# 云际分布记账模型、机理与关键技术展望

史佩昌[1,2],王怀民[1,2],傅 翔[1,2]

(1. 国防科技大学计算机学院并行与分布处理重点实验室,湖南长沙 410073;
2. 国防科技大学计算机学院复杂系统软件工程湖南省重点实验室,湖南长沙 410073)

**摘 要:** 云际计算是支持公有云、私有云、边缘云和微云等异源异质云服务以自主对等方式纵横协作共赢的新型计算模式,可为独立云服务实体间行为交互、信任构建和贡献度量等提供防篡改、可追溯能力支持,进而最大限度削弱阻碍不同利益攸关者协作的不确定性因素. 提升云际协作意愿和效率需要基于何种机理进行何种机制创新,是云际计算成长演化中需要进一步阐述的新问题. 本文首先以基于"数字空间证据"构建或增强信任关系为设计原则,提出了基于区块链的云际分布记账软件定义模型,并系统阐述了分布记账支撑云际服务独立性、可审计性以及释放云际协作潜能的内在机理;其次,面向云际复杂交互行为,深化并固化了云际分布记账运行逻辑流程及关键环节的设计,避免其在错综复杂要素综合作用下呈现不确定冲突和矛盾;再次,针对数据要素流通及复杂异步交互场景,细化并优化了云际分布记账合约逻辑模型;最后,论述了以分布共识、智能合约等为代表的云际分布记账核心技术及相应指标的现状,并对关键技术的目标属性体系、前瞻性挑战等进行了展望.

**关键词:** 云际计算;区块链;分布记账;分布共识;智能合约

**基金项目:** 国家自然科学基金(No.61772030);之江实验室重大科研项目(No.2021PE0AC01);国防科技创新项目

**中图分类号:** TP316.4 **文献标识码:** A **文章编号:** 0372-2112(2024)01-0019-15

**电子学报 URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211007

# The Inherent Mechanism, Model and Key Technique Prospects of JointCloud Computing Distributed Ledger

SHI Pei-chang[1,2], WANG Huai-min[1,2], FU Xiang[1,2]

(1. *National Key Laboratory of Parallel and Distributed Processing, College of Computer Science, National University of Defense Technology, Changsha, Hunan* 410073, *China*;
2. *Key Laboratory of Software Engineering for Complex Systems, College of Computer Science, National University of Defense Technology, Changsha, Hunan* 410073, *China*)

**Abstract:** JointCloud Computing is a new computing paradigm that supports heterogeneous cloud services such as public cloud, private cloud, edge cloud, and micro cloud to achieve a win-win situation with the autonomous peer, cooperation way. It provides tamper-proof, traceability support for behavior interactions, trust building, and contribution measurement between independent cloud service entities, thereby minimizing the uncertainties that hinder collaboration between different stakeholders. What principles and mechanisms need to be designed to improve the willingness and efficiency of JointCloud collaboration is a new proposition that needs to be further elaborated in the evolution of JointCloud computing. Firsthy, based on the design principle of building or enhancing trust relationship on the basis of "digital space evidence", this paper proposes the software-defined model of JointCloud distributed ledger (JCDL) based on BlockChain and systematically expounds the inherent mechanism of distributed ledger supporting the JointCloud service independence, auditability and unleashing the potential of JointCloud cooperation. Secondly, facing the complex interaction in JointCloud, it deepens and solidifies the design of the logical process and key aspects of the JCDL operation, so as to avoid the uncertain conflicts and contradictions under the comprehensive action of complicated elements. Thirdly, the logical model of JCDL contract is refined and optimized for the scenario of data asset flow and complex asynchronous interaction. Finally, the paper discusses the core technologies and corresponding indicators of JCDL represented by distributed consensus and smart contract and

收稿日期:2021-07-30;修回日期:2022-03-14;责任编辑:王天慧

looks forward to the target attribute system and forward-looking challenges of key techniques.

Key words: JointCloud computing; BlockChain; distributed ledger; distributed consensus; smart contract

Foundation Item(s): National Natural Science Foundation of China (No.61772030); Major Scientific Research Project of Zhejiang Lab (No.2021PE0AC01); GF Innovative Research Program

## 1 引言

云际计算[1,2]是支持公有云、私有云、边缘云和微云等异源异质云服务以自主对等方式纵横协作共赢的新型计算模式,可为独立云服务实体间行为交互、信任构建和贡献度量等提供防篡改、可追溯能力支持,进而最大限度削弱阻碍不同利益攸关者协作的不确定性因素.追求边际效用与成本的平衡,实现计算、存储和网络等云基础设施资源以及云上软件和数据等资源的互联互通、互操作及磋商协作,最大化挖掘已有资源潜能,是分散、对等和独立云服务提供者(Cloud Service Provider,CSP)及数据服务提供者(Data Service Provider,DSP)的理性选择.为降低供给侧和需求侧对等协作的信息不对称程度,以云际互联、云际存储和跨云计算等为核心关键技术,以分布云交易、分布云社区和分布云监管等为核心功能组成的云际协作环境[2],为上述多类型资源价值释放提供了基础支撑.为确保上述各类支撑服务的独立性、可信性及可审计性,基于区块链[3]的云际分布记账基础设施通过构建诸要素交互行为的"数字空间证据",并借助多次非合作博弈前提下的连续交易约束[4],可最大限度缓解信任随距离增大而不断衰减的趋势.本质上,云际分布记账将跨利益主体交互行为序列沉淀为不可篡改、可追溯和可审计的"数字空间证据"."数据空间证据"和连续交易约束,是多利益主体在非合作重复博弈前提下,达成合作"纳什均衡"的有力保证.在二者综合作用下,协作各方无论持有何种主观动机,客观行为都会更加理性、合规.从某种程度而言,协作各方之间由此构建了可靠的信任关系或已有的信任基础得到增强,进而云际协作意愿和效率预期可得到较大提升.

以云际分布记账上述功能及类似功能为基础的应用,主要有金融领域较为成熟的加密货币[3,5],以及云际计算领域正在探索的计算外包[6]、协作流程管理[7]、数字证据管理[8]、磋商博弈[2]和异步协同[9]等.计算外包应用面临的挑战即汇聚共享的云际计算[1,2]资源池通常不会由单个CSP提供、控制和管理.如何保护云服务消费者(Cloud Service Consumer,CSC)数据机密性和外包计算完整性,如何在不依赖可信第三方前提下便捷完成CSC支付和CSP服务提供之间的可信交互等,成为新约束下的现实难题.该方面的代表性探索:(1)CSP提供基于Intel SGX的可信执行环境,CSC将应用部署于多来源CSP的enclave实例中,确保CSC数据及状态的不可见[6];(2)同时引入基于区块链的支付通道技术[5],在每个enclave实例中部署准确计量计费的合约程序[6,10],确保支付过程的可信性及自动化;(3)引入代理角色[11],负责汇聚供给侧和需求侧的信息[6],并提供磋商协作支撑机制,例如云际竞价拍卖、云际智能推荐[2]等.协作流程管理应用面临的挑战:全球地理分布的协作主体(例如参与云际协作的CSP和DSP等),缺乏天然互信关系,缺少执行跨域协调、仲裁等职能的中心化组织结构.该方面的代表性探索:分析论证利用区块链解决该类问题的优势与挑战[11];考虑利用分布身份管理和访问控制机制,以动态和分布的方式解决云计算实体管理问题[12];考虑对协作业务流程进行软件定义和编程,将其实例作为智能合约运行[13]以提高效率和可信性.数字证据管理旨在利用哈希链等技术形成具有准确性、可靠性和权威性等特点[14]的防篡改记录.该方面的代表性探索:利用智能合约技术支持云平台中服务计量、验证、SLA违约处理、计费和仲裁[15]等.磋商博弈的挑战在于中心化系统存在欺骗和泄露风险,云际协作环境中竞价、谈判等功能[2]需要具有隐私保护、公平博弈等能力.该方面的技术路线考虑:基于智能合约和零知识证明[16]等构建防价格泄露[17]和可信交互的公平、良性磋商框架.异步协同是指为了不影响公有云、私有云、边缘云和微云等多类型利益主体协作进程,解决分布时钟难以达成一致前提下的异步协作难题.该方面的代表性研究主要集中在公平、高效和异步共识算法[9]的探索方面,与应用场景结合的异步协作模型研究尚处于起步阶段.

综上所述,云际分布记账面临的需求及挑战,从技术层面可概括为如下两个方面.

(1)非异步确定性云际协作场景的磋商协作问题.非异步是指某轮次协同的网络消息传递有明确延迟上界约束,或在延迟有保证但延迟时长不确定时,网络消息延迟的增长速度不会无限超过时间流逝的速度[18,19],即存在上界但未被事先知道[20].确定性是指每一个可信的进程都会在确定的轮次内输出结果[21].该类场景的代表性应用包括基础设施资源、平台资源、软件资源、进程、负载和数据的跨云磋商、互操作和迁移等.该类场景面临的挑战:基于以Hyperledger等为代表的联盟链技术,在提升效率、降低延时、增强安全性等

方面尚未形成面向多样化、异质需求的特定模型机理、先进技术和方法.

(2)异步非确定性云际协作场景的磋商协作问题. 异步是指除了网络消息的最终交付外,对网络消息延迟没有保证,流程的协同完全由消息传递事件驱动[18,19]. 非确定性是指在$r$轮($r$有可能增长至无穷大)后,非错误过程的未确定的概率趋近于零[21]. 该类场景的代表性应用包括万物互联跨域协同计算的互操作及磋商协作等. 该类场景面临的挑战:基于以 Hashgraph[9]等为代表的公平、高效共识技术,尚未形成面向新型协作需求,具有灵活性、适应性的软件定义模型、支撑技术和核心算法.

本文的内容组织如下:第 2 节给出云际分布记账的软件定义模型,以及内在运行机理;第 3 节分别提出了基于链结构的非异步确定性和基于图结构的异步非确定性云际分布记账运行态逻辑架构;第 4 节以云际数据非异步确定性可信流通以及云际数据异步非确定性可信协作为研究案例,系统阐述了两类软件定义模型;第 5 节系统梳理了相关研究进展、技术指标体系及先进技术指标(指标量化的国际领先值域),并提出了云际分布记账模型的理想目标属性;第 6 节总结全文.

## 2　云际分布记账的软件定义模型

云际协作对象可概括为以计算、存储和网络为代表的基础设施层资源,以开发和部署环境为代表的平台层资源,以托管管理和按需定制为代表的软件层资源,以平台运行、业务行为和用户信息为代表的数据资源等;协作粒度可分为虚拟机、容器、接口函数及运行态进程等. 云际分布记账重点聚焦于:在不依赖可信第三方的前提下对云际协作对象的贡献行为形成准确、防篡改和可追溯记录,并基于此进行价值转化. 本节将重点阐述基于何种机理构建何种云际分布记账模型.

### 2.1　云际分布记账的软件定义模型

当前,在云计算市场中占据主导地位的公有云,本质上是以单个 CSP 为核心的中心化服务模式. 云际计算则强调将现有模式引向开放合作、分布协作的新模式,以追求边际效用与成本的平衡,进而达成社会效益最大化. 然而,跨不同利益主体的云际协作,实质上是一种由多个具有对等地位的利益共同体形成的新型生产关系. 在多方(例如 CSP, CSC, DSP 等)对等协作过程中,云际分布记账基础设施需要提供规则公开透明、行为理性规范、贡献度量科学和价值回报公平等支撑. 云际分布记账借助区块链技术打通云际协作诸要素,进行各层次、各类型服务连接,提升协同效率,降低成本和风险. 以达成上述功能需求为目标导向的云际分布记账软件定义模型如图 1 所示.

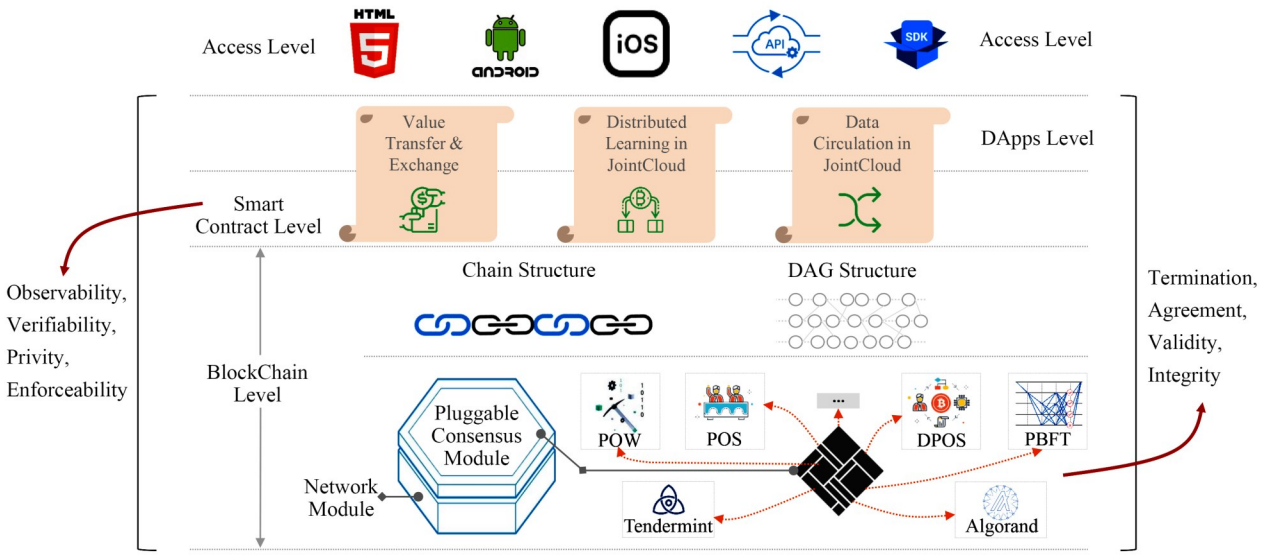


图 1　软件定义的云际分布记账基础设施模型

云际分布记账的软件定义模型如图 1 所示,从上往下可分为四个层次:访问层(Access Level)、分布式应用层(Distributed Applications Level, DApps Level)、合约层(Smart Contract Level)和区链层(BlockChain Level). 为确保支持用户多样化使用模式,访问层提供以 Web 形态为主的浏览器和服务器架构模式、以 Android 和

IOS为代表的移动应用模式、面向用户自主定制开发的应用程序接口(Application Programming Interface,API)模式和软件开发工具(Software Development Kit,SDK)模式;与用户业务紧密相关的少量、特定事务逻辑在前端实现;可平台化的通用事务逻辑在服务端实现.分布式应用层又称去中心化应用层,支持大量基于云际定制化区块链技术、共识算法和智能合约的去中心化应用开发及部署运行,确保数据、通证(Token)在应用自治的全生命周期各个关键环节流转过程中均能得到有效确认及安全防护,同时支持DApps认证流程或协作关系便捷变更,降低相应的开发和运维成本.合约层支持云际生态利益相关者以软件定义方式表达各种合约约束条件,例如价格、支付、SLA、机密性以及执行等,合约的输入、执行和输出均在链上进行以便最大限度减少恶意或偶发异常.此外,通过个体自主、多方见证方式自动执行,减少对可信第三方的依赖,提高群体自治水平,提升协作效率.云际分布记账合约遵循四个属性:可观察性(Observability),即支持云际合约相关方相互观察对方进而证明自身履行合约的能力;可验证性(Verifiability),即云际合约的履行或违约均可被主动验证或被动识别;可保密性(Privity),即云际合约的内容及执行可完全透明公开,也可明确限制合约履行相关范围,对于非相关第三方合约具备高度保密能力;强执行性(Enforceability),即信誉、内在激励机制、自执行性以及可验证性等支持云际合约在满足约束条件下的自动甚至强制执行的能力.链层,主要包括数据组织结构、共识模块和网络传播模块等.云际分布记账支持链式结构,例如Ethereum[5,22]和Hyperledger fabric[23]等,以及有向无环图(Directed Acyclic Graph,DAG)结构,例如Hashgraph[9]等.

链式结构中数据区块以首尾相连方式按照时间顺序进行组合,利用基于时序关系的区块验证和存储数据,利用分布共识生成和更新数据,利用密码学保证数据传输安全和受控访问,利用智能合约编程和操作数据.DAG结构与链式结构不同:前者数据组织的单元是仅涉及单个用户的单个或多个事务,后者数据组织的单元是涉及多个用户多个事务的区块.DAG数据单元间通过引用关系链接起来,从而形成具有半序关系的有向无环图.与区块链同步验证的特点相比,DAG可以异步并发写入事务,支持过程异步、结果同步,这使其天然具备更快捷、更高效的潜质.共识模块支持以工作量证明(Proof of Work,PoW)[3]、权益证明(Proof Of Stake,POS)[24]、委托权益证明(Delegated Proof Of Stake,DPOS)[25]、实用拜占庭容错(Practical Byzantine Fault Tolerance,PBFT)[26]、Tendermint[27]、Algorand[28]等为代表的共识算法可插拔,支持面向不同场景、不同数据组织结构进行共识定制及再设计.网络模块支持Gossip和Gossip about Gossip[9]等主流协议.其中拜占庭容错类共识需要满足:“每个非故障进程必形成一个输出”的可终止性(Termination);“所有非故障进程最终会形成相同输出”的一致性(Agreement);“每个进程始于相同输入必然得到相同输出”的正确性(Validity);“每个非故障进程共识结果的输入必然来自某一个非故障进程”的完整性(Integrity).

### 2.2 云际分布记账模型的内在机理

基于区块链构建云际分布记账模型,支持云际协作环境核心服务独立性、可信性的背后机理可从技术特性和功能效用两个角度来阐述.就技术特性而言,区块链是由大规模分布节点共同持有、维护的去中心化账本,账本由一系列包含若干事务信息的数据区块首尾相连而成.纵向来看每一个区块均包含前一个区块信息的哈希,横向来看每一个区块均被大量全球分布节点持有.因此,从功能效用的角度来看,删除或者篡改区块的难度非常大,区块链可追溯、防篡改的技术特性正是由此而来.运行于区块链之上的智能合约是一种在不依赖可信第三方的前提下,以数字方式促进、查证或加强合约磋商或履约的自动化协议,执行结果可追踪且不可逆转.可观察性、可验证性、可保密性和强执行性等是智能合约技术的典型特征.云际分布记账模型继承了原教旨主义的区块链和智能合约思维,这也是其面向多样化需求进行精巧组合设计及技术创新突破的力量源泉之所在.

本质而言,云际分布记账是支持分散对等的云际协作主体之间就共同关注的数字证据达成共识,以多中心、防篡改、可追溯方式在数字空间形成云际协作前、过程中及协作后的行为证据,进而推动云际生态规范、有序的分布式存证机制.云际分布记账模型主要改变了证据在数字空间的形成和记录方式.这一改变如何确保云际协作环境核心服务的独立性和可信性,蕴含其中的内在机理是什么?从博弈论的角度出发,也许可以给出合理的解释.云际协作诸要素交互行为的数字空间证据,使云际协作的连续博弈过程由一次性博弈转为了无限次或有限多次重复博弈.对于一次性博弈而言,互不合作是唯一的均衡,这种均衡结果由于缺少针对负反馈的惩罚,使不愿合作的参与者可以通过连续与不同对象的一次性博弈而获利,天然缺少互信的云际协作各方很难以可持续方式协作,进一步导致云际生态难以避免朝着恶性、无序方向衰退.对于无限次或有限多次重复博弈,Folk Theorem[4]认为博弈者之间总有可能达成合作均衡,这种均衡结果相当于增加了针对正反馈的奖励,而基于区块链的数字空间证据存证恰好可以实现这种正反馈,使云际

协作各方进行互动时会采取理性策略,拒绝在未来与不愿合作的人进行交互,从而切断了对方通过持续互动而获利的可能性. 只有有合作意愿的参与者,才有机会通过连续博弈获利,这有利于云际生态朝着良性、健康方向成长演化. 同时数字空间证据的构建是不依赖可信第三方的,因此"不依赖可信第三方是不可能达成公平交易的"[29,30]这一困境有望得到缓解,云际数字资产交付与加密货币支付的对等公平交易[31~33]有望达成. 并且,云际协作环境[1,2]中还加入了信誉因素,这意味着加重了对不合作行为的惩罚,强化了对合作行为的奖励. 换言之,云际协作各方由此构建了可靠的信任关系或已有的信任基础得到增强. 由此可见,基于云际分布记账模型形成数字空间证据,有利于推动云际生态朝着规范、有序方向发展.

综上所述,从技术特性视角看,基于数字空间证据和连续交易约束,利于促成云际生态中天然缺乏信任关系的不同利益相关方达成协作. 在功能效用方面,从广义拓展的角度看,云际分布记账可应用于数字金融、物联网、供应链管理和数字资产交易等领域. 上述领域的共同特征是不依赖中心层级结构的分布自治组织. 围绕分布自治组织的构建、运行和维护等方面,云际分布记账有利于促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系,保障数字生产要素在自治组织内部有序高效流动. 应用于分布自组织的云际分布记账在核心理念方面超越了狭义、经典的内涵及边界:(1)分布自治组织中的共识已经不再局限于语义无关的副本一致,而是拓展为主观的多值共识,即不同利益群体按照一定的治理结构和目标原则,就不同意见快速折中调和并收敛至意见一致,进而达成对自治组织群体成员有普遍约束的群体决策共识;(2)从链内治理向链外治理拓展,由数字世界基于分布共识的去信任化和智能合约的自动执行,转变为物理世界通过重复博弈构建信任并结合声誉、法律形成更强有力治理约束,克服人的有限理性和契约的不完备性;(3)在保障安全性和便利性的前提下,实现高效的帕累托最佳资源配置和新型生产关系构建,支持数据归属权确认、隐私保护及价值传递;(4)以低成本、高效率实现自证逻辑回归,构建支持数据可信、物权可信、合约可信及法人实体可信等的科学、公平与高效信任体系,利于形成以信用为基础的分布自治机制、流程甚至制度安排;(5)通过分散决策产生激励相容、结果均衡的规则或算法,以智能合约实现协作规则的差异化和可信化,以去中心化、信息共享、共识的新组织形式,支持网络中多节点间博弈,实现更大范围和更深层次的复杂交易.

## 3　云际分布记账运行态逻辑架构

云际分布记账通过提供价值交换、留痕存证、权益确认和品质彰显[34]等功能,支持云际资源发挥交换效用进而更多地释放其固有的使用价值,支持一切云际协作行为有"痕"可循、有"证"可查进而赋予云际生态可监管仲裁的能力,支持所有权、使用权和收益权的高效确认进而降低云际生态协作成本,支持以低成本、高效率方式彰显云际服务的高品质进而避免"劣币驱逐良币"并确保云际生态秩序的良性构建. 云际分布记账对云际生态秩序的构建具有十分积极的支撑意义. 为了降低云际分布记账在综合因素作用下可能呈现的急剧变化或不确定性,本节从运行态视角对云际分布记账的逻辑功能、边界和约束进行明确细致的阐述.

### 3.1　云际链式分布记账运行逻辑

云际链式分布记账是指底层采用类似于比特币[3]、以太坊[5,22]、Hyperledger Fabric[23]等为代表的链式结构技术体制. 从事务操作处理的视角来看,此类技术的特点:将单位时间内发生的所有事务汇聚成一个区块单元;后一个区块头部包含前一个区块哈希,前后区块之间形成一个基于哈希的强依赖关系;前一个区块被一定程度确认后,进行下一个区块的操作. 这里的确认意指相对意义下的"确定",即每一个区块都会在一个预定的轮次$r$之后达成一个确定性、难以被推翻的状态,这也是经典意义下有关"同步"[19]和"确定性"[21]概念内涵的同向拓展延伸. 因此,同步确定性也成了云际链式分布记账的一个代表性特征. 图2选取Hyperledger Fabric为底层支撑,构建了基于链结构的同步确定性分布记账模型. Fabric除了最初版本之外,近期版本均无拜占庭容错能力,因此仅适用于具有特定约束下联盟内部交互的场景,未来将选用具有拜占庭容错能力的联盟链作为底层支撑. 该类模型主要用于满足云际计算场景中确定性价值交换记录一类的应用需求. 由于云际计算是某种面向全球协同形式的云联盟,其生态系统中交易支付活动表现出了支付数量的大规模性、支付频率的不规律性和参与者身份的不对等性等特征. 大规模性是指从云际生态系统视角看,其涉及的交易支付活动远比当前任何单个云平台的规模都要大的多;不规律性是指交易支付频率波动性强,存在交易支付活动随云交易爆发而瞬间激增的现象;不对等性则指云际支付中部分CSP的节点联接度远大于其他CSP和CSC节点的联接度,容易出现中心化节点.

基于链结构的同步确定性分布记账模型如图2所示,其运行态逻辑主要从开发、部署和运行等三个阶段展开论述. 在开发阶段(Development Phase),用户根据需求撰写智能合约(Contract Coding),并在链下达成共识方式(Consensus Off-Chain)的支撑下编译成二进制字

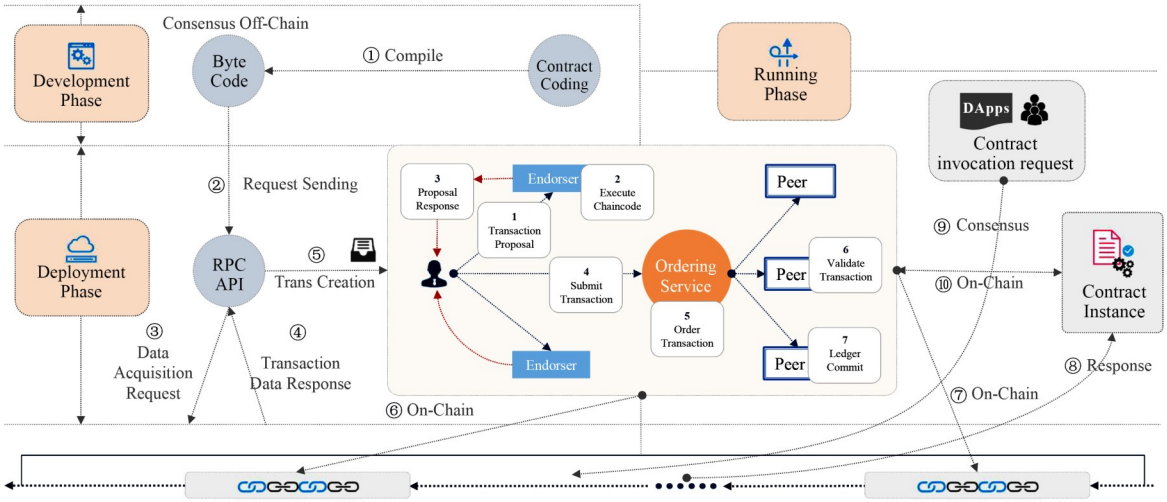


图2 基于链结构的同步确定性分布记账模型

节码，为部署阶段合约上链提供基础支持．在部署阶段(Deployment Phase)，用户首先通过远程过程调用(Remote Procedure Call，RPC)方式调用API，将智能合约以创建事务的方式完成上链部署．创建事务(部署合约)请求发出后(Request Sending)，首先从链上获取合约拟部署的区块高度、合约地址等信息(Transaction Data Response)，然后使用合约发布节点的地址或指定地址对合约进行签名，之后再将被签名事务(部署合约)通过Hyperledger Fabric共识过程后部署于区块链上．执行阶段(Running Phase)，智能合约共识上链后，分布式应用程序DApps可以通过合约地址和合约接口，例如变量、事件和调用方法(Contract invocation request)等实例化并执行合约(Contract Instance)，合约执行结果以事务创建方式通过Hyperledger Fabric共识过程后部署上链．该模型中Hyperledger Fabric共识过程贯穿于部署和运行两个阶段．共识过程中首先对用户创建的事务提议进行背书(Endorser)，即背书节点通过执行链码对事务的合法性进行验证并反馈响应．然后经过背书的事务提交至排序服务(Ordering Service)，排序服务节点负责确认事务之间的时序关系，并把排序后的事务打包成区块广播给通道中的成员(Peer)；最后，排序后的事务需要进行一系列包括事务数据完整性、是否重复、背书签名是否符合背书策略以及多版本并发控制[23]等的校验(Validate Transaction)，通过所有检验后将被标注为合法并写入账本(Ledger Commit)，确保多节点状态始终保持一致．

### 3.2 云际图式分布记账运行逻辑

基于图结构区块链技术的诞生，源于链结构区块链存在效率低、能耗高等问题．链结构的典型代表比特币约每十分钟出一个区块，受限于单个区块容量的上限，比特币的性能吞吐大约为7笔/s，区块中任一笔交易需要大约六个区块后才能被确认．比特币中的确认还不是理论概念下的最终确认，与以太坊相似存在51%算力攻击问题，即如果某群体控制51%以上的算力，经历六个区块后的确认区块依然存在被颠覆的风险．此外，比特币挖矿所需能耗非常高，甚至可能会超过全球电力总消耗．比特币正是以牺牲能耗换取安全．这会导致以挖矿模式为前提，拓展链结构的区块链技术在各行各业的推广应用必然面临能源瓶颈问题．考虑到链结构中区块打包无法并行执行并且挖矿引起的能耗开销过高，图结构将区块的链式存储结构转变为网状拓扑结构，使事务上链的操作可以并发执行，并且达成共识的过程无需以高能耗为前提的挖矿方式．图结构的典型代表是基于DAG的HashGraph[9]，其以单个事件(可包含单个节点的多笔交易)作为处理单元，支持异步并发写入事务，将链结构的“最长链共识”改为“最重链共识”．该语境下的异步与经典意义下的“异步”[19]内涵相近，即同一分支上的事务无需达到最终确认状态，即可进行下一个事务的处理．链结构中新发布的事务会加入到最长链，依次无限蔓延．而图结构中，每个新事务单元会主动同时链接到前面两个位于不同分支(其一为自己所在的分支)的有效单元，同时验证并确认各个单元的父单元以及父单元的父单元，依次迭代至创世单元．随着时间的推移，所有事务相互连接形成图状结构，事务的状态被延迟确认．该语境下的“非确定”即指“延迟确认”，这与经典意义下“概率性确认”[21]概念内涵略相近，即当$r$趋于无穷时，非错进程在$r$轮之后不确定的概率接近于零．该模式相对而言，复杂度更高，但被篡改的难度也更大．

基于图结构的异步非确定性分布记账模型如图3所示，其运行态逻辑主要围绕智能合约的生命周期展开论述，该方法的可终止性、正确性和安全性等均建立

在HashGraph[9]尚不完备但极具创新提升空间的理论基础上. 编程后的合约以事件C1的形式封装,包括时间戳、合约信息、指向所在分支的父指针及其他分支的父指针等. 随着时间的推移及其他事件的生成和传播,合约进入投票阶段(Voting Stage). 在投票阶段,如某些事件有路径可达事件C1,例如D4经B2可达C1,则称事件D4可见事件C1. 如图3所示,事件D2,D3,D4,C3,C4,B2,B3,A5等均可见事件C1. 以事件A5为例,A5到达C1的所有可达路径中,如果经过了A,B,C,D四个节点中的绝对多数节点(即不小于2/3)时,则称A5强可见C1. 当一个事件强可见绝对多数节点上的先前事件时(假设A5和A9均具备条件),则称事件A5,A9分别为新轮次(图3中第$R$,$R+1$轮)的第一个事件. 每一轮次的第一个事件即为该轮次见证人,例如,第$R$轮的A5,B5,C5,D5,第$R+1$轮的A9,B9,C10,D9. 当第$R$轮的见证人事件(例如A5,B5,C5,D5)均可被第$R+1$轮超过2/3即绝对多数见证人(例如A9,B9,C10,D9)可见时,则称该见证人为知名见证人. 假设第$R$轮中,事件C1对知名见证人A5,B5,C5,D5的全部或绝大多数可见,则事件C1达到了最终确认状态(Committing Stage). 第$R$轮知名见证人对事件C1的可见情况,需要第$R+1$轮的见证人进行统计(如图3所示,该阶段即为确认阶段). 因此,从时间维度看,事件C1需要经历投票和计票两个阶段后才有可能达成最终确认状态. 达成确认状态后的合约事件C1即具备了被调用、实例化及运行(Committed SC Instance)的条件.

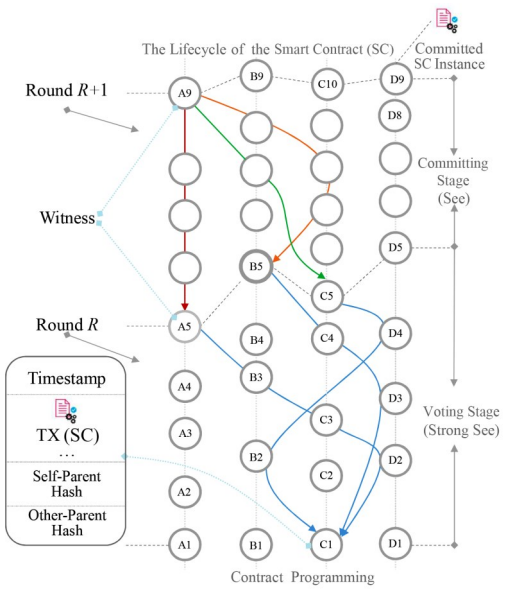


图3　基于图结构的异步非确定性分布记账模型

## 4　云际分布记账场景案例

云际分布记账模型在云计算和大数据领域的应用本质是:云际生态参与者如何在数字空间形成云基础设施资源协作和云上数据资源交互的行为证据. 准确而言,云际分布记账起源于计算、存储和网络资源交换行为的数字空间存证,发展于云际生态参与者协作交互行为的数字存证,实现云上数据流通与协作的复杂事务逻辑. 后者的复杂度及价值空间远大于前者. 因此,本文主要选取两类场景案例,剖析云际分布记账在两大垂直细分领域的运用逻辑和应用价值.

### 4.1　基于链结构的云际数据流通合约模型

在经典烟囱式信息系统建设模式下,独立服务实体自建信息系统的同时形成了大量内部数据孤岛,内外部数据的多样化互通需求面临复杂挑战. 随着以云际为代表的多云环境的出现,基础设施从自建服务器逐渐演变成"云"或"多云",例如,93%的服务实体采用多云策略平均使用2.2个公有云和2.2个私有云[35],以避免云平台锁定. 多云策略使服务实体的底层架构变得更加灵活,上层应用及数据需要具备不受限于位置、环境(是否跨云)和软硬件异构性的互联、互通和互操作能力[36],例如,41%的应用在云间集成数据[35]. 然而如何支持上层应用的快速连接、迁移和集成,特别是,如何支持上层数据快速流通、融合进而支持数据价值的持续积累和释放,已经成为关系到云际生态发展的挑战性问题. 数据是数字智能经济的"石油""燃料"和"基石". 数据的价值不仅在于单来源数据的数量和质量,更在于如何有效释放多来源融合数据的能量. 数据价值释放的本质在于多来源、多类型和多维度数据的融合,即把原本各自孤立的数据通过软件定义方式标识化、目录化,构建法律意义下数据归属权确认,技术层面数据稀缺性保证,交换流通安全及收益分红反馈等数据资产化支撑机制,深层次挖掘数据发展生产力并改善生产关系的战略价值.

云际数据资产化流通重点提供数据可信汇聚、存储和交换平台支撑,支持数据生产、建设和运营主体"敢于共享""易于共享"进而"乐于共享". 为此,本文提出一种基于链结构的云际数据流通合约模型(如图4所示),可为数据可信流通交换的数据服务协作环境提供运行支撑. 在数据服务协作环境中:(1)海量复杂的标识化数据汇聚形成数据目录,并辅以数据示例、用途、格式、定价、流通模式和SLA条款等说明;(2)提供不依赖可信第三方情况下从法律意义上明确数据归属的功能支持,并确保数据所有权鉴定过程中数据隐私不泄露;(3)为数据服务消费侧(Data Service Consumer, DSC)提供按照数据用途、数据价格和质量评价等维度的查询筛选功能;(4)为打破数据服务供需双方信息不对称,提供以综合推荐、竞价拍卖等为代表的双边多轮

磋商[37]机制;(5)利用区块链“数字空间存证”特性,实现对交易承诺、API调用、数据归属以及收益分红等行为的防篡改和可追溯记录,提供数据服务供需双方公平交换能力[29~31,33]支撑;(6)利用分布密钥管理机制、基于角色的访问控制、多重加密、安全外包计算、可信计算环境(Trust Execution Environment,TEE)与非可信GPU协同可信计算等技术实现兼顾DSP侧数据安全防护与DSC侧算法引擎、计算结果保护的流式数据流通共享;(7)构建基于API调用或DSC非首次数据价值创造的流式分红反馈机制,激励数据所有者动态、持续释放最新数据价值. 基于链结构的云际数据流通合约模型,支持数据服务协作环境提供标识化脱敏样本数据及基于TEE和GPU的多来源样本数据融合计算场景,进而支持DSC根据数据运算结果开发消费侧智能合约. 该合约模型同时支持DSP侧以智能合约的形式表达其对所持有数据的使用条款. DSC和DSP两侧合约上链的过程将遵循图2中的逻辑. 供需两侧合约将以分布方式进行部署,支持数据在DSP侧的可信计算环境中进行运算,确保数据对于DSC而言“可用无需见”,破解数据价值释放中存在的“可见不可用”或“可用需可见”等现实困境. DSP侧完成计算的中间结果在经过DSP审查后,可汇聚至某可信计算沙箱中,同时可根据需要提供基于角色的访问控制(Role-Based Access Control,RBAC)策略,进一步赋予供需多方对汇聚计算结果同时封存和同时开封的能力. 以智能合约形式存在的消费侧算法引擎对DSC的重要性如同数据之于DSP,都是核心战略资源. 如果DSC需要提升其算法引擎的保密性,可以在DSP侧“可信TEE和非可信GPU进行可信协同计算”的环境中使用RBAC策略,确保无DSC许可或在场情况下DSP无法复制算法引擎,进而一定程度上确保算法引擎在数字空间的稀缺性. 可信计算沙箱中的结果以API形式对外开放,支持供需多方对其进行结果审查和多来源数据的贡献度量,为DSC向DSP进行差异化收益分红提供支撑. 为满足数据流式流通和持续分红,图4中结果汇聚过程、结果审查和贡献量化过程、收益反馈过程将循环执行,直至整个流式流通过程结束. 流式流通过程结束后,支持对包含数据结果及算法引擎可信计算沙箱进行销毁. 上述所有环节的交互行为均遵循图2中的上链执行逻辑,以便在数字空间形成完整的交互行为记录.

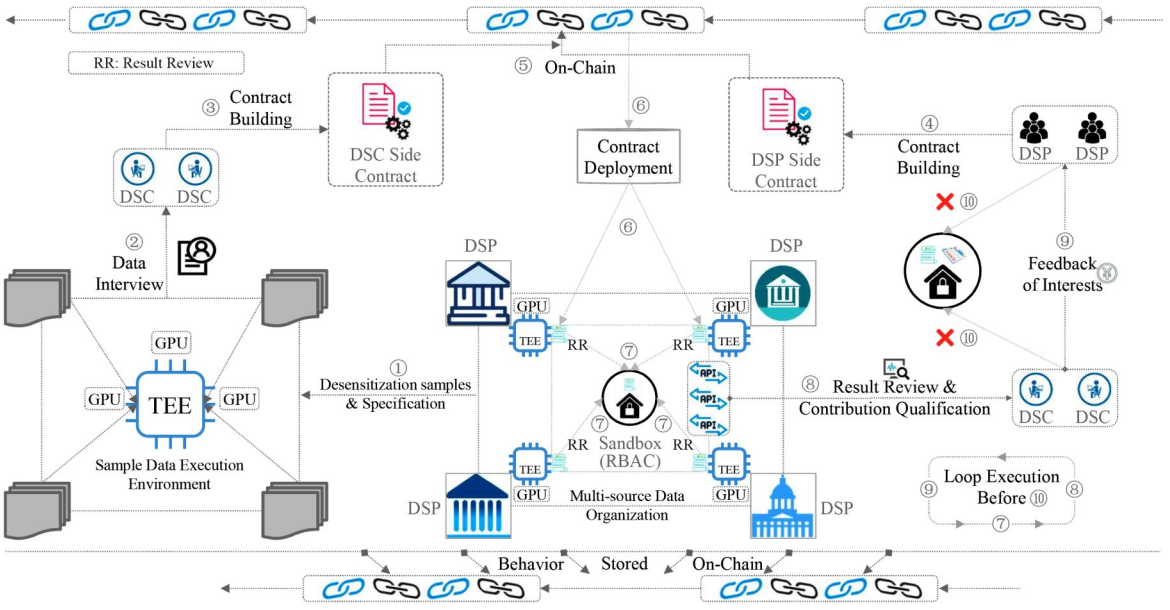


图4 基于链结构的云际数据流通合约模型

## 4.2 基于图结构的云际数据协作合约模型

在未来万物互联的大规模人机协同场景中,采用中心化机构建立信任,以宏观方式控制多层次细粒度交互,从成本和效率角度而言难以满足现实需求. 探索不完全依赖中心化机构的微观自治模式,是辅助宏观控制方式解决上述规模化、复杂化协同挑战的可行途径. 区块链技术具备提供不依赖中心化机构建立信任,进而支持微观自治的能力. 然而,链结构的区块链技术在性能吞吐和能耗开销等方面的局限,使具有更公平、更高效及异步拜占庭容错能力的图结构区块链技术成为解决上述挑战的可行候选. 然而这并不代表链式结构的区块链能够被图结构的区块链所替代. 在不同的场景需求下,不同数据结构的区块链具有不同的特征. 通常来讲,图结构的区块链往往需要固定全节点的数量,因此,链式结构相比图结构更加适用于相对开放的公有链场景,且通常所需的存储资源会更小. 基于图结

构的云际数据协作合约模型如图5所示,它填补了原生图结构区块链技术与应用场景需求之间的技术鸿沟.万物互联涉及不同领域、不同运营商和自组织网络利益主体之间的连接协作,多中心、多主体之间的协作交互关系在市场"无形之手"作用下必然演绎出复杂、异步交互行为逻辑.在万物互联场景中大规模利益主体之间的复杂、异步交互行为,是通过数据的连接和流通驱动完成的.复杂、异步交互行为的动态与不确定性直接决定了数据在时空维度流通与共识的范畴.这对以共识为基础构建万物互联场景下的信任基石,提出了新的技术需求:支持以软件定义的方式对共识范围进行按需定制与动态调整;支持物理世界异步协作方式引发的共识确认程度可查、可变焦.

基于图结构的云际数据协作合约模型如图5所示.任一条数据均被封装为一个事件,包含时间戳、事务数据、指向所在分支的父指针及其他分支的父指针.该数据事件将在协作行为逻辑的驱动下,在特定范围内传播,例如,扮演数据提供者角色的节点C发起数据事件C1,并指定其在扮演数据消费者角色的A,B和D节点间流通共享.由于图结构的云际分布记账采用Gossip通信协议,因此,数据将借助分布身份标识(Decentralized Identity,DID)和加密技术构筑数据流通特定空间.事务数据的组织格式如图5所示:根据公式 $TX[Data_i]=<<\tau_{c'}.[A,B,D],(Data_i)_{pub_A},(Data_i)_{pub_B},(Data_i)_{pub_D}>Priv_{C,}m>$,$m$=digest of $Data_i$.首先指定数据流通对象A,B,D,然后用三个数据消费者的公钥对数据消息进行加密,并将该条消息数据的摘要一并用节点C自身的私钥加密后发出.只有被指定的接收者才可用自己的私钥进行解密.该类业务通常适用于数据体量不大,但内容相对重要的消息类数据协作共享.基于图结构的云际分布记账沿用图3模型中关于可见、强可见、轮次、见证人、知名见证人、投票和计票等概念的内涵及逻辑.数据C1在第$R+2$轮次达成确定性状态,而在此之前,云际分布记账模型继续以异步的方式处理其他事务数据的流通及共识过程.

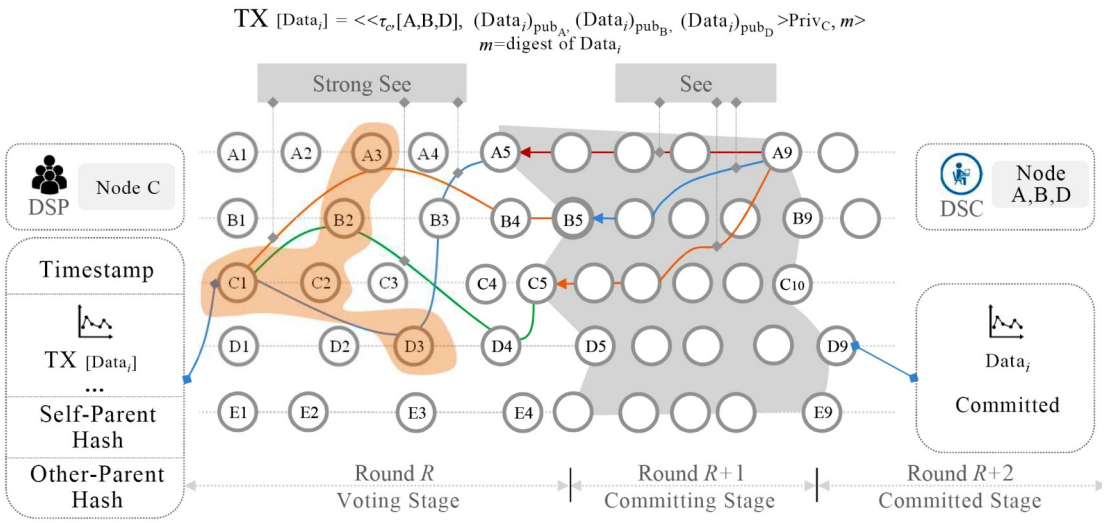


图5　基于图结构的云际数据协作合约模型

## 5　关键技术现状与未来趋势

本节主要论述以分布共识、智能合约等代表的云际分布记账关键技术体系,综述相关技术指标现状并对其目标属性的未来趋势进行前瞻.

### 5.1　分布共识技术

区块链技术起源于金融领域的比特币[3],除了以比特币为代表的公有链,还有以Hyperledger Fabric[23]为代表的联盟链以及私有链.公有链是完全开放的,每个节点均拥有一个匿名身份标识,不仅可以自由加入或退出,而且相互之间的事务信息在全网公开.联盟链和私有链均增加了准入控制机制,允许以不同权限等级实现对事务的提交和读取.非公有链类的共识,由于放宽了对去中心化程度的要求,对共识的参与者制定了诸多前提约束,使其具备了采用轻量级甚至半中心化共识协议的条件,这使其事务的处理过程更加高效.作为区块链技术的核心,本质而言,共识算法是维持大量不同地理位置分布的对等节点对变更信息达成共同认知的核心算法.

在计算机分布一致性领域,共识算法可分为崩溃容错(Crash Fault Tolerant,CFT)和拜占庭容错(Byzantine Fault Tolerant,BFT)两类.前者是无恶意节点的情况下的容错,失效节点可能宕机或失去响应,但不会主

动作恶;后者是有恶意节点的情况下的容错,失效节点会主动作恶以干扰共识的达成. 以 Paxos[38],Raft[39],Kafka[40] 等为代表的 CFT 类算法大多应用于环境相对可信且节点规模有限的分布式数据库[41] 或文件系统等场景. 以 POW[3],PoS[24],DPOS[25],PBFT[26],HoneyBadger[42],Algorand[28],Conflux[43],Tendermint[27],Casper[44],HotStuff[45],Dumbo[46]等为代表的 BFT 类算法,更加侧重于开放匿名环境中大量无信任关系节点间达成拜占庭容错共识的场景. 同时,针对加入了准入机制的联盟链场景,Bidl[47]是第一个为数据中心网络高度优化的联盟链共识算法,通过检测所有参与者的不当行为建立 deny-list,并基于此来替换或拒绝恶意参与者. 针对联盟链吞吐率较低、可扩展性不够等问题,研究者提出了 Kauri[48],通过利用一种新的流水线技术来提高共识效率. 针对现实场景中不需要严格一致性的场景,Wang 等[49]提出了一种出了一种弱一致性算法,只保持消息之间的相对位置的一致性,并将此共识算法应用于构建一个高性能区块链系统 Sphinx. 综上所述,现有区块链共识算法各有各的优缺点,任何一种算法都难以在所有场景下达到最优. 基于 PoW 的共识算法支持网络规模可扩展,允许成员节点自由加入,但事务处理能力有限. 例如,比特币最大的事务处理能力仅能达到 7 TPS. 基于多阶段提交的 BFT 类的共识算法具有较高的事务处理能力,但需要许可网络管理节点,其网络可扩展性较低. 例如,PBFT 在节点规模 $N$=8 的情况下,事务处理能力可达 16 000 TPS;在节点规模 $N$=64 的情况下,事务处理能力显著降至 3 000 TPS[42]. Tendermint[27] 和 Algorand[28] 等算法,在容错和事务处理能力方面与 PBFT 相当,容错能力为 33%,吞吐性能约为数千 TPS. 基于有向无环图结构的 IOTA[50] 等事务处理能力进一步得到了提升,但是存储资源的消耗要大于基于链式结构的区块链.

共识算法可从效能、安全和去中心化程度等三个维度来构建技术指标评价体系. 效能维度主要包括系统效率、可扩展性和能耗开销等. 系统效率维度主要包括出块的速度和每个区块中包含的事务数,即每秒处理交易数的能力,以及一个区块上链后达成确定性或概率性最终共识的确账延时. 可扩展性则表示在系统效能损失较小的情况下,节点数量的扩展能力. 能耗开销是指达成共识过程中的算力消耗和通信开销等. 安全维度主要包括抵御各种攻击(例如女巫攻击[51]、DDoS 攻击[52]、eclipse 攻击[53]、双花攻击[54]等)的能力、隐私保护和拜占庭容错等. Bitcoin[3]中分叉会造成大量算力浪费,为了避免分叉带来的不一致,不得不大大增加系统的事务确认延迟. PBFT[27]等基于投票类的算法以不出现分叉为目标之一,能够避免算力浪费且事务确认延迟较低,但是需要大量的通信开销(通信复杂度通常不小于 $O(n^2)$,其中 $n$ 为节点数量). 抗女巫攻击与 DDoS 攻击[25]则基本成了所有共识算法不可妥协的指标之一. PoW 算法依靠算力来竞争,恶意用户拥有多个节点身份并不会增加其竞争力,因此女巫攻击难以成功. 加入了准入机制的联盟链共识算法由于节点身份公开,因此也能抵御女巫攻击. 对于 DDoS 攻击,PoW 算法通过计算 hash 难题来确定记账人,能够做到记账人选择的随机性和不可预测性,因此可以防止攻击者事先对记账节点发起 DDoS 攻击;PBFT 等投票类算法适用于半同步的网络环境,通过超时失效检测来判断主节点是否被攻击,当主节点被 DDoS 攻击失效时,通常通过 view change 机制来更换主节点,从而保证共识进程不被中断. 对于隐私保护,Bitcoin 等系统追求身份隐藏,事务公开,然而,实际中有很多应用场景有信息不公开的需求. 拜占庭容错是指区块链系统可以容忍拜占庭错误节点,这也是区块链共识算法与可信场景中分布一致性算法的本质不同. 去中心化维度主要包括多中心化的程度(例如,完全去中心化或者存在一定程度的中心化)、节点自由进出区块链网络以及记账机会是否均等等. 这里的多中心化程度是指系统运行阶段而非设计阶段,例如比特币[3]在设计阶段是强中心的,运行之初表现出了去中心化的特点,也有分析认为近期 Bitcoin[3]的运行表现出较高的中心化程度. 实际中,也有大量场景不需要完全去中心化,这类场景只是需要提高多中心化的程度来降低系统的运行成本. 支持节点自由进出的共识算法无论对公有链还是联盟链,都更符合现实需要. 记账权的争夺更加平等是区块链系统是否民主和公平的体现. 分布共识技术本质通过在效能、安全和去中心化程度三个维度科学权衡,以适用于不同的场景. 在云际计算中,针对公有链的分布记账场景,应该考虑设计一种兼顾记账效率、记账权分配公平性和算力节约的共识算法,例如 PoPT[55];在云际联盟链分布记账场景下,应该考虑设计一种共识过程可监管前提下兼顾记账效率与节点规模的共识算法,例如 Jointgraph[56];然而在云际数据协作的场景下,则应该考虑设计一种共识范围可定制、程度可查看且支持隐私保护的共识算法,例如 Teegraph[57].

区块链技术的核心价值不在于经典意义下加密代币的发行,而在于拓展意义下的供需双方信息不对称以及信任随着距离增加而不断衰减等问题的解决. 然而,当前诸多技术指标并不能满足未来应用场景对终止性、一致性、正确性和完整性等的共识需求,同时,并不存在一个共识算法能够满足所有的应用场景[58]. 因此,如何从多个维度权衡技术指标,形成面向同步、半同步及异步网络场景的确定性或非确定性共识,是未

来的重要研究方向.

### 5.2 智能合约技术

智能合约是在不依赖信任中介的前提下自动执行约定条款,存储并自动运行于区块链的程序,其基本思想是在计算机中嵌入合同的概念. 本质上,智能合约通过对复杂交易进行编程,以达到扩展区块链应用范围的目的. 智能合约最早由 Szabo[59]于 1997 年提出,其具有可观察性、可验证性、隐私性和可执行性等四种基本目标属性. 独立实体通过智能合约形成利益关系并进而实现可信协作,合约参与方具有观察其履行情况,验证其是否履行或违反合同的能力.

Ethereum 是第一个推动智能合约[5,22]技术发展的公有链. 除此之外,代表性的智能合约平台还包括基于 RAFT 共识支持 Go 等合约语言的 HyperLedger Fabric[23],基于 POW 共识支持 RSK 和 BitML 等语言的比特币[3],基于 dBFT 共识支持 Java 等语言的 Neo[60],基于 BFT 共识支持多种语言的 Tendermint[27],基于多种灵活可插拔共识支持 Kotlin 语言的 R3 Corda[61]等. 新兴的智能合约技术推动了多个领域基于区块链的非金融应用从概念空间向现实空间落地. 代表性的去中心化应用领域包括医疗[62]、供应链[63]、商业过程管理[7]、物联网[12]、存证[8]、数字身份管理[64]和选举[65]等. 上述应用充分利用了区块链的经典及拓展特性,包括去中心化操作、防篡改的审计跟踪、数据溯源、安全和隐私等.

安全和性能是智能合约技术最为关注的两个方面. 运行于智能合约的通常是加密货币、数字资产或重要数据,一个很小的安全问题都可能引发非常严重的后果. 例如,2016 年加密货币领域分布自治组织(Decentralized Autonomous Organizations,DAO)平台由于代码问题导致损失 6 000 万美元. 然而,编写安全无缺陷合约代码是非常有挑战性的任务,Delmolino 等[66]认为大部分运行于 Ethereum 平台的智能合约均是脆弱的. OYENTE 工具[67]对 Ethereum 平台 19 366 个合约进行了分析,发现 45% 存在缺陷. 同时将智能合约的缺陷归为事务排序依赖、时间戳依赖、级联错误、可重入脆弱性等几类. 针对基于 PoS 共识的智能合约存在币崩塌的问题,一种综合合约拥有者信用[68]和 PoS 的新方法被提出,并有效解决了该类安全问题. 该信用的度量与拥有者拥有合约的数量有关,如果合约拥有者作弊,其在整个生态中的信用将大幅降低. 上述方法仅通过社会机制威慑合约拥有者一定程度上的可信,对解决外来攻击并无效果. Rodler 等[69]提出了一个以太坊智能合约安全框架 EVMPATCH,用于即时和自动地修补有缺陷的智能合约. EVMPATCH 为流行的以太坊区块链提供了一个字节码重写引擎,并透明自动地将常见的现成契约重写为可升级契约.

在隐私保护方面,Hawk[70]是一个创建隐私保护智能合约的框架,它将智能合约分为私有和公开两种. 私有合约包括参与者的输入数据和货币单位,这些对公开视图是保密的. 该框架引入了可以观察用户隐私数据的管理者. Enigma[71]是一种去中心化的计算网络,它在提供隐私保护前提下,支持不同参与方共享数据. Enigma 提供了一种图灵完备的脚本语言,创建支持私有数据的链下私有智能合约,公开部分在区块链中执行. 区块链控制系统的访问,链下私有数据以分布哈希形式存储,引入多方计算模型将数据切割成无意义的数据块并进行分布计算. 目前,虽然涌现了一些智能合约安全检测工具,但智能合约的准确性、脆弱性、隐私性、保密性和安全性等仍需要开展深入研究. 其中形式化验证分析方法[72]是提升智能合约安全性的一大重要方向. 但目前该方法还存在智能合约自动化验证、转换一致性、形式化工具信任以及形式化验证的评判标准等问题[73].

性能方面,高效的智能合约应该满足以下几点需求:(1)易于开发人员理解和使用;(2)开发人员只需关注商业逻辑,而不用担心隐私及安全问题;(3)合约代码可移植,运行平台不会成为瓶颈. 除了合约代码的运行效率之外,智能合约的性能还与其所依托的区块链的性能直接相关. 因此,提升智能合约的可扩展性一大方向便是提升区块链的可扩展性. Molina 等[74]提出一种高效的链上与链下混合执行合约的方法,该模型将去中心化的智能合约与中心化的可信第三方进行有机结合,达到提升吞吐性能和可扩展性的目的. Yu 等[75]提出一种流水线机制,将智能合约的执行与状态管理分离达到并发的目的,同时将智能合约的执行与区块的构建相分离,加速区块的构建和验证过程. 虽然现有的研究能够部分解决智能合约的性能问题,但是在诸如数据高效存储、状态快速确认等方面还需进一步提升[72]. 针对云际计算的应用场景,智能合约的设计与实际的业务相关,智能合约的本质是一种分布式的应用程序. 云际链跟其他平台所支持和的智能合约一样,都能够提供图灵完备的设计语言,其运行效率与共识算法的选择、代码的质量以及运行环境等密切相关.

以上研究打下了良好基础,但仍难以满足非金融领域的复杂多样化应用场景需求. 未来,智能合约技术的发展,需要面向多样化应用需求,综合考虑参与实体身份和数据的隐私保护,以及准确性、安全性、吞吐性能和执行延时等指标,并能够根据需求定制合约执行的边界和范围.

## 6 总结

云应用需求的爆发性、全域性和多样性等特征,使

单一云平台难以满足应用全时全域的多样化服务需求. 云间强边界、异构不兼容和互操作性差等客观因素成为提供跨云协作服务的潜在阻碍. 云际计算为供需两侧独立参与方的利益共享、开放协作提供了互操作及磋商协作的使能支撑,赋予协作各方跨地域纵横协作共赢、共同创造更大价值的能力,推动云际协作生态达成边际效用与成本的平衡,以及社会效益最大化. 互操作是基础,磋商协作是本质. 磋商协作的达成需要基于何种原理设计何种机制,是云际计算亟需进一步深化研究的重要问题. 为此,本文提出基于"数字空间证据"和连续交易约束,构建或增强信任关系的设计原则,提出了基于区块链的云际分布记账软件定义模型,并系统阐述了分布记账支撑云际服务独立性、可审计性以及释放云际协作潜能的内在机理;同时,为避免其在错综复杂要素综合作用下呈现不确定冲突和矛盾,针对数据资产化流通及复杂异步交互场景,深化、细化、优化并固化了基于链结构和图结构的云际分布记账运行逻辑流程及关键环节、云际分布记账合约逻辑. 为了满足未来云际复杂交互的技术创新需求,本文论述了以分布共识、智能合约等代表的云际分布记账关键技术及相应指标现状,并对相关核心技术的目标属性体系、前瞻性挑战等进行展望.

## 参考文献


[1] WANG H, SHI P, ZHANG Y. JointCloud: A cross-cloud cooperation architecture for integrated internet service customization[C]//2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE, 2017: 1846-1855.

[2] 史佩昌, 王怀民, 郑子彬, 等. 面向云际计算的自主对等协作环境[J]. 中国科学: 信息科学, 2017, 47(9): 20.
SHI P, WANG H, ZHENG Z, et al. Collaboration environment for JointCloud computing[J]. Scientia Sinica (Informationis), 2017, 47(9): 20. (in Chinese)

[3] SATOSHI N. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2019-12-10) [2021-07-30]. https://metzdowd.com.

[4] ABREU D, DUTTA P K, SMITH L. Folk theorems for repeated games: A NEU condition[J]. Econometrica, 1994, 64(4): 939-948.

[5] SIXT E. Ethereum[M]//Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017: 189-194.

[6] DANG H, LE T D, CHANG E C. Towards a marketplace for secure outsourced computations[M]//Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019: 790-808.

[7] JAN M, INGO M W. Blockchains for business process management—challenges and opportunities[J]. ACM Transactions on Management Information Systems, 2018, 9 (1): 1-16.

[8] GABRIELE D, STEFANO F, MORENO M. A blockchain-based flight data recorder for cloud accountability[C]//Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. New York: ACM, 2018: 93-98.

[9] LEEMON B. Hashgraph Consensus: Fair, Fast, Byzantine Fault Tolerance[R]. New York: Swirlds Tech Report, 2016: 1-24.

[10] MUSTAFA A B, ALBERTO S. Airtnt: Fair exchange payment for outsourced secure enclave computations[EB/OL]. (2018)[2021]. https://arxiv.org/abs/1805.06411.

[11] JAN M, INGO W. Blockchains for business process management-challenges and opportunities[J]. ACM Transactions on Management Information Systems (TMIS), 2018, 9(1): 1-16.

[12] SHI P C, WANG H M. Blockchain-based trusted data sharing among trusted stakeholders in IoT[J]. Software: Practice and Experience, 2021, 51(10): 2051-2064.

[13] INGO W. Untrusted business process monitoring and execution using blockchain[C]//Business Process Management: 14th International Conference. Cham: Springer International Publishing, 2016: 329-347.

[14] VICTORIA L. Blockchain and distributed ledgers as trusted recordkeeping systems: An archival theoretic evaluation framework[C]//Future Technologies Conference. Piscataway: IEEE, 2017: 41-48.

[15] 曾富来, 魏松杰, 莫冰. 基于区块链数据安全的仲裁方法: CN109685503A[P]. 2019-04-26.
ZENG F L, WEI S J, MO B. An arbitration method based on block chain data security: CN109685503A[P]. 2019-04-26. (in Chinese)

[16] RONALD C. Proofs of partial knowledge and simplified design of witness hiding protocols[C]//Annual International Cryptology Conference. Berlin: Springer, 1994: 174-187.

[17] CHEN Y. Blockchain based smart contract for bidding system[C]//2018 IEEE International Conference on Applied System Invention (ICASI). Piscataway: IEEE, 2018: 208-211.

[18] XIAO Y, ZHANG N, LI J, et al. Distributed consensus protocols and algorithms[M]//Blockchain for Distributed

Systems Security. Piscataway: Wiley-IEEE, 2019: 25-40.
[19] ATTYIA H, WELCH J. Computing Distributed: Fundamentals, Simulations, and Advanced Topics[M]. John Wiley & Sons, 2004, 19: 1-10.
[20] CYNTHIA D, NANCY L, LARRY S. Consensus in the presence of partial synchrony[J]. Journal of the ACM, 1988, 35(2): 288-323.
[21] BRACHA G. Asynchronous byzantine agreement protocols[J]. Information and Computation, 1987, 75(2): 130-143.
[22] VITALIK B. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform[R]. New York: Ethereum White Paper, 2014.
[23] ELLI A, ARTEM B, VITA B. Hyperledger fabric: A distributed operating system for permissioned blockchains [C]//Proceedings of the Thirteenth EuroSys Conference. New York: ACM, 2018: 1-15.
[24] KIAYIAS A, RUSSELL A, DAVID B. Ouroboros: A provably secure proof-of-stake blockchain protocol[C]// Annual International Cryptology Conference. Cham: Springer International Publishing, 2017: 357-388.
[25] XIAO Y, ZHANG N, LOU W J. A survey of distributed consensus protocols for blockchain networks[J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1432-1465.
[26] CASTRO M, ISKOV B. Practical byzantine fault tolerance[C]//Proceedings of the Third Symposium on Operating Systems Design and Implementation. Piscataway: IEEE, 1999: 173-186.
[27] BUCHMAN E. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains[D]. Guelph: University of Guelph, 2016.
[28] GILAD Y, HEMO R. Algorand: Scaling byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM, 2017: 51-68.
[29] PAGNIA H, GARTNER F C. On the Impossibility of Fair Exchange Without a Trusted Third Party[R]. Hawaii: Darmstadt University of Technology, 1999.
[30] YAO A C C. How to generate and exchange secrets[C]// 27th Annual Symposium on Foundations of Computer Science (SFCS 1986). Piscataway: IEEE, 1986: 162-167.
[31] DAO D, ALISTARH D, MUSAT C, et al. DataBright: Towards a global exchange for decentralized data ownership and trusted computation[EB/OL]. (2018) [2021]. https://arxiv.org/abs/1802.04780.pdf.
[32] DZIEMBOWSKI S, ECKEY L, FAUST S. FairSwap: How to fairly exchange digital goods[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 967-984.
[33] ECKEY L, FAUST S, SCHLOSSER B. OptiSwap: Fast Optimistic Fair Exchange[R]. Philadelphia: Cryptology ePrint Archive, 2019.
[34] 史佩昌, 尹浩, 沃天宇, 等. 软件定义的云际计算基础理论和方法研究进展[J]. 中国基础科学, 2019, 21(6):54-60.
SHI P C, YIN H, WO T, et al.Research progress on the basic theory and method of the software-defined Joint Cloud computing[J]. China Basic Science, 2019, 21(6): 54-60. (in Chinese)
[35] Corp RightScale. RightScale 2020 state of the cloud report from flexera[EB/OL]. (2020)[2021]. https://info.flexera.com/SLO-CMREPORT.
[36] HOUDA BOUZERZOUR N EL, GHAZOUANI S, et al. A survey on the service interoperability in cloud computing: Client-centric and provider-centric perspectives[J]. Software: Practice and Experience, 2020, 50(7): 1025-1060.
[37] PITTL B, STARFLINGER S, MACH W, et al. Bazaar-contract: A smart contract for binding multi-round bilateral negotiations on cloud markets[C]//2019 7th International Conference on Future Internet of Things and Cloud (FiCloud). Piscataway: IEEE, 2019: 147-154.
[38] LAMPORT L. Fast paxos[J]. Distributed Computing, 2006, 19(2): 79-103.
[39] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//Proceedings of the 2014 USENIX Annual Technical Conference. Philadelphia: USENIX, 2014: 305-319.
[40] KREPS J. Kafka: A distributed messaging system for log processing[C]//Proceedings of the NetDB. Piscataway: IEEE, 2011: 1-7.
[41] SUSAN B, DAVIDSON. Optimism and consistency in partitioned distributed database systems[J]. ACM Transactions on Database Systems, 1984, 9(3): 456-481.
[42] MILLER A, XIA Y, CROMAN K, et al. The honey badger of BFT protocols[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 31-42.
[43] LI C, LI P, ZHOU D, et al. Scaling nakamoto consensus to thousands of transactions per second[EB/OL]. (2018) [2021]. https://arxiv.org/abs/1805.03870.pdf.

[44] BUTERIN V, GRIFFITH V. Casper the friendly finality gadget[EB/OL]. (2017) [2021]. https://arxiv. org/abs/1710.09437.

[45] YIN M F, MALKHI D, REITER M K, et al. HotStuff: BFT consensus with linearity and responsiveness[C]//Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. New York: ACM, 2019: 347-356.

[46] GUO B Y, LU Z L, TANG Q, et al. Dumbo: Faster asynchronous BFT protocols[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 803-818.

[47] QI J, CHEN X S, JIANG Y P, et al. Bidl: A high-throughput, low-latency permissioned blockchain framework for datacenter networks[C]//Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles. New York: ACM, 2021: 18-34.

[48] NEIHEISER R, MATOS M, RODRIGUES L. Kauri: Scalable BFT consensus with pipelined tree-based dissemination and aggregation[C]//Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles. New York: ACM, 2021: 35-48.

[49] WANG Q, LI R J. A weak consensus algorithm and its application to high-performance blockchain[C]//IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2021: 1-10.

[50] DIVYA M, BIRADAR N B. IOTA-next generation block chain[J]. International Journal of Engineering and Computer Science, 2018, 7(4): 23823-23826.

[51] DOUCEUR J. The sybil attack[C]//International Workshop on Peer-to-Peer Systems. Berlin: Springer Berlin Heidelberg, 2002: 251-260.

[52] LI X, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems. 2020, 107: 841-853.

[53] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[C]//Proceedings of the 24th USENIX Conference on Security Symposium. New York: ACM, 2015: 129-144.

[54] KAEAME G, ANDROULAKI E, CAPKUN S. Two Bitcoins at the price of one? Double-spending attacks on fast payments in Bitcoin[J]. IACR Cryptology ePrint Archive, 2012: 248-265.

[55] FU X, WANG H, SHI P. Proof of previous transactions (PoPT): An efficient approach to consensus for JCLedger [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 51(4): 2415-2424.

[56] FU X, WANG H, SHI P, et al. Jointgraph: A DAG-based efficient consensus algorithm for consortium blockchains [J]. Software Practice and Experience, 2021, 51(10): 1987-1999.

[57] FU X, WANG H, SHI P, et al. Teegraph: Trusted execution environment and directed acyclic graph-based consensus algorithm for IoT blockchains[J]. Sciece China Information Sciences, 2022, 65(3): 139104.

[58] FU X, WANG H, SHI P. A survey of blockchain consensus algorithms: Mechanism, design and applications[J]. Science China Information Sciences, 2021, 64(2): 1-15.

[59] SZABO N. Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9): 1-21.

[60] ELAD E. NEO blockchain and smart contracts[J]. The Blockchain Developer, 2019, 2(9): 257-298.

[61] MOHANTY D. Corda architecture[J]. R3 Corda for Architects and Developers, 2019, 64(2): 49-60.

[62] KUO T T, KIM H E, OHNO-MACHADO L. Blockchain distributed ledger technologies for biomedical and health care applications[J]. Journal of the American Medical Informatics Association, 2017, 24(6): 1211-1220.

[63] KORPELA K, HALLIKAS J, DAHLBERG T. Digital supply chain transformation toward blockchain integration [C]//Proceedings of the 50th Hawaii International Conference on System Sciences (2017). Hawaii: IEEE, 2017: 1-5.

[64] MÜHLE A, GRÜNER A, GAYVORONSKAYA T, et al. A survey on essential components of a self-sovereign identity[J]. Computer Science Review, 2018, 30: 80-89.

[65] TSO R, LIU Z Y, HSIAO J H. Distributed e-voting and e-bidding systems based on smart contract[J]. Electronics 2019, 8(4): 422.

[66] DELMOLINO K, ARNETT M, KOSBA A, et al. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab[C]//Financial Cryptography and Data Security. Berlin: Springer Berlin Heidelberg, 2016: 79-94.

[67] LUU L, CHU D H, OLICKEL H, et al. Making smart contracts smarter[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 254-269.

[68] WATANABE H, FUJIMURA S, NAKADAIRA A, et al. Blockchain contract: Securing a blockchain applied to smart contracts[C]//2016 IEEE International Conference on Consumer Electronics (ICCE). Piscataway: IEEE, 2016: 467-468.

[69] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving

smart contracts[C]//2016 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE, 2016: 839-858.

[70] ZYSKIND G, PENTLAND A. Enigma: decentralized computation platform with guaranteed privacy[M]//New Solutions for Cybersecurity. New York: MIT Press, 2018: 425-456.

[71] LIU J, LIU Z. A survey on security verification of blockchain smart contracts[J]. IEEE Access, 2019, 7: 77894-77904.

[72] 朱健, 胡凯, 张伯钧. 智能合约的形式化验证方法研究综述[J]. 电子学报, 2021, 49(4): 792-804.
ZHU J, HU K, ZHANG B J. Review on formal verification of smart contract[J]. Acta Electonica Sinica, 2021, 49 (4): 792-804. (in Chinese)

[73] MOLINA-JIMENEZ C, SFYRAKIS I, SOLAIMAN E, et al. Implementation of smart contracts using hybrid architectures with on and off-blockchain components[C]//International Symposium on Cloud and Service Computing (SC2). Piscataway: IEEE, 2018: 1-8.

[74] YU L, TSAI W T, LI G N, et al. Smart-contract execution with concurrent block building[C]//2017 IEEE Symposium on Service-Oriented System Engineering (SOSE). Piscataway: IEEE, 2017: 160-167.

[75] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.
HE H W, YAN A, CHEN Z H. Survey of smart contract technology and application based on blockchain[J]. Journal of Computer Research and Development, 2018, 55 (11): 2452-2466. (in Chinese)

## 作者简介

**史佩昌**　男,1981年出生. 国防科技大学计算机学院副研究员. 主要研究方向为云际计算、区块链、分布式计算. 中国电子学会会员编号:E190016858M.
E-mail: pcmutates@163.com

**王怀民**　男,1962年出生. 国防科技大学计算机学院教授、中国科学院院士. 主要研究方向为分布式计算、云际计算、区块链、复杂智能软件系统.
E-mail: whm_w@163.com

**傅　翔**　男,1990年出生. 国防科技大学计算机学院助理研究员. 主要研究方向为区块链、分布式计算.
E-mail: fuxiang13@nudt.edu.cn