DOI:10.12158/j.2096-3203.2022.06.022

基于 Oracle 机制的电力 5G 可信数据上链技术

李大伟[1]，朱道华[2]，郭雅娟[2]，韦磊[3]，孙云晓[2]，刘伟[2]
（1. 南京工程学院计算机工程学院，江苏 南京 211167；2. 国网江苏省电力有限公司电力科学研究院，江苏 南京 211103；3. 国网江苏省电力有限公司，江苏 南京 210024）

摘 要：针对电力区块链应用系统中数据上链效率和可信性问题，研究了基于 5G 和预言机（Oracle）机制的可信数据上链技术。首先，讨论了区块链系统中数据上链方式，分析了适用于电力 5G 区块链的 Oracle 数据上链方法；然后，提出了基于分布式 Oracle 的电力 5G 业务系统可信数据上链技术，设计了基于云-边-端一体化的系统总体架构，以及数据源注册、评估、上链的工作流程，其中，通过区块链系统实现分布式数据的采集共享，基于门限签名算法和可验证随机函数实现数据源评估，评估算法由边缘物联代理节点运行以确保系统的安全性和可用性，并通过对 5G 切片任务划分和优化实现认证数据和业务数据的高效传输。最后，在基于电力 5G 区块链的用电信息采集系统中部署文中所提方案，从通信性能、业务性能、资源利用等方面进行实验验证。结果表明，所提方案在不同负载压力测试下数据平均传输时延约为 10 ms，误码率、丢包率小于 0.9%。在 100 量级并发业务请求情况下，较已有方案性能提升超过 80%，因而具有良好的可行性和推广价值。

关键词：区块链；预言机；5G；电力物联网；门限签名算法；数据上链
中图分类号：TM71 **文献标志码**：A **文章编号**：2096-3203（2022）06-0182-11

0 引言

5G 和区块链都是新型信息基础设施的重要建设内容。为贯彻落实国家战略，国网公司近年来大力推进这 2 项新型技术的研发和试点，且取得了丰硕的成果[1-3]。

电力区块链应用目前主要面临两方面挑战：一是区块链系统数据采集和处理过程需要共识节点间频繁的数据交互，为提高业务处理能力，需要高性能的网络降低端到端时延；二是区块链的共识机制仅能保证链上数据的安全可信，对链下数据源的数据质量难以鉴别，因此须研究可信数据上链技术[4]。

在提升网络性能方面，文献[5]研究了电力物联网边缘切片资源优化算法；文献[6]研究了电力 5G 差异化资源分配和经济性优化模型；文献[7]研究了切片全生命周期管理机制。上述技术可用于提升电力区块链应用系统节点间的数据传输性能，但缺少数据可信性保障。数据安全可信方面，文献[8]研究了电力用户间数据跨链查询共享问题；文献[9]研究了新能源交易系统的信任问题；文献[10]采用多种密码学算法解决了电力区块链应用系统中的网络信任问题；文献[11]研究了基于区块链的电力稳控系统终端身份认证问题。上述研究都将区块链系统中的数据作为整体研究，未考虑链上链下数据的可信协同。然而，当前 5G、大数据、物联网和人工智能等技术的融合应用为区块链系统提供了更广泛的数据来源，链下数据的上链质量对区块链系统中数据的整体可信具有重要影响[12-14]。

传统区块链系统中数据上链多根据应用场景设计专用的数据接口[15]，缺乏灵活性和可扩展性。区块链预言机（Oracle）是区块链外部信息写入区块链内部账本，实现链上链下数据协同的中间件，已受到越来越多的关注[16-17]。最早的 Oracle 系统是为以太坊区块链应用提供数据服务的 Oraclize[18]，Oraclize 通过 TLSNontary 实现链下数据的可信性证明，并通过云计算进行审计；Town Crier[19] 进一步利用英特尔软件防护扩展技术为以太坊智能合约提供数据源身份验证服务。以上 2 种方案皆为中心化数据上链方式，存在单点失败问题。分布式数据上链由多个 Oracle 节点组成认证网络，通过分布式共识和认证机制对数据源可信性进行验证。ChainLink[20] 是首个基于以太坊平台的分布式 Oracle，通过链上聚合和链下治理的方式实现了多 Oracle 对多数据源的认证，提高了数据源的可信性。DOS network[21] 和 Truora[22] 是国内分布式 Oracle 可信数据上链的实现方案，在链下数据验证和可信数据采集、上链等方面都取得了一定成果。

Oracle 在为区块链系统提供数据时，往往通过可信执行环境、安全多方计算等技术对链下数据源进行可信性验证评估，确保数据在上链前的可信性，其智能合约触发机制可与区块链系统实现有效

收稿日期：2022-06-20；修回日期：2022-09-21
基金项目：江苏省自然科学基金资助项目（BK20210928）

协同[23]。基于 Oracle 机制,可响应链下数据库查询、链下系统消息交互(如广播交易等)、数据清洗等请求,所得结果可及时返回到区块链系统中[24]。特别是在电力 5G 应用场景中,区块链处理的数据可能涉及多个数据源,Oracle 机制为电力业务可信数据上链提供了有效的解决方案。

文中基于分布式 Oracle 机制,研究边-端结合的电力 5G 区块链应用中可信数据采集和上链技术。通过建立数据源认证模型,实现电力区块链应用系统链上链下数据的有效协同;通过 5G 切片优化,确保电力 5G 业务满足既定的服务级别协议(service level agreement,SLA)要求。文中通过融合 5G 高性能通信能力和区块链数据可信管理优势,在新型电力系统中源网荷储多数据源互动和多能互补环境下,为构建安全可控、灵活高效、开放互动的电力区块链应用系统提供理论指导和实践依据。

1 数据上链方式

有效可信地采集数据对电力 5G 区块链应用系统安全可信性具有重要意义。电力区块链应用系统中涉及的数据可分为链上数据和链下数据 2 类。链上数据是指存储在分布式账本中的交易数据,这些数据由区块链节点通过共识算法记账产生,具有防篡改、可追溯的特征;链下数据是存储在电力业务系统中的数据。可信数据上链是指通过可控的方式将链下数据按照区块链能处理的格式上传到区块链,并经过共识算法被记录到区块链中的过程[25],上链方式可分为专用上链和基于 Oracle 上链 2 种。

1.1 专用上链方式

专用上链方式是指在系统研发时针对特定应用系统设计开发的数据上链模块,又分为软件方式和硬件方式。

软件方式为通过程序编码的方式实现链下数据源数据的获取,又称基于应用程序接口(application programming interface,API)的方式。通过开发相应的系统中间件实现链下数据与区块链应用系统的对接,在区块链应用开发时就同步开发数据获取 API 模块,如图 1 所示。此方式具有 2 个典型特征,一是适用于统一规划的区块链应用系统,链下数据多集中式存储,通过编码方式实现数据采集和上链;二是数据的可信性依赖于零知识证明、安全多方计算、联邦学习、同态加密等隐私计算技术,结合可信执行环境实现,本质上属于集中式的数据管理模式。

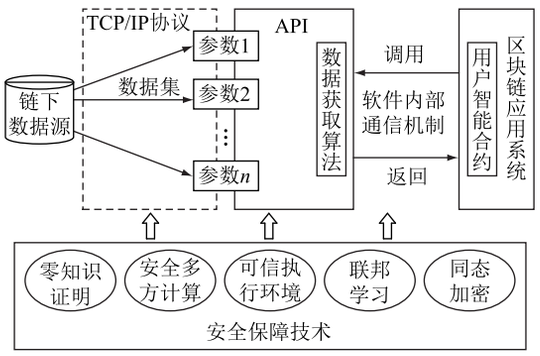

图 1 基于软件的数据上链

Fig.1 Software-based data feed

硬件方式则将具有数据采集上链功能的可信硬件模组嵌入到电力物联网终端等设备中,实现区块链数据采集功能。此方式可将物联网传感器获取的数据进行实时上链,具有安全性好、执行效率高等优点。但硬件模组需要与物联网终端高度集成,多为专用系统定制开发,因此兼容性和部署灵活性较低。

1.2 基于 Oracle 的上链方式

借助 Oracle 实现链下数据的可信性验证并进行数据上链是区块链应用系统链上链下数据协同的主要方式。Oracle 根据部署方式可分为中心化 Oracle、硬件 Oracle、分布式 Oracle 等类型。其中,中心化 Oracle 为集中式数据管理,由权威数据库作为数据源,适用于中心化部署的业务系统;硬件 Oracle 通过与物联网传感器硬件模组集成,实现数据获取;而分布式 Oracle 由多个节点和多个数据源同时获取数据,通过构建多节点 Oracle 网络和分布式安全算法对数据源的可信性进行评估,从而达到分布式链下数据源可信上链的目的,适用于大规模部署的电力业务系统。

基于 Oracle 的上链方式通过 Oracle 沟通用户智能合约和链下数据源,其过程为:用户智能合约向 Oracle 发起数据请求,Oracle 根据请求向外部数据源获取数据并反馈给用户智能合约,如图 2 所示。

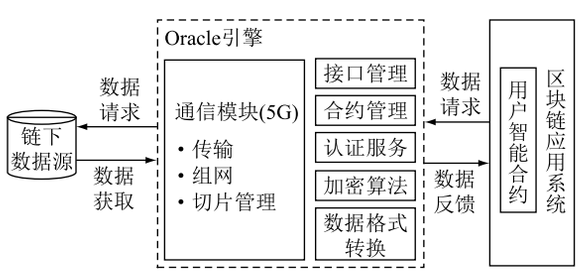

图 2 Oracle 架构

Fig.2 Oracle architecture

Oracle 引擎包含通信模块,可实现采集数据传

输、组网和切片管理，将通过可信认证的链下数据源的数据进行格式转换并写入区块链中。Oracle 可以直接获取链下数据并反馈到链上智能合约中，具有较高的执行效率，同时可以采用分布式部署和多种安全可信机制确保数据采集-传输-上链全过程的数据可信。

在基于 5G 通信的大型电力区块链应用系统中，往往存在多个链下数据源的情况，需要部署分布式 Oracle 组成分布式数据源认证网络，对某数据源的上链请求进行判决，确保上链数据的可信性。3 个链下电力数据源提供数据的情形如图 3 所示。

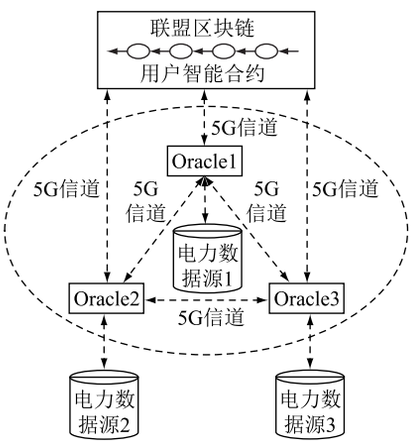

图 3　分布式 Oracle 网络

Fig.3　Distributed Oracle network

2　电力 5G 业务可信数据上链

2.1　数据上链架构

文中提出的电力 5G 可信数据上链模型基于分布式 Oracle，其体系架构见图 4。电力区块链应用系统构建在基于 5G 通信系统互联的云-边-端平台上，包括感知侧的电力物联网终端、边缘侧的边缘物联代理、Oracle 节点、联盟区块链系统、云平台应用系统等组成部分。电网云平台管理端和所有边缘物联代理组成联盟区块链的 peer 节点集合，每个节点上部署的 Oracle 组成分布式 Oracle 网络。5G 通信网络通过切片的方式为上述架构提供通信支持，网络切片分为用户认证切片、数据源认证切片和数据通信切片 3 类，分别实现电力应用系统的用户认证、Oracle 数据源认证和数据传输任务。其中，通过认证的电力应用系统用户可以接入系统平台，通过分布式 Oracle 网络确认的数据源可以将数据传输到边缘物联代理并通过数据通信切片进行业务数据的上链。

各功能模块的协作关系为：电力物联网终端在链下采集电力一二次设备和系统产生的数据，通过

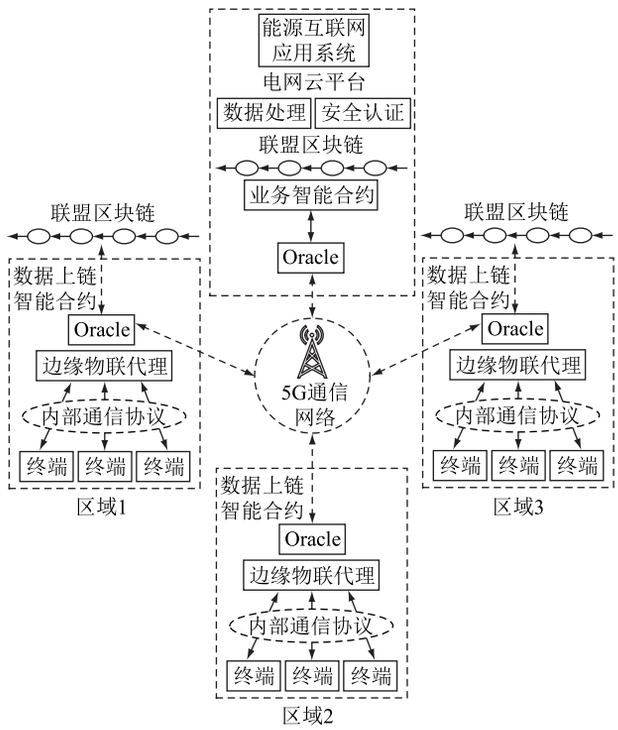

图 4　可信数据上链架构

Fig.4　Trusted data feed architecture

专用的内部通信协议与各自区域的边缘物联代理通信；边缘物联代理负责汇总所属区域内数据源的数据；所有 Oracle 节点组成分布式评估网络对链下数据源的数据进行可信性评估，通过评估的数据源由所属上行边缘物联代理的 Oracle 进行数据上链。其中，联盟区块链系统通过智能合约与所有 Oracle 节点进行互联，实现链下可信数据的共识记账。

2.2　数据上链流程

电力区块链应用系统由电力物联网终端（T）、边缘物联代理（E）、Oracle（O）、云端业务系统（B）、5G 切片管理器、联盟区块链（C）系统等组成，其工作流程如图 5 所示。

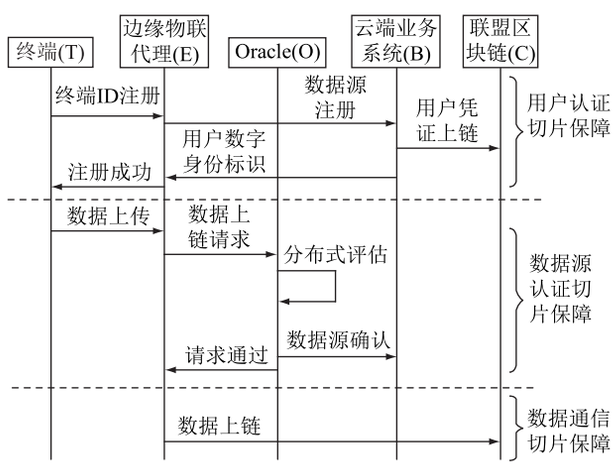

图 5　电力区块链应用系统工作流程

Fig.5　Power blackchain application system workflow

系统工作流程分为数据源注册、数据源评估和数据上链 3 个过程。

(1) 数据源注册。电力物联网终端接入系统前,首先用标识号(ID)向边缘物联代理进行注册:

$$\mathrm{T}\rightarrow\mathrm{E}:E(K_{\mathrm{T}\leftrightarrow\mathrm{E}},I_{\mathrm{T}}\parallel I_{\mathrm{B}}\parallel T_1) \tag{1}$$

式中:$K_{\mathrm{T}\leftrightarrow\mathrm{E}}$ 为 T 和 E 之间的共享密钥;I_{T} 为终端标识;I_{B} 为云端业务系统标识;T_1 为注册请求时间戳;$E(x,y)$ 为加密函数,有 2 个参数,第一个参数是加密用的密钥,第二个是被加密的明文,验证方可以通过共享密钥解密得到被加密的数据。

边缘物联代理使用密钥 $K_{\mathrm{T}\leftrightarrow\mathrm{E}}$ 解密得到终端的标识等信息,进行所属域内身份验证,验证通过后进行数据源注册:

$$\mathrm{E}\rightarrow\mathrm{B}:E(K_{\mathrm{E}\leftrightarrow\mathrm{B}},I_{\mathrm{E}}\parallel I_{\mathrm{O}}\parallel T_2) \tag{2}$$

式中:$K_{\mathrm{E}\leftrightarrow\mathrm{B}}$ 为 E 和 B 之间的共享密钥;I_{E} 为边缘物联代理的标识;I_{O} 为 Oracle 标识;T_2 为注册成功时间戳。

云端业务系统验证边缘物联代理的注册信息,通过后发送用户的数字身份标识 $I_{\mathrm{DID\text{-}T}}$:

$$\mathrm{B}\rightarrow\mathrm{E}:I_{\mathrm{DID\text{-}T}}=E(K_{\mathrm{E}\leftrightarrow\mathrm{B}},K_{\mathrm{O}\leftrightarrow\mathrm{C}}\parallel I_{\mathrm{O}}\parallel T_{\mathrm{ticket\text{-}O}}) \tag{3}$$

式中:$T_{\mathrm{ticket\text{-}O}}$ 为边缘物联代理访问云端业务系统的票据。计算方式为:

$$T_{\mathrm{ticket\text{-}O}}=E(K_{\mathrm{B}\leftrightarrow\mathrm{C}},I_{\mathrm{O}}\parallel T_3) \tag{4}$$

式中:$K_{\mathrm{B}\leftrightarrow\mathrm{C}}$ 为 B 和 C 之间的共享密钥;T_3 为票据生成时间戳。

获得终端分布式数字身份标识 $I_{\mathrm{DID\text{-}T}}$ 后,边缘物联代理向终端回复注册成功。

(2) 数据源评估。由分布式 Oracle 网络对数据源进行评估。当电力物联网终端上传数据到边缘物联代理之后,边缘物联代理发起数据上链请求,所有边缘物联代理上运行的 Oracle 组成评估组对此数据源进行联合评估并通过投票的方式提交结果。评估过程中交互数据通过数据源认证切片组成的 P2P(peer to peer)认证网络进行传输。评估通过后,数据源可通过上行边缘物联代理的 Oracle 实现数据上链,评估不通过则被退回并记录日志。评估过程分为以下 3 个步骤。

步骤一:所有边缘物联代理上的 Oracle 对被评估数据源的可信性进行评分,评分数据用基于 RSA 算法的可验证随机函数进行计算,任何接收方可通过评分者的公钥验证评分数据的可信性。具体如下。

设电力区块链应用系统中存在 n 个 Oracle 节点,记为 $\{O_i\mid 1\leqslant i\leqslant n\}$,这些节点组成分布式 Oracle 网络。其中,$O_i$ 对数据源 j 的可信性评分为 $S_{ij}(0\leqslant S_{ij}\leqslant 100)$,$S_{ij}$ 通过可验证随机函数进行发布和验证。

首先,发布评分的 Oracle 运行 RSA 算法得到签名密钥 (d,σ) 和公钥 (e,σ)。其中 $\sigma=pq$;p,q 均为 O_i 选取的大素数。整数 e,d 分别满足:

$$\begin{cases}1<e<\varphi(\sigma)\\ \gcd(e,\varphi(\sigma))=1\\ \varphi(\sigma)=(p-1)(q-1)\end{cases} \tag{5}$$

$$de\equiv 1\bmod(\varphi(\sigma)) \tag{6}$$

式中:gcd(·)为最大公约函数;mod(·)为取模函数。

其次,Oracle 节点使用私钥进行签名,计算 v_i,作为对数据源 j 的可信性评分证据。

$$v_i=S_{ij}^{d}\bmod(\sigma) \tag{7}$$

步骤二:分布式 Oracle 网络通过 (k,n) 门限签名算法对评分数据进行汇总,其中 k 为门限值。具体如下。

设分布式 Oracle 网络的公钥为 P_k,私钥为 S_k,p' 为大素数。选取有限域 $GF(p')$ 上系数为 a_i 的 $k-1$阶插值多项式 $f(x)$:

$$f(x)=S_k+\sum_{i=1}^{k-1}a_i x^i\bmod(p') \tag{8}$$

为每个 Oracle 选取子密钥生成参数 x_i,分配影子密钥 $(x_i,f(x_i))(1\leqslant i\leqslant n)$。当 Oracle 节点对数据源做出信任值评分后,提交 $E_{ij}=(S_{ij},v_i,x_i,f(x_i))$ 作为分布式评估凭据。

步骤三:数据源评估汇总。Oracle 节点通过 Raft 共识算法选出 leader 节点,汇总 Oracle 提交的评估数据。具体如下。

首先,获取至少 k 个 Oracle 提交的有效评估数据,即 $\{E_{ij}\mid j=1,2,\cdots,k\}$。验证过程使用 Oracle 节点的公钥进行验证,若 $S_{ij}=v_i^{e}\bmod(\varphi(\sigma))$ 成立,则说明节点提交了有效的数据。

其次,使用拉格朗日插值算法,获取 Oracle 网络的签名密钥:

$$\begin{cases}f(x)=\sum_{j=1}^{k}f(x_j)\prod_{\substack{l=1\\ l\neq j}}^{k}\dfrac{x-x_l}{x_j-x_l}\bmod(p')\\ S_k=f(0)\end{cases} \tag{9}$$

使用此签名密钥,提交分布式 Oracle 网络对数据源 j 的评分汇总,作为数据源评估的依据。

(3) 数据上链。通过评估后的数据源可以将链下数据进行上链存储,上链过程由 Oracle 触发智能合约实现。

首先,数据源上行边缘物联代理对数据进行规范化,规范化过程参考 T/CESA 6002—2017。其中,业务数据主要包括事务数据和实体数据。事务数

据描述区块链系统上具体业务动作，事务列表中的每一项表示一种业务操作，事务数据定义为<事务标识(哈希值)，事务类型，签名者，时间戳>。实体数据描述事务的静态属性，定义为<发起方地址，接受方地址，附加数据，备注>。

其次，通过智能合约实现数据上链。智能合约每次调用时从区块链上读取合约逻辑和上一个状态，执行后将新的状态存入区块并在所有节点中发布。由于数据源已通过可信性评估，在共识算法运行过程中，该边缘物联代理所在的 peer 节点直接作为 leader 节点进行记账，生成新的区块，实现数据上链。此过程包括合约生成、合约发布、合约执行 3 个步骤。

步骤一：合约生成。智能合约部署于 peer 节点上，其中包含了数据源的认证信息。对于可信的数据源，智能合约对其数据上链事务进行了程序化和规范化。

步骤二：合约发布。新智能合约经过创建者数字签名后，以访问地址和哈希摘要的方式发布到区块链上，区块链其他节点据此对合约的完整性进行验证。合约的发布过程实现了所有节点对该智能合约有效性的共识。

步骤三：合约执行。由数据源的数据上传事件触发合约执行，在调用过程中更新本地账本状态，调用完成后确认交易并向其他节点广播交易。由于合约中携带了验证信息，所以可以安全高效地上传数据。

2.3 上链过程切片优化

电力 5G 端到端切片运行和管理主要由通信服务管理(communication service management function，CSMF)、网络切片管理(network slice management function，NSMF)、网络切片子网管理(network slice subnet management function，NSSMF)等部件完成。其中，CSMF 将电力业务目标和需求映射为端到端网络切片需求并传递到 NSMF，NSMF 根据各子网能力进行端到端切片设计，产生切片实例并进行编排管理，进而将整个网络切片的 SLA 分解为不同切片子网(例如核心网切片子网、无线网切片子网和承载网切片子网)的 SLA，同时将子网部署需求传递到 NSSMF。核心网、传输网和无线网均有各自的 NSSMF，主要实现子网内切片部署、运行和监控。

设 $S=\{S_u,S_d,S_c\}$ 为电力 5G 区块链应用系统的切片集合，其中 S_u 为用户身份认证切片；S_d 为数据源评估切片；S_c 为数据上链传输切片。3 类切片具有用户和数据源身份注册认证、数据源评估和数据上链传输的顺次协同关系，即通过用户身份认证后才可以进行数据源评估，之后才能进行可信数据上链传输。$X_u(\gamma)\in\{0,1\}$，$X_d(\gamma)\in\{0,1\}$，$X_c(\gamma)\in\{0,1\}$ 为任务指派变量，值为 1 表示将对应的任务指派给相应切片。即：

$$X_x(\gamma)=\begin{cases}0 & \text{不指派 } x \text{ 任务给切片 } \gamma\\ 1 & \text{将 } x \text{ 任务指派给切片 } \gamma\end{cases} \tag{10}$$

其中，$x\in\{u,d,c\}$ 为任务类型变量，u,d,c 分别代表用户和数据源身份注册认证、数据源评估以及可信数据上链传输 3 种任务类型。

每种任务类型包含一系列并发运行的子任务，例如数据源评估任务可包含多个并发的数据源评估子任务，系统根据任务类型分配相应的网络资源构建对应 5G 网络切片，如图 6 所示。

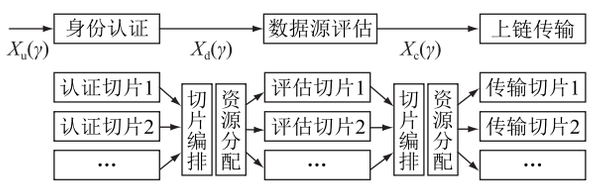

图 6 切片任务分配示意

Fig.6 Schematic diagram of slicing task allocation

设切片传输带宽为 β；第 i 个 Oracle 节点到 5G 基站间的传输损耗为 L_i；当前切片接入的 Oracle 数量为 n_s；发射功率为 S；噪声总功率为 N。当资源分配均衡时，第 i 个 Oracle 节点的数据传输速率 R_O 为：

$$R_O=\frac{\beta L_i}{n_s+1}\log_2\left(1+\frac{S}{N}\right) \tag{11}$$

设系统中可提供服务的 5G 基站数量为 m，第 i 个 Oracle 需要上链的数据量为 D_i，则系统传输的总数据量为：

$$D_{total}=\sum_{i=1}^{n}D_i \tag{12}$$

系统总传输能力为：

$$T_{total}=\sum_{i=1}^{n}\sum_{\gamma=1}^{m}R_OX_u(\gamma)+\sum_{i=1}^{n}\sum_{\gamma=1}^{m}R_OX_d(\gamma)+\sum_{i=1}^{n}\sum_{\gamma=1}^{m}R_OX_c(\gamma) \tag{13}$$

总时延可表示为：

$$L=D_{total}/T_{total} \tag{14}$$

对上述时延函数进行优化可以得到最优数据上链的资源配置方案。

3 应用验证

3.1 应用场景

应用验证场景为 5G 通信环境中基于区块链的

用电信息采集系统(文中简称为用采系统)。用采系统是对电力用户的用电信息进行采集、处理和实时监控的信息系统,具有用电信息自动采集、分析、监控和智能交互等功能。应用验证使用的系统架构如图 7 所示。

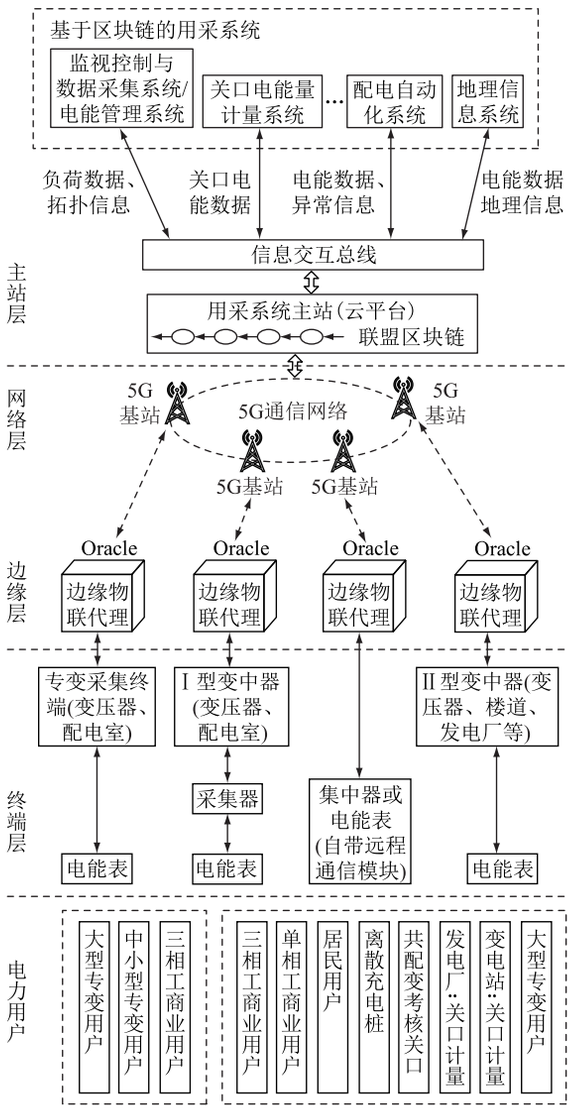

图 7　应用验证架构

Fig.7　Application verification architecture

验证场景中的用采系统由主站层、网络层、边缘层、终端层组成。向上为电力应用系统提供服务,数据交互由营销系统及其他应用系统通过相应接口实现;向下通过电能表、采集器等数据采集装置接入电力用户系统。主站层集中部署于省电力公司,直接采集全省范围内的所有现场终端和表计,集中处理信息采集、数据存储和业务应用。用采系统主站的数据采集分为定时自动采集、随机召测和主动上报 3 种,文中验证场景采用定时自动采集方式。其中,专变采集终端上行数据为 538 B,下行数据为 248 B,控制指令为 40 B。集中抄表终端包含 240 个单相表,12 个三相表,轮询周期为 15 min,数据包发送速率为 1.2 Kb/s。其他主要参数参考 Q/GDW 1376.1—2013 进行设置。

验证系统采用 Hyperledger Fabric1.4 搭建联盟区块链系统。在云端用采系统主站、各边缘物联代理中部署 peer 节点,其中物理节点 5 个,硬件采用 Xeon Silver 4114 处理器,内存为 64 GB DDR4,SAS 2.4 TB 硬盘,操作系统采用 Ubuntu 18.04,部署 Docker 17.06.2、Docker Compose 1.14、Node.js 8.9.x。为扩大验证规模,部署基于 Docker 实现的虚拟节点 20 个。边缘物联代理上的 peer 节点部署 Oracle 机制,智能合约使用 Go 语言编制,验证系统的共识算法采用更适合电力生产环境的 Raft 共识算法。将仿真时间划分为不定长度的时间片 term,在每个 term 内,所有 peer 节点通过选举产生 leader 节点进行记账,若某个 Oracle 所在的 peer 节点完成了数据源认证,则自动选择为下一 term 的 leader 节点。

网络层采用 5G 进行通信,5G 网络主要包含集中单元(centralized unit,CU)、分布单元(distribute unit,DU)、有源天线单元(active antenna unit,AAU),其架构如图 8 所示。

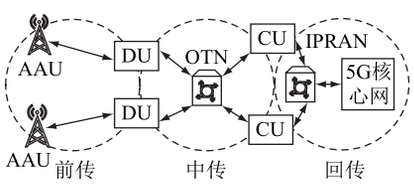

图 8　5G 网络架构

Fig.8　5G network architecture

其中,AAU 到 DU 的前传采用光纤直连模式,速率为 25 Gb/s;DU 和 CU 的中传和 CU 以上的回传采用分组增强型光传送网(optical transport network,OTN)结合互联协议化无线接入网(internet protocol radio access network,IPRAN)模式,速率为 50 Gb/s。采用的主要设备如表 1 所示。

表 1　5G 设备

Table 1　5G equipment

设备	型号
核心网交换机	华为 CE8861
基带处理单元	BBU5900
基带板	UBBPg2a
主控板	UMPTe3
AAU	AAU5613
电源	DCDU-12B 48 V

3.2　通信性能

为验证电力 5G 区块链节点间组网和切片优化

方案的通信有效性，测试网络对 10 Kb 数据包和 1 Kb 数据包 2 种规格的数据包传输性能。2 种数据包规格分别对应采集数据和控制指令的传输能力。每组测试采样 20 次，每次采样做 80%、40%、10%这 3 种不同负载情况下共 90 次数据传输，测试结果取每种情况的平均值。

10 Kb 上行时延曲线如图 9 所示。在此传输情况下，时延总体趋势平缓。其中，80%负载情况下，时延在 10 ms 左右；40%负载情况下，时延较 80%负载下降约 10%；10%负载情况下，时延进一步降低，均值在 8.6 ms 左右。

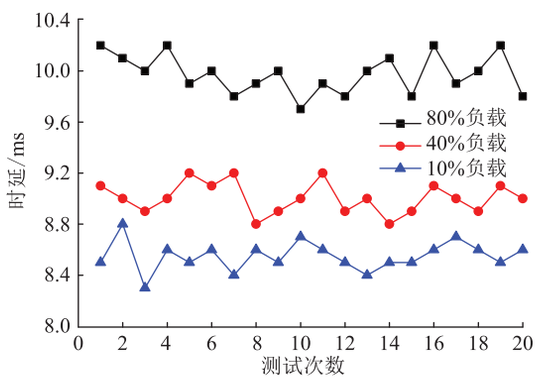

图 9　10 Kb 上行时延曲线

Fig.9　10 Kb uplink delay curves

10 Kb 下行时延曲线如图 10 所示。可以看出，在 40%负载和 10%负载的情况下，下行时延较上行时延进一步降低，其均值稳定在 6 ms 和 4 ms 左右。

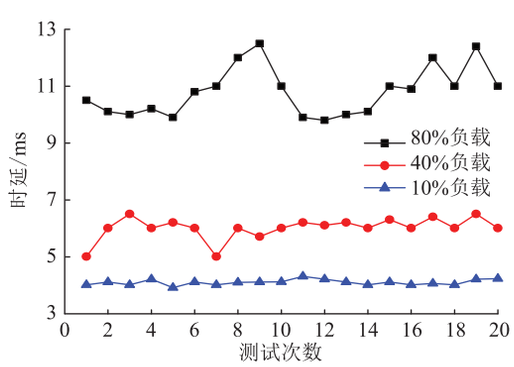

图 10　10 Kb 下行时延曲线

Fig.10　10 Kb downlink delay curves

从 10 Kb 上、下行测试结果来看，基于 5G 的通信系统可有效支撑 Oracle 节点之间以 P2P 方式进行可信性认证和数据传输。而 10 Kb 数据包的大小正好符合专变采集终端等用采系统采集设备的数据传输规格，因而能有力支撑用采系统的数据采集性能。

对于控制指令等小数据包的传输性能也是通信网络的重要指标。图 11 和图 12 分别为 1 Kb 数据包上行和下行的时延曲线。其中，上行数据在 40%负载情况下网络传输时延均值为 8.5 ms，较同等情况下的 10 Kb 数据包的传输性能提高 5%。下行数据在 40%负载情况下性能较同等情况下 10 Kb 数据包的传输性能提高 30%。

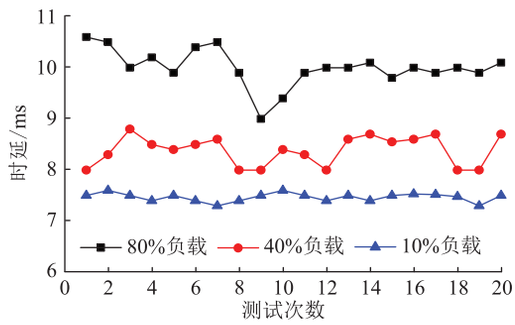

图 11　1 Kb 上行时延曲线

Fig.11　1 Kb uplink delay curves

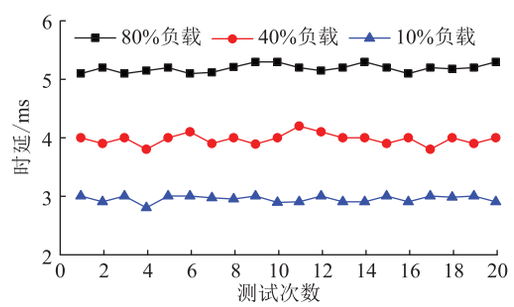

图 12　1 Kb 下行时延曲线

Fig.12　1 Kb downlink delay curves

网络抖动是描述时延变化程度的指标，可以表示网络拥塞时排队延迟导致的端到端数据传输性能，因此是研究网络实时性的重要参数。不同数据传输规格在 80%负载情况下的抖动情况如图 13 所示。

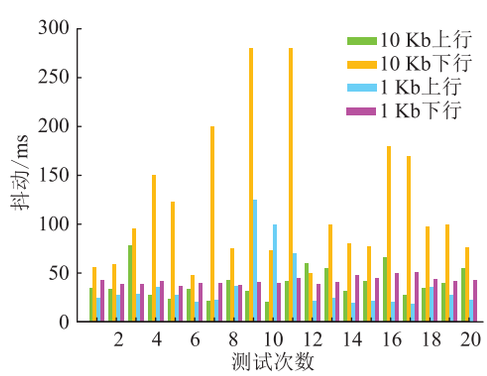

图 13　不同传输规格下抖动对比

Fig.13　Jitter comparison under different data volumes

从实验数据可以看出，在高负载情况下，10 Kb 上行、1 Kb 上行和 1 Kb 下行具有较低的抖动，但 10 Kb 下行抖动数据较大，这是因为 10 Kb 下行的数据在高负载情况下数据传输请求明显集中，导致排队延迟较大，这也是进一步优化网络的方向。

为进一步测试网络的传输能力和传输质量,在80%负载情况下通过加载额外的测试流量,测试丢包率和误码率。丢包率为网络传输过程中丢失数据包数量占所有发送数据包的比率,是反映网络吞吐性能的重要指标。误码率为传输过程中的误码占所有传输总码数的比率,是衡量网络数据传输精确性的指标。实验过程通过在被测通信链路两端加载双向流量进行压力测试,取 10 次测量的平均值,测试结果如图 14 所示。

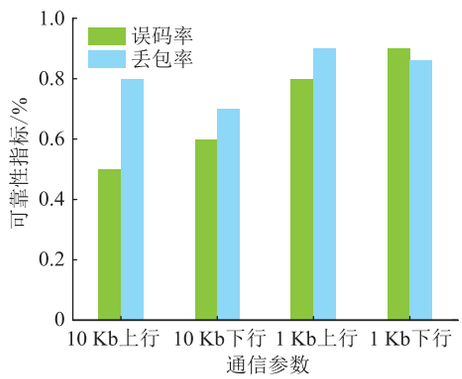

图 14 误码率和丢包率分析

Fig.14 Analysis of bit error rate and packet loss rate

从实验数据可以看出,1 Kb 小数据包和 10 Kb 大数据包在上行和下行通信过程中的丢包率和误码率都没有超过 0.9%,具有较好的通信质量,能满足电力 5G 业务需求。

3.3 业务性能

文中从用采业务的角度进行分析和验证,重点研究注册认证、数据源评估、数据召测等业务的时延、成功率等性能指标。图 15 为 0~100 并发区间内不同业务从请求到完成的时延曲线。

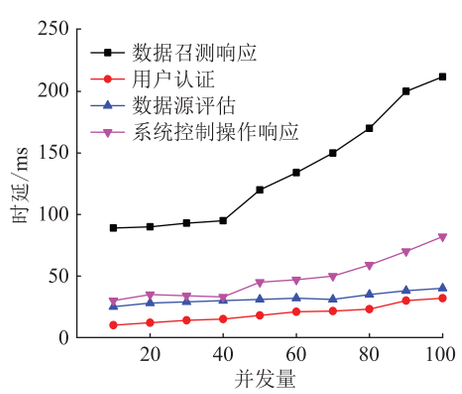

图 15 业务时延

Fig.15 Service delay

从实验数据可以看出,数据召测响应时延最大,在 40 并发量之前时延低于 100 ms,当并发量超过 40 时业务响应时间增加量较大,最大时延接近 250 ms。相比于数据召测响应,其他 3 类业务时延较低,均值在 100 ms 以下。其中,系统控制操作响应时延大于数据源评估时延,用户认证时延最低。这是因为文中方案对用户认证和数据源评估采用了更好的切片优化方案,加之数据传输量相对较小,所以能保证响应更快速。

图 16 为在不同并发量情况下运行 Oracle 的节点平均性能。随着并发量增加,节点的中央处理器(central processing unit,CPU)和内存占用呈增加趋势。其中,CPU 平均利用率在 60%以下时随并发量增加的增长趋势明显,之后趋于平缓。而内存平均利用率的增长率保持在一个相对固定的值,整体呈线性增长趋势。

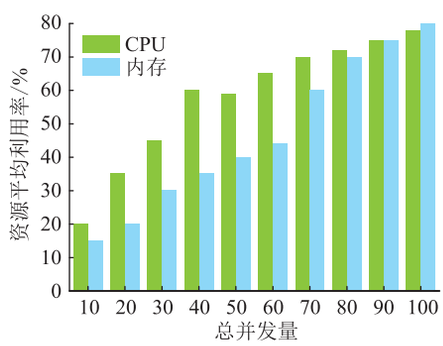

图 16 系统资源消耗

Fig.16 System resource consumption

为进一步验证方案的有效性,文中选取了文献[9-11]中的电力区块链应用系统进行对比分析。图 17 为在相同资源配置下不同电力区块链应用方案的时延对比曲线。通过综合对比,文中所提方案在时延指标上与已有方案相比具有显著优势,在 100 量级并发业务请求情况下,较已有方案性能提升超过 80% ,这是因为文中方案实现了数据上链前和上链中的两级优化。上链前,在对 5G 切片进行优化调度的基础上,实现了 S_u,S_d,S_e 这 3 类切片的细粒度并发任务分配,以及针对 Oracle 节点数($n=24$)、基站部署($m=2$)和数据传输量($D_i=t\times10$ Kb,t 为单位时间)的优化配置,使节点间的通信时延大幅度降低;上链中,采用分布式 Oracle 网络对数据源进行验证后直接上链,验证过程和上链过程的通信由不同 5G 切片承载,对于验证通过的可信数据源,采用直接上链的方式,减少了区块链系统共识记账的复杂度。对比文献中,文献[9]与文中方案的时延最为接近;文献[10]融合运用多种密码学技术确保数据安全可信,因而具有较高的计算开销;而文献[11]采用了终端入网和认证 2 个过程实现数据上链,但节点间传输信息量增加,造成了额外的时间开销。

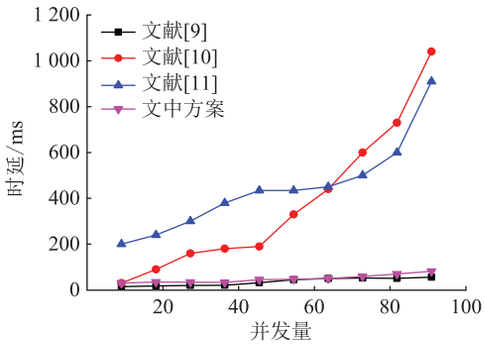

图 17　已有方案时延对比曲线

Fig.17　Delay comparison curves of existing schemes

基于区块链的应用系统中对数据的认证评估是产生时延的主要因素。为验证所提基于门限签名算法和可验证随机函数的分布式 Oracle 数据源认证的优势，通过实验对比同等条件下不同方案在认证阶段和评估阶段的时延组成情况，结果如图 18 所示。

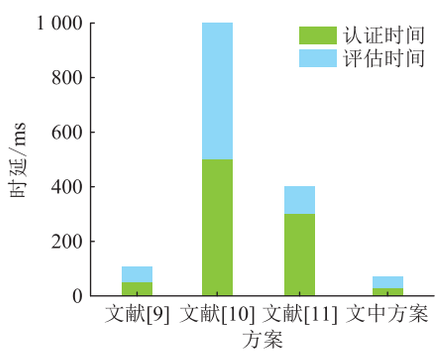

图 18　已有方案认证评估时延组成对比

Fig.18　Comparison of delay composition for authentication evaluation of existing schemes

由图 18 可以看出，文中方案在认证时间和评估时间以及总时间方面都具有显著优势，这是因为文中方案将主要运算开销分布于系统资源相对丰富的边缘侧，各边缘物联代理之间通过高性能的 5G 网络进行通信，在很大程度上提高了认证效率。

文中方案中基于门限签名算法实现了分布式 Oracle 网络对数据源的认证过程。对于门限方案，参与评估的 peer 节点数量和门限值的数量会对签名性能产生一定影响。为研究此规律，文中设计了不同节点数量 n 和门限值 k 组合情况下的认证时延和一次认证成功率，如图 19、图 20 所示。

从数据可以得出，随着参与评估的 peer 节点数量增加，认证时延有所增加，认证成功率呈降低趋势，这是因为分布式 Oracle 网络规模的增加导致共享密钥分发量增加，认证交互次数和随机数验证次数也相应增加。在相同的 peer 节点数量下，随着门限值增加，认证时延也会增加，认证成功率同样会

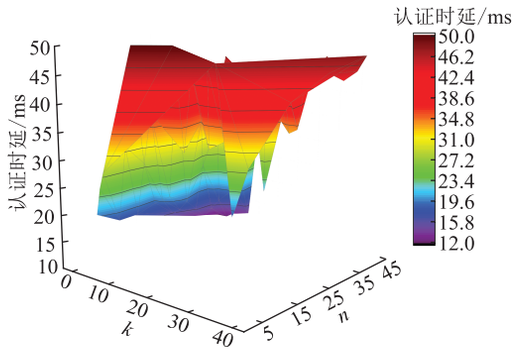

图 19　不同门限值对认证时间的影响

Fig.19　Influence of different threshold values on authentication time

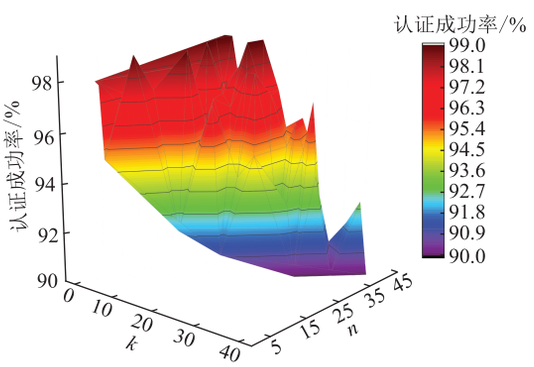

图 20　不同门限值的一次认证成功率

Fig.20　Primary authentication success rates with different threshold values

降低，这是因为增加门限值相当于增加了安全等级，插值多项式的次数也相应增加，被认证的数据源需要有更多的 Oracle 节点对其背书，因此系统总体性能下降。尽管如此，系统总的时延仍然保持在 50 ms 以下，一次认证成功率保持在 90%以上，这是因为 5G 通信的高效能和文中所提方案的有效性保证了系统总体运行性能。

4　结语

区块链系统数据上链性能是制约电力区块链应用推广的重要因素，存在的主要问题包括两方面，一是区块链的共识机制涉及大量的 P2P 信息交互，传统网络通信手段难以满足这种高并发和低时延的要求；二是智能合约对链下数据源的认证能力弱，须引入 Oracle 机制进行数据源可信性验证，随着电力区块链应用规模增加，验证的有效性和可靠性须进一步提高。文中基于上述两方面问题，研究了基于 5G 切片的分布式 Oracle 网络可信数据上链的架构、认证算法和流程，并对 5G 切片部署方式进行了优化。实验表明，所提方案在通信性能、业务性能、资源利用等方面具有优势。进一步研究将侧

重于基于安全多方计算和隐私计算的跨域异构数据源相互认证方案及其应用试点。

本文得到国网江苏省电力有限公司科技项目“5G 确定性网络技术与电力业务适配性研究与应用”(J2021125)资助,谨此致谢!

参考文献:

[1] 王智慧,汪洋,孟萨出拉,等.5G 技术架构及电力应用关键技术概述[J]. 电力信息与通信技术,2020,18(8):8-19.
WANG Zhihui, WANG Yang, MENG Sachula, et al. 5G technology architecture and key technologies of power application[J]. Electric Power Information and Communication Technology, 2020,18(8):8-19.

[2] 梅文明,王栋. 区块链技术在电力领域应用场景的探索分析[J]. 电力信息与通信技术,2020,18(2):21-29.
MEI Wenming, WANG Dong. Exploration and analysis of power application scenarios for blockchain technology[J]. Electric Power Information and Communication Technology, 2020, 18(2): 21-29.

[3] 李大伟,宋春晓,李斌,等. 电力区块链基础设施架构及其设计与实现[J]. 电力工程技术,2021,40(2):93-100.
LI Dawei, SONG Chunxiao, LI Bin, et al. Blockchain technology in power system: infrastructure architecture, design and implementation[J]. Electric Power Engineering Technology, 2021, 40(2):93-100.

[4] GAO J B, OBOUR AGYEKUM K O B, SIFAH E B, et al. A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks[J]. IEEE Internet of Things Journal, 2020, 7(5):4278-4291.

[5] 陈俊,黄飞宇,黎作明. 基于 DQN 的电力物联网 5G 边缘切片资源管理研究[J]. 电测与仪表,2022,59(1):155-161.
CHEN Jun, HUANG Feiyu, LI Zuoming. Research on DQN-based 5G edge slicing resource management of power Internet of Things[J]. Electrical Measurement & Instrumentation, 2022, 59(1):155-161.

[6] 于浩,汪筱巍,王韬,等. 基于 SDN 与 NFV 的电力 5G 网络切片差异化资源分配方案[J]. 电测与仪表,2021,58(9):89-95.
YU Hao, WANG Xiaowei, WANG Tao, et al. Differential resource allocation scheme for electric 5G network slices based on SDN and NFV[J]. Electrical Measurement & Instrumentation, 2021,58(9):89-95.

[7] 贺金红,张港红,高建. 5G 切片技术在电力物联网应用的智能化管理[J]. 电力信息与通信技术,2020,18(5):19-25.
HE Jinhong, ZHANG Ganghong, GAO Jian. Intelligent management of 5G slices in the application of power Internet of Things [J]. Electric Power Information and Communication Technology, 2020, 18(5):19-25.

[8] 许俊晓,崔昊杨,江超,等. 电力用户信息的多区块链管理及跨链查询方法研究[J/OL]. 电测与仪表,2022:1-9[2022-06-20]. https://kns.cnki.net/kcms/detail/23.1202.th.20220302.1645.006.html.
XU Junxiao, CUI Haoyang, JIANG Chao, et al. Research on multi-blockchain management and cross-chain query method of power user information[J/OL]. Electrical Measurement& Instrumentation, 2022: 1-9[2022-06-20]. https://kns.cnki.net/kcms/detail/23.1202.th.20220302.1645.006.html.

[9] 张显,冯景丽,常新,等. 基于区块链技术的绿色电力交易系统设计及应用[J/OL]. 电力系统自动化,2022:1-12[2022-06-20]. https://kns.cnki.net/kcms/detail/32.1180.TP.20220308.1130.002.html.
ZHANG Xian, FENG Jingli, CHANG Xin, et al. Design andapplication of green power trading system based on blockchain technology[J/OL]. Automation of Electric Power Systems, 2022: 1-12[2022-06-20]. https://kns.cnki.net/kcms/detail/32.1180.TP.20220308.1130.002.html.

[10] 赵丙镇,陈智雨,闫龙川,等. 基于区块链架构的电力业务交易数据隐私保护[J]. 电力系统自动化,2021,45(17):20-26.
ZHAO Bingzhen, CHEN Zhiyu, YAN Longchuan, et al. Privacy protection of power business transaction data based on blockchain framework[J]. Automation of Electric Power Systems, 2021,45(17):20-26.

[11] 陈汹,朱钰,封科,等. 基于区块链的电力系统安全稳定控制终端身份认证[J]. 广西师范大学学报(自然科学版),2020,38(2):8-18.
CHEN Xiong, ZHU Yu, FENG Ke, et al. Identity authentication of power system safety and stability control terminals based on blockchain[J]. Journal of Guangxi Normal University (Natural Science Edition), 2020, 38(2):8-18.

[12] CHAER A, SALAH K, LIMA C, et al. Blockchain for 5G: opportunities and challenges[C]//2019 IEEE Globecom Workshops. Waikoloa, HI, USA. IEEE, 2019:1-6.

[13] VALTANEN K, BACKMAN J, YRJÖLÄ S. Blockchain-powered value creation in the 5G and smart grid use cases[J]. IEEE Access, 7:25690-25707.

[14] YANG H, LIANG Y S, YUAN J Q, et al. Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5G and beyond[J]. IEEE Transactions on Industrial Informatics, 2020, Issue:1.

[15] 郭媛媛,李赓,牟华. 跨境贸易区块链溯源数据上链方式研究[J]. 数字通信世界,2020(8):76-79.
GUO Yuanyuan, LI Geng, MU Hua. Research on the way of uploading traceability data of cross-border trade blockchain [J]. Digital Communication World, 2020(8):76-79.

[16] WANG S, LU H, SUN X K, et al. A novel blockchain oracle implementation scheme based on application specific knowledge engines[C]//2019 IEEE International Conference on Service Operations and Logistics, and Informatics. Zhengzhou, China. IEEE, 2019:258-262.

[17] CHISHTI M S, SUFYAN F, BANERJEE A. Decentralized on-chain data access via smart contracts in ethereum blockchain [J]. IEEE Transactions on Network and Service Management, 2022, 19(1):174-187.

[18] Documentation of provable [EB/OL]. [2022-06-20]. https://docs.provable.xyz.

[19] ZHANG F, CECCHETTI E, CROMAN K, et al. Town crier: an authenticated data feed for smart contracts [C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria. New York: ACM, 2016: 270-282.

[20] LORENZ B, CHRISTIAN C, BENEDICT C, et al. Chainlink 2.0: next steps in the evolution of decentralized Oracle networks [EB/OL]. [2022-06-20]. https://research. chain. link/whitepaper-v2.pdf? _ga = 2.89191442.80128620716654-83992-784756542.1665483992.

[21] DOS NETWORK. DOS network white paper [EB/OL]. [2022-06-20]. https://s3. amazonaws. com/whitepaper. dos/DOS + Network+Technical+Whitepaper.pdf.

[22] FISCO BCOS. Truora document [EB/OL]. [2022-06-20]. https://truora.readthedocs.io/zh_CN/latest/.

[23] BENIICHE A, ROSTAMI S, MAIER M. Robonomics in the 6G era: playing the trust game with on-chaining oracles and persuasive robots [J]. IEEE Access, 9: 46949-46959.

[24] WANG Y H, LIU H M, WANG J H, et al. Efficient data interaction of blockchain smart contract with oracle mechanism [C]//2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference. Chongqing, China. IEEE, 2020: 1000-1003.

[25] 毕丹阳, 张钰雯, 毕雅晴. 基于预言机的可信数据上链技术 [J]. 信息通信技术与政策, 2021, 47(9): 79-84.
BI Danyang, ZHANG Yuwen, BI Yaqing. Trusted data feed technology based on Oracle [J]. Information and Communications Technology and Policy, 2021, 47(9): 79-84.

作者简介:


李大伟

李大伟(1981), 男, 博士, 副教授, 研究方向为电力 5G 通信、区块链、信息安全、电力物联网技术(E-mail: lidw@ njit.edu.cn);

朱道华(1987), 男, 博士, 高级工程师, 从事无线通信技术相关工作;

郭雅娟(1975), 女, 硕士, 研究员级高级工程师, 从事电力信息通信技术相关工作。

Power 5G trusted data feed technology based on Oracle mechanism

LI Dawei[1], ZHU Daohua[2], GUO Yajuan[2], WEI Lei[3], SUN Yunxiao[2], LIU Wei[2]

(1. School of Computer Engineering, Nanjing Institute of Technology, Nanjing 211167, China;
2. State Grid Jiangsu Electric Power Co., Ltd. Research Institute, Nanjing 211103, China;
3. State Grid Jiangsu Electric Power Co., Ltd., Nanjing 210024, China)

Abstract: Aiming at the efficiency and credibility of data feed in power blockchain application system, the trusted data feed technology based on 5G and Oracle mechanism is studied. Firstly, the data feed method in the blockchain system is discussed, and the Oracle data feed method applicable to the power 5G blockchain is analyzed. Secondly, the trusted data feed technology of the power 5G business system based on distributed Oracle is proposed, and the overall system architecture based on cloud-edge-terminal integration is designed, as well as the workflow of data source registration, evaluation and on chaining. Among them, the distributed data collection and sharing are realized through the blockchain system, and the data source evaluation is realized based on threshold signature algorithm and verifiable random function. The evaluation algorithm is run by the edge Internet of Things (IoT) agent node to ensure the security and availability of the system. Through the division and optimization of 5G slice tasks, the efficient transmission of authentication data and business data is achieved. Finally, the proposed scheme is deployed in the electricity 5G blockchain based power information acquisition system, and experimental verification is carried out from the aspects of communication performance, business performance, resource utilization, etc. The results show that the average data transmission delay of the proposed scheme under different load stress tests is about 10 ms, and the bit error rate and packet loss rate are less than 0.9%. In the case of 100-level concurrent service requests, the performance of the scheme is improved by more than 80% compared with the existing schemes, so it has good feasibility and promotion value.

Keywords: blockchain; Oracle; 5G; power Internet of Things; threshold signature algorithm; data feed

(编辑　陆海霞)