

# 基于区块链的算力并网交易平台研究

2023年12月

# 目 录

一、研究背景 .....	1
(一) 算力交易平台国内发展现状 .....	1
(二) 算力交易平台海外发展现状 .....	2
二、问题与挑战 .....	5
三、关键技术 .....	7
(一) 分布式数字身份与可信凭证技术 .....	7
(二) 链上链下结合的交易处理技术 .....	9
(三) 多维度激励机制 .....	9
(四) 数据访问控制 .....	10
(五) 算力资源调度 .....	11
(六) 区块链监管 .....	11
四、解决方案 .....	13
(一) 数字身份链 .....	13
(二) 交易链 .....	14
1、交易模式 .....	14
2、数据访问授权机制 .....	18
3、激励机制 .....	18
4、资源调度机制 .....	20
5、交易监管 .....	26
(三) 算力交易平台 DAPP .....	28
(四) 交易服务通道控制器 .....	28
五、总结与展望 .....	34
术语与缩略词表 .....	35
参考文献 .....	36

# 一、研究背景

2020 年以来，国家发布了以“新基建”为导向的一系列加快数字化基础设施建设的政策，旨在提升“联结+计算”能力，重塑产业升级模式。2021 年 5 月，国家四部委发布《全国一体化大数据中心协同创新体系算力枢纽实施方案》，提出“东数西算”架构，打通网络传输，提升跨区域算力调度水平。随着网络通信设备、云计算、边缘计算等基础设施算力能力持续提升，算力泛在化已成为趋势，呈现云网边端多级计算服务架构。算力并网可以整合各种算力资源，形成一个统一的算力网络，对各类应用提供普适多样的算力服务。区块链的防篡改、可追溯、分布式等特性可以为算力并网提供交易技术支撑，激发算力服务提供商的积极性，同时为用户提供安全、可靠且便捷的统一算力服务交易接口，有助于构建基于算力的价值网络，推动基于算力的共享经济和数字经济的发展。

## （一）算力交易平台国内发展现状

国内目前算力并网技术主要以政府机构为主导，联合上游硬件厂和下游云计算、科学计算和网络服务提供商，构建算力交易平台。比较有代表性的有宁夏的“东数西算”一体化算力交易平台、国家新兴互联网交换中心主导的上海算力交易平台（SHIXP）以及中国信通院牵头的全国一体化算力算网调度平台。

### ● “东数西算”一体化算力服务平台

东数西算一体化算力服务平台 2023 年 2 月 24 日在宁夏银川正式上线运营。作为国内首个算力交易平台，该平台通过资源整合，已将曙光、华为、中兴、阿里云、天翼云等国内大算力领先的企业，国家信息中心、北京大数据研究院等国内主要的大数据机构，以及商汤、百度等大模型头部企业共计 27 家纳入平台。该平台作为国内首个可以支持算力交易调度的应用系统，为智算、超算、通用算力等各类算力产品提供算力发现、供需撮合、交易购买、调度使用等综合服务，将有效结合东西部算力发展需求，助力形成自由流通、按需配置、有效共享的数据要素市场，赋能东西部数字化发展。

### ● 上海算力交易平台

在 2023 年 4 月 26 日举办的“算力浦江”（首届）数字经济发展论坛上，上海算力（试运行）交易平台正式启动，这是依托国家（上海）新型互联网交换中心（简称“SHIXP”）平台交换架构的独特性，先行先试探索打造的全国首个算力交易集中平台。依托 SHIXP，上海算力（试运行）交易平台的近景目标是：到 2023 年底，初步建成算力调度平台，探索算力交易运营机制；进一步扩大交换流量规模，实现上海市内算力资源调度。据悉，上海电信、上海移动、上海联通、上海铁塔、东方有线、腾讯云、有孚云等已入驻上海算力（试运行）交易平台。本次论坛上，14 家首批入驻算力交易平台的企业与 SHIXP 分别签约，将展开深度合作，资源共享、协同合作，共同推进数字产业的发展。目前上海算力指数排名位列全国第一，综合算力指数排名位列全国第二。截至 2022 年底，上海在用标准机架数 41.5 万，同比增长 15%，算力总规模近 9E flops。

#### ● 全国一体化算力算网调度平台

2023 年 6 月 5 日，由国家工业和信息化部主办，中国信息通信研究院等承办的“算力创新发展高峰论坛”在京召开。会上，中国信通院联合中国电信共同发布我国首个实现多元异构算力调度的全国性平台——“全国一体化算力算网调度平台（1.0 版）”。该平台统一整合通用算力、并行算力、边缘算力等多源异构算力资源，实现不同厂家、不同硬件结构资源池的算力智能管理分发调度。尤其在对算力要求较高的 AI 训练应用中，该平台通过整合跨资源池、跨平台、跨厂商的异构算力实现分配调度。目前，已有天翼云、华为云、阿里云等云服务厂家接入该平台。“全国一体化算力算网调度平台”的发布，不仅有利于贯彻落实国家“东数西算”工程要求，促进东部数字经济产业链向西部延伸拓展，同时还将推动算力资源的精准配置和按需获取，有效降低算力能源消耗，助力区域协调发展和信息通信行业碳达峰、碳中和目标达成。

## （二）算力交易平台海外发展现状

海外算力并网项目大多基于现有的分布式计算（Distributed computing）和云计算（Cloud computing）项目进行开发和扩展。本节主要介绍两个规模和知名度最高的项目：美国的 BOINC<sup>[6]</sup>和欧盟的 EGI<sup>[7]</sup>。

- 伯克利开放计算网络（Berkeley Open Infrastructure for Network Computing, BOINC）

BOINC 是由伯克利提出的网络计算开放基础设施项目。其主要面向志愿计算（Volunteer computing，是一种分布式计算构架）的开源中间件分布式计算系统。BOINC 最早设计是用于支持 SETI@Home 项目，该项目旨在通过计算分析外太空无线电信号来探索地外生命和文明的研究计划。目前 BOINC 已经在医药学、分子生物学、数学、语言学、气候变化研究、环境科学以及星体物理学等领域展开了广泛的应用。截止 2021 年 11 月，BOINC 项目包含了 34236 名志愿者、136341 台活跃计算节点共计 20.164PetaFLOPS 算力。BOINC 的软件系统可以将并入计算网络中结点的空闲 CPU 和 GPU 用于共享计算网络中的科学计算任务。2008 年 BOINC 与英伟达合作开发了 BOINC 系统的 CUDA 支持。2009 年与 ATi/AMD 合作新增了 ATi/AMD GPU 的计算支持。BOINC 系统中有一套可信计算系统（Credit system），通过该系统来防止故障硬件和欺诈。同时对返回的计算结果进行校验，保证计算结果的可靠性。

目前 BOINC 正在与区块链技术进行整合，通过 BOINC 完成的计算任务会反馈积分，用户可以将积分兑换 COP 代币。目前 BOINC 和区块链结合方式还比较简单，主要就是积分，未来 BOINC 计划基于智能合约让其产生真的代币，同时也会和一些知名的公链进行合作，在区块链上进行深耕。

- 欧洲网格计算基础设施（European Grid Infrastructure, EGI）

2008 年 5 月，为了利用网格计算技术促进科学计算和科技进步，欧盟提出建立 EGI，欧洲网格计算基础设施。EGI 旨在通过利用网格计算技术将欧盟成员国的计算基础设施进行连接，共同服务于欧盟在生物医药、星体科学、高能物理、生物信息学等领域的科学计算项目。截止 2021 年，EGI 项目已经累计为 78,100 位用户提供了 508 万云 CPU 时、支撑了 27 项欧盟科研计划和 450 万次作业提交，参与贡献的有超过 800 个终端和多达 150 个数据中心。

根据不同的应用实例，EGI 向研究人员和社区提供包括批量计算（Batch computing）、交互计算（Interactive computing）、联邦数据访问（Federated access and data federation）、数据空间（Data space）以及服务部署（Service hosting）等服务。批量计算服务为用户提供批量计算访问的 API 接口，其通过 EGI 计算集

群提供的高吞吐量计算、在线云存储和负载管理模块根据计算任务需要提供量化、可扩展和成本资源优化的计算服务。交互计算服务基于 Jupyter Notebooks 提供交互式数据分析和可视化的接口，同时通过 EGI 社区提供的云存储、云计算以及相关技术服务支持为用户提供一站式、易用的交互式科学计算体验。联邦数据访问 和数据空间服务基于联邦学习技术，提供安全、透明的数据访问与计算服务，为 EGI 社区提供安全、高效、多样化的数据访问与使用技术解决方案。服务部署模块基于 EGI 联邦计算集群和 EGI 网络，提供安全、高效、高可用的专用服务器节点供用户部署计算服务。

## 二、问题与挑战

基于区块链的算力并网交易平台面临的挑战主要包括以下几方面：交易效率、交易安全、交易多样性、交易激励因素复杂性、交易可监管性以及资源调度。

- 交易效率

交易数据上链过程的开销大且比较耗时，简单概括上链过程包括交易数据入账队列、打包新区块、交易共识（如 DPOS、PBFT 共识）、以及广播到所有节点进行存储。由此可见，数据上链的开销包括共识开销、计算开销、网络开销及存储开销，而且上链过程受队列调度、共识算法处理、网络广播等因素影响，会产生时间延迟。因此并不是所有数据都应该上链，而要充分考虑开销和效率，让无需上链的数据（如：非全局性的、无需多方共识的、数据量大的、计算繁杂的）放到链下处理。以下棋为例进行说明，棋手的每一步棋并不需要实时上链，而在棋局结束时，比如总共下了几百手，那么将这几百手的记录汇总起来，连同输赢结果上链，以便记录战绩。对弈双方的每步棋的数据可以通过链外系统进行通信，可以达到实时、高效的数据传输。算力交易具有小额、高频交易特征，给系统处理性能带来很大挑战。

- 交易安全

交易安全问题，主要涉及两方面，包括数字身份安全和数据（包含交易数据和用户数据）隐私安全。

- (1) 数字身份安全

针对分布式系统，用户身份被假冒会造成很大损失，比如在 NFT 平台艺术家劳夫曼的作品在他不知情的情况下被拍卖。因此用户数字身份安全认证及数字身份管理对交易平台来说至关重要。

- (2) 数据隐私安全

对于分布式交易系统，交易数据是否公开，不公开的话应该允许哪些用户查看，另外也要解决用户隐私数据保护问题。

- 交易多样性

算力供应商和用户对计费的策略需求不尽相同，因此，如何支持丰富多样的算力交易模式，提出一种可以满足用户和供应商多样性需求的算力交易模型也是本项目的一个难点。另外还需要解决信息孤岛问题，支持交易数据在不同平台之

间可信流转。

- 交易激励因素复杂性

常见的竞价机制是按价格优先与时间优先的原则排序，将买卖指令配对竞价成交，但算力交易平台需要结合激励条件（如低碳、绿色能源优先、电力利用率、公益、慈善等社会效益）对算力竞价机制做一些调整，构建一套结合竞价与激励机制的参数模型，把多维度的数据综合考量，达到更好的社会效益。

- 交易可监管性

监管对于保障交易系统的用户权益至关重要，因此需要对区块链交易进行监管，设计出可追溯可屏蔽的面向监管友好的区块链交易平台。目前公有链在国内不被法律允许，因此普遍使用联盟链技术，联盟链监管存在以下挑战：一方面，不同平台间未建立有效的信息共享机制，不互通不协同，存在封闭性、敏感性、异构性的难题；另一方面，传统的监管技术往往难以涵盖持续变化的监管需求，也难以适应各种异构底层区块链技术。

- 资源调度

算力资源调度机制主要根据用户提供的需求与现有算力资源实例之间按照预定的评分函数和规则进行匹配，然后选择得分较高的算力解决方案为用户进行分配和调度。现有资源调度方案中预设的评分函数和规则往往是根据经验调整好的固定参数，难以根据市场和用户需求的变化来动态地进行调整。因此，构建一套基于数据驱动的算力调度方案有助于平台适应市场需求变化并提高用户满意度。



### 三、关键技术

本平台涉及的关键技术包括：分布式数字身份与可信凭证技术、链上链下结合的交易处理技术、多维度激励机制、数据访问控制、算力资源调度及区块链监管。

#### （一）分布式数字身份与可信凭证技术

随着数字经济的发展，越来越多的事务处理依赖数字身份及数字凭证。物理身份无法满足在线使用的要求，因为物理文档的数字副本很容易伪造，而且合法性难以进行远程验证。传统的物理凭证及其电子化凭证无法有效应对高频请求、海量数据、隐私安全和不断出现的新型数字化场景的挑战。为了解决这些挑战，分布式数字身份技术被提出并得到快速发展，自2019年W3C分布式身份标识符工作组（DIWC: Decentralized Identifier Working Group）发布分布式身份标识符的首个工作草案以来，分布式身份标识相关的标准与规范持续扩展完善，目前主要有5个技术规范，如下表所示。

表 1 分布式身份标识相关的技术规范

序号	规范名称	描述
1	分布式身份标识符（DID: Decentralized Identifier <sup>[1]</sup> ）	DID 是一种全局唯一的数字身份标识符，具有分布式、可解析性及可验证性。与传统标识符的区别是数据自主存储而不是集中托管，标识符自生成、自分配、自管理而不是统一分配，数据真实性由加密算法背书而不是由权威机构背书。
2	DID 文档（DID Document）	DID 文档并不包含用户身份数据相关的内容（如姓名、年龄、住址、手机号等），而只是包含描述 DID 相关的一些信息（包含 DID 标识符、公钥列表、公钥详细信息诸如所有者、加密算法等），它通常储存在一个与 DID 关联

		的分布式系统中，可以通过 DID 检索到。
3	DID 解析器 (DID Resolver)	DID 解析器的作用是通过 DID 来获取 DID 文档，其接口 API 用于接收 DID 查找请求、执行相应的 DID 方法以检索对应的 DID 文档、并返回文档。
4	可验证凭证 (VC: Verifiable Credential [2])	可验证凭证 VC 通常是权威实体为另一个实体的某些属性做背书而发出的描述性声明，并附加自己的数字签名；VC 规范定义了可验证凭证的数据格式，形成数据跨域跨机构交互的一种标准。
5	身份存储库 (Identity Hub)	身份存储库允许用户以安全而隐私的方式存储其敏感数据，未经用户授权不允许访问；即数据由用户控制，用户可以选择以任何方式存储数据，且只有通过用户授权后，才可以允许第三方访问。

以上5个技术规范被广泛应用到分布式数字身份与可信数字凭证系统的构建中，确保数字身份和数字凭证可以在不同网络和平台上的互操作。分布式数字身份与可信数字凭证系统通常包含以下4种用户：凭证持有者、VC签发者 (Issuer)、VC验证者及权威机构。权威机构是一种特殊实体，具有认证用户身份的能力，例如认证某一个用户为VC签发者。VC签发者通常是授权机构（如学校、医院、政府部门等），可注册凭证模板、签发可验证凭证。一个VC凭证的主要操作过程包括：

- (1) VC签发者根据业务特征设计并定义凭证模板，在模板中可以要求凭证声明内容包括哪些属性或数据字段，并规定哪些属性是必需的或可选的。
- (2) VC签发者公布凭证模板，并提供相应凭证的签发服务；
- (3) 凭证申请者（即持有者）选择一个凭证模板，填写凭证声明内容，并提交凭证创建申请；
- (4) VC 签发者获取凭证创建申请后，审核对应的凭证声明内容，当审核通过，签发该VC 凭证，为凭证签名等。
- (5) 凭证持有者拿到VC凭证后，可根据需要把该凭证出示给VC验证者。
- (6) VC验证者检验凭证是否真实，具体包括校验凭证是否是由

VC签发者签发的、校验持有者和VC签发者的身份、验证披露的数据是否真实。

## （二）链上链下结合的交易处理技术

区块链的去中心化、分布式存储、数据防篡改、可追溯、依靠密码学提供信任背书、按智能合约自动执行等特点为分布式交易平台提供了有力的技术支持。在比特币、以太坊等公有链上的交易往往通过加密货币（如比特币、以太币）实现。在比特币网络中，每一笔交易都需要全网广播，通知矿工，并产生一些费用打赏矿工（作为记账激励），而且网络的记账规则大大限制了交易速度，对于小额高频交易的场景非常不适用。针对以上问题，业界提出了链上链下结合的交易处理技术，闪电网络就是属于此类技术方法，其目的是为了实现在高效且低成本的交易。原先所有交易都在比特币网络上进行，交易记录都被记载在比特币网络这个大账本上，也就是说数据都是上链的。而闪电网络是比特币网络在链下的扩充，在闪电网络上进行的交易并不会记录到比特币的大账本上，这些交易是在链下完成的，它允许交易双方建立交易通道，并成为两个闪电网络节点，后续双方的交易都通过该通道完成，中间的交易数据不上链，因此也不用付手续费，交易效率得到了很大提高。已建立的支付通道可以被后续其它交易使用作为支付中转通道，从而形成一个依附于比特币网络的支付通道网络。只有在建立通道和关闭通道才需要在比特币网络上进行，这两个过程要全网广播上链。由于其高效和低成本的特点，闪电网络技术也被其它区块链系统所采纳使用。

## （三）多维度激励机制

目前，基于区块链的算力网络或资源分配调度的激励方法，主要有以下3种：

- BOINC<sup>[6]</sup>是由伯克利提出的网络计算开放基础设施项目，是全球最大的分布式计算项目。它是一种面向志愿计算（Volunteer computing）的开源中间件分布式计算系统。当前该平台正在与区块链技术进行整合，其主要激励机制是通过积分与COP代币实现，激励机制简单描述如下：算力供给用户在BOINC平台上完成计算任务后会获得反馈积分，积分可以进一步兑换成COP代币，COP代币就是其主要激励。未来BOINC计划基于智能合约让其产生专用的代币。

- BCERA<sup>[9]</sup>是由北京邮电大学和首都师范大学共同提出了一种区块链赋能的资源调度算法，不同于现有的资源调度方法，BCERA是依赖于一个区块链结构来实现的分布式计算资源调度方法，BCERA中的区块链节点通过求解任务调度优化问题来实现区块链的共识，从而避免了共识所带来的额外开销和时延，同时还提升了系统的可扩展性和鲁棒性。BCERA的激励机制主要由两部分组成，分别是（a）奖励：设定任务发布者使用资源的奖励。（b）处罚：对未能完成计算任务或提供虚假信息的节点予以处罚。
- ShareBC<sup>[8]</sup>是由中山大学提出了一种区块链赋能物联网数据共享激励框架，利用分片技术把区块链网络分割成多个支持并行处理数据共享交易的异步共识区，从而形成一个分层的数据共享方案；ShareBC利用智能合约实现了一种支持分层的数据拍卖模型的共享激励机制，解决了多层数据分配优化问题，优化的目标是最大化共享数据资源给用户带来的效用与访问数据资源的传输成本之间的差值。

以上方法并未考虑多维度的激励因素，包括低碳、节能、慈善、公益等。

#### （四）数据访问控制

在传统访问控制下，用户披露的信息往往超过了获取权限需要的范围，这种授权方式严重加大了用户隐私泄露的风险。为了增强隐私安全策略，可以使用证明代替明文、零知识证明、属性加密、匿名凭证等一系列策略和算法，使用户尽量减少甚至消除敏感信息的披露。

设计基于密文-策略的属性加密，构建由ANDGate（表示属性满足该节点下的所有属性条件）、ORGate（代表属性集合满足该节点下的某一属性集合条件）及LeafNode（代表属性节点）构成的带访问权限设置的访问树结构；基于属性的访问控制（包括对主体属性、客体属性、环境属性以及访问控制规则或策略的评估计算）实现细粒度的授权管理；基于匿名凭证，对声明信息仅提供有关声明结果的密码学验证方法，并不包含声明数据的明文或密文（例如对年满18周岁的认证，而不实际提供出生日期）。

基于以上密码学方法与策略，可以对身份数据及数字凭证的内容属性做选择

性信息披露，支持披露信息最小化，且防范第三方利用披露信息推测实体的现实身份或在其它场景中的身份，增强隐私保护。

## （五）算力资源调度

目前算力资源调度方法主要有以下几种：方案 1，季玲玲等人<sup>[10]</sup>面向数据中心与超算中心提出了一种基于评分排序的算力调度方法。其通过给定候选计算结点的算力满足程度、调度成本、算力性能、网络响应时间等特征带入预先定义好的评分函数打分，最后获得得分最高的算力资源结点作为调度目标算力资源节点。方案 2，王洪全等人<sup>[11]</sup>提出了一种面向容器集群的算力调度方法，该方法在构建集群时需要计算资源的基准算力进行标定，然后根据用户给定的计算需求与标定的计算资源算力进行比较，筛选得到算力大于等于用户计算需求的结点；当筛选后满足用户需求的计算节点为多个时，根据节点剩余内存数最大的结点作为当前最优分配结点。

前述方案 1 和方案 2 都是针对现有云计算基础设施的资源调度方法。现有方案均适配算力交易平台构架，在获取用户需求后对自身资源池进行匹配，然后根据资源池内满足用户计算需求结点的其他属性选择最优的向用户提供服务。在该应用场景下，资源调度问题实际上转化为一个检索重排序问题。通过阅读这些方案可以发现其存在以下缺陷：（1）评分函数结构和参数固定，难以反映用户的历史需求偏好，即所有用户共享相同的评分函数；（2）在对检索结果进行排序时选取的标准固定、单一，即机械地按照节点剩余内存或延迟等特定参数选择“最优”的结点提供服务。针对上述缺陷，基于计算最优传输理论，本课题提出一种数据驱动的算力交易平台资源调度方法。

## （六）区块链监管

采用不同区块链底层技术的业务链的数据结构和通信协议互不相同，业务链与监管系统之间的通信协议接口也不一样，因此业务链之间、业务链与监管系统之间互通难、互认难、互信难、互访难。为了实现对区块链上交易数据的监管，本课题研究新型区块结构、哈希锁定、公证人机制和侧链/中继、数据访问泛化等技术，提出了即插即用、高可扩展、自适应强等特点的联盟链自适应监管技术，

支持联盟链与监管系统之间数据可靠传递，适应主流区块的不同区块结构，实现监管系统与业务链之间的数据交互；支持在不可篡改前提下，满足监管需求的违规数据屏蔽。

## 四、解决方案

基于区块链的算力并网交易平台系统架构如图1所示，它包括数字身份链、交易链、算力交易平台DAPP（去中心化应用程序）、以及与交易链节点关联的交易服务通道控制器（Service Channel Controller）。

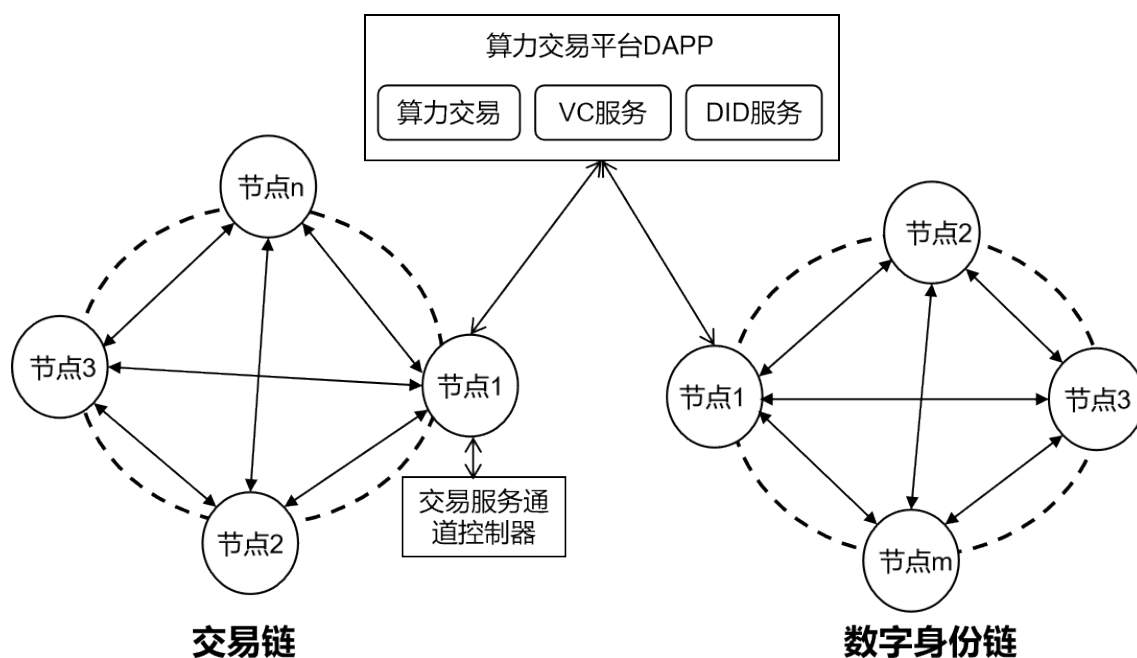


图 1 算力交易系统架构

### （一）数字身份链

数字身份链上保存用户的数字身份DID文档、用户相关的数字可验证凭证（如某种算力服务资质VC证明）。用户注册DID身份后，系统会给用户分配一个DID号，DID的私钥由用户保管，而对应的公钥保存在DID文档中，DID文档会写入数字身份链（即上链存储）。

用户分为算力供给用户（简称供给用户），算力消费用户（简称消费用户）以及权威机构用户；当一个用户注册为算力供给用户时，权威机构用户可以为其提供身份认证服务，比如基于KYC（Know Your Customer）认证（一种实名认证机制，一般通过诸如提供身份证明和常住地址等手段来核实用户身份），当认证通过后，供给用户成为一种具有DID身份的授权机构（凭证签发者即Issuer）用户，Issuer可以注册交易凭证模板，并签发交易VC凭证。算力消费用户的注册认证也

是由权威机构用户完成的，与算力供给用户相比，其认证相对宽松与简单，算力消费用户是一个具有DID身份的普通用户。权威机构用户是一种特殊用户，它通常是该系统的管理用户，具有为供给用户和消费用户提供身份认证的能力；同时权威机构会注册供给用户的资质认证凭证模板，并为供给用户提供资质凭证签发服务。

## （二）交易链

交易链上保存与交易相关的数据，所有交易数据以可验证凭证的方式保存到交易链上。算力交易通常包含一项交易启动事件，该事件表示交易双方对某一个交易合同或协议达成共识并开始按该协议进行交易；同时算力交易一般是按时计费的，所以要求具有定时结算的机制；在交易双方结束交易时，也会触发一个交易结算。基于算力交易的以上特点，本方案提出了一种支持灵活交易模式的算力交易方法，基于可验证数字凭证（W3C的VC标准）设计交易数据模型，允许算力供给用户定义并发布定制的交易模式。

另外在交易链上，本方案提出一种算力交易激励方法，设计智能合约程序，综合考虑多种激励条件，形成一种满足不同用户需求的交易方案推荐与撮合机制；在资源调度方面，提出了一种数据驱动的算力资源调度方法；在交易监管方面，提出了一种异构联盟链自适应监管架构以及多种面向联盟链监管的数据屏蔽方法。

### 1、交易模式

本方案提出了以下4个关键数据结构包括2种CPT（Claim Protocol Type）模板和2种VC凭证，如下：

#### （1）CPT（Claim Protocol Type）模板

CPT 模板，一种数字凭证模板，它定义了凭证声明包含的数据字段及各字段的数据类型，并声明哪些字段是必需的。

#### ● 交易启动CPT模板

启动一个交易的模板，由供给用户定义并注册，一个模板样例如下：



```

{
  "title": "模板名称",
  "description": "模板描述",
  "type": "object",
  "properties": {
    "pdid": {
      "type": "string",
      "description": "供给用户 DID"
    },
    "cdid": {
      "type": "string",
      "description": "消费用户 DID"
    },
    "spec": {
      "type": "string",
      "description": "算力规格, 如每秒多少 GFLOPS, MFLOPS, TFLOPS 或PFLOPS"
    },
    "price": {
      "type": "float",
      "description": "每分钟的价格, 单位元"
    },
    "minCost": {
      "type": "float",
      "description": "最小开销即起步计价, 单位元"
    },
    "checkinCptId": {
      "type": "integer",
      "description": "结算模板 ID"
    },
    "encryption": {
      "type": "string",
      "description": "加密方式, 如: 明文、CP-ABE"
    }
  },
  "required": [
    "pdid",
    "cdid",
    "spec",
    "price",
    "checkinId"
  ]
}

```

其中properties是声明内容包含的数据字段，required定义了哪些字段是必需。

### ● 交易结算CPT模板

进行交易结算上链的模板，由供给用户定义并注册，模板样例如下：

```

{
  "title": "模板名称",
  "description": "模板描述",
  "type": "object",
  "properties": {
    "pdid": {
      "type": "string",
      "description": "供给用户 DID"
    },
    "cdid": {
      "type": "string",
      "description": "消费用户 DID"
    },
    "cost": {
      "type": "float",
      "description": "结算费用, 单位元"
    },
    "startTs": {
      "type": "TIMESTAMP",
      "description": "结算周期起始时间"
    },
    "endTs": {
      "type": "TIMESTAMP",
      "description": "结算周期结束时间"
    },
    "tradeType": {
      "type": "string",
    }
  }
}

```

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要  
下载或阅读全文，请访问：

<https://d.book118.com/428011137121006103>