面向智能共享的内生可信网络体系架构

郭少勇，齐芃苑，代美玲，邱雪松，亓峰，张平
（北京邮电大学网络与交换技术国家重点实验室，北京 100876）

摘 要：针对网络智能共享需求，将区块链、人工智能等技术与网络融合，提出面向智能共享的内生可信网络体系架构，使网络资产共享具有内生可信。基于分布式联盟区块链，提出链上标识、链下信息关联的融合机制实现网络资源可信共享，设计可信共享协议实现共享数据安全实时交换，基于智能合约提出网络资源调度和服务组合方法实现服务可信共享。最后将所提架构应用于域名解析、跨域认证、虚拟网络运营等去中心化场景,实现了区块链与网络融合，支撑网络资产内生可信共享。

关键词：内生可信；共享；标识；区块链；去中心化
中图分类号：TN915.02
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020193

Endogenous trusted network architecture for intelligent sharing

GUO Shaoyong, QI Yuanyuan, DAI Meiling, QIU Xuesong, QI Feng, ZHANG Ping
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: To address the needs of intelligent sharing of network resources, blockchain and artificial intelligence were integrated with the network, and an endogenous trusted resource intelligent sharing network architecture was proposed to make network asset sharing have endogenous trust. Based on distributed alliance blockchain, an integration mechanism of on-chain identification and off-chain resource was proposed to achieve credible management of network resources. Security and trusted sharing protocols for network data was designed to synchronize data consensus within the network. Based on smart contract, network resource scheduling and service composition methods were presented to achieve trusted service sharing. Finally, the proposed architecture was applied to decentralized scenarios such as domain name resolution, cross domain authentication, and virtual network operation. The proposed architecture realizes the integration of blockchain and network and supports the endogenous trusted sharing of network assets.

Key words: endogenous trusted, sharing, identification, blockchain, decentralized

1 引言

随着新一代信息通信基础设施的建设发展，终端、边缘、网络、云通过共享释放富裕的通信、计算和存储等网络资源，支撑网络数据分发，提升网络服务能力，共享资源、数据和服务等网络资产，逐步构建价值交换互联网，成为网络发展的重要方向。但是对于以共享为核心驱动的融合网络，信任成为制约网络演进的关键问题，极大地限制了异构资源聚合、数据分发与服务提供的能力，阻碍了网络空间的健康有序发展。

区块链技术作为一种多方备份的分布式账本技术，通过共识约束的技术手段，可在一定程度上解决异构网络共享时的不信任与利益分配不公平

收稿日期：2020−06−12；**修回日期**：2020−08−25
通信作者：邱雪松，xsqiu@bupt.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2019YFB2102302）；国家自然科学基金资助项目（No.62071070）；教育部区场链核心计划基金资助项目（No.2020KJ010802）
Foundation Items: The National Key Research and Development Program of China (No.2019YFB2102302), The National Natural Science Foundation of China (No.62071070), Ministry of Education Blockchain Core Project (No.2020KJ010802)

等问题[1-2]。为此，许多学者将区块链应用于网络共享以解决信任问题，主要聚焦于融合架构、资源可信管理、数据共享访问、跨域服务协同等方面。Rosa 等[3]提出了基于区块链的跨域网络可信共享运营的框架，支持跨域资源对外提供统一的可信共享服务，推动新网络运营模式的建设。Yin 等[4]提出了一种去中心化的可信“超链接网络”架构，用于实现未来网络数据的可信共享与分发。Sharma 等[5-6]提出了基于区块链的“云−边−端”软件定义三层可信融合架构，实现资源安全可信管理，减轻安全攻击并提供实时分析服务，支撑网络服务提供商和消费者之间的可信交易。曾诗钦等[7]概述了区块链技术的特点，探讨了区块链与智慧城市、工业互联网融合应用。Wu 等[8]提出了一种软件定义的区块链网络构建方式，通过动态管理区块链节点来适应性大规模网络，提升网络的可信服务水平。Xu 等[9]提出了一种基于区块链得到分散式资源的管理方法，通过请求在数据中心之间的迁移和调度来降低能耗成本。Rawat 等[10]提出了一种融合软件定义、边缘计算、区块链技术的无线网络虚拟化管理机制，用于防止无线侧由于双花攻击等不可信行为造成的异构无线资源分配不公平性现象的发生。Feng 等[11]提出了基于区块链的移动边缘计算卸载和资源分配策略，构建了基于深度强化学习的协作计算卸载和资源分配算法来解决马尔可夫决策进程问题，但忽略了跨域资源动态预测与调整带来的安全可信的问题。Abbas 等[12]提出了基于区块链技术的软件定义架构，采用公有链和私有链来实现网络安全性与物联网效益的兼容，但区块链的效率成为制约该架构的可用性和可扩展性。Nicolas 等[13]提出了基于区块链的内容可信分发服务机制，利用可信中介通过网络功能服务链实现内容提供者与请求者共享，但难以满足异构网络共享的需求。

本文将区块链、人工智能等技术与网络融合，提出面向智能共享的内生可信网络体系架构，构建全节点、轻节点协同的联盟链，提出链上标识、链下信息关联的融合机制，设计数据安全可信的共享交换协议，基于智能合约，提出网络资源智能调度和服务组合方法，提供支持多方互信兼具公平性的网络共享服务，实现网络智能共享。

2　网络共享需求与挑战

以公共/私有的终端、边缘、网络、云构成的异构网络，其共享包含资源、数据与服务 3 个层面的网络资产，具体需求和挑战如下。

1) 异构网络资源共享。旨在释放广分布且闲散的通信、计算与存储资源，聚合形成巨大的网络资源能力，为丰富与拓展业务模式奠定基础。传统共享模式往往采用集中管理实现异构资源共享，该方式常常受到多方主体间的信任危机，难以支撑大规模异构网络资源的共享[14]。将区块链技术与异构网络资源相融合，成为当前许多学者和机构解决异构网络资源间信任问题关注的焦点，通常采用异构网络资源信息全量上链的方式，但区块链系统性能低下，难以满足大规模异构网络资源的海量信息共享的效率要求，限制了基于区块链的异构网络资源可信共享环境的可用性。如何利用区块链技术，实现链上、链下网络资源信息的融合成为研究热点。

2) 异构网络数据共享。旨在突破孤立、分散分布的网络数据共享瓶颈，实现网络数据的融合治理、知识学习与规律演化，衍生出网络共享数据的新价值。传统跨域封闭的网络数据由于行业、用户等自私行为，易造成网络数据隐私泄露与篡改不可信等现象，出现大量网络数据孤岛问题[15]。目前，将区块链与网络数据共享融合，已成为许多学者或机构解决网络数据孤岛问题的共识。通常是将区块链作为数据存储的介质[16-17]，但该方式存在区块链系统效率与增量数据管理、区块格式与网络数据适配等矛盾。如何保障区块链网络与网络数据的管理、存储与共享等兼容性和适应性成为研究焦点。

3) 异构网络服务共享。旨在聚合跨域分布的网络服务，提升网络服务能力，实现服务收益自动化分配，丰富与拓展未来网络业务模式。传统异构网络服务共享通常借鉴“市场模式”，建立统一服务平台，采用统一定价或者多轮协商机制，制定共享服务收益的分配模型。但是中心化网络服务共享缺乏监督技术手段，造成用户隐私易被泄露且收益分配不透明的现象，阻碍了网络服务的开放与发展[18]。已有学者通过引入区块链技术，建立众筹的共享服务机制，但该研究尚在初期。如何利用区块链技术，在兼顾网络服务提供者与使用者之间的隐私保护的同时，保障共享服务收益分配的公平性，成为研究趋势[19-20]。

3　内生可信网络体系架构

在区块链与网络共享的融合过程中，将资源、

数据与服务等网络资产信息全部注册到区块链上进行管理，会由于区块链链上资产信息管理与共识效率的限制，造成基于区块链的异构网络资源可信共享环境的不可用。为此，引入网络标识体系，用于资源、数据与服务等网络资产的识别与发现、数据的可信共享、兼具隐私保护的服务组合等，如图 1 所示。将资源、数据与服务作为网络资产进行描述建模，并抽取关键资产信息与标识映射，构建基于标识的网络资产管理机制，通过标识与关键资产信息的链上注册与管理，支持标识解析映射与定位到链下网络资产，实现链上标识、链下资产信息的融合管理模式。

基于网络标识，进一步构建基于区块链的内生可信网络架构，如图 2 所示。它由五层组成，分别是终端设备层、网络层、区块链层、平台层和应用层。此架构在逻辑上通过将联盟链与终端设备、网络设备集成，实现异构云网资源可信共享，利用软件定义技术，构建可信的虚拟网络运行环境，形成网络资源、数据

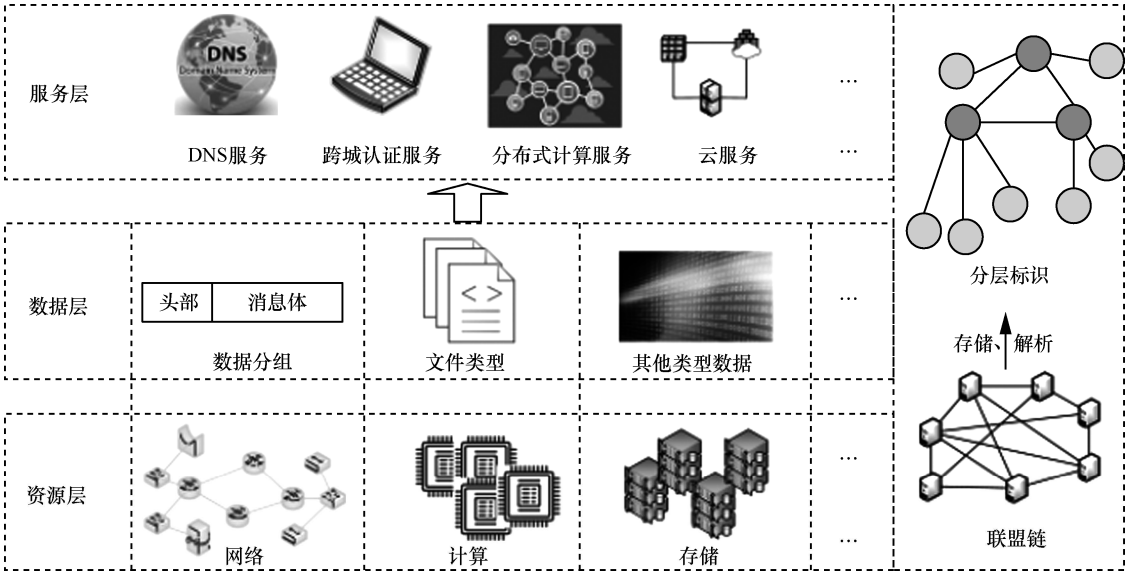


图 1　基于标识的网络共享模型

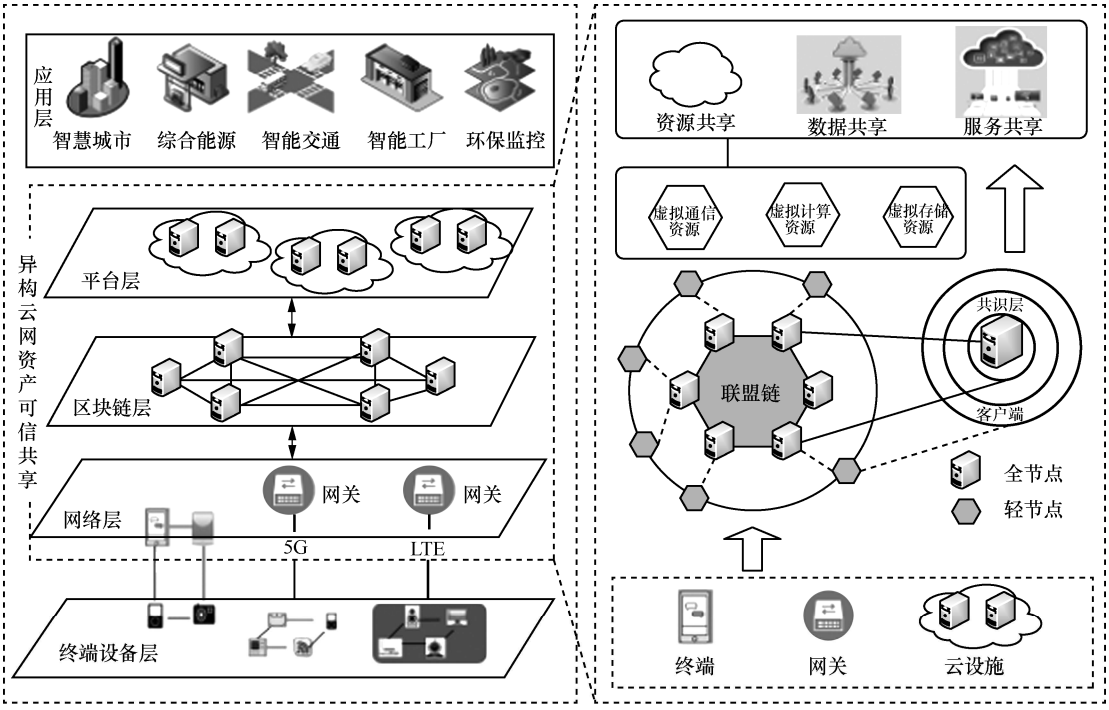


图 2　面向智能共享的内生可信网络体系架构

与服务等资产对外可信共享的服务平台，通过按需服务提供共享资产，满足差异化的应用需求。

该内生可信共享网络构建的核心思想是：在异构网络中利用计算与通信能力较强的终端、网关或云服务器节点组成联盟链的全节点，其他节点作为轻节点，将异构网络资产连接成对等多方互信的联盟，将网络资源、数据与服务等关键信息映射到标识并进行链上管理，通过改进实用拜占庭容错（PBFT, practical Byzantine fault tolerance）共识算法实现全节点间的快速共识达成，而轻节点仅部署区块链客户端，参与联盟链上标识与关键资产信息的缓存和可信校验。

将异构网络的资源、数据与服务等资产信息，通过在区块链平台注册、溯源与行为审计，实现异构网络资源、数据、服务等资产接入、运行、退出全生命周期的信任管理，使共享网络资产具有内在信任管理机制，本文称之为内生可信。同时，在内生可信共享网络中，支持面向应用需求提供网络资源、数据与服务等共享资产的智能分配与优化，确保内生可信网络的智能共享能力，解决应用场景的适配性问题。

本文所提架构的关键技术包括分布式联盟链构建、网络资产共享模型、网络数据可信共享协议、共享资源智能调度、共享服务组合等，这些将在第 4 节展开详细介绍。

4　关键技术

4.1　支撑内生可信的分布式联盟链构建

为了有效支撑面向智能共享的内生可信网络的构建，需先建立相适配的高效区块链平台。制约区块链与网络共享融合的性能瓶颈主要体现在联盟链结构、节点规模与部署、共识机制与通信协议等[21]。为此本文采用了全节点与轻节点的方式形成联盟链结构[22]，但是要控制全节点的数量与规模，防止由于联盟节点过多而带来性能下降的问题。

同时，考虑到网络规模，也可以进一步设计主从链的架构，如图 3 所示。主链和从链本质上是联盟区块链。主链是公正可信的，可以确保异构网络跨域共享时，通过跨链技术确保资源、数据与服务等网络资产提供源是可信的。每个从链代表一个独立的网络共享域，连接设备可以在从链上进行身份的可信验证。

主链是按时间顺序线性排列的节点链，用于解析跨链资产认证请求，作为实现跨链可信认证和交互的可信共享。主链的联盟链节点一般由政府、运营商、银行、大型国企或央企、互联网企业等公共受信任的组织构建和维护。

为了实现区域性的异构网络共享，原则上可以根据区域性需求开发从链，这需要标准化跨链协议和资产管理模式。网络共享域中的所有成员都可以通过从链将所有网络资产直接共享。由于从链代表独立的网络共享域，存在网络拓扑异构的现象，因此提供的跨链协议中应包含跨链合约模板。从链节点只需实现模板中的函数接口，即可与主链进行通信，实现资产共享。从链节点由一些静态网络设备和服务器维护。块头保存块的哈希值以及上一个块、Merkle 树的根、块构造函数的签名和时间戳，

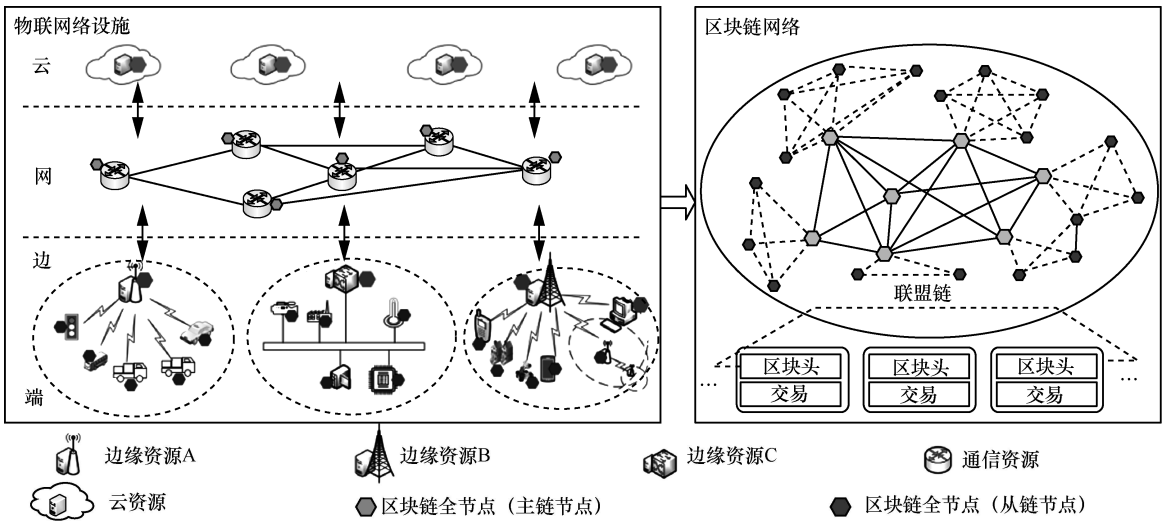


图 3　支撑内生可信的分布式联盟链构建

块主体记录此域和其他域中网络资产可信身份验证信息。

区块链网络依靠节点相互协作来保证网络安全，这需要限制其中恶意节点的数量。恶意节点可能向网络发起攻击，导致交易回退（失败），阻止新的交易，甚至重复使用加密货币。为抵御以上攻击，保证区块链网络的安全稳定，通常存在 3 种区块链节点安全管理方法。1) 基于信誉的节点管理方法。区块链网络对每一个参与网络的节点进行行为评估，形成节点信誉体系，并对信誉值低于系统阈值的节点进行相应处罚。2) 权威节点为主的节点管理方法。网络中接入多个权威资源节点，保证共识过程中的矿工节点大多数（例如 51%、2/3 等）为权威节点。3) 基于可信计算的节点管理方法。通过运用可信计算技术，保证接入设备行为的安全性。考虑到提出支撑内生可信的分布式联盟链接入节点类型多样、网络环境复杂等特性，本文采用基于信誉的区块链节点管理方法，设计基于信誉的独立拜占庭容错共识算法，保证区块链网络的稳定运行。

从链节点主要用于生成从链块、维护从链，并与主链和网络设备通信。为了提高可信认证的效率，将节点分为 3 类：通信节点、验证节点和候选节点。建立信誉值选择机制以对节点进行分类，因为不同的节点具有不同的信誉值。每类节点的功能介绍如下。

1) 通信节点。通信节点用于与主链进行通信，信誉度最高。当需要选择新的通信节点时，选择信誉值最高的验证节点作为新的通信节点。

2) 验证节点。验证节点用于达成共识并构建从属链的块。当验证节点的信誉值低于某个候选节点的信誉值时，它将转向候选节点，并选择该候选节点作为验证节点。

3) 候选节点。候选节点主要负责传输数据。刚加入从属链网络的所有节点都是候选节点，可以通过增加信誉值来转向验证节点。本文架构中主链和从链都采用联盟链。

在共识过程中，联盟链不能保证没有故障节点（拜占庭节点），因此仍然使用传统的 PBFT 共识算法[23-25]。但是由于节点数量众多且共识频繁，使用传统的 PBFT 共识算法无疑会增加通信开销和网络时延。因此，基于 PBFT 共识算法，本文针对从链设计了一种新的基于信誉值的独立拜占庭容错共识算法（RIBFT, independent Byzantine fault tolerance algorithm based on reputation）。与传统的 PBFT 算法相比，RIBFT 的改进如下。

1) PBFT 是 C/S 模式，而 RIBFT 不需要客户端充当请求的发起者，因此将其更改为 P2P 网络拓扑响应模式。该请求直接由主节点（构成块的节点）发起，要求每个共识节点独立侦听区块链中的交易，并确保块信息和每个节点的视图数一致。其中，智能合约通过在验证节点中随机选择主节点，信誉值较高的验证节点更有可能被选作主节点。

2) PBFT 共识需要整个网络参与。随着节点的增加，时间复杂度越来越高，而 RIBFT 仅需完成验证节点的共识。由于共识节点为信誉度较高的验证节点，大大降低了拜占庭节点的发生概率，减少了等待时间，提高了共识效率。

由于共识节点由智能合约自动选择，确保了投票过程的透明性和无损修改，进而确保共识节点的有效性。信誉值越高，该节点被选为主节点的可能性就越大。与传统的 PBFT 算法相比，RIBFT 的主节点成为拜占庭节点的概率大大降低，共识效率提高。

4.2 基于标识的异构网络资产共享模型

面向智能共享的内生可信网络需要一种轻量级的网络资产管理机制，支持跨域异构网络资产的安全高效可信共享。为此，提出一种基于标识的异构网络资产共享模型，将网络资产信息映射到标识中，实现标识和网络资产信息分离，构建链上标识、链下信息的应用模式，实现管理域内及域间的资产高效可信共享，如图 4 所示。

考虑资产标识需要的唯一性、有效性、隐私保护及可识别性等特性，设计资产标识包括两部分：区块链域和资产域。区块链域由资产注册时其信息存储的区块链号、链内块号及块内序号构成。区块链号为可选字段，表示资产注册信息所在的区块链，当用户所请求资产处于同一管理域内时，可省略该部分；链内块号表示改标编码所对应的区块的编号；块内序号表示该资产信息所在的块内条目的位置。通过解析[链号].[链内块号].[块内序号]，可获得处理后的资产信息。资产域与区块链域用“/”分割，包括标准标识、资产标识和资产版本标识。标准标识表示某种已存在的资产标识方法，资产标识表示在该类标识方法下对资产的编码，资产版本标识表示当前资产较上一次注册后发生的更新变

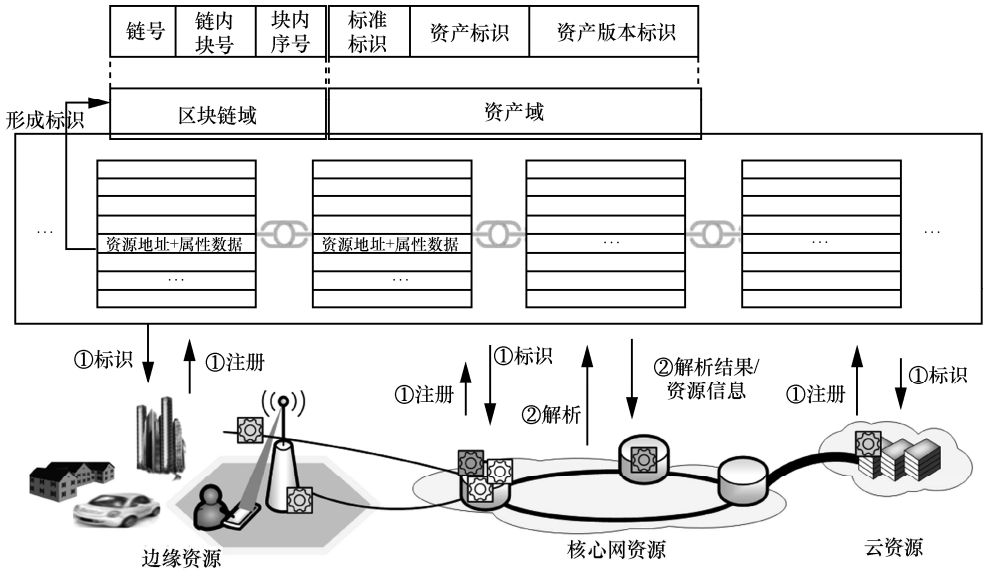


图 4　基于区块链的异构网络资产标识

化。通过解析[标准标识].[资产标识].[资产版本标识]，可得到唯一网络资产。

基于标识的异构网络资产共享模型的资产共享过程主要包括 3 个部分：资产注册、资产匹配、资产共享。其中存在 5 种参与实体，即资产请求者、认证机构、内生资产区块链、异构网络资产和资产提供者。

1) 资产注册

基于标识的异构网络资产共享模型中，内生资产区块链网络拓扑去中心化，各网络资产配置区块链应用共同维护该资产链。异构网络资产在实现资产共享前需由资产提供者向内生资产区块链提交资产注册，申请完成资产注册。

完成资产注册的网络资产获得全网唯一的资产标识，其格式为管理机构标识://链号.链内块号.块内序号/标准标识.资产标识.资产版本标识。该标识及相关资产信息被存储在内生资产区块链上，标识将体现该资产所属管理域、资产信息块内位置等，相关信息指明资产价格、资产大小及资产类型等相关属性。资产请求者在进行资产请求时可以从维护的内生资产区块链中获得资产信息，通过匹配算法选择自身所需资产，并通过 P2P 方式完成资产协商与资产交易。

2) 资产匹配

服务请求者在向内生资产区块链提交服务请求交易，该交易将触发智能合约，内生链通过资产匹配算法获得与服务请求者需求相适应的服务资产列表，资产共享双方通过网络数据安全可信共享交互协议（4.3 节）完成资产共享协商。

3) 资产共享

完成资产共享协商的交易双方将签订资产共享协议，该协议以交易的形式被记录至区块链上。完成签订后，开始正式资产共享。资产共享过程中，通过网络数据安全可信共享交互协议（4.3 节）完成数据交互。此外，资产共享双方可依据区块链数据进行相互监督，一旦某一方出现违反协议的行为，另一方可对其进行追责。

4.3　网络数据可信共享协议

网络数据可信共享协议旨在实现网络数据的安全交换，为面向智能共享的内生可信网络提供数据可信共享保障。

交换协议在设计上依赖全网唯一的资产标识（同 4.2 节）。网络资产完成资产注册时获得该标识，并一直拥有该标识，直到资产退出该资产共享网络。在该标识对应的区块链中，将存储数据交换时的公钥用于数据认证与数据解密。当资产交易双方有交互需求时，发起方将以目标方的加密公钥完成数据的加密，并以自身私钥实现数据的签名，将目标方标识与处理后数据打包为传输数据分组，保证交互内容不被篡改、伪造。发起方或数据中继以标识为寻址目标，将标识解析请求打包为区块链交易，发送至区块链网络，触发标识解析智能合约。合约根据交易内容获得资产标识，验证交互资产是否处于当前管理域。若是，则查找标识内区块及块

内序号字段对应的区块数据，获得资产转发端口或资产网络地址（依赖具体互联网传输协议），并将其返回至请求发起者。请求发起者依据该返回信息，转发签名加密后的数据分组。若交互资产不存在于当前管理域，需实现跨管理域信息交互，将重新打包标识解析请求为全网区块链交易，获得域外资产访问方式及相关数据验证信息（用于实现数据交互过程中的数据鉴权及数据安全保障）。完成数据传输后，目标方将以区块链上相应信息完成对数据的解密及认证，实现安全可信数据交互。

以下一代新兴网络——信息中心网络（ICN, information-centric networking）为例，结合基于区块链的标识，可实现安全可信的网络数据共享交互。网络中每个实体及数据都拥有一个全网唯一的基于区块链的标识，网络中继作为数据分组转发节点配置区块链客户端，实现区块链实体及数据标识信息的缓存。当交互数据分组以兴趣分组形式到达目标方时，根据中继缓存的数据标识信息是否一致，判断该兴趣分组是否应安全可信，是否该被转发或是否已查询到响应内容应该按原路返回经加密签名处理的数据分组。

如图 5 所示，数据消费者希望向数据提供者请求数据，他们将进行相互的通信。考虑 ICN“发布/订阅”式的数据获取方式，数据消费者 B 形成兴趣分组，通过标识服务同步区块链网络中数据提供者 C 的相关信息，包括其公钥及对应访问地址。为保证该兴趣分组的安全可信，利用 C 的公钥加密数据分组，并利用 B 的公钥签名数据分组。完成加密签名的数据分组将依据 ICN 传输规则，转发至下一个中继节点，其中每个中继节点将不定时同步区块链中各资产位置，作为其转发依据。当兴趣分组传输至数据提供者 C 后，同样获取区块链网络中消费者 B 的对应公钥，对数据分组实现加密签名并根据 ICN 规则回传数据分组。消费者 B 接收数据分组验签并解密，获得数据。

4.4 基于智能合约的网络资源智能调度方法

基于智能合约的网络资源智能调度方法对注册到联盟链中的异构网络资源，以“资源共享池”的形式，实现可信管理与智能分配。

资源请求用户向可信的“资源共享池”以区块链交易形式提出资源请求，该请求首先被分配到最近的资源服务节点，通过区块链节点完成请求者身份的认证。资源请求者在服务请求中将对资源需求、本身地理位置等信息进行描述，完成身份认证的用户服务请求将被发送至深度强化学习（DRL, deep reinforcement learning）驱动的网络最优化引

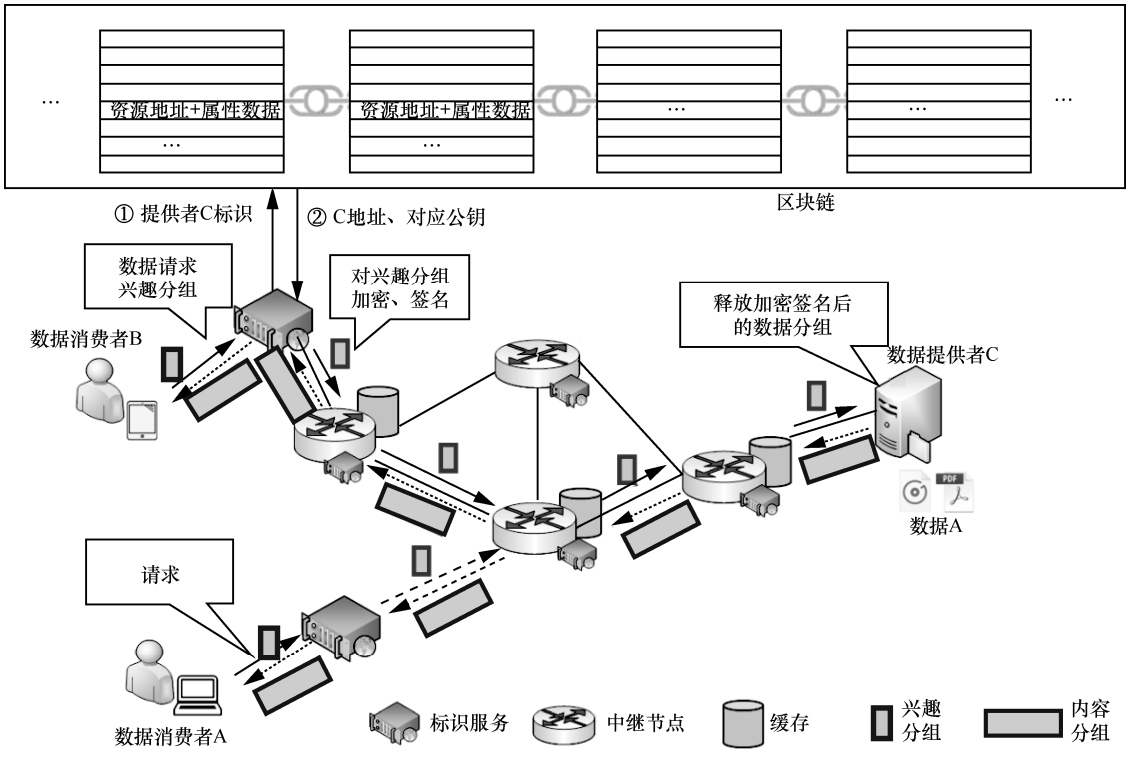


图 5 ICN 网络数据安全可信交互

擎，该引擎基于智能合约技术，调用资源智能调度方法，计算最优化服务编排[26-29]。该智能调度方法首先判定用户附近资源能否满足服务需求，若能，完成分配；若不能，则将该请求发送至远端云服务层，依据全网信息再次计算最优化资源分配。

如图 6 所示，基于智能合约的资源智能调度主要包括接收服务/资源请求、完成用户认证、执行资源智能调度算法、得出最优化资源组合方案、完成业务部署、对外可信服务、自动分配收益、注册服务交易。用户获得资源/服务提供主要包括 5 个步骤，即用户注册认证、服务资源调度、最优化服务调度、服务提供、服务交易注册。在用户注册认证过程中，通过登录控制智能合约请求服务之前，需要在区块链模块上注册用户信息（包括用户的设备 ID、加密数据的密钥和设备属性）。这些信息将在用户每次请求服务时进行身份验证。在服务资源调度中，调用 DRL 驱动的网络最优化引擎，实现基于智能合约的最优化资源调度分配。在服务提供过程中，根据上一步分配结果，完成服务功能虚拟部署，为用户提供服务。服务完成后，将触发区块链智能合约自动进行收益分配，避免人为主观干预，确保收益分配公平。最后，服务结束通过智能合约，将服务交易记录到区块链上。

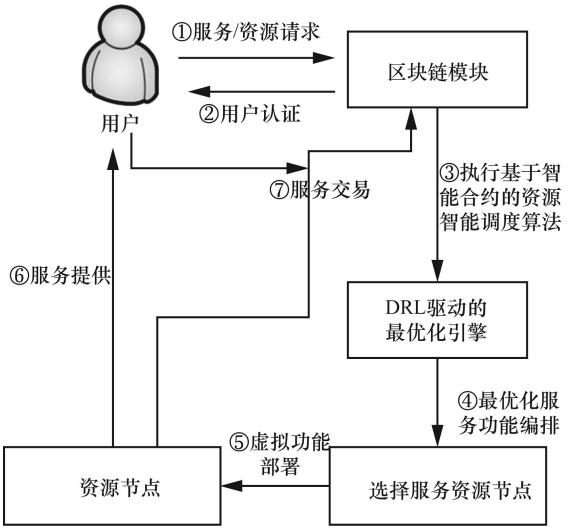


图 6　基于智能合约的资源智能调度流程

4.5　基于智能合约的共享服务组合方法

智能合约根据链上的资产及资产间交易，对发生在链上的业务逻辑进行实现，并对外提供接口。为了简化用户的操作，用户通过区块链的客户端应用程序提交方法及参数后完成合约封装，然后合约将自动生成并部署到链上。其过程如图 7 所示。

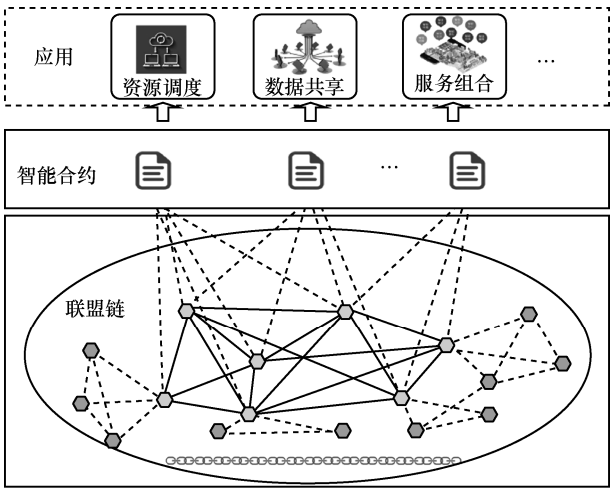


图 7　基于智能合约的共享服务组合方法

由于智能合约结构简单，功能单一，难以满足复杂的业务需求[30-31]，因此可以引入服务组合的思想，对合约提供的服务进行组合，以提供更加强大而丰富的服务。在该过程中，需对智能合约的服务自动生成、自主封装、自适应集成等关键技术展开研究。

针对网络服务自动生成，可借鉴传统 Web 服务的网络服务描述语言（WSDL, Web service description language）等形式化描述技术[32-34]展开针对智能合约的进一步深入，达成对智能合约服务的规范化描述，结合对应的业务服务模型，形成具体的合约模型。

在服务可信发布过程中，需设计严格的校验环节，避免错误合约发布对链造成的破坏。首先需对合约内容进行理论证明及模型检测，通过后执行一致性测试，确保合约的文本与代码效力一致。

服务自适应集成过程中，可采用关联分析等机器学习技术，基于关联知识与关联推荐的服务组合方法，根据要执行的任务和待解决的问题，动态地自动选取合适的智能合约进行自动组合，使智能合约组合的实现更加灵活、高效。

5　内生可信的共享网络应用

5.1　可信共享网络虚拟运营应用

在融合区块链技术的内生可信的共享网络中，利用资产标识，将虚拟化的网络资源注册到链上，构建基于联盟链的可信共享网络虚拟运营平台，实现网络资源的虚拟化调度、运行状态可信监测和质

量可信评估等虚拟化运营。具体是以智能合约作为可信共享网络虚拟运营平台的访问入口，支持网络资源注册、虚拟分配和状态监测等功能，控制网络资源的访问权限，实现网络资产共享的可信校验，提供共享网络资产的按需智能提供，避免全量信息上链带来的效率问题。

可信共享网络虚拟运营可以应用于专用通信网络（如能源领域信息通信基础设施）的开放共享中，部署结构如图 8 所示，该场景主要是以能源互联网信息通信、运营商信息通信等基础设施的开放共享为目的，支撑区域性综合能源服务等业务场景的开展。

以综合能源服务为例，在业务属地通信现场部署本平台的接入装置，实现各种业务终端的接入，以及属地化现场通信网络资产的接入，通过资产与标识解耦，链上存储资产的标识、公钥与签名，链下存储资产信息，实现了资产可信标识服务。平台通过调用 SDN 控制器的北向接口获取所需的各项资产，并对基础设施层资产进行编排，维护网络的拓扑和状态等信息；并将底层物理网络抽象为不同的虚拟 SDN 以承载不同业务，同时还可以依据不同的业务需求提供区域化或跨域的、服务定制化、可信安全的网络承载能力。

5.2 去中心的域名解析系统

本文提出的面向智能共享的内生可信网络，利用标识实现网络资源、数据、服务等资产的链上管理，可以作为网络数据与服务的去中心化的域名解析系统（DNS, domain name system）解决方案。通过标识在区块链平台内的数据和服务共享 2 个关键技术，可以有效提供去中心化的域名解析机制，解决集中式网络架构中采取中心制递归式域名解析体系中由于断网导致“解析中心”的“孤立式风险”和“致盲式风险”，以及由于停服导致 “发布中心”的“消失式风险”和“劫持式风险”[35-36]等问题。

在该网络架构中，利用联盟链实现如图 9 所示的域名存储与解析架构，形成支撑内生可信网络去中心化域名解析的解决方案。利用智能合约脚本，将域名授权合同与管理流程以软件定义的方式在共识链中智能合约化，合约覆盖域名授权/召回、授权转移/赎回、授权逾期/续期、域名争议解决等全域名生命周期事务。

为了同时满足去中心化 DNS 高效运行、可被监管的需求，可以采用基于异构节点的混合式域名共识链功能组织结构，其中平衡节点专注于域名数据更新所需的共识计算，超级节点在参与域名数据更新所需共识计算的同时，还承担巨量域名数据存储、解析服务、域名安全威胁分析等能力，异构节点协同工作，提供高效安全可信的解析服务。递归解析器、监管机构和域名拥有者通过访问部署于超级节点之上的不同功能的智能合约实现对域名的解析、监管和注册。

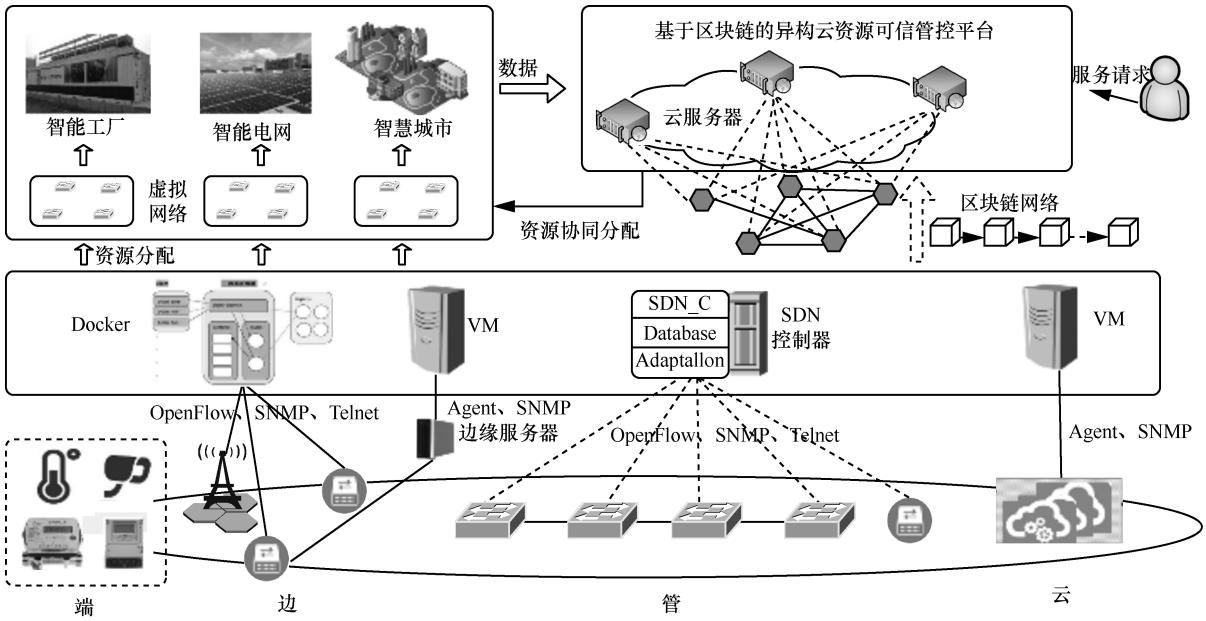


图 8 可信共享网络虚拟运营平台

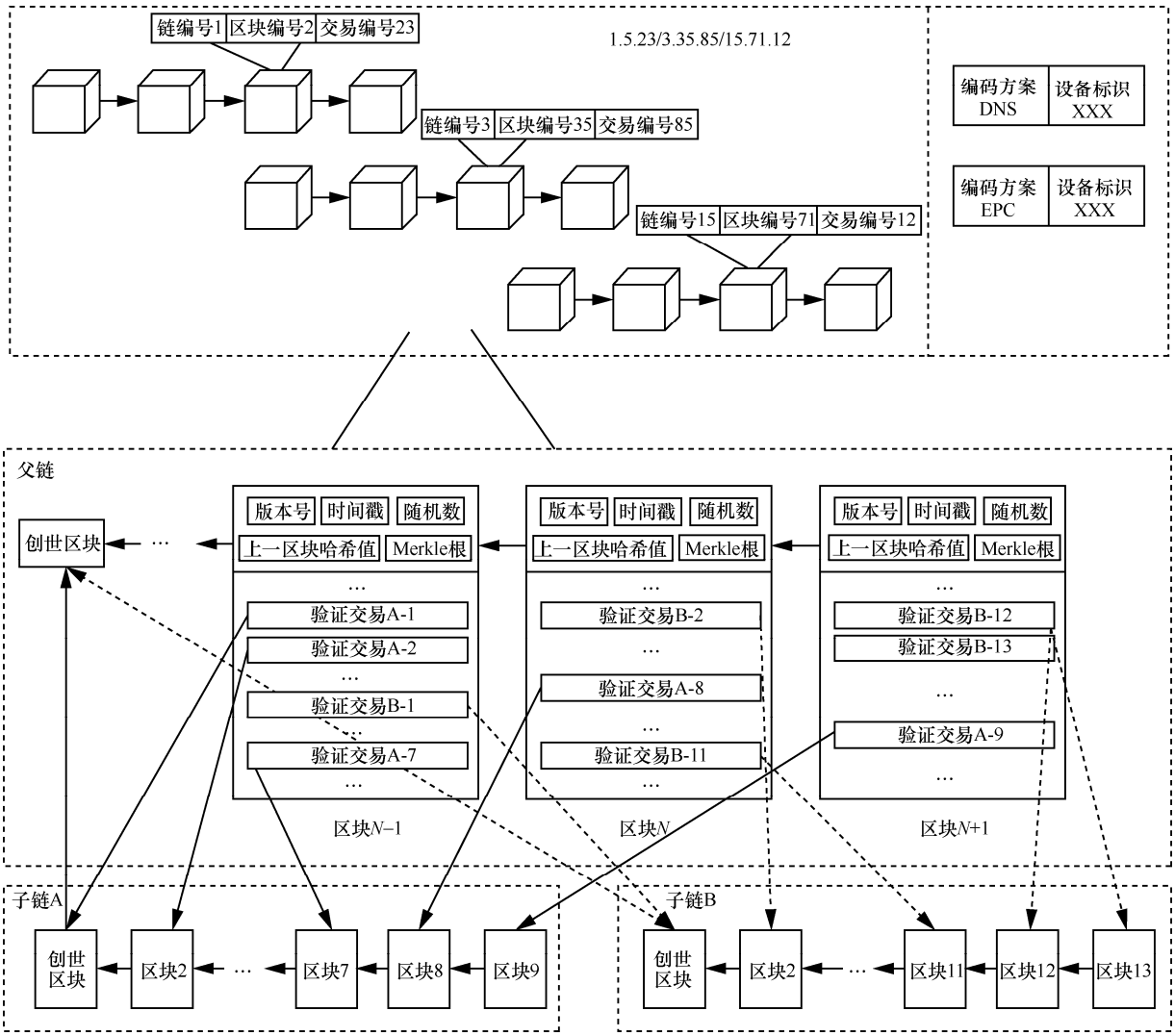


图 9　基于联盟链的域名存储与解析架构

为支持域名可信高效解析，本文设计了链上存储域名索引、链下存储完整域名信息的数据模型。在此模型中，将域名记录等查询频繁、变更频率低的少量主数据进行上链存储；将域名区文件、日志记录等大量过程数据进行链下存储，提升域名解析效率；同时，利用基于哈希算法建立链上链下数据可信关联，确保域名数据的完备性、统一性和实时性。

面向智能共享的内生可信网络架构除了应用于去中心化域名解析服务外，还可以支撑物联网标识服务、未来网络数据寻址服务、各类码号资源解析服务等类似应用场景[37-38]。

5.3　分布式可信网络认证服务

利用基于标识的网络数据与服务可信共享技术，可以形成分布式可信网络认证服务的解决方案，用于解决现有的认证体系一般针对独立的异构网络体系且存在资源共享效率低、数据规范不统一和物理隔离等问题[39-40]。

在面向智能共享的内生可信网络中，采用主从链方式，构建了如图 10 所示的分布式可信认证服务系统，通过链上将同一身份不同认证数据进行可信统一映射，利用智能合约提供可信认证服务，即可以兼容原有的 CA（certificate authority）身份认证机制，在减小系统升级换代所需的额外工作量的同时，又支持区块链本地认证与跨域跨平台的身份认证信息共享。该方案有效提高了网络的认证效率，打破了行业信息壁垒。

通过采用面向智能共享的内生可信网络中一条主链以及多个从链，构建基于主从链的分布式可信认证解决方案。主链上存储验证区块，该区块按

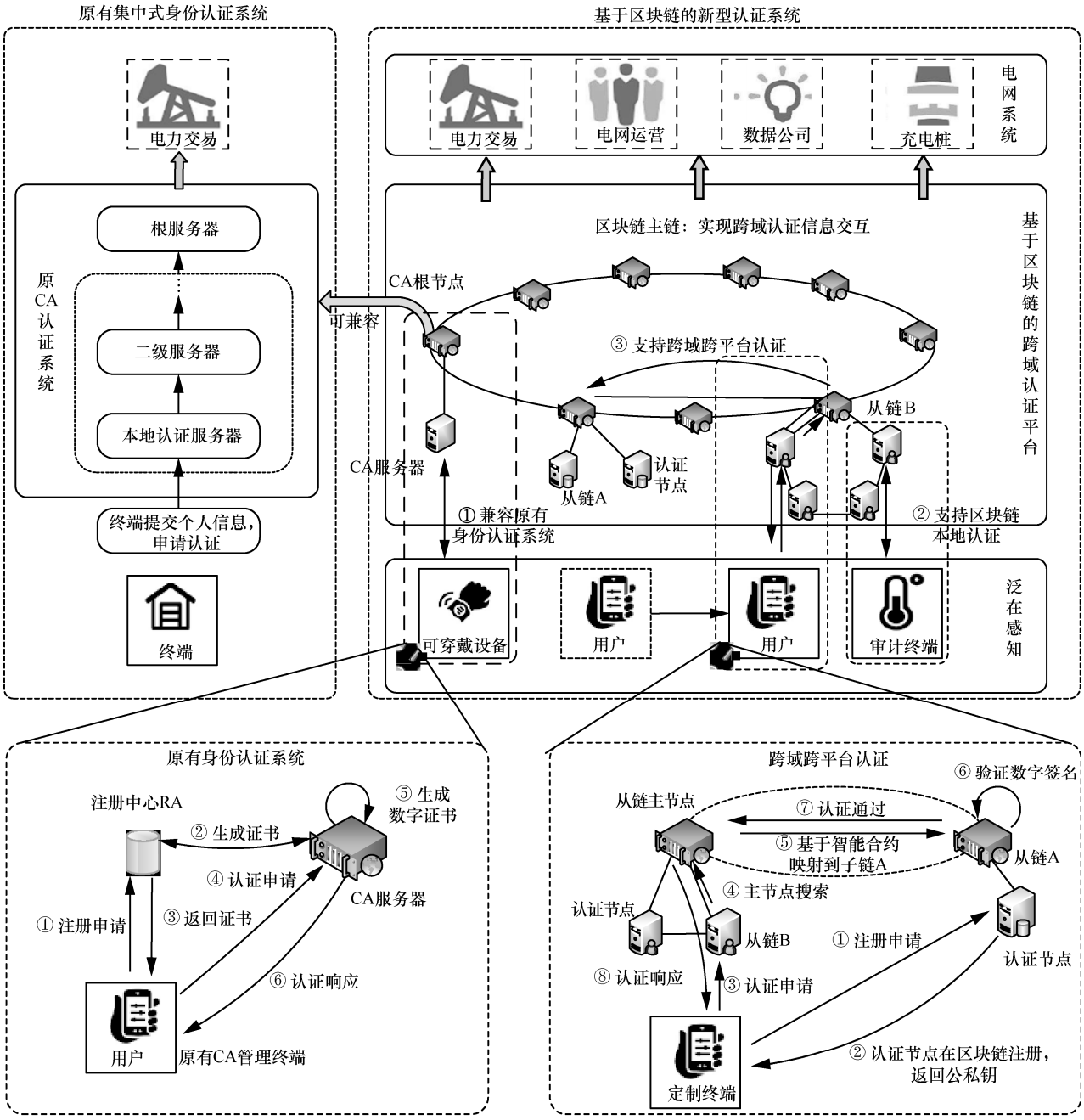


图 10 跨域分布式认证系统

照时间顺序线性链接，验证区块作为链上区块的索引；从链上存储实际业务数据，多个从链链接到主链构成主从链模型。验证区块存储从链数据区块摘要信息，保证数据的全局一致性。为支持业务系统交互的高并发要求，设计灵活的区块数据索引方法，不同从链存储不同类型的数字资产，满足各业务系统的不同业务特点，保障数据的高效共享与不可篡改，确保该区块的哈希值总能在主链被索引，从而支持身份认证信息的跨域查询与共享。该主从链遵从联盟链架构，作为分布式可信网络认证服务的基础，将各业务系统管理者作为联盟中的成员。联盟链保证了大量数据的统一数据共享，且安全性较公有链更高，安全可靠。从链架构拥有一定的独立性，可响应不同电力业务系统的自定义需求。

考虑到大部分现有网络系统采用基于 CA 的身份认证机制，原认证系统的取代耗费大量成本，本文系统可基于区块链主从式架构兼容原有 CA 认证系统。将 CA 认证系统的根服务器作为主链中的主

节点之一，使原有 CA 认证系统管理的智能终端通过 CA 获取数字证书的认证方式不变，身份认证信息存储于根服务器之中。与此同时，作为联盟链的一部分，根服务器存储的认证数据同样支持跨域查询与共享，由此实现对原有 CA 身份认证系统的兼容与跨域认证信息共享。

以一次跨域认证流程为例，假设 A、B 为 2 个不同的域，终端已经在 A 域注册过，试图通过 B 域的认证。在传统流程中，A 域的认证许可位于中心化 CA 系统，B 域需经过多次解析、重定向校验之后获取到由 A 域 CA 签发的终端认证。在本文设想的架构中，经过基于多链的认证信息共享，可以大幅提高跨域网络认证的效率。在引入区块链的前提下，A 域、B 域均部署有区块链节点支撑分布式的网络认证。当终端在 A 域认证之后，由于认证信息已经通过共识存储到链上，B 域对终端的认证只需请求 B 域区块链节点查询终端认证状态即可，不需要再请求 A 域节点协作。特别是，本文架构对原有的中心化认证体系具有充分的兼容性，即原 A 域的中心化 CA 只需将终端信息写入链上即可。

6　结束语

本文以实现网络资产共享为目的，融合区块链、人工智能等技术，构建了面向智能共享的内生可信网络体系架构，提出了基于标识的网络资产共享理论与模型，基于联盟区块链，利用链上标识、链下资产信息关联的信用融合机制实现网络资源、数据与服务的可信共享，设计安全可信共享协议实现网络数据安全可信实时交换，利用智能合约聚合可信资源、数据与服务实现智能调度和服务组合，解决网络使用者/所有者间不信任与中心化利益分配不公平的问题，并将该体系结构在虚拟运营、域名解析、跨域认证等场景中进行应用。未来将进一步完善内生可信网络架构的协议、设备、系统的设计方案，为大规模试点应用奠定理论与工程基础。

参考文献：

[1] EYAL I. Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities[J]. Computer, 2017, 50(9): 38-49.

[2] TSCHORSCH F, SCHEUERMANN B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. IEEE Communications Surveys Tutorials, 2016, 18(3): 2084-2123.

[3] ROSA R V, ROTHENBERG C E. Blockchain-based decentralized applications for multiple administrative domain networking[J]. IEEE Communications Standards Magazine, 2018, 2(3): 29-37.

[4] YIN H, GUO D C, WANG K, et al. Hyperconnected network: a decentralized trusted computing and networking paradigm[J]. IEEE Network, 2018, 32(1): 112-117.

[5] SHARMA P K, SINGH S, JEONG Y, et al. DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks[J]. IEEE Communications Magazine, 2017, 55(9): 78-85.

[6] SHARMA P K, RATHORE S, JEONG Y, et al. SoftEdgeNet: SDN based energy-efficient distributed network architecture for edge computing[J]. IEEE Communications Magazine, 2018, 56(12): 104-111.

[7] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. A survey of blockchain technology research: principles, progress and applications[J]. Journal on Communications, 2020, 41(1): 134-151.

[8] WU J, DONG M X, OTA K, et al. Application-aware consensus management for software-defined intelligent blockchain in IoT[J]. IEEE Network, 2020, 34(1): 69-75.

[9] XU C, WANG K, GUO M. Intelligent resource management in blockchain-based cloud datacenters[J]. IEEE Cloud Computing, 2017, 4(6): 50-59.

[10] RAWAT D B. Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization[J]. IEEE Communications Magazine, 2019, 57(10): 50-55.

[11] FENG J, YU F R, PEI Q, et al. Cooperative computation offloading and resource allocation for blockchain-enabled mobile edge computing: a deep reinforcement learning approach[J]. IEEE Internet of Things Journal, 2019, doi: 10.1109/JIOT.2019.2961707.

[12] ABBAS Y, PARIZI R M, ALI D, et al. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security[J]. IEEE Transactions on Services Computing, 2020, doi: 10.1109/TSC.2020.2966970.

[13] NICOLAS H, NICOLAS N. A model for collaborative blockchain-based video delivery relying on advanced network services chains[J]. IEEE Communications Magazine, 2017, 55(9): 70-76.

[14] GUO S Y, DAI Y, GUO S, et al. Blockchain meets edge computing stackelberg game and double auction based task offloading for mobile blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, doi: 10.1109/TVT.2020.2982000.

[15] ZHANG S, WU J, ZHU Y. Construction of distributed and heterogeneous data sharing platform[C]//2009 International Conference on Web Information Systems and Mining. Piscataway: IEEE Press, 2009: 696-700.

[16] LI Y, HUANG J Q, QIN S Z, et al. Big data model of security sharing based on blockchain[C]//2017 3rd International Conference on Big Data Computing and Communications. Piscataway: IEEE Press, 2017: 117-121.

[17] WANG Z, TIAN Y, ZHU J. Data sharing and tracing scheme based on blockchain[C]//2018 8th International Conference on Logistics, Informatics and Service Sciences. Piscataway: IEEE Press, 2018: 1-6.

[18] ZHU J, XIE W, LI L, et al. Software service defined network: centralized network information service[C]//2013 IEEE SDN for Future Networks and Services. Piscataway: IEEE Press, 2013: 1-7.

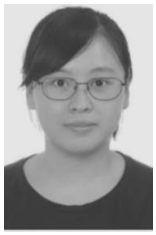
[19] DAI Y, XU D, MAHARAJN S, et al. Blockchain and deep reinforce-

ment learning empowered intelligent 5G beyond[J]. IEEE Network, 2019, 33(3): 10-17.
[20] GUO F, YU F R, ZHANG H, et al. Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing[J]. IEEE Transactions on Wireless Communications, 2020, 19(3): 1689-1703.
[21] LI Z, KANG J, YU R, et al. Consortium blockchain for secure energy trading in industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3690-3700.
[22] PALAI A, VORA M, SHAH A. Empowering light nodes in blockchains with block summarization[C]//2018 9th IFIP International Conference on New Technologies. Piscataway: IEEE Press, 2018: 1-5.
[23] LI Y X, WANG Z, FAN J, et al. An extensible consensus algorithm based on PBFT[C]//2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Piscataway: IEEE Press, 2019: 17-23.
[24] TONG W, DONG X, ZHENG J. Trust-PBFT: a peertrust-based practical Byzantine consensus algorithm[C]//2019 International Conference on Networking and Network Applications. Piscataway: IEEE Press, 2019: 344-349.
[25] HE L, HUO Z. An improvement of consensus fault tolerant algorithm applied to alliance chain[C]//2019 IEEE 9th International Conference on Electronics Information and Emergency Communication. Piscataway: IEEE Press, 2019: 1-4.
[26] LI M, WANG J, YANG A J, et al. CrowdBC: a blockchain-based decentralized framework for crowdsourcing[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(6): 1251-1266.
[27] REBELLO G A F, ALVARENGA I D, SANZ I J, et al. BSec-NFVO: a blockchain-based security for network function virtualization orchestration[C]//2019 IEEE International Conference on Communications. Piscataway: IEEE Press, 2019: 1-6.
[28] SINGH M, AUJLA G S S, SINGH A, et al. Deep learning based blockchain framework for secure software defined industrial networks[J]. IEEE Transactions on Industrial Informatics, 2020, doi: 10.1109/TII.2020.2968946.
[29] GUO S Y, DAI Y, XU S Y, et al. Trusted cloudedge network resource management: DRL-driven service function chain orchestration for IoT[J]. IEEE Internet of Things Journal, 2019, doi: 10.1109/JIOT.2019.2951593.
[30] THOMAS H, DAVID L S, ALEX P. Trusted data: a new framework for identity and data sharing[M]. Massachusetts: MIT Press, 2019.
[31] LIU X, CHEN R, CHEN Y, et al. Off-chain data fetching architecture for ethereum smart contract[C]//2018 International Conference on Cloud Computing, Big Data and Blockchain. Piscataway: IEEE Press, 2018: 1-4.
[32] DEVANATHAN V, SUNDARAMURTHY S. A novel method and environment for scalable Web services orchestration[C]//2016 IEEE World Congress on Services. Piscataway: IEEE Press, 2016: 128-129.
[33] DOSHI M, ANURADHA G. Proposed framework for semantic Web services[C]//2014 International Conference on Advances in Communication and Computing Technologies. Piscataway: IEEE Press, 2014: 1-5.
[34] MISBAH A, ETTALBI A. Towards a standard WSDL implementation of multiview Web services[C]//2016 5th International Conference on Multimedia Computing and Systems. Piscataway: IEEE Press, 2016: 195-199.
[35] DUAN X, YAN Z, GENG G, et al. DNSLedger: decentralized and distributed name resolution for ubiquitous IoT[C]//2018 IEEE International Conference on Consumer Electronics. Piscataway: IEEE Press, 2018: 1-3.
[36] LI H, WU J X, YANG X, et al. MIN: co-governing multi-identifier network architecture and its prototype on operator's network[J]. IEEE Access, 2020, 8: 36569-36581.
[37] WANG X, LI K, LI H, et al. ConsortiumDNS: a distributed domain name service based on consortium chain[C]//2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems. Piscataway: IEEE Press, 2017: 617-620.
[38] YU Z, XUE D, FAN J, et al. DNSTSM: DNS cache resources trusted sharing model based on consortium blockchain[J]. IEEE Access, 2020, 8: 13640-13650.
[39] GUO S Y, HU X, ZHOU Z Q, et al. Trust access authentication in vehicular network based on blockchain[J]. China Communications, 2019, 16(6): 18-30.
[40] GUO S Y, HU X, GUO S, et al. Blockchain meets edge computing: a distributed and trusted authentication system[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 1972-1983.

[作者简介]

郭少勇（1985− ），男，河北邢台人，博士，北京邮电大学副教授，主要研究方向为物联网与区块链。

齐芫苑（1998− ），女，河北保定人，北京邮电大学硕士生，主要研究方向为物联网与区块链。



代美玲（1995− ），女，重庆人，北京邮电大学博士生，主要研究方向为区块链、边缘计算与云计算。

邱雪松（1973− ），男，江西上饶人，博士，北京邮电大学教授、博士生导师，主要研究方向为网络与业务管理、物联网与区块链。

亓峰（1971− ），男，山东济南人，博士，北京邮电大学教授、博士生导师，主要研究方向为通信软件。

张平（1959− ），男，陕西汉中人，中国工程院院士，北京邮电大学教授、博士生导师，主要研究方向为移动通信系统与网络。