智能合约: 架构及进展

欧阳丽炜[1,2] 王 帅[1,2] 袁 勇[1,3] 倪晓春[1,3] 王飞跃[1,3,4]

摘 要 智能合约是一种无需中介、自我验证、自动执行合约条款的计算机交易协议, 近年来随着区块链技术的日益普及而备受关注. 区块链上的智能合约具有去中心化、去信任、可编程、不可篡改等特性, 可灵活嵌入各种数据和资产, 帮助实现安全高效的信息交换、价值转移和资产管理, 最终有望深入变革传统商业模式和社会生产关系, 为构建可编程资产、系统和社会奠定基础. 本文致力于以区块链智能合约为研究对象, 对已有的研究成果进行全面梳理和系统概述, 提出了智能合约的基础架构模型并以此为研究框架阐述了智能合约的运行机制与基础架构, 总结了智能合约的研究挑战与进展, 介绍了智能合约的技术优势与典型应用领域, 讨论了智能合约的发展趋势, 以期为智能合约的后续研究提供参考.

关键词 区块链, 智能合约, 运行机制, 基础架构, 平行区块链

引用格式 欧阳丽炜, 王帅, 袁勇, 倪晓春, 王飞跃. 智能合约: 架构及进展. 自动化学报, 2019, **45**(3): 445−457

DOI 10.16383/j.aas.c180586

Smart Contracts: Architecture and Research Progresses

OUYANG Li-Wei[1,2] WANG Shuai[1,2] YUAN Yong[1,3] NI Xiao-Chun[1,3] WANG Fei-Yue[1,3,4]

Abstract Smart contracts are computerized transaction protocols that can self-verify and self-execute the terms of contracts without a trusted third-party intermediary. In recent years, smart contracts have attracted intensive attention with the increasing popularity of their main computational architecture, i.e., blockchain. Blockchain-enabled smart contracts are decentralized, trustless, programmable, and tamper-resistant, they can be flexibly embedded into a variety of data and assets to help achieve secure and efficient information exchange, value transfer and asset management. Thus, they are expected to deepen the revolution of traditional business models and social production relationships, and lay the foundation for building programmable assets, systems and societies. This article is dedicated to a comprehensive analysis and systematic overview of blockchain-enabled smart contracts. Specifically, we proposed a basic model of smart contracts which employs a six-layer architecture and used it as a research framework to explain the operating mechanism and infrastructure of smart contracts. We also summarized their research challenges and recent progresses, introduced their technical advantages and typical application fields, and discussed their future development trends. This article is aimed at providing helpful guidance and reference for future research efforts of blockchain-enabled smart contracts.

Key words Blockchain, smart contracts, operating mechanism, basic framework, parallel blockchain

Citation Ouyang Li-Wei, Wang Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Smart contracts: architecture and research progresses. *Acta Automatica Sinica*, 2019, **45**(3): 445−457

智能合约的概念最早于 1994 年由美国计算机科学家 Nick Szabo 提出并定义为 “一套以数字形式指定的承诺, 包括合约参与方可以在上面执行这些承诺的协议”[1], 其设计初衷是在无需第三方可信权威的情况下, 作为执行合约条款的计算机交易协议, 嵌入某些由数字形式控制具有价值的物理实体, 担任合约各方共同信任的代理, 高效安全履行合约并创建多种智能资产. 自动贩卖机、销售点情报管理系统 (Point of sales, POS)、电子数据交换系统 (Electronic data intercharge, EDI) 都可看作是智能合约的雏形. 囿于当时计算场景的限制, 很长一段时间内智能合约没有得到广泛的应用.

直到 2008 年, 化名为 “中本聪” (Satoshi Nakamoto) 的学者提出了一种无需信任即可进行点对点交易的加密数字货币系统−比特币[2], 人们发现其底层技术区块链与智能合约天然契合: 区块链可借助智能合约的可编程性封装分

收稿日期 2018-09-03 录用日期 2018-11-01
Manuscript received September 3, 2018; accepted November 1, 2018
国家自然科学基金 (71472174, 61533019, 71702182, 71232006, 61233001, 71402178), 青岛智能产业智库基金资助
Supported by National Natural Science Foundation of China (71472174, 61533019, 71702182, 71232006, 61233001, 71402178), 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. 中国科学院大学 北京 100049 3. 青岛智能产业技术研究院 青岛 266109 4. 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 for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 2. University of Chinese Academy of Sciences, Beijing 100049 3. Qingdao Academy of Intelligent Industries, Qingdao 266109 4. Research Center of Military Computational Experiments and Parallel Systems, National University of Defense Technology, Changsha 410073

布式节点的复杂行为; 智能合约可借助区块链的去中心化基础架构在去信任、可执行环境中有效实现. 自此, 智能合约重焕新生, 区块链逐渐成为智能合约最主要的计算场景, 智能合约也被赋予了新的含义.

目前业内尚未形成公认的智能合约定义, 我们认为: 狭义的智能合约可看作是运行在分布式账本上预置规则、具有状态、条件响应的, 可封装、验证、执行分布式节点复杂行为, 完成信息交换、价值转移和资产管理的计算机程序. 广义的智能合约则是无需中介、自我验证、自动执行合约条款的计算机交易协议. 按照其设计目的可分为: 旨在作为法律的替代和补充的智能法律合约, 旨在作为功能型软件的智能软件合约以及旨在引入新型合约关系的智能替代合约 (如在物联网中约定机器对机器商业行为的智能合约)[3]. 本文主要研究运行在区块链上的智能合约, 它们具有区块链数据去中心化、去信任、不可篡改、匿名可溯源等一般特性.

基于比特币图灵不完备字节码语言 OP-RETURN 的比特币脚本是最早应用于区块链的智能合约, 由于 OP-RETURN 的计算能力非常有限, 不支持循环语句, 只能实现基本的算术、逻辑运算及验证加密功能, 早期的智能合约通常无法具有复杂逻辑[4]. 以太坊作为世界上首个内置了图灵完备编程语言并正式引入智能合约概念的公有区块链, 是目前最为流行的智能合约开发平台. 以太坊的核心是可执行任意复杂算法编码的以太坊虚拟机 (Ethereum virtual machine, EVM), 所有部署在以太坊上的智能合约都将被编译成 EVM 字节码, 在矿工本地隔离的 EVM 中执行[5]. 用户可以按照自身意愿在以太坊平台上高效快速地开发出包括加密货币在内的多种智能合约和建立在智能合约上的去中心化应用 (Decentralized applications, DApps). 以太坊的出现改变了区块链及智能合约的应用格局, 使其不再局限于数字货币, 开始有机会构建更宏观的金融系统并应用到其他社会领域.

尽管近年来智能合约发展迅猛, 其仍面临着许多不可忽视的挑战. 以众所周知的 “The DAO” 事件为例, 2016 年 6 月, 攻击者就通过调用众筹项目 “The DAO” 中智能合约的可重入性函数窃取了价值大约 6 000 万美元的以太币, 由于智能合约不可篡改的特性, 以太坊最终被迫执行硬分叉挽回损失, 而又因其匿名性, 攻击者目前仍逍遥法外[6]. 除类似的安全漏洞外, 智能合约还存在缺乏可信数据源、隐私问题、性能问题和法律问题等其他挑战亟待解决. 考虑到在智能合约的产业应用如火如荼展开的同时, 行业内尚缺乏统一的技术标准和研究框架, 本文致力于以区块链智能合约为研究对象, 对已有的研究成果进行全面的梳理, 首次提出智能合约的基础架构模型, 并以此为基础概述了智能合约的运行机制、研究挑战及进展、应用领域和发展趋势等, 以期为智能合约的后续研究提供参考.

本文的组织结构为: 第 1 节系统概述智能合约, 包括区块链技术简介、智能合约运行机制及主流开发平台总结, 首次提出并详细阐述了智能合约的基础架构模型; 第 2 节结合智能合约基础架构模型归纳了智能合约的研究挑战及进展, 包括隐私问题、法律问题、安全问题、机制设计与性能问题和智能合约的形式化验证等; 第 3 节以金融、管理、医疗、物联网与供应链为例, 介绍了智能合约的典型应用领域; 第 4 节展望了智能合约未来可能的发展趋势; 第 5 节总结了本文内容.

1 智能合约运行机制与基础模型

1.1 区块链简介

区块链是一种将数据区块按照时间顺序组合成的链式结构, 是去中心化系统中各节点共享且共同维护的分布式数据账本[7], 具体的: 各节点由 P2P 组网方式相互连通和交互, 受激励机制激励贡献自身算力, 根据数据验证机制及传播协议, 执行、验证并传播一段时间内生成的有效交易数据, 同时利用 Merkle 树、哈希算法、时间戳等技术加密、生成数据区块, 依据共识算法争夺记账权, 最终获得记账权的节点 (矿工), 将其生成的数据区块链接到区块链主链上并获得相应奖励, 其余节点更新区块链账本.

区块链具有去信任、去中心化、开放自治、匿名可溯源、信息不可篡改等特性, 自问世以来就显示出广阔的应用前景, 吸引了学术界和工业界的大量关注, 目前区块链技术已被应用于医疗、金融、物联网、能源等诸多领域. 一般来说, 区块链可按许可权限分为公有区块链、联盟区块链和私有区块链, 其中, 公有链面向全球所有用户, 任何人都可以在其中读取数据和发送交易; 联盟链由若干业务相关的机构共同参与管理, 每个机构都运行着一个或多个节点, 读写权限仅对联盟内的节点有限度地开放; 私有链的读写权限由某个组织或机构控制, 参与节点的资格被严格限制.

基于区块链的分布式架构、共识算法等, 智能合约允许相互不信任的用户在不需要任何第三方可信中介或权威的情况下完成交易, 同时, 数字形式的智能合约可灵活嵌入各种有形或无形的资产、交易和数据中, 实现主动或被动的资产、信息管理与控制, 逐步构建可编程的智能资产、系统及社会.

1.2 智能合约的运行机制

智能合约的运行机制如图 1 所示, 智能合约一般具有值和状态两个属性, 代码中用 If-Then 和

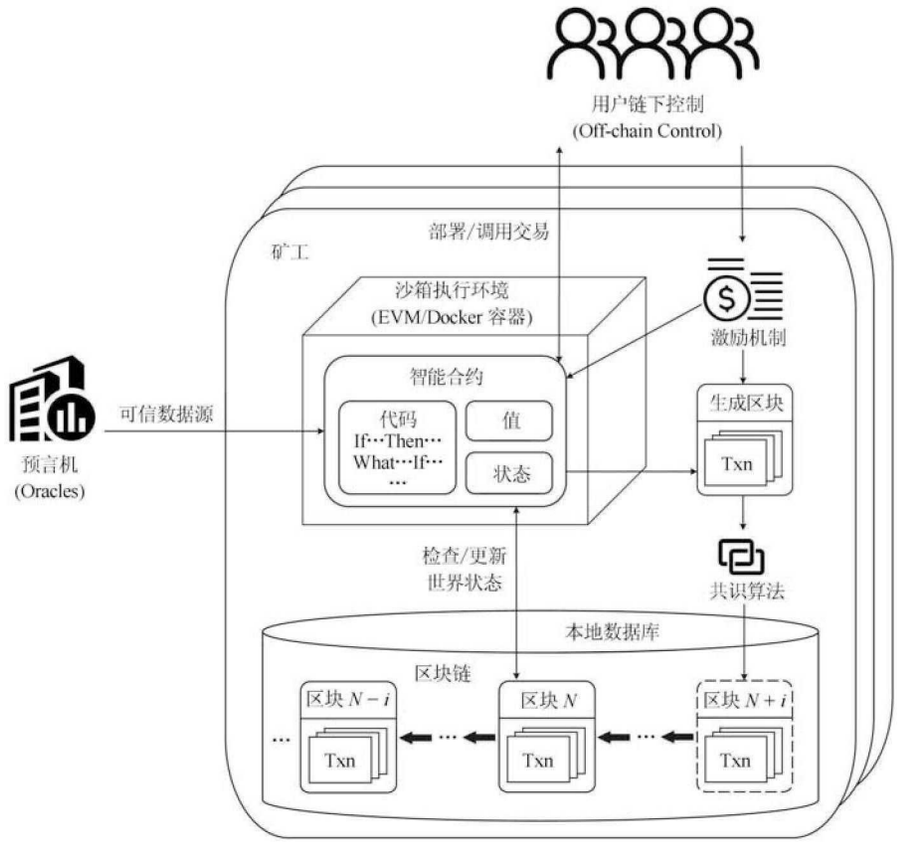

图 1　智能合约的运行机制

Fig. 1　The operating mechanism of smart contracts

What-If 语句预置了合约条款的相应触发场景和响应规则, 智能合约经多方共同协定、各自签署后随用户发起的交易 (Transaction, Txn) 提交, 经 P2P 网络传播、矿工验证后存储在区块链特定区块中, 用户得到返回的合约地址及合约接口等信息后即可通过发起交易来调用合约. 矿工受系统预设的激励机制激励, 将贡献自身算力来验证交易, 矿工收到合约创建或调用交易后在本地沙箱执行环境 (如以太坊虚拟机) 中创建合约或执行合约代码, 合约代码根据可信外部数据源 (也称为预言机, Oracles) 和世界状态的检查信息自动判断当前所处场景是否满足合约触发条件以严格执行响应规则并更新世界状态. 交易验证有效后被打包进新的数据区块, 新区块经共识算法认证后链接到区块链主链, 所有更新生效.

由于区块链种类及运行机制的差异, 不同平台上智能合约的运行机制也有所不同, 以太坊和超级账本是目前应用最广泛的两种智能合约开发平台, 它们的智能合约运行机制最具代表性, 以下将以这两种平台为例, 阐述智能合约的运行机制.

1) 以太坊

以太坊在整体上可看作是一个基于交易的状态机: 起始于一个创世 (Genesis) 状态, 然后随着交易的执行, 状态逐步改变一直到最终状态, 这个最终状态就是以太坊世界的权威版本[5]. 以太坊中引入了账户的概念以取代比特币未花费交易输出 (Unspent transaction output, UTXO) 模型, 账户分为外部账户和合约账户两类, 两类账户都具有与之关联的账户状态和账户地址, 都可以存储以太坊专用加密货币以太币, 区别在于外部账户由用户私钥控制, 没有代码与之关联, 合约账户由合约代码控制, 有代码与之关联.

用户只能通过外部账户在以太坊中发起交易, 交易可以包含二进制交易负载数据 (Payload) 和以太币, 交易执行过程中可能产生一系列消息调用. 当交易或消息调用的接收者为以太坊指定地址 $\emptyset$ 时, 创建合约. 新合约账户地址由合约创建者的地址和该地址发出过的交易数量 Nonce 计算得到, 创建合约交易的 Payload 被编译为 EVM 字节码执行, 执行的输出作为合约代码被永久存储. 当接收者为合约账户时, 合约账户内代码被激发在本地 EVM 中执行, Payload 作为合约的输入参数, 可信数据源则为合约提供必要外部世界信息. 所有执行结束后, 返回执行结果, 完整交易经矿工广播验证后和新的世界状态一起存入区块链.

考虑到以太坊交易伴随带宽消耗, 存储消耗, 计算消耗等, 为了激励全球算力的投入和合理分配使用权, 避免系统因恶意程序走向失控, 以太坊中所有程序的执行都需要支付费用. 各种操作费用以 Gas 为单位计算, 任意的程序片段都可以根据规则计算出消耗的燃料数量, 完整交易的发起者需支付所有执行费用. 交易完成后, 剩余的燃料以购买时的价格退回到交易发送者账户, 未退回的费用作为挖出包含此交易区块的矿工的奖励. 若交易执行过程中发生燃料不足 (Out of gas, OOG)、堆栈溢出、无效指令等异常而中止, 交易将成为无效交易, 已消耗 Gas 仍作为矿工贡献其计算资源的奖励.

2) 超级账本

超级账本 (Hyperledger fabric) 最早是由国际商业机器公司 (International business machines corporation, IBM) 牵头发起的致力于打造区块链技术开源规范和标准的联盟链, 2015 年起成为开源项目并移交给 Linux 基金会维护. 不同于比特币、以太坊等全球共享的公有链, 超级账本只允许获得许可的相关商业组织参与、共享和维护, 由于这些商业组织之间本身就有一定的信任基础, 超级账本被认为并非完全去中心化.

超级账本使用模块化的体系结构, 开发者可按需求在平台上自由组合可插拔的会员服务、共识算法、加密算法等组件组成目标网络及应用. 链码 (Chaincode) 是超级账本中的智能合约, 开发者利用链码与超级账本交互以开发业务、定义资产和管理去中心化应用. 联盟链中每个组织成员都拥有和维护代表该组织利益的一个或多个 Peer 节点, 联盟链由多个组织的 Peer 节点共同构成. Peer 节点是链码及分布式账本的宿主, 可在 Docker 容器中运行链码, 实现对分布式账本上键–值对或其他状态数据库的读/写操作, 从而更新和维护账本.

超级账本的运行过程包含三个阶段[8]:

提议 (Proposal): 应用程序创建一个包含账本更新的交易提议 (Proposal), 并将该提议发送给链码中背书策略指定的背书节点集合 (Endorsing peers set) 作签名背书. 每个背书节点独立地执行链码并生成各自的交易提议响应后, 将响应值、读/写集合和签名等返回给应用程序. 当应用程序收集到足够数量的背书节点响应后, 提议阶段结束.

打包 (Packaging): 应用程序验证背书节点的响应值、读/写集合和签名等, 确认所收到的交易提议响应一致后, 将交易提交给排序节点 (Orderer). 排序节点对收到的众多交易进行排序并分批打包成数据区块后将数据区块广播给所有与之相连接的 Peer 节点.

验证 (Validation): 与排序节点相连接的 Peer 节点逐一验证数据区块中的交易, 确保交易严格依照事先确定的背书策略由所有对应的组织签名背书. 验证通过后, 所有 Peer 节点将新的数据区块添加至当前区块链的末端, 更新账本. 需要注意的是, 此阶段不需要运行链码, 链码仅在提议阶段运行.

1.3 智能合约的基础模型

本节将结合区块链上智能合约的设计流程、应用现状及发展趋势, 归纳智能合约生命周期并提出智能合约基础模型, 该模型一方面囊括智能合约全生命周期中的关键技术, 另一方面对智能合约技术体系中的关键要素进行划分, 体现智能合约核心的研究方向和发展趋势, 为智能合约研究体系的建立与完善提供参考, 奠定基础.

智能合约的生命周期根据其运行机制可概括为协商、开发、部署、运维、学习和自毁六个阶段, 其中开发阶段包括合约上链前的合约测试, 学习阶段包括智能合约的运行反馈与合约更新等. 图 2 所示为智能合约的基础架构模型, 模型自底向上由基础设施层、合约层、运维层、智能层、表现层和应用层组成, 以下将分层进行阐述.

基础设施层: 封装了支持智能合约及其衍生应用实现的所有基础设施, 包括分布式账本及其关键技术、开发环境和可信数据源等, 这些基础设施的选择将在一定程度上影响智能合约的设计模式和合约属性.

1) 分布式账本及其关键技术: 智能合约的执行与交互需要依靠共识算法、激励机制及 P2P 通信网络等区块链关键技术实现, 最终执行结果将记入由全体节点共同维护的分布式账本. 不同的共识算法和激励机制将影响智能合约的设计模式、执行效率和安全性能. 以激励机制为例, 以太坊中智能合约的开发需要额外考虑燃料消耗问题, 设计合约时需避免出现燃料耗尽异常 (OOG) 和死代码 (Dead code)、无用描述、昂贵循环等高耗燃操作.

2) 开发环境: 狭义的智能合约可看作是运行在区块链上的计算机程序, 作为计算机程序, 智能合约的开发、部署和调用将涉及到包括编程语言、集成开发环境 (IDE)、开发框架、客户端和钱包等多种专用开发工具. 以钱包为例, 除作为存储加密货币的电子钱包外, 通常还承担启动节点, 部署合约、调用合约等功能.

3) 预言机 (Oracles): 为保证区块链网络的安全, 智能合约一般运行在隔离的沙箱执行环境中 (如以太坊的 EVM 及超级账本的 Docker 容器等), 除交易的附加数据外, 预言机可提供可信外部数据源供合约查询外部世界的世界状态或触发合约执行. 同时, 为保持分布式节点的合约执行结果一致, 智能

图 2　智能合约基础架构模型

Fig. 2　A basic framework of smart contracts

合约也通过查询预言机实现随机性.

合约层: 封装了静态的合约数据, 包括合约各方达成一致的合约条款、合约条款代码化后的情景−应对型规则和合约创建者指定的合约与外界以及合约与合约之间的交互准则等. 合约层可看作是智能合约的静态数据库, 封装了所有智能合约调用、执行、通信规则.

以智能合约从协商、开发到部署的生命周期为顺序, 合约各方将首先就合约内容进行协商, 合约内容可以是法律条文、商业逻辑和意向协定等. 此时的智能合约类似于传统合约, 立契者无需具有专门的技术背景, 只需根据法学、商学、经济学知识对合约内容进行谈判与博弈, 探讨合约的法律效力和经济效益等合约属性. 随后, 专业的计算机从业者利用算法设计、程序开发等软件工程技术将以自然语言描述的合约内容编码为区块链上可运行的 “If-Then” 或 “What-If” 式情景−应对型规则, 并按照平台特性和立契者意愿补充必要的智能合约与用户之间、智能合约与智能合约之间的访问权限与通信方式等.

运维层: 封装了一系列对合约层中静态合约数据的动态操作, 包括机制设计、形式化验证、安全性检查、维护更新、自毁等. 智能合约的应用通常关乎真实世界的经济利益, 恶意的、错误的、有漏洞的智能合约会带来巨大的经济损失, 运维层是保证智能合约能够按照设计者意愿正确、安全、高效运行的关键.

以智能合约从协商到自毁的全生命周期为序, 机制设计利用信息和激励理论帮助合约高效实现其功能. 形式化验证与安全性检查在合约正式部署上链前以严格的数学方法证明合约代码的正确性和安全性, 保证合约代码完全按照创建者的本意执行. 维护更新在合约部署上链后维护合约正常运行并在合约功能难以满足需求或合约出现可修复漏洞等必要时升级合约. 最后, 当智能合约生命周期结束或出现不可修复的高危漏洞时, 合约可以进行自毁操作以保障网络安全. 需要注意的是, 合约的更新与自毁将仅体现在新区块的区块数据中, 历史区块链数据始终存在且不可篡改.

智能层: 封装了各类智能算法, 包括感知、推理、学习、决策和社交等, 为前三层构建的可完全按照创建者意愿在区块链系统中安全高效执行的智能合约增添了智能性. 需要指出的是, 当前的智能合约并不具备智能性, 只能按照预置的规则执行相应的动作. 但是, 我们认为未来的智能合约将不仅可以按照预定义的 “If-Then” 式语句自动执行, 更可以具备未知场景下 “What-If” 式智能推演、计算实验, 以及自主决策等功能.

运行在区块链上的各类智能合约可看作是用

户的软件代理 (或称软件机器人), 由于计算机程序具有强大的可操作性, 随着认知计算、强化学习、生成式对抗网络 (Generative adversarial network, GAN) 等人工智能技术的快速发展, 这些软件代理将逐渐具备智能性: 一方面, 代理个体将从基础的感知, 推理和学习出发逐步实现任务选择, 优先级排序, 目标导向行为 (Goal-directed behaviors), 自主决策等功能: 另一方面, 代理群体将通过彼此间的交互通信、协调合作、冲突消解等具备一定的社交性. 这些自治软件代理在智能层的学习、协作结果也将反馈到合约层和运维层, 优化合约设计和运维方案, 最终实现自主自治的多代理系统, 从自动化合约转变为真正意义上的智能化合约.

表现层: 封装了智能合约在实际应用中的各类具体表现形式. 包括去中心化应用 (Decentralized application, DApp)、去中心化自治组织 (Decentralized autonomous organization, DAO)、去中心化自治企业 (Decentralized autonomous corporation, DAC) 和去中心化自治社会 (Decentralized autonomous society, DAS) 等.

区块链是具有普适性的去中心化技术架构, 可封装节点复杂行为的智能合约相当于区块链的应用接口, 帮助区块链的分布式架构植入不同场景. 通过将核心的法律条文、商业逻辑和意向协定存储在智能合约中, 可产生各种各样的去中心化应用 (DApp), 而利用前四层构建的多代理系统, 又可逐步演化出各类去中心化自治组织 (DAO, 亦称去中心化自治企业, DAC) 和去中心化自治社会 (DAS), 这些表现形式有望改进传统的商业模式和社会生产关系, 为可编程社会奠定基础, 并最终促成分布式人工智能的实现. 以 DAO 为例, 只需将组织的管理制度和规则以智能合约的形式预先编码在区块链上, 即可实现组织在无中心或权威控制干预下的自主运行. 同时, 由于 DAO 中的成员可以通过购买股份、代币 (Token), 或提供服务的形式成为股东并分享收益, DAO 被认为是一种对传统 "自顶向下" 金字塔式层级管理的颠覆性变革, 可有效降低组织的运营成本, 减少管理摩擦, 提高决策民主化.

应用层: 封装了智能合约及其表现形式的具体应用领域. 理论上, 区块链及智能合约可应用于各行各业, 金融、物联网、医疗、供应链等均是其典型应用领域. 我们将在第 3 节详细讨论.

需要特别指出的是, 由于智能合约的研究和应用尚处于早期阶段, 此处提出的智能合约架构模型是一个理想模型. 模型中部分要素 (特别是智能层中自主自治的多智能体等) 仍在探索之中, 尚未完全实现. 但考虑到他们是智能合约未来重要的发展方向, 本文仍将其纳入模型中, 以提供一定的前瞻性.

2 智能合约的研究挑战与进展

作为一种快速发展的新兴技术, 智能合约存在一些可能制约其发展的问题亟待解决. 本节将结合上节提出的智能合约基础架构模型, 从隐私、法律、安全、机制设计、性能等问题出发, 概述智能合约技术的研究挑战与最新进展.

2.1 隐私问题

根据智能合约运行机制, 智能合约的隐私问题可分为可信数据源隐私问题和合约数据隐私问题两类, 涉及到基础架构模型中的基础设施层和合约层.

区块链的匿名性并没有完全解决智能合约的隐私问题. 区块链数据通常是完全公开透明的 (尤其是对公有链), 任何人都可经由公开查询获取账户余额、交易信息和合约内容等, 以金融场景为例, 股票交易常被视为机密信息, 完全公开的股票交易智能合约将难以保证用户的隐私. Meiklejohn 等曾利用比特币找零地址推算出部分大宗客户以及这些客户间的交易行为[9], Ron 等则通过分析比特币交易图谱, 获取了某些用户行为的统计特征[10]. 另外, 某些智能合约在执行时需要向区块链系统请求查询外部可信数据源, 这些请求操作通常是公开的, 用户隐私也将因此受到威胁. 这些隐私问题可能导致攻击者对区块链或智能合约的去匿名攻击.

为此, Kosba 等提出了一个旨在保护用户隐私的智能合约开发框架 Hawk[11]. 在 Hawk 中, 所有财务交易信息不会被显式地记录在区块链上, 智能合约分为私密合约和公共合约, 私人数据和相关财务信息写入私密合约后只有合约拥有者可见. Zhang 等提出了一种可信数据输入系统 Town Crier[12], Town Crier 允许用户发送私密数据请求, 具体地, 合约在发送请求之前用 Town Crier 的公钥加密请求, Town Crier 收到请求后利用私钥解密, 从而保证区块链中其他用户无法查看请求内容.

2.2 法律问题

智能合约的法律问题主要体现在合约层中传统合约向智能合约的转化: 传统合约中法律条文 (湿代码) 和智能合约中技术规则 (干代码) 间存在巨大的语言鸿沟, 前者为了对各种无法精确预见的新案例或边缘案例实现高度的通用性, 常使用一些微妙的、模糊的和灵活的语言在更高的抽象层次起草, 而后者为了降低系统的安全风险, 须使用严格而正式的语言描述定义明确的类别、预先定义的条件和精确规定的方法, 两者在转化时将不可避免地存在翻译误差继而影响智能合约的法律效力.

常见的智能合约法律问题包括: 1) 智能合约意思表示真实性不足. 智能合约的编码偏差或立契时

的欺诈行为将导致智能合约无法反映立契者真实意愿, 我国《合同法》规定基于重大误解的合同为可撤销合同, 而智能合约一般不可撤销. 2) 智能合约存在不可预见情形. 现阶段智能合约只能处理预定义代码, 无法应对不可预料的情势变更或边缘案例. 3) 智能合约难以追责或事后救济. 智能合约具有匿名性, 立契者可能为无行为能力或限制行为能力人, 恶意合约或因编码偏差导致重大误解时, 各方责任难以界定而短时间内难以补救等. 针对这些法律问题, 更具体的法律条文表述、更全面的技术规则补充、规范的语言转化方法以及有效的合约法律审计都是可行的解决方案. 此外, 智能层构建的多代理系统中具备感知、推理、学习、决策和社交能力的软件代理也有望结合人工智能技术积累法律案例经验, 模仿现实世界的法官和律师, 应对未知场景下的辩论和审判[13].

2.3　安全问题

运维层中的安全问题是制约智能合约发展的主要问题: 已部署上链的智能合约是不可逆转的, 其潜在的安全问题一旦引发就难以被修复, 由此造成的经济损失将难以挽回, 同时, 区块链的匿名性可能为恶意用户提供便利, 继而引发现实世界的安全问题. 因此, 本文将智能合约的安全问题分为漏洞合约安全问题和恶意合约安全问题两类.

1) 漏洞合约. 设计一个安全的智能合约的难点在于所有网络参与者都可能出于自身利益攻击或欺骗智能合约, 设计者必须预见一切可能的恶意行为并设置应对措施, 而传统的程序开发人员很难具备如此完美的编程能力和缜密的经济思维.

以太坊上智能合约的 12 种安全漏洞可分为 Solidity 编程语言漏洞, EVM 虚拟机执行漏洞和区块链系统漏洞三个层次[14]. 交易顺序依赖 (Transaction ordering dependence, TOD)、时间戳依赖 (Timestamp dependence)、可重入性 (Reentrancy vulnerability) 和处理异常 (Mishandled exceptions) 是其中常见的四种漏洞, 攻击者可通过更改交易顺序、修改时间戳、调用可重入函数、触发处理异常等影响智能合约执行结果或窃取资金. 为此, Luu 等提出了一种可检查上述 4 种潜在安全漏洞的符号执行工具 Oyente[15], 经 Oyente 检查发现, 在 19 366 个以太坊智能合约中, 有 8 833 个存在上述至少一种安全漏洞.

此外, 无可信数据源和待优化智能合约也将带来一定经济损失, 攻击者可通过向合约输入虚假数据获取经济效益, 用户则需为无用代码额外付费. Chen 等提出了一个名为 Gasper 的智能合约高耗燃操作检测工具[16], 可自动发现死代码、无用描述和昂贵的循环操作等. 利用 Gasper, 他们发现在以太坊中部署的超过 80 % 的智能合约 (4 240 个智能合约) 至少存在上述一种高耗燃操作, 而这些高耗燃操作一旦被大量调用就可能引发拒绝服务攻击.

2) 恶意合约. 区块链及智能合约的去中心化、匿名性同样可能助长恶意合约的产生. 违法者可通过发布恶意的智能合约对区块链系统和用户发起攻击, 也可利用合约实现匿名的犯罪交易, 导致机密信息的泄露、密钥窃取或各种真实世界的犯罪行为. Juels 等提出了一种恶意智能合约 — PwdTheft, 用于盗取用户密码并保证立契者和违法者之间的公平交易[17]. “丝绸之路” 是一个匿名的国际线上市场, 它通常作为一个隐藏服务运作, 并使用比特币作为支付媒介[18]. 丝绸之路上销售的大部分商品都是现实世界中被控制的商品, 如毒品、枪支等. 智能合约将使这些地下市场交易更加便捷, 最终对社会造成危害.

2.4　机制设计与性能问题

除上述几种常见的研究挑战之外, 智能合约的机制设计问题和性能问题也不容忽视, 完善合理的机制设计和优秀稳定的合约性能是智能合约 “杀手级应用” 得以落地, 智能合约应用范围得以扩大, 智能合约促成的分布式人工智能和可编程社会得以实现的重要支撑.

机制设计: 机制设计理论是研究在自由选择、自愿交换、信息不完全及决策分散化的条件下, 通过设计一套机制 (规则或制度) 来达到既定目标的理论[19]. 众所周知, 非对称信息容易造成资源配置的帕累托无效率, 这是组织设计中的核心难题. 借助于机制设计理论, 设计者可以通过设计一组激励机制来减少或避免效率损失, 从而使得参与者的个体利益与组织或社会的整体利益相一致, 实现整体系统的激励相容. 对于智能合约而言, 机制设计可以决定智能合约实现其目标功能的方式, 不同的制度安排和组织结构在交易费用、激励效果和资源配置效率等方面将产生重要影响, 合理的机制设计需充分应用经济学、商学、法学等多学科交叉知识, 对合约立契者专业背景具有极高的要求, 有必要对此进行深入研究.

性能问题: 智能合约的性能问题可分为合约层设计导致的合约本身性能问题和基础设施层导致的区块链系统性能问题两类. 待优化的合约机制设计和待优化的智能合约将增加合约执行成本, 降低合约执行效率, 区块链系统本身存在的吞吐量低、交易延迟、能耗过高、容量和带宽限制等性能问题也将在一定程度上限制智能合约的性能[20]. 以区块链系统的吞吐量限制为例, 现行的区块链系统中, 智能合

约是按顺序串行执行的, 每秒可执行的合约数量非常有限且不能兼容流行的多核和集群架构, 难以满足广泛应用的需求. Dickerson 等针对此提出了一种智能合约并行执行框架[21], 允许独立非冲突的合约同时进行, 从而提高系统吞吐量, 改善智能合约执行性能.

为使行文清晰, 图 3 总结了第 2.1～2.4 节中所述智能合约研究挑战、典型问题、涉及到的模型要素和要素层次等.

2.5 智能合约的形式化验证

运维层中的形式化验证是解决智能合约安全问题的重要手段, 也是智能合约的重要研究方向. 智能合约的形式化验证是指利用精确的数学手段和强大的分析工具在合约的设计、开发、测试过程中验证智能合约是否满足公平性、正确性、可达性、有界性和无二义性等预期的关键性质, 以规范合约的生成和执行, 提高合约的可靠性和执行力, 支持规模化智能合约的高效生成[22].

智能合约的形式化验证是解决智能合约安全问题的重要思路. 在合约上链前进行形式化验证可避免一些常见的安全漏洞, 目前已有一些针对合约静态或动态分析的安全性检查工具, 如 Oyente 和 Mythril[23], 他们都是将合约字节码绘制成控制流图后分析常见的安全漏洞, 美中不足的是, 这种方式无法验证合约的功能正确性, 可检测的安全漏洞有限且可能引发错误的警报. Bhargavan 等提出了一种针对以太坊 Solidity 合约功能正确性验证框架[24], 它将 Solidity 语言和 EVM 字节码转换为 F* 语言后验证代码的各种属性, 既可排除漏洞也可计算合约消耗 Gas 限制. 类似的智能合约形式化验证工具还有 ZEUS[25]、Manticore[26]、Securify[27]、Solgraph[28] 等. 目前这些验证工具大多停留在试验阶段, 尚未在真实系统中证明其可靠性, 市场中仍亟需完备的、规范的、有指导意义的形式化验证框架, 这将促使形式化验证成为未来智能合约的重要发展方向.

3 智能合约的应用

随着区块链技术的逐渐兴起, 智能合约的应用日益广泛, 本节以金融、管理、医疗、物联网和供应链为例, 介绍其应用优势及应用方向.

3.1 金融

区块链天然的账本属性使得智能合约在金融领域有显著的技术优势: 区块链提供的点对点、去信任交易环境和强大的算力保障可简化金融交易的流程, 确保金融交易的安全, 可追溯、不可篡改、公开透明的分布式账本可便于金融机构对交易行为进行监管[29], 在此基础上, 智能合约不仅可以利用自动执行的代码封装节点复杂的金融行为以提高自动化交易水平, 而且可以将区块链上的任意资产写入代码或进行标记以创建智能资产, 实现可编程货币和可编程金融体系.

基于这些技术优势, 由高盛、摩根大通等财团组成的 R3 区块链联盟率先尝试将智能合约应用于资产清算领域, 利用智能合约在区块链平台 Corda 上进行点对点清算, 以解决传统清算方式需要涉及大

研究挑战	典型问题	涉及到的模型要素	要素层次
隐私问题	可信数据源隐私问题	预言机	基础设施层
	合约数据隐私问题	分布式账本及其关键技术	
		交互准则	合约层
法律问题	难以追责或事后救济	分布式账本及其关键技术	基础设施层
	意思表示真实性不足	法律条文/商业逻辑/意向协定、情景—应对型规则	合约层
	存在不可预见情形		
安全问题	漏洞合约	分布式账本及其关键技术	基础设施层
		开发环境	
		预言机	
		情景—应对型规则	合约层
	恶意合约	法律条文/商业逻辑/意向协定	
机制设计问题	机制设计	机制设计	运维层
性能问题	区块链性能问题	分布式账本及其关键技术	基础设施层
	待优化的智能合约	情景—应对型规则	合约层
	待优化的机制设计	机制设计	运维层

图 3 智能合约的研究挑战

Fig. 3 The research challenges of smart contracts

量机构完成复杂审批和对账所导致的效率低下问题. 目前, 已有超过 200 家银行、金融机构、监管机构和行业协会参与了 Corda 上的清算结算测试[30−31]. 此外, 智能合约也可为保险行业提供高效、安全、透明的合约保障, 提高索赔处理的速度, 降低人工处理索赔的成本. Gatteschi 等与 Bertani 等设计了一种旅行保险智能合约, 一旦合约检测到如航班延误等满足要求的赔偿条件即可自动补偿旅客[32−33]. 智能合约还可应用于电子商务, 智能合约降低了合约的签订成本, 合约双方无需支付高昂的中介费用, 且可利用智能合约自动完成交易. ECoinmerce 是一种去中心化的数字资产交易市场, 借助智能合约, 任何用户可在 ECoinmerce 上创建、购买、出售和转租他们的数字资产[34]. 类似的应用还有 Slock.it, 它允许用户基于区块链出租房地产、汽车、智能设备、路由器等有形资产, 这些资产经智能合约编码获得身份认证后即可作为智能资产直接完成复杂协议[35].

3.2 管理

传统的组织管理是自上而下的“金字塔型”架构, 容易产生机构臃肿、管理层次多、管理成本高、责任界定不明、信息传递不畅、权力集中在上层而下层自主性小、创新潜能难以有效释放等问题. 智能合约和 DAO 将对管理领域带来革命性影响. 智能合约可以将管理规则代码化, 代码设定完成后, 组织即可按照既定的规则自主运行. 组织中的每个个体, 包括决策的制定者、执行者、监督者等都可以通过持有组织的股份权益, 或提供服务的形式来成为组织的股东和参与者 (即前文所述的 DAO). DAO 使得每个个体均参与到组织的治理, 从而充分激发个体的创造性, 提高组织决策民主化. 此外, 编码在智能合约上的各项管理规则均公开透明, 也有助于杜绝各类腐败和不当行为的产生.

目前, 智能合约在管理领域的应用尚处于初级阶段, 典型应用包括业务流程管理、选举投票、存证和版权管理等. 业务流程管理是指对跨部门/组织的业务流程 (如生产流程、各类行政申请流程、财务审批流程、人事处理流程) 等进行自动化设计、执行和监控. Beck 等和 Weber 等指出, 随着区块链技术的发展, 绝大多数业务流程的控制流以及业务逻辑将会被编码为智能合约, 从而使得业务流程相关的程式/项目/运营管理等愈加去中心化和安全可信[36−37]. 在选举投票领域, 智能合约通过预先设置好的规则可以低成本、高效率地实现政治选举、企业股东投票、预测市场[38] 等应用, 同时区块链保障了投票结果的真实和不可篡改性. McCorry 等提出一种运行在以太坊上的 E-voting 智能合约实施方案[39]. Horizon State、Ropsten 等 DApp 亦支持类似应用. 在存证和版权管理领域, Rosa 等提出应用智能合约来对知识产权进行存在性证明以及著作权认证[40]. legalXchain 开发的开放式平台—IP360 数据权益保护平台可以对各类形态电子数据提供确权、云监测、区块链追踪溯源、云取证、司法通道、维权等服务[41].

3.3 医疗

医疗技术的发展高度依赖历史病例、临床试验等医疗数据的共享, 由于医疗数据不可避免地包含大量个人隐私数据, 其访问和共享一直受到严格的限制. 患者个人难以控制自己的医疗数据访问权限, 隐私性难以保证, 医疗工作者需花费大量时间精力向相关部门提交申请进行权限审查并在数据使用前完成数据校验保证可靠性, 工作效率很低, 并且存在医疗数据被篡改、泄露以及数据传输不安全等风险.

基于区块链的医疗智能合约可有效解决上述问题, 在区块链去中心化、不可篡改、可追溯的网络环境中, 医疗数据可被加密存储在区块链上, 患者对其个人数据享有完整的控制权, 通过智能合约设置访问权限, 用户可实现高效安全的点对点数据共享, 无需担心数据泄露与篡改, 数据可靠性得到充分保障. 三种较为典型的医疗智能合约有: 1) 医疗信息存储和共享, 例如, MeDShare[42] 为共享医疗数据提供溯源及审计服务, 其设计采用了智能合约和访问控制机制, 可有效追踪数据行为, 并在违规实体违反数据权限时撤销访问; MedRec[43] 是一个去中心化的电子病历管理系统 (Electronic medical records management system), 可以实现患者、卫生管理当局、医疗研究机构之间高效的数据分享. 2) 医学研究型智能合约, Kuo 等提出了名为 ModelChain 的框架[44], 该框架基于区块链进行医疗预测建模. 每个参与者都可对模型参数估计做出贡献, 而不需要透露任何私人健康信息. 3) 药品溯源及打假, 如医疗药品联盟链 MediLedger[45], 电子处方平台 BlockMedx[46] 等可用于加强对处方类药物的溯源能力.

3.4 物联网与供应链

得益于智能设备、信息技术和传感技术的快速发展, 近年来物联网技术发展迅猛, 传统的中心化互联网体系已经难以满足其发展需求. 首先, 物联网将产生海量数据, 中心化的存储方式需要投入并维护大量的基础设施, 成本高昂; 其次, 将数据汇总至单一的中心控制系统将不可避免地产生数据安全隐患, 一旦中心节点被攻击损失难以估计; 最后, 由于物联网应用将涉及诸多领域, 不同运营商、自组织网络的加入将造成多中心、多主体同时存在, 只有当各主体间存在互信环境, 物联网才可协调工作.

由此可见, 物联网与去中心化去信任的区块链

架构的结合将成为必然的发展趋势, 智能合约将在此过程中实现物联网复杂流程的自动化, 促进资源共享, 保证安全与效率, 节约成本. Dorri 等提出了一种基于区块链及智能合约的智能家居模型[47−48], 探讨了模型中的各种交互流程, 并通过仿真实验证明了此模型将显著降低物联网设备的日常管理费用. Zhang 等提出了一种物联网电子商务模型, 利用基于智能合约的点对点交易实现物联网上智能资产和付费数据的交易[49]. Zhang 等提出了基于智能合约的物联网设备访问控制模型, 该模型由多个访问控制合约、一个决策合约和一个注册合约组成, 可实现对物联网系统的分布式可信任访问控制[50]. IoTeX 则是一个以隐私为中心区块链驱动的去中心化物联网网络, 支持包括共享经济、智能家居、身份管理与供应链在内的多种物联网生态系统[51].

与物联网类似, 供应链通常包含许多利益相关者, 如生产者、加工者、批发商、零售商和消费者等, 其相关合约将涉及到复杂的多方动态协调, 可见性有限, 各方数据难以兼容, 商品跟踪成本高昂且存在盲点. 通过将产品从生产到出售的全过程写入智能合约, 供应链将具有实时可见性, 产品可追溯可验证, 欺诈和盗窃风险降低, 且运营成本低廉. 其代表性的应用有棉花供应链[52], 医疗药品供应链[53] 等.

4 智能合约的发展趋势与展望

首先在法律层面, 考虑到智能合约意思表示真实性不足、存在不可预见情形、难以追责、缺乏事后救济等法律问题, 在很长一段时间内, 智能合约将与传统合约互为补充, 协同进步: 对智能合约来说, 为充分保障其法律效力, 智能合约将逐步深入对法律法规的理解, 建立智能合约条款语言的审查和转化标准, 减少语言转化过程中的翻译误差并形成规范的合约法律审计标准; 对传统合约来说, 为应对智能合约催生的新型法律应用场景, 需对现行法律进行补充、调整, 以《民商法》、《合同法》为例, 今后需明确在何种情况下可认定智能合约由当事人意思表示一致、合意达成.

其次在性能和隐私层面, 目前智能合约受到区块链系统本身性能限制, 尚无法处理复杂逻辑和高吞吐量数据, 缺乏隐私保护, 更无法实现跨链, 第二层扩展解决方案 (Layer 2 scaling solution, Layer 2)[54] 是大幅改善区块链及智能合约性能的可行办法, 以 Taxa[55] 区块链为例, 它们的基本思路是通过可信硬件为智能合约创造隔离的链下执行环境, 公有链作为 “共识层” 记录最终的通证 (Token) 支付和合约状态转换结果, 借此将智能合约的执行与公有链的共识机制分离, 实现部分链上操作的链外管理, 促成高性能、高隐私、可跨链的智能合约.

再次在智能层面, 目前的智能合约仅是一系列的 “If-Then” 式情景−应对型规则, 并不具备真正意义上的智能性. 我们相信, 随着以深度学习、认知计算为代表的人工智能技术的发展, 未来的智能合约将具备感知、学习、推理等传统意义上智能, 即这些智能体可由 BDI (信念 Belief、愿望 Desire 和意图 Intention) 模型来表述. 更进一步, 众多智能合约智能体通过协作和演化形成复杂社会系统, 该系统具有高度的社会复杂性和工程复杂性, 因此不可避免地具有 “默顿系统” 不确定性、多样性和复杂性等特性[56]. 区块链技术有望实现软件定义的去中心化社会系统, 特别地, 可以利用智能合约将各项管理规则、奖惩标准等以程序化代码的形式部署上链, 任何组织和个体均需在既定规则下行事, 否则将会承担相应后果. 如此一来, 就有望将 “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[57].

ACP 方法 (人工社会 Artificial systems、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、完整的研究框架[58]. 我们认为, ACP 方法可以自然地与区块链及其智能合约相结合, 实现智能合约驱动的平行组织/社会管理. 首先, 区块链中的每个节点都是分布式系统中的一个自主、自治的智能体, 众多智能体将通过智能合约构成各类形态的 DApp, 形成特定组织形式的 DAO/DAC, 并最终聚合成为 DAS[59]. 其次, 智能合约的智能性使其可进行各种 “What-If” 类型的虚拟实验设计、智能推演以及结果评估, 从而观察和评估各类参数配置、功能模块和体系架构在不同实验场景下的性能表现, 并预测其演化规律[60]. 在该阶段, 平行学习[61]、知识自动化[56] 等将发挥重要作用. 最后, 区块链与物联网结合所形成的智能资产使得联通现实物理世界与虚拟网络空间成为可能, 并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. 袁勇和王飞跃提出了平行区块链的概念框架、基础理论和研究方法体系, 平行区块链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, 实现描述、预测、引导相结合的区块链系统管理与决策[62].

最后, 区块链网络上大量自治节点的自主运行以及节点间通过智能合约的互动协作, 使得该分布式系统健壮的同时兼备较高的灵活性. 譬如, 未来 DAO 中的软件代理将会在得到授权后替代人类经理人负责组织协调和业务决策, 并向其他的软件代理学习并彼此展开竞争. 一定周期后, 软件代理还会自动评估收益率并对决策做出调整. 这将有助于区块链技术适应各类复杂多变的应用场景, 进一步促

进分布式人工智能的发展, 为未来可编程社会奠定基础.

5 结论

随着区块链技术的普及和应用不断深入, 新兴的智能合约技术在学术界和产业界吸引了广泛的关注. 智能合约去中心化、去信任、自治自足、不可篡改等特性允许合约各方在无需任何信任基础或第三方可信权威的情况下完成交易, 同时, 其可嵌入的数字形式有望促成各类可编程的智能资产、系统和社会, 深入变革金融、管理、医疗、物联网等诸多传统领域. 在大量商业应用不断涌现的同时, 相关学术研究特别是基础理论研究还处于早期阶段, 行业内尚缺乏方向性研究框架和共同的话语体系. 为此, 本文对智能合约技术的运行机制、主流平台、关键技术、应用领域、研究挑战与进展进行了全面的梳理, 讨论了智能合约的发展趋势, 特别地, 我们首先归纳了智能合约的生命周期, 并以此为序首次提出了智能合约基础架构模型, 该模型自底向上分为六个层次, 充分体现了智能合约的核心研究方向. 本文研究工作以期为未来智能合约研究提供有益的启发与参考.

References

1 Szabo N. Smart contracts [Online], avaliable: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, November 5, 2018

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

3 Stark J. Making sense of blockchain smart contracts [Online], available: https://www.coindesk.com/making-sense-smart-contracts/, November 5, 2018

4 Bartoletti M, Pompianu L. An empirical analysis of smart contracts: platforms, applications, and design patterns. In: Proceedings of the International Conference on Financial Cryptography and Data Security. Springer, Cham, 2017. 494−509

5 Wood G. Ethereum: A secure decentralized generalized transaction ledger (EIP-150 revision) [Online] , avaliable: http://gavwood.com/paper.pdf, November 5, 2018

6 Wikipedia: The DAO (organization) [Online], available: https://en.wikipedia.org/wiki/The_DAO_(organization), November 5, 2018

7 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)

8 Hyperledger fabric website [Online], available: https://www.hyperledger.org/projects/fabric, November 5, 2018

9 Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker G M, et al. A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference. New York, USA: ACM, 2013. 127−140

10 Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph. In: Proceedings of the 2013 International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013. 6−24

11 Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of the 37th Symposium on Security and Privacy. New York, USA: IEEE, 2016. 839−858

12 Zhang F, Cecchetti E, Croman K, Juels A, Shi Elaine. Town crier: an authenticated data feed for smart contracts. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM, 2016. 270−282

13 Ye P J, Wang S, Wang F Y. A general cognitive architecture for agent-based modeling in artificial societies. *IEEE Transactions on Computational Social Systems*, 2018, **5**(1): 176−185

14 Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts. In: Proceedings of the 2017 International Conference on Principles of Security and Trust. Springer, Berlin, Heidelberg, 2017. 164−186

15 Luu L, Chu D H, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM, 2016. 254−269

16 Chen T, Li X Q, Luo X P, Zhang X S. Under-optimized smart contracts devour your money. In: Proceedings of the 4th International Conference on Software Analysis, Evolution and Reengineerin. New York, USA: IEEE, 2017. 442−446

17 Juels A, Kosba A, Shi E. The ring of gyges: investigating the future of criminal smart contracts. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM, 2016. 283−295

18 Christin N. Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd International Conference on World Wide Web. New York, USA: ACM, 2013. 213−224

19 Erdman A G, Sandor G N. *Mechanical Design (3rd ed): Analysis and Synthesis (Vol.1)*. Englewood Cliffs: Prentice-Hall, 1997

20 Zeng Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Scaling blockchain towards bitcoin: key technologies, constraints and related issues. *Acta Automatica Sinica*, DOI: 10.16383/j.aas.c180100
(曾帅, 袁勇, 倪晓春, 王飞跃. 面向比特币的区块链扩容: 关键技术、制约因素与衍生问题. 自动化学报, DOI: 10.16383/j.aas.c180100)

21 Dickerson T, Gazzillo P, Herlihy M, Koskinen E. Adding concurrency to smart contracts. In: Proceedings of the 2017 ACM Symposium on Principles of Distributed Computing. New York, USA: ACM, 2017. 303−312

22 Hu Kai, Bai Xiao-Min, Gao Ling-Chao, Dong Ai-Qiang. Formal verification method of smart contract. *Journal of Information Security Research*, 2016, **2**(12): 1080−1089
(胡凯, 白晓敏, 高灵超, 董爱强. 智能合约的形式化验证方法. 信息安全研究, 2016, **2**(12): 1080−1089)

23 Mythril website [Online], available: https://github.com/b-mueller/mythril/, November 5, 2018

24 Bhargavan K, Delignat-Lavaud A, Fournet C, Gollamudi A, Gonthier G, Kobeissi N, et al. Short paper: formal verification of smart contracts. In: Proceedings of the 2016 ACM Workshop on Programming Languages and 23 Analysis for Security. New York, USA: ACM, 2016. 91−96

25 Kalra S, Goel S, Dhawan M, Sharma S. Zeus: analyzing safety of smart contracts [Online], available: http://pages.cpsc.ucalgary.ca/~joel.reardon/blockchain/readings/ndss2018_09-1_Kalra_paper.pdf, November 5, 2018

26 Manticore website [Online], available: https://github.com/trailofbits/manticore, November 5, 2018

27 Tsankov P, Dan A, Cohen D D, et al. Securify: practical security analysis of smart contracts. In: Proceedings of the 25th ACM Conference on Computer and Communications Security. New York, USA: ACM, 2018. 67-82

28 Solgraph website [Online], available: https://github.com/raineorshine/solgraph, November 5, 2018

29 Qiao Hai-Shu, Xie Shan-Shan. The latest development of theoretical research on blockchain finance. *Financial Theory and Practice*, 2017, (3): 75−79
(乔海曙, 谢姗珊. 区块链金融理论研究的最新进展. 金融理论与实践, 2017, (3): 75−79)

30 Peters G W, Panayi E. *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*. Berlin: Springer International Publishing, 2016. 5−10

31 Corda website [Online], available: https://docs.corda.net/, November 5, 2018

32 Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaria V. Blockchain and smart contracts for insurance: is the technology mature enough. *Future Internet*, 2018, **10**(2): 20

33 Bertani T, Butkute K, Canessa F. Smart flight insurance−insureth [Online], available: https://mkvd.s3.amazonaws.com/apps/InsurEth.pdf, November 5, 2018

34 ECoinmerce: decentralized marketplace [Online], available: https://www.ecoinmerce.io/, November 5, 2018

35 Slock.it: enabling the economy of things [Online], available: https://slock.it/, November 5, 2018

36 Beck R, Avital M, Rossi M, Thatcher J B. Blockchain technology in business and information systems research. *Business & Information Systems Engineering*, 2017, **59**(6): 381−384

37 Weber I, Gramoli V, Ponomarev A, Staples M, Holz R, Tran A B, et al. On availability for blockchain-based systems. In: Proceedings of the International Symposium on Reliable Distributed Systems. New York, USA: IEEE, 2017. 64−73

38 Wang S, Ni X C, Yuan Y, Wang X, Ouyang L W, Wang F Y. A preliminary research of prediction markets based on blockchain powered smart contracts. In: Proceedings of the 2018 International Conference on Blockchain (Blockchain-2018. New York, USA: IEEE, 2018. 1287−1293

39 McCorry P, Shahandashti S F, Hao F. A smart contract for boardroom voting with maximum voter privacy. In: Proceedings of the 2017 International Conference on Financial Cryptography and Data Security. Springer, Cham, 2017. 357−375

40 Rosa J L, Gibovic D, Torres-Padrosa V, Maicher L, Miralles F, Fakdi A, et al. On intellectual property in online open innovation for SME by means of blockchain and smart contracts. In: Proceedings of the 3rd Annual World Open Innovation Conference. Barcelona, Spain, 2016

41 IP360 website [Online], available: https://www.ip360.net.cn/index, November 5, 2018

42 Xia Q, Sifah E B, Asamoah K O, Gao J B, Du X J, Guizani M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 2017, **5**(99): 14757−14767

43 Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. In: Proceedings of the 2nd International Conference on Open and Big Data. New York, USA: IEEE, 2016. 25−30

44 Kuo T T, Ohno-Machado L. ModelChain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *Computers and Society*, arXiv: 1802.01746

45 Mediledger website [Online],available: https://www.mediledger. com/, November 5, 2018

46 BlockMedx website [Online], available: https://blockmedx.com/en/, November 5, 2018

47 Dorri A, Kanhere S S, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: the case study of a smart home. In: Proceedings of the 2017 International Conference on Pervasive Computing and Communications Workshops. New York, USA: IEEE, 2017. 618−623

48 Dorri A, Kanhere S S, Jurdak R. Towards an optimized blockchain for IoT. In: Proceedings of the 2017 International Conference on Internet-Of-Things Design and Implementation, Pittsburgh. New York, USA: IEEE, 2017. 173−178

49 Zhang Y, Wen J T. An IoT electric business model based on the protocol of bitcoin. In: Proceedings of 18th International Conference on Intelligence in Next Generation Networks. New York, USA: IEEE, 2015. 184−191

50 Zhang Y Y, Kasahara S, Shen Y L, Jiang X H, Wan J X. Smart contract-based access control for the Internet of Things. *Cryptography and Security*, arXiv:1802.04410

51 IoTeX website [Online], available: https://iotex.io/, November 5, 2018

52 Byrne R O. How blockchain can transform the supply chain [Online], available: https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/, November 5, 2018

53 Bocek T, Rodrigues B B, Strasser T, Stiller B. Blockchains everywhere — a use-case of blockchains in the pharma supply-chain. In: Proceedings of the 2017 Symposium on Integrated Network and Service Management. New York, USA: IEEE, 2017. 772−777

54 Stark J. Making sense of ethereum′s layer2 scaling solutions: state channels, plasma, and truebit [Online], available: https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4, November 5, 2018

55 Taxa Website [Online], available: https://taxa.network/, November 5, 2018

56 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)

57 Wang Fei-Yue, Wang Xiao, Yuan Yong, Wang Tao, Lin Yi-Lun. Social computing and computational societies: the fouyndation and consequence of smart societies. *China 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)

58 Wang Fei-Yue. Artificial societies, computational experiments, and parallel systems: a discussion on computational theory of complex social-economic systems. *Complex System 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)

59 Wang F Y, Yuan Y, Wang X, Qin R. Societies 5.0: a new paradigm for computational social systems research. *IEEE Transactions on Computational Social Systems*, 2018, **5**(1): 2−8

60 Zhang J J, Wang F Y, Wang Q, Hao D, Yang X. Parallel dispatch: a new paradigm of electrical power system dispatch. *IEEE/CAA Journal of Automatica Sinica*, 2018, **5**(1): 311−319

61 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)

62 Yuan Yong, Wang Fei-Yue. Parallel blockchain: concept, methods and issues. *Acta Automatica Sinica*, 2017, **43**(10): 1703−1712
(袁勇, 王飞跃. 平行区块链: 概念、方法与内涵辨析. 自动化学报, 2017, **43**(10): 1703−1712)

欧阳丽炜 中国科学院自动化研究所硕士研究生. 2018 年于西安交通大学获得自动化专业学士学位. 主要研究方向为社会计算与区块链.
E-mail: ouyangliwei2018@ia.ac.cn
(**OUYANG Li-Wei** Master student at the Institute of Automation, Chinese Academy of Sciences. She received her bachelor degree in automation from Xi′an Jiaotong University in 2018. Her research interest covers social computing and blockchain.)

王 帅 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博士研究生. 2015 年于中国科学院大学获得控制工程专业硕士学位. 主要研究方向为社会计算, 平行管理, 区块链以及智能合约. E-mail: wangshuai2015@ia.ac.cn
(**WANG Shuai** Ph. D. candidate at The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He received his master degree in control engineering from the University of Chinese Academy of Sciences in 2015. His research interest covers social computing, parallel management, blockchain, and smart contract.)

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. 主要研究方向为社会计算, 计算广告学与区块链. 本文通信作者.
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 received his Ph. D. degree in computer software and theory from Shandong University of Science and Technology in 2008. His research interest covers social computing, computational advertising and blockchain. Corresponding author of this paper.)

倪晓春 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工程师. 2008 年于大连海事大学获得管理科学与工程专业硕士学位. 主要研究方向为社会计算与区块链.
E-mail: xiaochun.ni@ia.ac.cn
(**NI Xiao-Chun** Engineer at The State Key Laboratory for Management and Control of Complex Systems, Instituteof Automation, Chinese Academy of Sciences. He received his master degree in management science and engineering from Dalian Maritime University in 2008. His research interest covers social computing 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, 平行智能以及知识自动化.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** State specially appointed expert and director of the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. Professor 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.)