基于智能合约与区块链的算力交易机制

Computing Power Trading Mechanism Based on Smart Contract and Blockchain

吕航/LYU Hang，李佳聪/LI Jiacong，
雷波/LEI Bo，解云鹏/XIE Yunpeng

（中国电信股份有限公司研究院，中国 北京 102209）
(Research Institute of China Telecom Corporation, Beijing 102209, China)

DOI：10.12142/ZTETJ.202204011
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20220722.1742.018.html
网络出版日期：2022-07-25
收稿日期：2022-06-05

摘要：针对算力交易这一关键问题，结合智能合约与区块链技术，提出了一种去中心化、去平台化的的算力资源交易的机制。首先，以区块链技术为基础构建算力交易的框架，并充分考虑对算力交易潜在攻击的防御保护；其次，算力交易过程引入智能合约，实现去平台化后各个节点协调统一的交易流程和一致性机制；最后，算力用户对算力资源的服务评价可通过智能合约生产出服务质量评分区块，完善算力交易的整个过程。

关键词：算力网络；区块链；智能合约；算力交易；数字签名

Abstract: Concerning computing power trading and combining with smart contracts and blockchain technology, a decentralized mechanism for computing power resource trading is proposed. First, a framework of computing power transaction based on blockchain technology is built, which fully considers the defense and protection of potential attacks on computing power transactions; second, the smart contract is introduced in the computing power transaction process to realize the unified transaction process and consistency mechanism of distributed nodes; Finally, the service evaluation of computing power resources by computing power users can produce service quality score blocks through smart contracts to improve the whole process of computing power transaction.

Keywords: computing power network; blockchain, smart contract; computing power trading; digital signature

以5G、智能宽带等为代表的新型网络技术的发展和商用规模化的部署，带动了工业互联网、车联网、智慧医疗、智慧商业等垂直行业应用的蓬勃发展。行业应用需要大量的设备，同时还会产生海量的数据。据统计，到2025年，全球网联设备总数将超过270亿，而全球的数据总量则将达到142.6 ZB，这些都需要巨量的算力资源来支撑。算力资源已不再是单一的云资源池的形式，而是由云资源与广泛部署的边缘节点共同构成。在这种演进的趋势下，算力资源的协同是关键要点，算力网络应时而生。通过无处不在的网络连接，算力网络整合多级算力、存储等，为不同的行业提供最佳的资源分配方案，进而实现整网资源的最优使用[1-2]。

2021年5月，国家发展和改革委员会、工业和信息化部等四部委提出联合布局全国算力网络国家枢纽节点的“东数西算”工程，打通网络传输通道，提升跨区域算力调度能力。这将算力网络的发展和应用提升到了国家发展战略的高度。

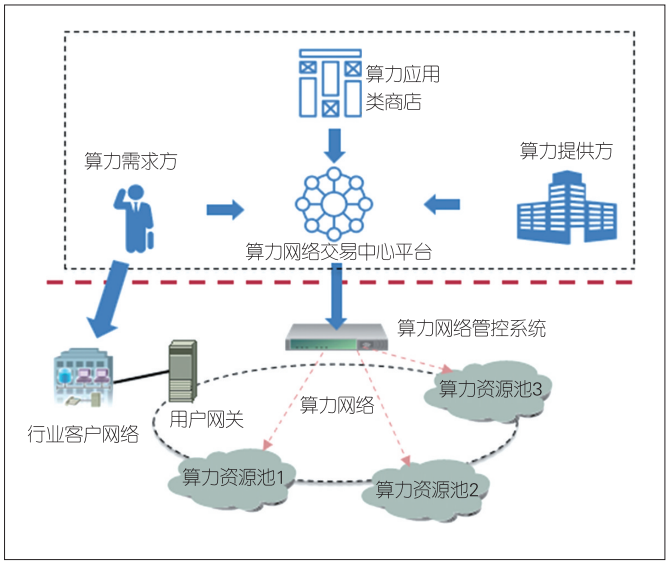
算力通过网络提供给行业应用，这就形成了算力的需求方和供应方。在商用场景中，就形成了算力交易，而交易也同样通过网络完成。结合智能合约及区块链技术，我们提出了一种去中心化、去平台化的可靠算力交易机制和方案，适用于中小行业用户的算力交易场景[3-5]。

1 基于区块链技术构建算力交易框架

区块链技术利用块链式数据结构进行数据验证与存储。从本质上讲，区块链是一个共享数据库，存储于其中的数据或信息具有不可伪造、去中心化、透明化、分布式存储等特征。基于密码技术，区块链允许多个参与者共同维护一组一致的信息或事实，实现去中心化的共识机制。各个区块主体在时间维度上形成了区块链，行间链路表示区块主体之间的互联，增强了信息的可追踪性和安全可靠性。目前区块链技术在金融、物流、工业制造、医疗、物联网等领域有着广泛应用。

1.1 算力网络中的算力交易

一般情况下，在线交易系统采用的是中心化交易模式。售卖方的信息、交易记录等数据由特定的第三方平台存储和管理，交易双方充分信任此第三方平台。在算力网络场景中，算力交易也可以采用中心平台的方式来实现，如图1所示[6]。

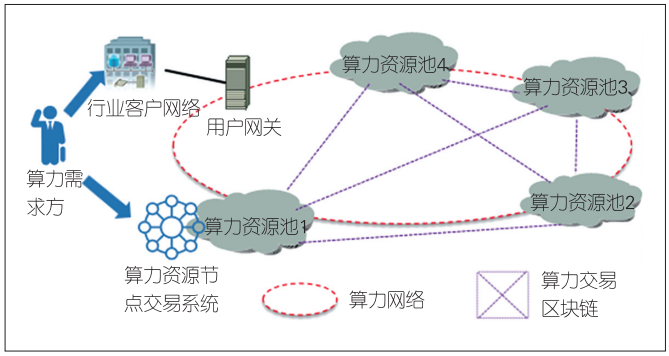


▲图1 算力交易通用交易模型

如图1所示，第三方构建算力网络交易中心平台。算力需求方在平台浏览所有算力提供方的资源信息，并进行选择；随后，根据算力价格进行订购结算，并在算力资源池进行计算业务；算力服务合同到期后，需求方卸载算力业务，释放资源。随着算力业务的不断增加，不同的需求方与不同的算力资源提供方之间的交易量也在不断增加，中心平台运行和维护工作的复杂度和成本也越来越高。如果有攻击方对中心平台发起攻击，包括截获、篡改、伪造交易信息，或对平台发起拒绝服务的攻击，将导致交易停止，造成难以估量的损失。

1.2 基于区块链的算力交易

如前所述，区块链采用分布式账本的方式，以链式数据结构存储交易信息，并将信息保存在所有上链节点中[8–10]。去中心化的部署特点可以很好地解决集中部署算力交易平台中运维成本高的问题。同时，分布部署以及链式的数据存储模式，也显著增加了攻击方的攻击难度和成本。基于区块链技术的算力交易体系不再建设中心交易平台，算力资源池构建区块链（联盟链或私有链）、交易数据上链存储，参考模型如图2所示。



▲图2 基于区块链的算力交易结构模型

在图2中，算力网络为算力需求方和算力资源方提供了算力服务的基础设施。算力资源方构建了算力区块链，算力需求方则在链上对各个算力资源节点进行资源浏览、交易历史查询、资源价格评价，以及算力交易、结算。所有的交易过程中产生的数据都存储在每个链节点，不再需要中心平台，因此任一节点都存储所有节点的交易数据，且任何数据都是真实不可篡改的。

2 智能合约结合区块链的算力交易方案设计

2.1 区块数据结构设计

区块链链上的数据是公开透明的，所有用户都可以查看。算力交易会引起商业竞争，甚至会引起恶意攻击，这就会产生攻击节点与正常节点对数据区块的生产竞争。为确保交易的安全可信，算力需求方与资源提供方都要首先向第三方的数字证书签发机构（CA）申请数字证书和私钥，用于对交易结果进行签名确认，之后才能进行算力交易。

假设制造某个完整的交易流程需要产生n个区块，α为正常节点制造下一个区块的概率，β为攻击节点制造下个区块的可能性。作为正常交易，α值大于β。再假设，攻击方要伪造一条攻击链，需要产生m个区块才能取代诚实链，那么攻击方成功替换诚实链的概率如公式（1）和（2）。

$$P_\eta = \sum_{i=1}^{m}\left[\frac{\left(\frac{n\beta}{\alpha}\right)^i}{i!\ e^{\left(\frac{n\beta}{\alpha}\right)}}\left(\frac{\beta}{\alpha}\right)^{n-i}\right] \quad m > n, \tag{1}$$

$$P_\eta = \sum_{i=1}^{m}\left[\frac{\left(\frac{n\beta}{\alpha}\right)^i}{i!\ e^{\left(\frac{n\beta}{\alpha}\right)}}\right] \quad m \leqslant n。 \tag{2}$$

从公式（1）和（2）可看出，区块数n越多，P_η就会越小，攻击难度就会越大。因此，我们在设计交易区块时，尽量使用多区块来描述一个算力交易。本文中，我们设计了4

种交易区块，从而构建一个完整的交易过程。

$$T_{\text{pro}} = \sum_{i=1}^{n} \delta \frac{D_i}{W}, \tag{3}$$

$$T_{\text{val}} = \sum_{i=1}^{n} \varepsilon t_i, \tag{4}$$

$$T = T_{\text{pro}} + T_{\text{val}}。 \tag{5}$$

公式（3）—（5）中，T_{pro}、T_{val}分别是区块链生产及验证的时间。其中，δ、ε分别是生产和验证的系数，D和W分别是每个区块的数据容量和传输带宽，而t则为区块的验证时间。在生产区块时，需要用户的私钥生成签名，因此攻击节点需要额外的大量时间来伪造用户签名，从而难以与正常节点争夺区块生产权。

图3—6定义了4种区块数据结构。这4种区块构建了完整的算力交易流程。

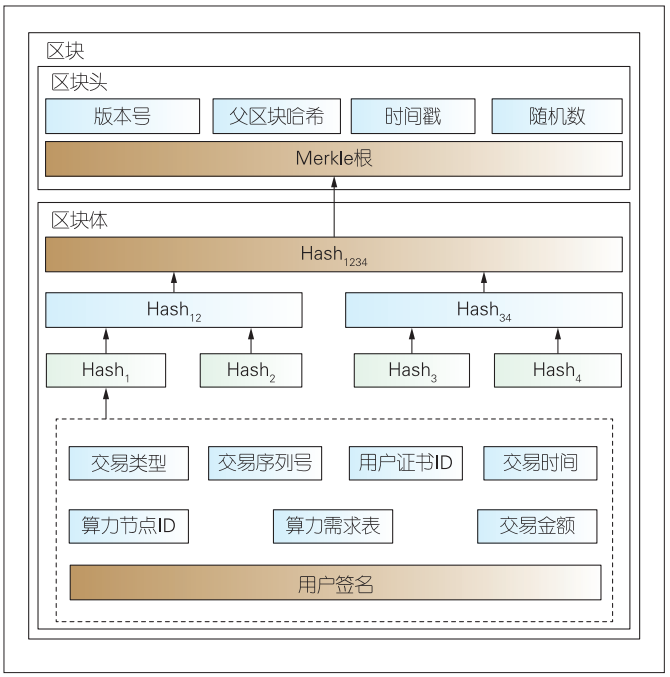
（1）需求方浏览记录区块：用户每次登录算力资源节点，对该节点所能提供的资源、历史记录以及用户评分情况进行浏览，而浏览记录形成区块。

（2）需求方订购算力申请区块：需求方确定使用该节点的算力资源后即可下订单，并根据资源方的架构，形成交易金额，然后向资源方提出申请。

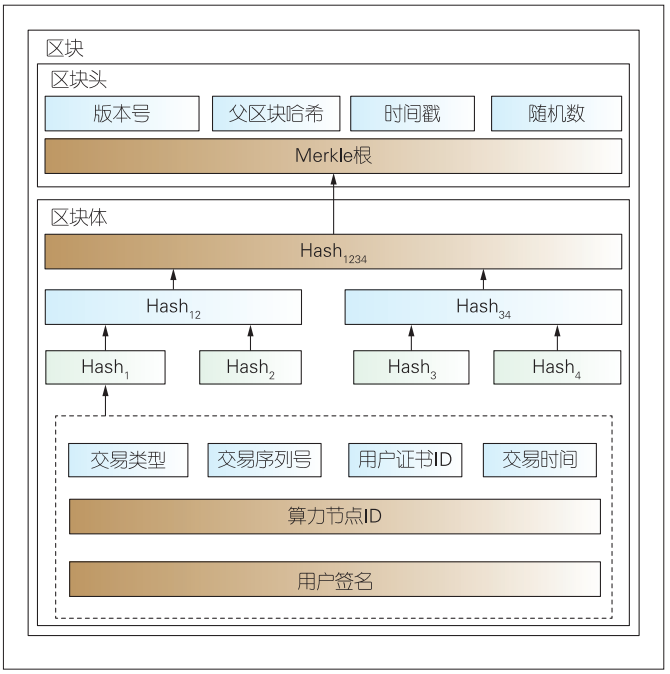
（3）算力交易成功记录区块：资源节点收到需求方的订购请求后，对资源需求和价格进行确认，然后签订合约。

（4）需求方对算力资源使用体验进行评分的区块：在完成算力服务后，需求方对资源方提供的服务进行评分，包括总分以及分项评分。这4种区块结构的字段内容是相互关联的。

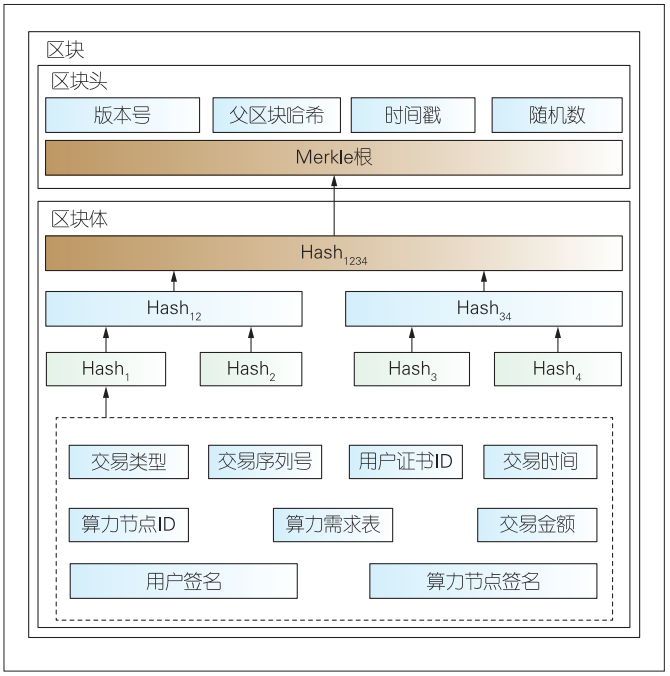
• 交易类型：具体包括ConType_1、ConType_2、ConType_3、ConType_4，分别代表上述的4类区块。



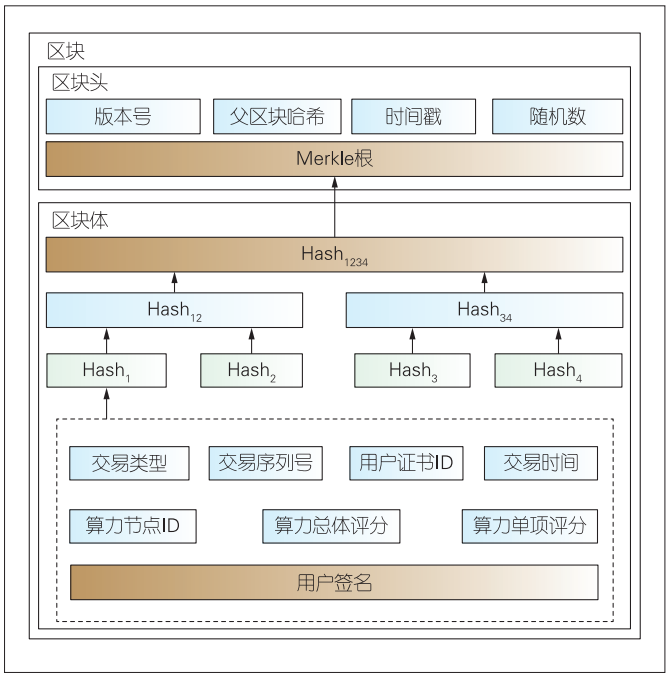
▲图4　算力交易区块数据结构2——需求方算力资源订购申请



▲图3　算力交易区块数据结构1——需求方浏览记录



▲图5　算力交易区块数据结构3——算力交易成功记录



▲图6 算力交易区块数据结构4——算力资源使用体验评分

• 交易序列号：区块的标识号，其中ConType_2、ConType_3、ConType_4的序列号与最近的ConType_1的区块序列号一致，表明这是一项交易的4个连续动作所产生的记录。

• 用户证书ID：即需求方数字证书的ID号，任何人都可以通过该ID号在CA的轻型目录访问协议（LDAP）站点获取该用户的数字证书，以对该用户的签名进行验证。

• 用户签名：用户用自身的私钥对记录的哈希值进行加密签名。

• 算力节点ID：算力资源节点的身份信息，通过该ID号可以检索资源节点的公钥。

• 交易时间：用户在算力资源节点生成记录的时间。

• 算力需求表：在ConType_2、ConType_3两种类型区块中存在。需求方浏览算力资源节点，选择符合自身需求的算力资源以及使用周期，形成需求列表。

• 交易金额：在ConType_2、ConType_3两种类型区块中存在，是用户订购算力资源的使用费用。

• 算力单项评分：用户订购并使用算力资源后，进行业务卸载，再对每项资源的使用效果进行打分；

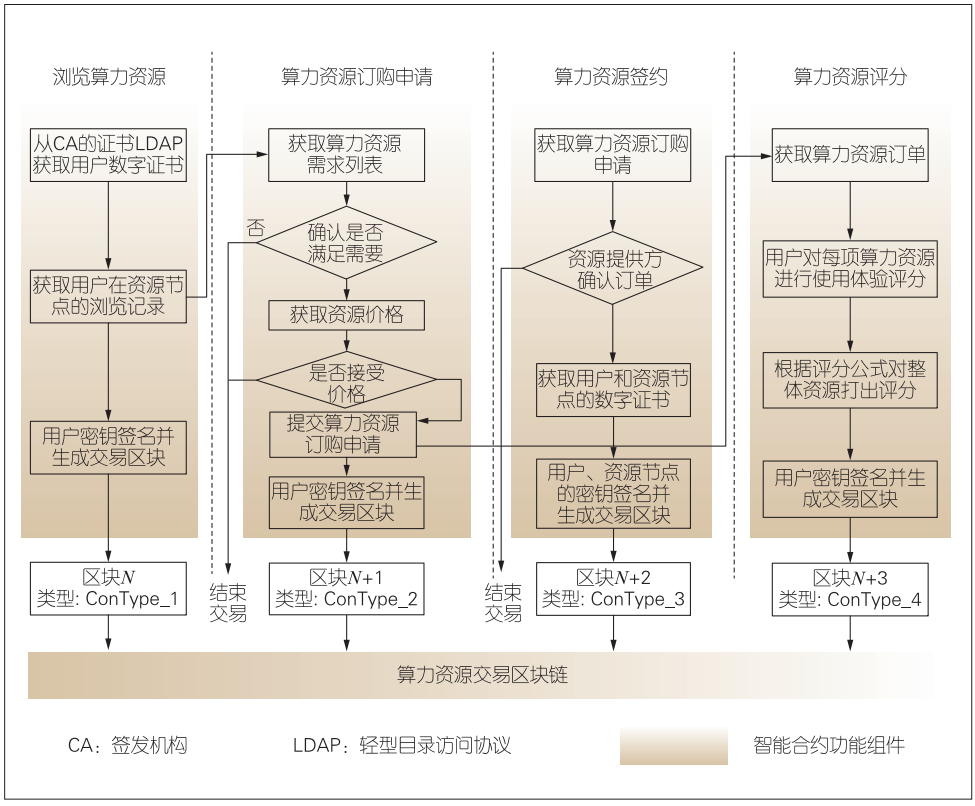
• 算力总体评分：用户对算力分项进行评分后，对所有分项进行加权累计形成一个最终评分值。算力效果评分和单项评分都可被其他用户浏览。该评分为潜在需求方提供决策参考，同时也对资源提供方起到督促作用。

• 算力节点签名：在ConType_2、ConType_3两种类型区块中存在，对提供的算力资源和价格进行确认。

2.2 基于智能合约与区块链的算力交易模型

1996年，SZABO首次提出了智能合约。智能合约被定义为数字合约条款，无须第三方干预，合约的代码经过认证后嵌入区块链中，在一定条件下触发便可自动执行。智能合约可以确保所有节点的算力交易过程具有一致性以及可靠性。上述的4种区块类型，都由智能合约来完成生产。本文提出的区块链结合智能合约的算力交易方案模型如图7所示[11]。

图7中，灰色框部分即为智能合约的可执行功能。这些功能与相关用户接口（UI）界面协同，在算力需求方通过界面进行资源浏览、下单、签约及资源使用评价等操作时，即



▲图7 基于区块链智能合约的算力交易模型

可触发智能合约的代码运行。智能合约也分为四大模块，同时分别输出4种区块数据。

（1）需求方（用户）登录算力资源节点，通过UI界面浏览节点的算力资源、使用的历史记录以及评价，从而触发智能合约。合约通过界面获取用户的证书ID，对浏览记录数据进行签名，并输出形成区块数据。区块类型为ConType_1，用户签名（UserSign）方式如下：

$$TX_{\text{UserSign}} = \text{Encrypt}[UK\_pri, \text{Hash}(\text{ContracNo}\| \text{ContractTime}\| \text{ComputingPoolID})]。 \quad (6)$$

用户签名内容包括交易序列号、交易时间以及资源节点的ID号等，而*UK_pri*为用户私钥，Hash（）为哈希运算，可以是MD5或者是SHA1等哈希算法。

（2）用户如接受资源的使用价格，则提出订单申请。订单包括算力资源内容、性能数量要求以及使用时限等，订单申请将触发智能合约自动运行。智能合约在与用户交互完成订单确认后，获取用户私钥，生成订单签名并生产交易区块。区块类型为ConType_2，签名形式如下：

$$TX_{\text{UserSign}} = \text{Encrypt}[UK\_pri, \text{Hash}(\text{ContracNo}\| \text{ContractTime}\| \text{ComputingPoolID}\|\text{RequirementList}\| \text{ContractValue})]。 \quad (7)$$

用户签名的内容包括交易序列号、交易时间、资源节点的ID号、资源需求列表以及合约金额等，在进行哈希运算后用私钥完成数字签名。

（3）当资源节点收到用户的资源订单时，如同意接受该订单，则触发智能合约自动执行。智能合约分别获取节点私钥和用户私钥，并做二重签名（用户签名和节点签名），然后生产出类型为ConType_3的区块。用户签名与公式（7）一致，而节点签名则只需对用户的签名再做一次签名即可。

$$TX_{\text{CPSign}} = \text{Encrypt}(CPK\_pri, TX_{\text{UserSign}}), \quad (8)$$

其中，*CPK_pri*为资源节点的私钥。

（4）算力资源订单到期后，用户登录节点，并对此算力服务进行评分。评分包括逐项评分以及总体评分。算力资源列表中包括各项资源，具体如公式（9）。

$$R=\{m_1, m_2, \cdots, m_i, \cdots, m_M\}\ i\in\{1, 2, \cdots, M\}。 \quad (9)$$

*M*为算力资源节点提供的资源种类数量，包括中央处理器（CPU）、内存、存储、硬盘输入输出（IO）能力、图形处理器（GPU）以及网络吞吐能力等。用户对每一项资源进行评分，智能合约触发执行后，打出总评分。

$$S_{\text{oa}} = \sum_{i=1}^{M} \delta_i S_i, \quad (10)$$

其中，S_i为某单项算力资源的评分，δ_i为该资源加权评分系数。评分完毕后，用户私钥进行签名并生产类型为Con - Type_4的区块，签名如公式（11）。

$$TX_{\text{UserSign}} = \text{Encrypt}[UK\_pri, \text{Hash}(\text{ContracNo}\| \text{ContractTime}\| \text{ComputingPoolID}\|\text{OverallScore}\| \text{ScoreList})]。 \quad (11)$$

用户签名包括交易序列号、交易时间、资源节点的ID号、整体评分以及单项评分列表。在交易过程中，由智能合约生产的区块经过区块链验证后上链广播至各个节点。

智能合约是条件触发自动执行的，在交易系统和区块链之间构建了可信赖、安全的连接桥梁。在实现上，智能合约与节点的交易界面可独立开发部署，交易系统的代码不能入链。资源提供方自主提供UI界面，向需求方展现可供交易的算力资源及定价，而智能合约可以通过回调、订阅等方式与UI界面通信，或者封装成执行库被平台调度。目前比较通用的智能合约开发语言包括Solidity、Sepent、LLL等。

3 结束语

在算网融合不断发展的大趋势下，算力交易的关键技术与机制是一个很重要的发展方向。本文中，我们首先提出了一种基于智能合约结合区块链的算力交易方法，充分应用了区块链去中心化以及分布式数据同步及存储的技术优势，将算力交易分布在各个算力资源节点。其次，在区块生产过程中，多交易区块的设计及加密数字签名，能显著提升攻击链争夺区块生产权的难度，在降低建设及运行成本的同时，有效提高了交易的可靠性与安全性。然后，利用区块链不可篡改的技术特性，我们还设计了评分机制，帮助潜在需求方获取算力资源节点运营历史情况及服务质量。最终，形成智能合约结合区块链的算力交易的价值与方案。未来，我们将紧跟算力网络技术和算力交易需求的发展脚步，持续关注相关的去中心化的算力交易实现方案。

参考文献

[1] 雷波, 陈运清. 边缘计算与算力网络: 5G+AI时代的新型算力平台与网络连接 [J]. 中国信息化, 2020(12): 113
[2] 赵慧玲. 边缘计算与算力网络专题导读 [J]. 中兴通讯技术, 2021, 27(3): 1-2. DOI: 10.12142/ZTETJ.202103001
[3] 施泉生, 黄晓辉, 胡伟, 等. 基于区块链的改进智能合约电力交易模型 [J]. 电力工程技术, 2022, 41(1): 11-18. DOI: 10.12158/j.2096-3203.2022.01.002
[4] 胡博明, 陈晓丰, 胡大裟, 等. 基于区块链智能合约的安全投票系统 [J]. 现代电子技术, 2022, 45(6): 180-186. DOI: 10.16652/j.issn.1004-373x.2022.06.033
[5] CCSA.面向业务体验的算力需求量化与建模研究 [EB/OL].(2022-05-06)[2022-06-14].https://max.book118.com/html/2022/0505/7152016003004120.shtm
[6] 雷波, 赵倩颖. CPN: 一种计算/网络资源联合优化方案探讨 [J]. 数据与计算发展

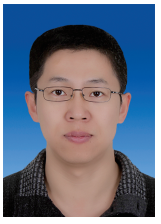
前沿, 2020, 2(4): 55–64. DOI: 10.11871/jfdc.issn.2096–742X.2020.04.005
[7] 雷波, 赵倩颖, 赵慧玲. 边缘计算与算力网络综述 [J]. 中兴通讯技术, 2021, 27(3):3–6. DOI: 10.12142/ZTETJ.202103002
[8] 何涛, 曹畅, 唐雄燕, 等. 面向6G需求的算力网络技术 [J]. 移动通信, 2020, 44(6): 131–135
[9] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展 [J]. 计算机学报, 2021, 44(1): 1–27. DOI: 10.11897/SP.J.1016.2021.00001
[10] ETSI. Mobile edge computing (MEC): bandwidth management API: ETSI GS MEC015 [S]. 2017
[11] 周鑫, 邓莉荣, 王彬, 等. 基于联盟链的去中心化能源交易系统 [J]. 全球能源互联网, 2019, 2(6): 556–565. DOI: 10.19705/j. cnki. issn2096–5125.2019.06.005

作 者 简 介

吕航，中国电信股份有限公司研究院网络技术研究所工程师、CCSA TC610边缘计算组副组长；主要研究领域为5G行业专网、边缘计算、算力网络以及5G行业解决方案等；发表论文多篇。

李佳聪，中国电信股份有限公司研究院工程师；主要研究领域为5G网络、算力网络、未来网络等；发表论文10余篇。

雷波，中国电信股份有限公司研究院网络技术研究所副所长、正高级工程师，中国科学院计算机网络信息中心客座研究员，北京邮电大学兼职教授，同时兼任CCSA TC617边缘计算产业发展及标准推进委员会副主席、边缘计算网络基础设施工作组（ECNI）联执主席、CCSA TC614网络5.0联盟管理与运营组组长以及算力网络特别工作组副组长等；主要研究领域为未来网络技术、新型数据中心网络、边缘计算与算力网络等；出版专著4本，发表论文10余篇。



解云鹏，中国电信股份有限公司研究院正高级工程师、CCSA TC614架构组副组长、网络5.0产业和技术创新联盟架构组副组长；主要研究领域为未来网络、算力网络、IP城域网、数据中心网络等；获发明专利20余项，出版合著专著4本，发表论文10余篇。