配机制引导各节点合理地合作、避免出现因算力过度集中而导致的安全性问题是亟待解决的研究问题.

2.5 合约层

合约层封装区块链系统的各类脚本代码、算法以及由此生成的更为复杂的智能合约. 如果说数据、网络和共识三个层次作为区块链底层 "虚拟机" 分别承担数据表示、数据传播和数据验证功能的话, 合约层则是建立在区块链虚拟机之上的商业逻辑和算法, 是实现区块链系统灵活编程和操作数据的基础. 包括比特币在内的数字加密货币大多采用非图灵完备的简单脚本代码来编程控制交易过程, 这也是智能合约的雏形; 随着技术的发展, 目前已经出现以太坊等图灵完备的可实现更为复杂和灵活的智能合约的脚本语言, 使得区块链能够支持宏观金融和社会系统的诸多应用. 本节将以比特币脚本为例, 从技术角度简述合约层的基本技术和方法; 关于智能合约的延伸内容将在第 5 节讨论.

比特币采用一种简单的、基于堆栈的、从左向右处理的脚本语言, 而一个脚本本质上是附着在比特币交易上的一组指令的列表. 比特币交易依赖于两类脚本来加以验证, 即锁定脚本和解锁脚本, 二者的不同组合可在比特币交易中衍生出无限数量的控制条件. 其中, 锁定脚本是附着在交易输出值上的 "障碍", 规定以后花费这笔交易输出的条件; 解锁脚本则是满足被锁定脚本在一个输出上设定的花费条件的脚本, 同时它将允许输出被消费. 举例来说, 大多数比特币交易均是采用接受者的公钥加密和私钥解密, 因而其对应的 P2PKH (Pay to public key hash) 标准交易脚本中的锁定脚本即是使用接受者的公钥实现阻止输出功能, 而使用私钥对应的数字签名来加以解锁[19].

比特币脚本系统可以实现灵活的交易控制. 例如, 通过规定某个时间段 (如一周) 作为解锁条件, 可以实现延时支付; 通过规定接受者和担保人必须共同私钥签名才能支配一笔比特币, 可以实现担保交易; 通过设计一种可根据外部信息源核查某概率事件是否发生的规则并作为解锁脚本附着在一定数量的比特币交易上, 即可实现博彩和预测市场等类型的应用; 通过设定 N 个私钥集合中至少提供 M 个私钥才可解锁, 可实现 $M-N$ 型多重签名, 即 N 个潜在接受者中至少有 M 个同意签名才可实现支付. 多重签名可广泛应用于公司决策、财务监督、中介担保甚至遗产分配等场景.

比特币脚本是智能合约的雏形, 催生了人类历史上第一种可编程的全球性货币. 然而, 比特币脚本系统是非图灵完备的, 其中不存在复杂循环和流控制, 这在损失一定灵活性的同时能够极大地降低复杂性和不确定性, 并能够避免因无限循环等逻辑炸弹而造成拒绝服务等类型的安全性攻击. 为提高脚本系统的灵活性和可扩展性, 研究者已经尝试在比特币协议之上叠加新的协议, 以满足在区块链上构建更为复杂的智能合约的需求. 以太坊已经研发出一套图灵完备的脚本语言, 用户可基于以太坊构建任意复杂和精确定义的智能合约与去中心化应用, 从而为基于区块链构建可编程的金融与社会系统奠定了基础[4].

3 区块链的应用场景

由区块链独特的技术设计可见, 区块链系统具有分布式高冗余存储、时序数据且不可篡改和伪造、去中心化信用、自动执行的智能合约、安全和隐私保护等显著的特点, 这使得区块链技术不仅可以成功应用于数字加密货币领域, 同时在经济、金融和社会系统中也存在广泛的应用场景. 根据区块链技术应用的现状, 本文将区块链目前的主要应用笼统地归纳为数字货币、数据存储、数据鉴证、金融交易、资产管理和选举投票共六个场景, 并概述除数字货币外的五大应用场景以及区块链的三种应用模式.

数据存储: 区块链的高冗余存储 (每个节点存储一份数据)、去中心化、高安全性和隐私保护等特点使其特别适合存储和保护重要隐私数据, 以避免因中心化机构遭受攻击或权限管理不当而造成的大规模数据丢失或泄露. 与比特币交易数据类似地, 任意数据均可通过哈希运算生成相应的 Merkle 树并打包记入区块链, 通过系统内共识节点的算力和非对称加密技术来保证安全性. 区块链的多重签名技术可以灵活配置数据访问的权限, 例如必须获得指定 5 个人中 3 个人的私钥授权才可获得访问权限. 目前, 利用区块链来存储个人健康数据 (如电子病历、基因数据等) 是极具前景的应用领域, 此外存储各类重要电子文件 (视频、图片、文本等) 乃至人类思想和意识等也有一定应用空间[7].

数据鉴证: 区块链数据带有时间戳、由共识节点共同验证和记录、不可篡改和伪造, 这些特点使得区块链可广泛应用于各类数据公证和审计场景. 例如, 区块链可以永久地安全存储由政府机构核发的各类许可证、登记表、执照、证明、认证和记录等, 并可在任意时间点方便地证明某项数据的存在性和一定程度上的真实性. 包括德勤在内的多家专业审计公司已经部署区块链技术来帮助其审计师实现低成本和高效地实时审计; Factom 公司则基于区块链

设计了一套准确的、可核查的和不可更改的审计公证流程与方法[26].

金融交易: 区块链技术与金融市场应用有非常高的契合度. 区块链可以在去中心化系统中自发地产生信用, 能够建立无中心机构信用背书的金融市场, 从而在很大程度上实现了 "金融脱媒", 这对第三方支付、资金托管等存在中介机构的商业模式来说是颠覆性的变革; 在互联网金融领域, 区块链特别适合或者已经应用于股权众筹、P2P 网络借贷和互联网保险等商业模式; 证券和银行业务也是区块链的重要应用领域, 传统证券交易需要经过中央结算机构、银行、证券公司和交易所等中心机构的多重协调, 而利用区块链自动化智能合约和可编程的特点, 能够极大地降低成本和提高效率, 避免繁琐的中心化清算交割过程, 实现方便快捷的金融产品交易; 同时, 区块链和比特币的即时到帐的特点可使得银行实现比 SWIFT 代码体系更为快捷、经济和安全的跨境转账; 这也是目前 R3CEV 和纳斯达克等各大银行、证券商和金融机构相继投入区块链技术研发的重要原因.

资产管理: 区块链在资产管理领域的应用具有广泛前景, 能够实现有形和无形资产的确权、授权和实时监控. 对于无形资产来说, 基于时间戳技术和不可篡改等特点, 可以将区块链技术应用于知识产权保护、域名管理、积分管理等领域; 而对有形资产来说, 通过结合物联网技术为资产设计唯一标识并部署到区块链上, 能够形成 "数字智能资产", 实现基于区块链的分布式资产授权和控制. 例如, 通过对房屋、车辆等实物资产的区块链密钥授权, 可以基于特定权限来发放和回收资产的使用权, 有助于 Airbnb 等房屋租赁或车辆租赁等商业模式实现自动化的资产交接; 通过结合物联网的资产标记和识别技术, 还可以利用区块链实现灵活的供应链管理和产品溯源等功能.

选举投票: 投票是区块链技术在政治事务中的代表性应用. 基于区块链的分布式共识验证、不可篡改等特点, 可以低成本高效地实现政治选举、企业股东投票等应用; 同时, 区块链也支持用户个体对特定议题的投票. 例如, 通过记录用户对特定事件是否发生的投票, 可以将区块链应用于博彩和预测市场等场景[27]; 通过记录用户对特定产品的投票评分与建议, 可以实现大规模用户众包设计产品的 "社会制造" 模式等.

根据实际应用场景和需求, 区块链技术已经演化出三种应用模式, 即公共链 (Public blockchain)、联盟链 (Consortium blockchain) 和私有链 (Private blockchain). 公共链是完全去中心化的区块链, 分布式系统的任何节点均可参与链上数据的读写、验证和共识过程, 并根据其 PoW 或 PoS 贡献获得相应的经济激励. 比特币是公共链的典型代表. 联盟链则是部分去中心化 (或称多中心化) 的区块链, 适用于多个实体构成的组织或联盟, 其共识过程受到预定义的一组节点控制, 例如生成区块需要获得 10 个预选的共识节点中的 5 个节点确认; 私有链则是完全中心化的区块链, 适用于特定机构的内部数据管理与审计等, 其写入权限由中心机构控制, 而读取权限可视需求有选择性地对外开放. 需要说明的是, 由于去中心化程度不同, 联盟链和私有链可能不完全符合第 2 节提出的区块链模型, 例如中心化程度较高的区块链可能不需要设计激励层中的经济激励等.

4 区块链的现存问题

作为近年来兴起并快速发展的新技术, 区块链必然会面临各种制约其发展的问题和障碍. 本节将从安全、效率、资源和博弈四方面概述区块链技术有待解决的问题.

4.1 安全问题

安全性威胁是区块链迄今为止所面临的最重要的问题. 其中, 基于 PoW 共识过程的区块链主要面临的是 51 % 攻击问题, 即节点通过掌握全网超过 51 % 的算力就有能力成功篡改和伪造区块链数据. 以比特币为例, 据统计中国大型矿池的算力已占全网总算力的 60 % 以上, 理论上这些矿池可以通过合作实施 51 % 攻击, 从而实现比特币的双重支付[1]. 虽然实际系统中为掌握全网 51 % 算力所需的成本投入远超成功实施攻击后的收益, 但 51 % 攻击的安全性威胁始终存在. 基于 PoS 共识过程在一定程度上解决了 51 % 攻击问题, 但同时也引入了区块分叉时的 N@S (Nothing at stake) 攻击问题. 研究者已经提出通过构造同时依赖高算力和高内存的 PoW 共识算法来部分解决 51 % 攻击问题[4], 更为安全和有效的共识机制尚有待于更加深入的研究和设计.

区块链的非对称加密机制也将随着数学、密码学和计算技术的发展而变的越来越脆弱. 据估计, 以目前天河二号的算力来说, 产生比特币 SHA256 哈希算法的一个哈希碰撞大约需要 2^{48} 年, 但随着量子计算机等新计算技术的发展, 未来非对称加密算法具有一定的破解可能性, 这也是区块链技术面临的潜在安全威胁.

区块链的隐私保护也存在安全性风险. 区块链系统内各节点并非完全匿名, 而是通过类似电子邮件地址的地址标识 (例如比特币公钥地址) 来实现数据传输. 虽然地址标识并未直接与真实世界的人物身份相关联, 但区块链数据是完全公开透明的, 随着各类反匿名身份甄别技术的发展, 实现部分重点目

标的定位和识别仍是有可能的.

4.2 效率问题

区块链效率也是制约其应用的重要因素. 首先是区块膨胀问题: 区块链要求系统内每个节点保存一份数据备份, 这对于日益增长的海量数据存储来说是极为困难的. 以比特币为例, 完全同步自创世区块至今的区块数据需要约 60 GB 存储空间, 虽然轻量级节点可部分解决此问题, 但适用于更大规模的工业级解决方案仍有待研发[28]. 其次是交易效率问题: 比特币区块链目前每秒仅能处理 7 笔交易, 这极大地限制了区块链在大多数金融系统高频交易场景中的应用 (例如 VISA 信用卡每秒最多可处理 10 000 笔交易)[1]; 最后是交易确认时间问题: 比特币区块生成时间为 10 分钟, 因而交易确认时间一般为 10 分钟, 这在一定程度上限制了比特币在小额交易和时间敏感交易中的应用.

4.3 资源问题

PoW 共识过程高度依赖区块链网络节点贡献的算力, 这些算力主要用于解决 SHA256 哈希和随机数搜索, 除此之外并不产生任何实际社会价值, 因而一般意义上认为这些算力资源是被 “浪费” 掉了, 同时被浪费掉的还有大量的电力资源. 随着比特币的日益普及和专业挖矿设备的出现, 比特币生态圈已经在资本和设备方面呈现出明显的军备竞赛态势, 逐渐成为高耗能的资本密集型行业, 进一步凸显了资源消耗问题的重要性. 因此, 如何能有效汇集分布式节点的网络算力来解决实际问题, 是区块链技术需要解决的重要问题. 研究者目前已经开始尝试解决此问题, 例如 Primecoin (质数币) 要求各节点在共识过程中找到素数的最长链条 (坎宁安链和双向双链) 而非无意义的 SHA256 哈希值[29]. 未来的潜在发展趋势是设计行之有效的交互机制来汇聚和利用分布式共识节点的群体智能, 以辅助解决大规模的实际问题.

4.4 博弈问题

区块链网络作为去中心化的分布式系统, 其各节点在交互过程中不可避免地会存在相互竞争与合作的博弈关系, 这在比特币挖矿过程中尤为明显. 通常来说, 比特币矿池间可以通过相互合作保持各自稳定的收益. 然而, 矿池可以通过称为区块截留攻击 (Block withholding attacks) 的方式、通过伪装为对手矿池的矿工、享受对手矿池的收益但不实际贡献完整工作量证明来攻击其他矿池, 从而降低对手矿池的收益. 如果矿池相互攻击, 则双方获得的收益均少于不攻击对方的收益. 当矿池收益函数满足特定条件时, 这种攻击和竞争将会造成 “囚徒困境” 博弈结局[30]. 如何设计合理的惩罚函数来抑制非理性竞争、使得合作成为重复性矿池博弈的稳定均衡解, 尚需进一步深入研究. 此外, 正如前文提到的, 区块链共识过程本质上是众包过程, 如何设计激励相容的共识机制, 使得去中心化系统中的自利节点能够自发地实施区块数据的验证和记账工作, 并提高系统内非理性行为的成本以抑制安全性攻击和威胁, 是区块链有待解决的重要科学问题.

5 基于区块链的智能合约

智能合约概念最早在 1994 年由学者 Nick Szabo 提出, 最初被定义为一套以数字形式定义的承诺, 包括合约参与方可以在上面执行这些承诺的协议, 其设计初衷是希望通过将智能合约内置到物理实体来创造各种灵活可控的智能资产. 由于计算手段的落后和应用场景的缺失, 智能合约并未受到研究者的广泛关注.

区块链技术的出现重新定义了智能合约. 智能合约是区块链的核心构成要素 (合约层), 是由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的计算机程序, 能够实现主动或被动的处理数据, 接受、储存和发送价值, 以及控制和管理各类链上智能资产等功能. 智能合约作为一种嵌入式程序化合约, 可以内置在任何区块链数据、交易、有形或无形资产上, 形成可编程控制的软件定义的系统、市场和资产. 智能合约不仅为传统金融资产的发行、交易、创造和管理提供了创新性的解决方案, 同时能够在社会系统中的资产管理、合同管理、监管执法等事务中发挥重要作用.

具体说来, 智能合约是一组情景—应对型的程序化规则和逻辑, 是部署在区块链上的去中心化、可信共享的程序代码. 智能合约同样具有区块链数据的一般特征, 如分布式记录、存储和验证, 不可篡改和伪造等. 签署合约的各参与方就合约内容、违约条件、违约责任和外部核查数据源达成一致, 必要时检查和测试合约代码以确保无误后, 以智能合约的形式部署在区块链上, 即可不依赖任何中心机构地自动化代表各签署方执行合约. 智能合约的可编程特性使得签署方可以增加任意复杂的条款.

智能合约的运作机理如图 5 所示: 通常情况下, 智能合约经各方签署后, 以程序代码的形式附着在区块链数据 (例如一笔比特币交易) 上, 经 P2P 网络传播和节点验证后记入区块链的特定区块中. 智能合约封装了预定义的若干状态及转换规则、触发合约执行的情景 (如到达特定时间或发生特定事件等)、特定情景下的应对行动等. 区块链可实时监控智能合约的状态, 并通过核查外部数据源、确认满足特定触发条件后激活并执行合约.

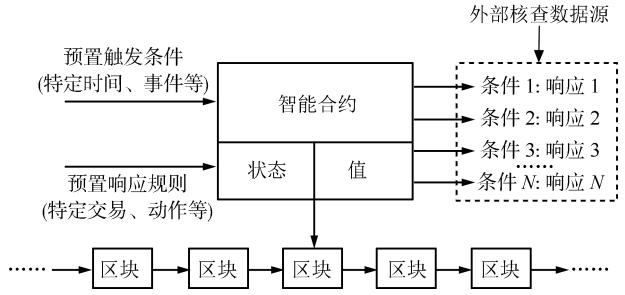


图 5 智能合约的运作机理

Fig. 5 The rationale of smart contracts

区块链和智能合约有极为广阔的应用场景. 例如, 互联网金融领域的股权众筹或 P2P 网络借贷等商业模式可以通过区块链和智能合约加以实现. 传统方式是通过股权众筹或 P2P 借贷的交易所或网络平台作为中心机构完成资金募集、管理和投资, 实际操作过程中容易出现因中心机构的信用缺失而导致的资金风险. 利用智能合约, 这些功能均可以封装在去中心化可信的区块链上自动执行. 区块链可记录每一笔融资, 当成功达到特定融资额度时计算每个投资人的股权份额, 或在一段时间内未达到融资额度时自动将资金退还给投资人. 再如, 通过将房屋和车辆等实体资产进行非对称加密, 并嵌入含有特定访问控制规则的智能合约后部署在区块链上, 使用者符合特定的访问权限或执行特定操作 (如付款) 后就可使用这些资产, 这能够有效解决房屋或车辆租赁商业模式中资产交接和使用许可方面的痛点.

智能合约具有自治、自足和去中心化等特征. 自治表示合约一旦启动就会自动运行, 而不需要其他签署方进行任何干预; 自足则意味着合约能够通过提供服务或发行资产来获取资金, 并在需要时使用这些资金; 去中心化则意味着智能合约是由去中心化存储和验证的程序代码而非中心化实体来保障执行的合约, 能在很大程度上保证合约的公平和公正性[1].

智能合约对于区块链技术来说具有重要的意义. 一方面, 智能合约是区块链的激活器, 为静态的底层区块链数据赋予了灵活可编程的机制和算法, 并为构建区块链 2.0 和 3.0 时代的可编程金融系统与社会系统奠定了基础; 另一方面, 智能合约的自动化和可编程特性使其可封装分布式区块链系统中各节点的复杂行为, 成为区块链构成的虚拟世界中的软件代理机器人, 这有助于促进区块链技术在各类分布式人工智能系统中的应用, 使得基于区块链技术构建各类去中心化应用 (Decentralized application, Dapp)、去中心化自治组织 (Decentralized autonomous organization, DAO)、去中心化自治公司 (Decentralized autonomous corporation, DAC) 甚至去中心化自治社会 (Decentralized autonomous society, DAS) 成为可能.

就现状而言, 区块链和智能合约技术的主要发展趋势是由自动化向智能化方向演化. 现存的各类智能合约及其应用的本质逻辑大多仍是根据预定义场景的 “IF-THEN” 类型的条件响应规则, 能够满足目前自动化交易和数据处理的需求. 未来的智能合约应具备根据未知场景的 “WHAT-IF” 推演、计算实验和一定程度上的自主决策功能, 从而实现由目前 “自动化” 合约向真正的 “智能” 合约的飞跃[31−32].

6 区块链驱动的平行社会

互联网近年来的迅猛发展及其与物理世界的深度耦合与强力反馈, 已经根本性地改变了现代社会的生产、生活与管理决策模式, 形成了现实物理世界 – 虚拟网络空间紧密耦合、虚实互动和协同演化的平行社会空间, 催生了 “互联网 +” 和工业 4.0 等一系列国家战略. 未来社会的发展趋势则必将从物理 + 网络的 CPS 实际世界 (Cyber-physical systems, CPS) 走向精神层面的人工世界, 形成物理 + 网络 + 人工的人–机–物一体化的三元耦合系统, 称为社会物理信息系统 (Cyber-physical-social systems, CPSS). 目前, 基于 CPSS 的平行社会已现端倪, 其核心和本质特征是虚实互动与平行演化[33].

区块链是实现 CPSS 平行社会的基础架构之一, 其主要贡献是为分布式社会系统和分布式人工智能研究提供了一套行之有效的去中心化的数据结构、交互机制和计算模式, 并为实现平行社会奠定了坚实的数据基础和信用基础. 就数据基础而言, 管理学家爱德华戴明曾说过: 除了上帝, 所有人必须以数据说话. 然而在中心化社会系统中, 数据通常掌握在政府和大型企业等 “少数人” 手中, 为少数人 “说话”, 其公正性、权威性甚至安全性可能都无法保证. 区块链数据则通过高度冗余的分布式节点存储, 掌握在 “所有人” 手中, 能够做到真正的 “数据民主”. 就信用基础而言, 中心化社会系统因其高度工程复杂性和社会复杂性而不可避免地会存在 “默顿系统” 的特性, 即不确定性、多样性和复杂性, 社会系统中的中心机构和规则制定者可能会因个体利益而出现失信行为; 区块链技术有助于实现软件定义的社会系统, 其基本理念就是剔除中心化机构、将不可预测的行为以智能合约的程序化代码形式提前部署和固化在区块链数据中, 事后不可伪造和篡改并自动化执行, 从而在一定程度上能够将 “默顿” 社会系统转化为可全面观察、可主动控制、可精确预测的 “牛顿” 社会系统[34].

ACP (人工社会 Artificial societies、计算实验

Computational experiments 和平行执行 Parallel execution) 方法是迄今为止平行社会管理领域唯一成体系化的、完整的研究框架, 是复杂性科学在新时代平行社会环境下的逻辑延展和创新[35]. ACP 方法可以自然地与区块链技术相结合, 实现区块链驱动的平行社会管理. 首先, 区块链的 P2P 组网、分布式共识协作和基于贡献的经济激励等机制本身就是分布式社会系统的自然建模, 其中每个节点都将作为分布式系统中的一个自主和自治的智能体 (Agent). 随着区块链生态体系的完善, 区块链各共识节点和日益复杂与自治的智能合约将通过参与各种形式的 Dapp, 形成特定组织形式的 DAC 和 DAO, 最终形成 DAS, 即 ACP 中的人工社会[36]. 其次, 智能合约的可编程特性使得区块链可进行各种 "WHAT-IF" 类型的虚拟实验设计、场景推演和结果评估, 通过这种计算实验过程获得并自动或半自动地执行最优决策. 最后, 区块链与物联网等相结合形成的智能资产使得联通现实物理世界和虚拟网络空间成为可能, 并可通过真实和人工社会系统的虚实互动和平行调谐实现社会管理和决策的协同优化. 不难预见, 未来现实物理世界的实体资产都登记为链上智能资产的时候, 就是区块链驱动的平行社会到来之时.

7 结束语

随着以比特币为代表的数字加密货币的强势崛起, 新兴的区块链技术逐渐成为学术界和产业界的热点研究课题. 区块链技术的去中心化信用、不可篡改和可编程等特点, 使其在数字加密货币、金融和社会系统中有广泛的应用前景. 然而, 与蓬勃发展的区块链商业应用相比, 区块链的基础理论和技术研究仍处于起步阶段, 许多更为本质性的、对区块链产业发展至关重要的科学问题亟待研究跟进. 本文系统地梳理了区块链技术的基本原理、技术、方法与应用, 以期为未来研究提供有益的启发与借鉴.

References

1 Swan M. *Blockchain: Blueprint for a New Economy*. USA: O′Reilly Media Inc., 2015.

2 Technical report by the UK government chief scientific adviser [Online], available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, February 21, 2016

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

4 Ethereum White Paper. A next-generation smart contract and decentralized application platform [Online], available: https://github.com/ethereum/wiki/wiki/White-Paper, November 12, 2015

5 Ding Wei. Block chain based instrument data management system. *China Instrumentation*, 2015, (10): 15−17
(丁未. 基于区块链技术的仪器数据管理创新系统. 中国仪器仪表, 2015, (10): 15−17)

6 Zhao He, Li Xiao-Feng, Zhan Li-Kui, Wu Zhong-Cheng. Data integrity protection method for microorganism sampling robots based on blockchain technology. *Journal of Huazhong University of Science and Technology (Natural Science Edition)*, 2015, **43**(Z1): 216−219
(赵赫, 李晓风, 占礼葵, 吴仲城. 基于区块链技术的采样机器人数据保护方法. 华中科技大学学报 (自然科学版), 2015, **43**(增刊): 216−219)

7 Swan M. Blockchain thinking: the brain as a decentralized autonomous corporation. *IEEE Technology and Society Magazine*, 2015, **34**(4): 41−52

8 Davidson Eric. Letter. *New Scientist*, 2015, **228**(3043): 52−52

9 Anonymous. New kid on the blockchain. *New Scientist*, 2015, **225**(3009): 7

10 Godsiff P. Bitcoin: bubble or blockchain. In: Proceedings of the 9th KES International Conference on Agent and Multi-Agent Systems: Technologies and Applications (KES-AMSTA). Sorrento, Italy: Springer, 2015, **38**: 191−203

11 Kraft D. Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, 2016, **9**(2): 397−413

12 Wilson D, Ateniese G. From pretty good to great: enhancing PGP using Bitcoin and the blockchain. In: Proceedings of the 9th International Conference on Network and System Security. New York: Springer International Publishing, 2015, **9408**: 368−375

13 Zyskind G, Nathan O, Pentland A S. Decentralizing privacy: using blockchain to protect personal data. In: Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW 2015). San Jose, CA: IEEE, 2015. 180−184

14 Kypriotaki K N, Zamani E D, Giaglis G M. From Bitcoin to decentralized autonomous corporations: extending the application scope of decentralized peer-to-peer networks and blockchains. In: Proceedings of the 17th International Conference on Enterprise Information Systems(ICEIS2015). 2015, **3**: 284−290

15 Blockchain Monitoring Website [Online], available: https://blockchain.info/, January 8, 2016

16 Cryptocurrency Monitoring Website [Online], available: http://coinmarketcap.com/, November 24, 2015

17 World Economic Forum Survey [Online], available: http://www.coinfox.info/news/3184-world-economic-forum-survey-10-of-global-gdp-may-be-stored-with-blockchain-technology-by-2027, February 21, 2016

18 CoinDesk Report [Online], available: http://www.bitcoin86.com/news/3527.html, February 21, 2016

19 Antonopoulos A M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. USA: O′Reilly Media Inc., 2014.

20 Fan Jie, Yi Le-Tian, Shu Ji-Wu. Research on the technologies of Byzantine system. *Journal of Software*, 2013, **24**(6): 1346−1360
(范捷, 易乐天, 舒继武. 拜占庭系统技术研究综述. 软件学报, 2013, **24**(6): 1346−1360)

21 Bitcoin Sourcecode [Online], available: https://github.com/bitcoin/bitcoin/, January 18, 2016

22 Merkle R C. Protocols for public key cryptosystems. In: Proceedings of the 1980 IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE, 1980. 122

23 Larimer D. Transactions as proof-of-stake [Online], available: http://7fvhfe.com1.z0.glb.clouddn.com/@/wp-content/uploads/2014/01/TransactionsAsProofOfStake10.pdf, 2013

24 Larimer D. Delegated proof-of-stake white paper [Online], available: http://www.bts.hk/dpos-baipishu.html, 2014

25 Bitcoinmining Article [Online], available: https://www.bitcoinmining.com/bitcoin-mining-pools, December 8, 2015

26 Factom White Paper [Online], available: http://bite01.com/bit/1421, December 29, 2015

27 Brito J, Shadab H, Castillo A. Bitcoin financial regulation: securities, derivatives, prediction markets, and gambling. *The Columbia Science & Technology Law Review*, 2014, **16**: 144−221

28 Eyal I, Efe Gencer A, Sirer E G, van Renesse R. Bitcoin-NG: a scalable blockchain protocol. *Cryptography and Security*, arXiv: 1510.02037

29 Primecoin Website [Online], available: http:// primecoin.io/, February 9, 2016

30 Courtois N T, Bahack L. On subversive miner strategies and block withholding attack in Bitcoin digital currency. *Cryptography and Security*, arXiv: 1402.1718

31 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)

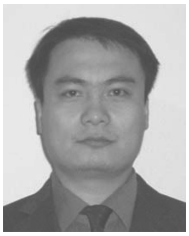
32 Wang Fei-Yue, Qiu Xiao-Gang, Zeng Da-Jun, Cao Zhi-Dong, Fan Zong-Chen. A computational experimental platform for emergency response based on parallel systems. *Complex Systems and Complexity Science*, 2010, **7**(4): 1−10
(王飞跃, 邱晓刚, 曾大军, 曹志冬, 樊宗臣. 基于平行系统的非常规突发事件计算实验平台研究. 复杂系统与复杂性科学, 2010, **7**(4): 1−10)

33 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**(5−6): 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**(5−6): 460−469)

34 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)

35 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)

36 Wang Fei-Yue, Jiang Zheng-Hua, Dai Ru-Wei. Population studies and artificial societies: a discussion of artificial population systems and their applications. *Complex Systems and Complexity Science*, 2005, **2**(1): 1−9
(王飞跃, 蒋正华, 戴汝为. 人口问题与人工社会方法: 人工人口系统的设想与应用. 复杂系统与复杂性科学, 2005, **2**(1): 1−9)



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. 2008 年于山东科技大学获得计算机软件与理论专业博士学位. 主要研究方向为商务智能与计算广告学. 本文通信作者. E-mail: yong.yuan@ia.ac.cn
(**YUAN Yong** Associate professor at the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences. He received his Ph. D. degree in computer software and theory from Shandong University of Science and Technology in 2008. His research interest covers business intelligence and computational advertising. Corresponding author of this paper.)

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. 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 of Management and Control for 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. His research interest covers modeling, analysis, and control of intelligent systems and complex systems.)