基于区块链的分布式资源授权系统设计

张　义，李　桐，王　钺
（清华大学　电子工程系，北京　100084）

摘　要：在当今数字化时代，随着云计算、物联网和分布式网络的兴起，资源的分散性和多样性日益增加，要求用创新性的方法来确保这些资源的安全、高效和公平的利用，分布式资源的有效管理和授权使用已经成为一个至关重要的研究问题。创新性地提出了一套全面的分布式资源授权使用框架，旨在为各种应用场景提供可扩展性和可定制性的解决方案。该系统采用了主链对齐一或多条并行侧链的基础系统架构，内设基于同步机制和监管机制等算法模块。通过区块链技术的去中心化、不可篡改和安全性特性，侧链技术的扩展性，有效应对了性能和灵活性问题。本研究的成果具有广泛的应用潜力，不仅可以用于数字资产管理，还可以扩展到诸如物联网设备授权、智能合约交互等领域。系统设计为分布式资源管理带来了突破性的创新，为构建更加安全、高效的数字社会奠定了坚实的基础。

关键词：区块链；分布式资源；资源授权使用；侧链
中图分类号：TP393　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2024. 05. 008
引用格式：张义，李桐，王钺. 基于区块链的分布式资源授权系统设计[J]. 网络安全与数据治理，2024，43(5)：52 - 60.

Design of a distributed resource authorization system based on blockchain

Zhang Yi, Li Tong, Wang Yue
(Department of Electronic Engineering, Tsinghua University, Beijing 100084, China)

Abstract: In this digital age, with the rise of cloud computing, the Internet of Things, and distributed networks, the dispersion and diversity of resources are increasing. Innovative methods are required to ensure the secure, efficient, and fair utilization of these resources. The effective management and authorization of distributed resources have become a crucial research issue. This paper innovatively proposes a comprehensive distributed resource authorization framework based on the problem of distributed resource authorization usage, aiming to provide scalable and customizable solutions for various application scenarios. The system adopts a basic system architecture of aligning one or more parallel side chains on the main chain, with built-in algorithm modules such as synchronization mechanism and supervision mechanism. Through the decentralization, immutability, and security features of blockchain technology, the scalability of sidechain technology effectively addresses performance and flexibility issues. The results of this study have broad application potential, not only for digital asset management, but also for areas such as IoT device authorization and smart contract interaction. The system design has brought breakthrough innovation to distributed resource management, laying a solid foundation for building a more secure and efficient digital society.

Key words: blockchain; distributed resources; authorized use of resources; lateral chain

0　引言

随着科技的不断进步和全球经济的快速发展，越来越多的行业和领域都开始依赖于分布式资源[1]来支持其运营和发展。分布式资源的定义涉及在多个地理位置或网络节点上分散分布的各类资源。这些资源可以是物理的，如土地、房屋、能源及自然资源；也可以是数字的，例如分布在不同服务器和网络中的计算能力、存储空间和数据。分布式资源的关键特征在于其所有权和控制权的分散性，资源类型的异质性，以及对高效协调和管理机制的需求。

在分布式资源的管理和应用上，需要考虑资源的多样性和位置的分散性，这要求制定有效的管理策略和技术协调机制。例如，分布式能源系统中不同地理位置的能源资源需通过有效的策略进行管理和调度以实现最大

化利用。在数字资源方面，如云计算资源，需要依赖于先进的网络协议和算法来实现资源的高效分配和利用。

在土地方面，房屋分布在城市、乡村和各个地理位置。每座房屋都具有独特的特点，包括地理位置、面积、设施等等。这些房屋资源分散在各个地方，通常由不同的房地产开发商、业主或租赁公司拥有和管理。这种分散的性质使得房屋租赁[2]成为一种典型授权使用的分布式资源案例。租户通过租赁协议获得了对特定房屋的使用权，但并不拥有该房屋的所有权。这个协议规定了租户可以使用房屋的时间、租金支付方式、责任和权利等方面的条件。通过租赁协议，租户获得了对分布在不同地点的房屋资源的访问权限，而这些资源是由各种不同的房地产所有者提供的。

同时，数据也是一种极其宝贵的分布式资源，分布在不同地点、服务器和数据库中。这些数据包括个人信息、企业数据、科研数据、金融数据等，它们分散存储在各个组织、云服务器[3]、边缘设备[4-5]以及在线平台中，构成了一个庞大而复杂的数据生态系统。以个人隐私数据为例，这种数据通常由不同的组织、应用程序和服务提供商收集和存储。用户在使用应用程序或在线服务时，通常需要授权这些实体来访问其数据，以便提供个性化的服务或功能。用户授权应用程序或服务访问其位置信息、社交媒体帐户、购物习惯等数据，以获取相关推荐或定制内容。由此可见，如何合理使用一些分布式的资源成为当下需要解决的问题。

分布式资源授权使用是一种确保分布在不同地点或系统中的资源被安全、合法地访问和利用的机制。这种机制实际上是一种分布式信任机制，它需要确保各方在没有中心权威机构的情况下，可以相互信任、合作和交互，通过明确定义访问权限、控制资源的使用方式，并使用安全技术来保障资源的安全性、可用性和可追溯性。

这意味着需要建立一种安全、透明和可验证的方式，来管理分布式资源的访问和使用权限。在区块链技术的支持下可以保证只有满足特定条件的参与者可以获得资源的访问权。这种方法不仅可以增加安全性，还可以提高资源的可追溯性和透明度，降低纠纷的风险。综上，本文率先提出了分布式资源授权使用问题，针对这个问题，创新性的提出了一种分布式资源授权使用框架。

在不同领域，资源的访问和使用需要透明性、隐私保护以及防止未经授权的访问或篡改。传统的中心化授权体系存在安全和信任问题。实现分布式资源授权使用系统需要综合考虑并解决各种挑战，以确保系统能够安全、高效、可靠地授权用户对资源的访问。

因此需要创新的解决方案来实现更安全、可信和高效的分布式资源授权使用。区块链技术通过其去中心化、智能合约和不可篡改的特性，将为这些问题和挑战提供了一个有前景的解决方案。

2008 年，中本聪提出了去中心化加密货币 - 比特币[6]的设计构想。2009 年，比特币系统开始运行，标志着比特币的正式诞生。伴随着以太坊等开源区块链平台的诞生以及大量去中心化应用的落地，区块链技术在更多的行业中得到了应用。目前，在区块链技术方面，国外侧重于 BFT 共识算法[7]、子链[8]等底层关键技术。国内则侧重于哈希锁定[9]、分布式私钥控制[10]、隐私数据授权访问[11]等中间层关键技术，以及分布式应用、智能合约[12]等应用层关键技术。袁勇等[13]给出了区块链基本模型，以比特币为例将非许可链分为数据层、网络层、共识层、激励层、合约层和应用层；邵奇峰等[14]结合开源项目细节，对比了多种企业级区块链的技术特点；Yang 等[15]总结了基于区块链的网络服务架构的特点、挑战和发展趋势；韩璇等[16]系统性归纳了区块链安全问题的研究现状；Ali 等[17]总结了区块链在物联网方面的应用研究进展、趋势。

面对分布式资源授权使用这一问题，对区块链技术提出了新的挑战。

本文解决分布式资源授权使用问题的方案和传统区块链解决方案相比，都涉及到分布式信任机制，但它们解决的问题、设计特点以及应用场景有一些相同点和不同点。相同点在于，二者都旨在建立成功的分布式信任机制，使参与者之间能够进行安全、可信任的交互，而无需依赖中心化的权威机构。其次都通过去中心化的方式来维护系统的可信性和安全性，避免了单一点的故障和控制。最后传统区块链解决方案使用区块链技术来确保交易数据的不可篡改性，分布式授权也会采取类似的机制来确保授权数据的完整性和不可篡改性。不同点在于，分布式授权通常更侧重于授权和许可问题，例如授权访问资源、服务或功能。同时需要考虑多次授权的情况，即授权者可能会多次授权不同的操作或资源访问。这需要一个更灵活的授权管理系统。而传统区块链解决方案更广泛地应用于数字货币、智能合约和记录交易历史等领域。其次分布式授权通常需要考虑计量和计费问题，因为不同的授权可能需要不同的费用，并且需要记录和报告这些费用。最后在交易频次方面，传统区块链解决方案上的交易通常是公开的，而分布式授权可能涉及频率较高但更敏感的授权请求，而且会涉及审计和审查等问题，因此需要不同的性能和安全考虑。

因此，本文中实现分布式资源授权使用系统的特点涵盖了多个关键领域，包括强化的安全性、保持操作的

一致性、优化的性能与扩展性，以及全面的审计和监控机制。系统设计确保只有授权用户或实体能够访问资源。同时，为了保证在分布式环境中的决策一致性，系统采用了以太坊[18] POA（Proof of Authority）的共识机制。此外，考虑到大规模用户和资源的管理，该系统通过主侧链同步机制被设计为具备高性能和良好的可扩展性，以应对高负载情况下的稳定运行和请求处理。最后，通过监管机制，例如细致的审计日志和监控系统，可以有效地跟踪和记录资源访问的各个方面，为审查和故障排除提供支持。这些特点共同构成了一个全面、高效且安全的分布式资源授权使用系统。

具体来说，本研究的主要贡献在于针对分布式资源授权使用系统中的性能和安全性挑战，提出了一种全新的分布式资源授权使用系统框架。为了处理大规模交易和数据存储时的性能瓶颈，仅使用单一链是不可行的。首先，单一链可能无法承载大量的交易和数据处理，导致系统性能下降。其次，单一链上的所有交易和数据都需要经过共识机制的验证和记录，这可能会导致交易处理速度变慢。此外，单一链上存储的数据量可能会随着系统的扩展而增加，进而影响系统的可扩展性。

本文采用的同步机制为侧链技术，通过双向挂钩算法将部分交易和数据处理从主区块链转移到侧链，显著提高了系统的处理能力和可扩展性。同时，主链上存储了关键的授权数据，以确保授权信息的安全性和不可篡改性。最后根据不同应用场景，分别使用弱 SPV 和强合约权限控制算法。这一监管机制有效地利用了区块链的去中心化和安全性特点，确保了数据的完整性和可靠性。

通过结合使用区块链和侧链的方法，本文框架支持更加灵活和定制化的授权策略，满足了多样化的应用场景和用户需求。同时，侧链的引入也优化了存储和计算成本，提高了系统的经济效益和可持续性。总之，本研究为分布式资源授权使用系统带来了一种更加高效、安全且灵活的解决方案，有效应对了当前面临的主要挑战。

本文详细设计了一套框架解决分布式资源授权使用问题，通过框架中的两种机制实现有效的资源控制和授权使用，并提出测试方案。首先回顾了区块链技术的研究现状，介绍了分布式资源授权使用问题中可能遇到的挑战，将传统区块链解决方案和分布式授权进行了对比分析。其次对分布式资源授权使用问题的解析以及架构设计的介绍，包括介绍框架中的两种机制实现有效的资源控制和授权使用。最后给出系统测试方案与结论。经过测试，本框架可以改善区块链网络的可扩展性和效率。

1　分布式资源授权使用问题

在各种应用场景中，转移使用权的问题被抽象为一种分布式资源授权使用的核心问题。这个问题的关键在于确保使用权能够合理地在多个参与方之间进行转移和授权。其中权属交易是与分布式资源授权使用问题密切相关的关键概念，它包括了资源的所有权和授权使用。权属交易通常涉及资源的转移、授权和管理，涵盖了多个参与方之间的合作和协调。从这个角度来看，权属交易可以被视为分布式资源授权使用问题的核心。

在权属交易中，资源的拥有者可以将其资源的使用权分配给其他参与方，这些参与方可以是个人、组织或智能合同。这种权属交易的目标是确保资源的合理分配和管理，以满足参与方的需求，并确保资源的有效利用。

分布式资源授权使用问题涉及多个参与方之间的资源控制和协调，以便实现权属交易的有效执行。这包括确保资源的所有权得到尊重、资源的授权使用符合法规和协议，以及资源的转移和分配能够顺畅进行。

然而，由于分布式系统的特性，资源的授权使用涉及多个参与方之间的协调和管理，因此存在一些挑战和问题需要克服。解决这个问题需要考虑多方的权益和合作，以建立可信的权属交易机制。这正是本系统框架致力于解决的核心问题。

当前权属交易存在交易量低、传输速度慢、访问速度慢以及缺乏监管机制等问题（如图 1 所示），因此提出分布式资源授权使用框架。该框架基于分布式系统的原理，通过将资源和权限的管理分散到网络中的多条链上，以提高整体的交易效率和访问速度。

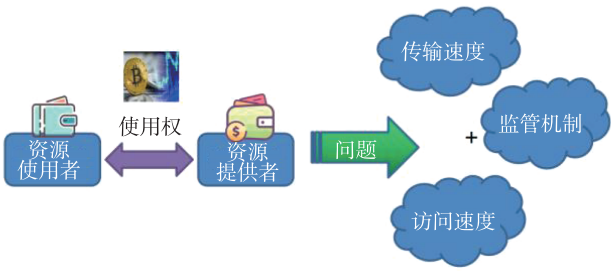

图 1　分布式资源授权使用问题

2　分布式资源授权使用框架

本文提出一套框架与两种机制进行合理的分布式资源授权使用。不同于以往的单一区块链系统，针对分布式资源种类繁杂、分布广泛的特点，本文的分布式资源授权使用系统创新性地采取了一条多功能主链连接一条或多条简洁单一功能的并行侧链的处理方式。基于同步机制和监管机制，有效地完成资源提供者分配使用权，资源使用者按需行使使用权的闭环架构设计。

该框架分为主链和侧链，主链用于资源提供者将使用权发放出去，侧链用于资源使用者利用使用权代币行

使使用权，两条链用双向挂钩机制进行联系（如图 2 所示）。主链功能比较复杂，主要负责资源提供者和交易中心之间的大额资源流通，用于整体处理多笔交易，其中需要包括交易数量的限制、监督记录等功能。侧链则可以视为是部署在不同地区、应用于不同币种的负责多次小额交易的流通处，它有很多条并行且互不干扰的链，其功能较为单一简洁，主要负责资源使用者和回收站之间的使用权交易。因此一条主链应该对应一条或者多条侧链。

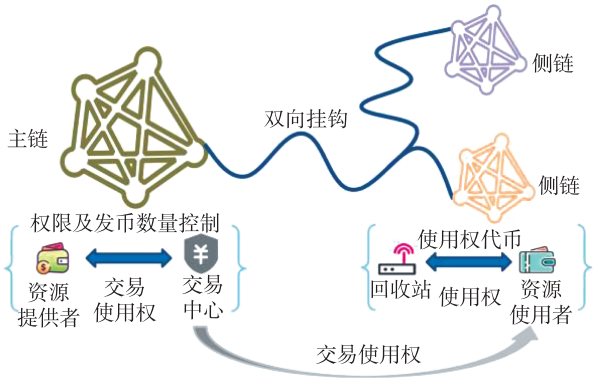

图 2　分布式资源授权使用框架

首先，该框架由多条链完成资源传输交易，解决了传统集中式系统中交易量低的问题。由于交易分布在不同的链上，可以大大减少链上的负担，从而提高交易的并发性和总体交易量。其次，框架利用双向挂钩的算法，使得资源的传输速度得到显著提升。在各个链的互相传输信息的基础上，通过并行处理的方式提高资源的访问速度。回收站的引入实现交易分区域划分，大大提高了用户访问速度。此外，分布式资源授权使用框架还引入了监管机制，以解决传统系统中缺乏有效监管的问题。通过使用智能合约、链下等技术手段，可以实现对交易和资源使用的全程监管和可追溯性，确保资源的合法使用和交易的公正性。整体架构设计如图 3 所示。

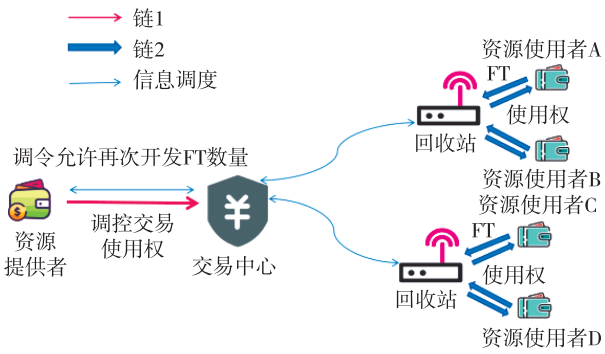

图 3　整体系统架构图

图 3 展示了分布式资源授权使用的系统框架设计。红色箭头表示主链，蓝色和橙色箭头表示 n 个侧链，蓝色细线表示消息传输，其中每个区域中的每个场景使用一个单独的链。

首先，所有资源提供者根据需要通过交易中心将使用权交易给主链上所有区域的所有资源使用者，完成授权使用权。之后，在每个区域和场景域中，资源提供者从每个区域中的回收站获得相应的使用权限。同时，资源提供者也将与回收站进行其他使用权交易。最后，回收站会将信息发送回总交易中心，由总交易中心决定是否命令数据组件开发商再次开发。其中在主链上的角色包括：负责宏观监管功能的交易中心，具有相应的货币发行监管机制和启动增发的逻辑功能，还有所有的资源提供者。在侧链上的角色主要有负责监管和汇总功能的回收站模块，所有的资源使用者。最后，构建了一个具有一个主链和多个侧链的区块链系统。

综上所述，分布式资源授权使用框架通过分散资源、提高访问速度以及引入监管机制等方式，有望解决当前面临的交易量低、传输速度慢、访问速度慢和缺乏监管机制等问题，为用户提供更高效、安全和可信赖的资源交易环境。

3　分布式资源授权使用通用机制

分布式资源授权使用的框架设计主要涉及两个通用机制：同步机制和监管机制。

3.1　同步机制

同步机制是指在分布式系统中，对资源的访问进行同步和协调，以确保多个节点或进程不会同时访问或修改资源，从而避免资源冲突和数据不一致性。

在讨论同步机制的框架下，本文专注于以太坊侧链、双向挂钩机制以及回收站模块，确保整个系统的协调运作和数据一致性。

3.1.1　以太坊侧链与双向挂钩

在处理大规模交易量方面，单一主链的架构面临显著挑战。由于主流区块链如比特币和以太坊强调去中心化和安全性，它们在设计上对每个区块的大小和生成频率设定了限制。这种设计导致了处理交易的速度和容量上的固有限制。

随着交易请求的增加，这些限制导致了一系列问题，如交易确认时间的延长和交易费用的上升，影响了用户体验和整个系统的效率。为了应对这一挑战，侧链技术被提出作为一种解决方案。侧链是与主链平行运行的独立区块链，能够承担部分交易处理和数据存储的任务。通过将交易从主链迁移到侧链，可以显著减轻主链的负

担，提高整个网络的处理能力。

侧链技术的引入不仅提高了交易处理的频率和规模，而且保持了主链的核心特性，如安全性和去中心化。这种架构使得在侧链上进行的交易既快速又低成本，同时保留了主链的安全保障。因此，侧链提供了一种有效的解决方案，以增强区块链技术的可扩展性和应用实用性。

主链和侧链采用双向挂钩机构连接。双向挂钩允许使用权属代币从区块链主链转移到侧区块链。使用权属代币实际上并没有被转移，而是被暂时锁定，而相同数量的相等使用权属代币在侧区块链上解锁。当相同数量的使用权属代币再次锁定在侧区块链上时，原始代币将被解锁。这基本上是双向挂钩想要实现的功能。

如图 4 所示，实现双向挂钩的一个可能选择是让一个交易所负责监控锁定的币和解锁的相等代币。交易所将在解锁辅助代币之前对币进行锁定。

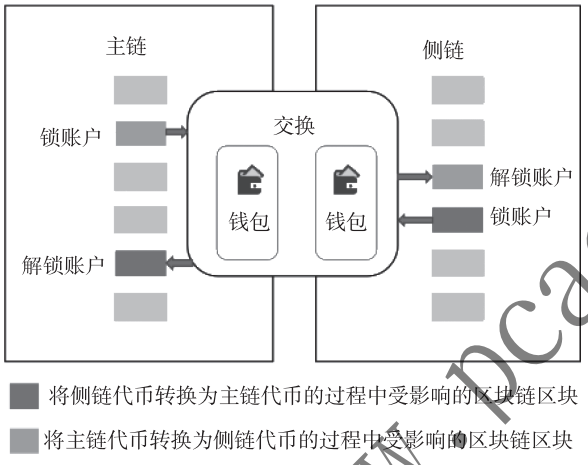

图 4　双向挂钩

本系统中使用的是通过引入部分监管模块进行监听及打印。对于每次交易，需要交易权属后将信息监听，可以对发币控制等操作进行指导。具体来说，在每次交易发生后，会详细记录交易数据的各个元件的权属情况。这包括记录每个交易的参与者、交易的金额、交易时间等关键信息。模块可以将这些信息输出到后台。

3. 1. 2　以太坊的共识机制

本框架采用权益证明（Proof of Authority，PoA），由特定的权威节点或验证者来生成新区块。在 PoA 机制中，事先指定了几个权威节点作为网络的验证者，这些验证者具有生成新区块的权限。与工作量证明（PoW）或权益证明（PoS）不同，PoA 并不依赖于计算能力或代币持有量，而是依赖于验证者的身份和信誉。在使用 PoA 机制的网络中，验证者通常是已知的实体或组织，被信任具有维护网络安全和有效性的责任。这种机制适用于需要高度中心化管理和控制的场景，例如企业内部区块链网络或特定联盟中的链。通过使用 PoA 机制，网络可以实现更高的交易吞吐量和更低的能源消耗。

3. 1. 3　回收站模块

针对访问速度的问题，引入了一个新的本地回收站，负责回收资源使用者的使用权代币。同时也是侧链上和主链进行双向挂钩的地址，具有一些专属的功能，比如快速处理收集到的代币，进行同步，记录，限制和监管等。

由一个监管机构负责监督和维护传输系统的正常运行。如图 5 所示，回收站系统用于回收不同类型的使用权代币，并为它们分配访问权限。当一定数量的代币被回收时，侧链和主链之间的互动功能会被激活，用于封装和交易整个代币。这使得资源提供者能够继续销售后续的使用权。

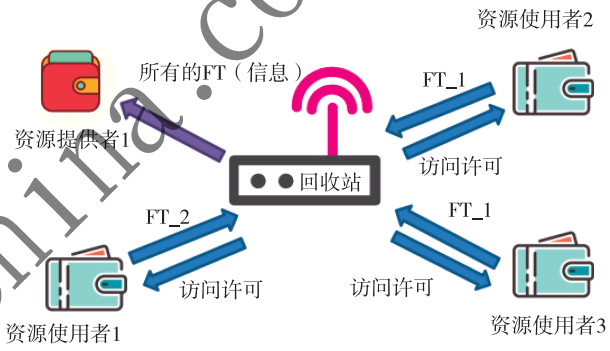

图 5　回收站模块框架

在回收站中，数据应用开发者可以获得对使用权代币链接的访问权限。为了实现这一点，回收站会基于时间生成哈希 ID，并将其加密到要访问的组件中，确保只有获得授权的开发者才能访问相关的数据组件。回收站的功能类似于之前的监督锁定和解锁使用权代币交换的功能。它提供了一种机制，通过回收和重新分配使用权代币，以确保合适的权限和访问控制，以及分布式资源的持续销售。

3. 2　监管机制

监管机制是指通过一个中央管理节点或者授权服务器来控制资源的分发和访问权限。

在设计监管机制的框架时，本文重点关注交易中心，及其涉及两种算法机制：弱 SPV 线下权限控制算法和强合约线上权限控制算法。这些是实现高效、安全和合规的监管体系的基石，共同构成了监管机制的核心。

3. 2. 1　交易中心

针对溯源监管的要求，提出交易中心的概念。交易中心内部负责监管信息、控制代币分发以及实现溯源等功能。

监管信息：交易中心作为一个核心组成部分，承担

监管信息的职责。它收集、存储和管理有关交易和授权的信息。这包括参与方的身份验证、交易细节、许可授权历史等数据。通过监管信息，交易中心能够提供实时的、准确的数据，以支持监管机构、合规团队和其他相关方对系统操作的跟踪和监管。

代币分发控制：交易中心在代币发行和分发方面发挥关键作用。它可以创建新的代币或数字资产，并确保它们按照规定的策略和规则进行分发。这可以包括预定的代币释放时间表、分发给特定用户或角色的代币数量等。通过这种方式，交易中心可以实现对代币供应的有效控制，确保系统的稳定性和可持续性。

溯源和审计：交易中心通过记录和存储所有交易的细节，为溯源和审计提供了必要的数据。这对于监管合规、解决纠纷和审计交易历史非常重要。交易中心的记录可以被用于验证交易的合法性，确定任何潜在的违规行为，并跟踪交易的来源和去向。这种透明度有助于建立信任，并确保系统的安全性和合法性。

用户身份验证和许可授权：作为系统的中心枢纽，交易中心负责验证用户身份，并执行许可授权策略。它可以根据用户的身份和角色来管理他们对系统资源的访问权限。这种许可授权可以是静态的，也可以根据动态条件进行调整。通过这种方式，交易中心确保只有授权用户能够执行特定的操作和访问特定的资源。

综上所述，交易中心在分布式资源授权使用框架中扮演了至关重要的角色。它不仅为监管机构提供了监管信息和审计工具，还确保了代币的合理分发和系统资源的有效管理。交易中心的功能使整个系统更加透明、可信、合规，并支持了资源的安全和可控使用。

3.2.2 弱 SPV 线下权限控制算法

为了完善监管体系，提出两种授权和权限控制算法机制应用在交易中心模块上，分为链上和链下两个算法。

第一种算法为利用 SPV 在线下进行监管机制的引入，在区块链中，签名被广泛用于验证和授权事务的有效性和身份。本系统中主要是应用于授权和权限控制，其中有两个过程，即签名过程和验证过程。

交易中心为了实现对货币发行过程的监管，采用了一种名为交易中心链外授权的算法，即 SPV 加密验证。该算法确保只有经过授权的资源提供者才能发行货币。

如图 6 所示，当资源提供者有发币意向时，需调用发币函数并提供相关信息，如货币数量和发行时间等。为了获得授权，开发商需要向交易中心提交一个包含 SPV 签名的请求。

在这一过程中，交易中心生成一个 SPV 签名，通过使用私钥对特定的交易信息进行加密得到。这个私钥只有交易中心掌握。开发商将发币请求和交易中心生成的 SPV 签名一同提交给发币函数。

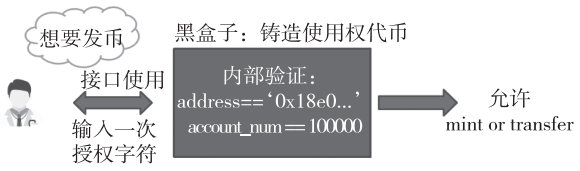

图 6　交易中心链外授权—SPV 加密验证

发币函数对提交的发币请求进行验证，包括验证开发商的身份和授权情况。然后，使用交易中心的公钥来解密 SPV 签名，以验证其有效性和正确性。只有在解密成功并验证通过的情况下，发币函数才会执行发币操作，将相关信息记录到区块链中并向网络添加新的货币。优点在于它能够在区块链之外进行操作，从而减少了区块链上的负担。然而，缺点是尽管链下操作可以减轻链上的负担，但安全性方面需要额外的保障。设计和实现适当的加密机制以保护链下操作的安全性可能变得更加复杂。

3.2.3 强合约权限链上控制算法机制

另一种授权和权限控制的算法机制是通过智能合约内部实现的。在这种机制中，交易中心可以授予其他资源提供者发币的权限，并对其发币数量进行限制。

通过在智能合约中编写代码，交易中心可以创建一个权限系统，控制哪些开发者有权发行新的代币，以及限制每个开发者可以发行的最大数量。

这种机制的实现方式可以根据具体需求进行设计。交易中心可以在智能合约中维护一个权限列表，记录哪些开发者被授予发币权限。当一个开发者尝试发行新的代币时，智能合约会验证该开发者是否在权限列表中，并检查发币数量是否超过了限制。通过在智能合约中实现授权和权限控制机制，可以确保只有经过授权的开发者才能发行新的代币，并限制其发行数量。这种方式可以提高系统的安全性和可信度，并为开发者提供一个可靠的发币框架。这种授权和权限控制算法机制利用了区块链的特性，并通过智能合约的设计来实现。

其中的优点包括：首先利用区块链的不可篡改性和去中心化特点，确保授权和权限控制的可靠性和透明性。智能合约的执行结果可以被所有参与者验证和审计，从而增强了系统的安全性。其次是设计的灵活性，智能合约可以根据具体需求进行设计和修改。通过编写智能合约的代码，可以灵活地定义授权规则和权限控制逻辑，以适应不同的应用场景和需求变化。

最后是安全性，通过智能合约的内部实现，授权和权限控制可以得到强大的加密和验证机制的支持。这确保了数据和操作的安全性，并降低了潜在的风险和漏洞。

然而，这种机制可能会加重链上的负担。由于智能合约需要在区块链上执行，每个授权和权限验证都需要消耗一定的计算资源和存储空间。因此，当权限列表和授权操作较为频繁时，可能会对链上的性能和吞吐量产生一定的影响。为了平衡安全性和链上负担，需要仔细设计和优化智能合约的逻辑，以减少不必要的计算和存储开销。同时，随着区块链技术的进一步发展，不断优化和扩展链上的处理能力，可以缓解这种负担带来的影响。

4　系统的合约方案测试

本节将通过设计测试方法对合约及方案进行可行性验证。

4.1　通用机制测试

在本技术架构中，权属交换功能主要指的是基于区块链的资源所有权和使用权的转移。研究旨在更新通用机制中主链侧链同步机制和监管机制。通过分析优势和挑战，旨在为进一步研究和改进这些机制提供基础，以推动区块链技术的发展。

通过交易中心链上授权的方式，将监管需求写入智能合约中，利用区块链执行合约来实现一次授权一次操作的机制。具体而言，交易中心会将授权发币的相关规则和条件编写成智能合约，并将其部署到区块链上。合约中会包含交易中心定义的授权函数，用于授予特定资源提供者发币的权限。同时，还会定义发币操作的限制条件，例如最大发币量。

当资源提供者希望发行货币时，其需要向交易中心发起授权请求。交易中心通过直接调用合约中的授权函数来完成授权操作。在授权过程中，智能合约会根据预先设定的规则和条件进行验证，包括验证开发商的身份和授权的发币数量是否符合限制。一旦授权验证通过，智能合约会执行发币操作，并将相关信息记录到区块链中。此时，该资源提供者就获得了发币权限，并受到最大发币量的限制。

测试此合约的正确性验证方式：

（1）测试资源提供者设置使用权代币正确的名称、符号和最大发行量；

（2）测试默认情况下授权者是交易中心；

（3）测试交易中心授权新的资源提供者发币；

（4）测试不允许资源提供者未经允许移除自己；

（5）测试允许交易中心移除其他资源提供者；

（6）测试不允许其他账户移除资源提供者；

（7）测试允许资源提供者进行使用权代币发行；

（8）测试不允许超过最大发行量使用权代币。

4.2　综合场景测试

研究设置了一个虚拟化环境，旨在简单地模拟分布式资源授权使用的交易场景，并评估主侧链桥接机制在小额交易中的性能和效率。资源开发者在主链上向交易中心发送使用权代币，之后资源使用者通过侧链行使使用权的代币，之后传到回收站收集，侧链上的回收站通过双向挂钩与主链进行代币同步对齐，最终实现一个代币闭环的系统。实验将统计整个交易过程所花费的时间，以评估主侧链桥接机制在小额交易场景中的性能和效率。

具体来说，以 ERC20 的以太坊同质化代币，使用基于 POA 的共识协议为基础。该环境用虚拟机搭建，包含两条链，其中一条是主链（称为 M 链），另一条是侧链（称为 S 链）。主链配置为单核处理器，使用 Main Chain Port 为 7545 和 Network ID 为 1337 的设置，而侧链也配置为单核处理器，使用 Side Chain Port 为 8545 和 Network ID 为 1338 的设置。

实验模拟了资源开发者（A）向交易中心（B）转移了 X 个主链币的情况，并在转移过程中锁定了交易中心的传输权限。由于交易中心和侧链共享相同的地址，因此能够以零额外成本的方式将数量同步到侧链。随后，交易中心将 Y 个侧链币传送到资源使用者的账户（C），资源使用者随后将使用的 Y 个侧链币分成 N 次，每次传送 M 个侧链币至回收站（D）。回收站负责统计，并在交易中心解锁相应的 Y 个主链币的权限。最终，交易中心将 Y 个主链币回传给资源开发者，完成了侧链上的小额交易过程。值得注意的是，实验能够精确统计整个交易过程所花费的时间，以评估主侧链桥接机制针对小额交易的性能和效率。

在开始主侧链时间对比之前，开展两项附加实验，以更深入地探索与主实验相关的一些关键因素。

实验 1 旨在研究核数与传输时间之间的关系。实验的背景在于，核数可能会对区块链网络的性能产生重要影响，可能导致通信开销的增加。通过实验 1，希望确定核数对传输时间的影响，更好地理解网络的性能特征。

实验 1：核数和传输时间的关系

给 X、Y、N、M 赋值：X = 100 000，Y = 1 000，10 000，50 000，N = 100，1 000，5 000，M = 10，core = 1，2。

实验结果（如表 1 所示）显示，增加核数（或节点数量）在区块链网络中表现出了正比的性能提升。

表 1　核数和传输时间的关系

传输量级	1 核/s	2 核/s	时间减少率/%
100（次数）×10（token）	7. 067	3. 504	50. 42
1 000（次数）×10（token）	50. 784	25. 089	50. 59
5 000（次数）×10（token）	233. 211	116. 289	50. 13

实验2关键因素是小额传输代币数量（M）与传输时间之间的关系。在区块链中，快速和高效的小额交易对于许多应用至关重要，以便更好地理解区块链网络的可扩展性和响应时间。

实验2：小额传输代币数量M与传输时间的关系

给X、Y、N、M赋值：X = 100 000，Y = 1 000，10 000，50 000，N = 100，1 000，5 000，M = 10，50，100。

实验结果（如表2所示）显示，小额传输代币数量（M）对传输时间没有显著影响，即增加小额传输代币数量并没有导致传输时间的明显增加或减少。这表明，区块链网络在处理小额交易时表现出了稳定的性能。

表2　小额传输代币数量与传输时间的关系（s）

传输量级	10 token	50 token	100 token
100（次数）×10（token）	2.682	2.698	2.667
1 000（次数）×10（token）	24.472	26.601	25.423
5 000（次数）×10（token）	118.289	119.245	118.762

主实验着重研究了主链侧链桥接机制对区块链性能的影响。侧链可以扩展主链的功能，并允许更多的交易和智能合约执行。然而，引入侧链也可能引入一定的传输延迟和复杂性。因此，主实验旨在深入研究主链侧链桥接机制，以及它如何影响区块链的性能。

实验3：主链侧链桥接机制对区块链性能的影响

给X、Y、N、M赋值：X = 100 000，Y = 1 000，10 000，50 000，N = 100，1 000，5 000，M = 10

实验结果（如表3所示）显示，主侧链桥接机制相对于单链传输，能够减少了大约48%的交易时间。其中不到50%的性能损耗主要由双向挂钩同步机制和主侧链记录的交易类型和功能的一些差异而导致。这表明主侧链桥接机制在处理小额交易时具有明显的性能优势，同时具有较高的可解释性和安全性，为区块链生态系统中的小额交易提供了更高效的解决方案，对于改善区块链网络的可扩展性和效率具有重要的指导意义。

表3　单链与主侧链桥接机制传输时间减少率对比

传输量级	单链传输/s	主侧链桥接/s	时间减少率/%
100（次数）×10(token)	6.21	3.285	47.1
1 000（次数）×10(token)	50.558	27.205	46.19
5 000（次数）×10(token)	253.99	131.027	48.4

5　结论

为解决分布式资源授权使用问题，本文创新性地提出了一个分布式资源授权使用框架，向多个领域的分布式资源授权使用问题提供了有力的工具和解决方案。通过引入一条主链对应一或多条简单侧链的方式，在同步机制和监管机制的支撑下，通过引入交易中心、回收站模块，采用链上链下鉴权等策略，为资源授权交换使用提供了创新性的方法。这些方法有效地增强了资源的可追踪性和可控性，降低了潜在的滥用和误用风险，使资源交换和权属交换变得更加透明高效。经过初步验证，该解决方案在技术上具备可行性，能够满足在可监管状态下进行资源交换以及权属交换的功能需求。本研究为日益复杂的分布式资源授权使用问题提供了一种有效的解决途径，不仅在理论上具备重要意义，也在实际应用中具有广泛的应用前景。

参考文献

[1] CLEARWATER S H. Market-based control: a paradigm for distributed resource allocation [M]. World Scientific, 1996.

[2] 翁清. 租赁方式与我国房屋租赁市场发展研究 [J]. 现代商贸工业, 2009, 21 (1): 309-310.

[3] QIAN L, LUO Z, DU Y, et al. Cloud computing: an overview [C]// Proceedings of Cloud Computing: First International Conference, 1. Springer Berlin Heidelberg, 2009: 626-631.

[4] 施巍松, 孙辉, 曹杰, 等. 边缘计算：万物互联时代新型计算模型 [J]. 计算机研究与发展, 2017, 54 (5): 907-924.

[5] CAO K, LIU Y, MENG G, et al. An overview on edge computing research [J]. IEEE Access, 2020, 8: 85714-85728.

[6] VRANKEN H. Sustainability of bitcoin and blockchains [J]. Current Opinion in Environmental Sustainability, 2017, 28: 1-9.

[7] MURATOV F, LEBEDEV A, IUSHKEVICH N, et al. YAC: BFT consensus algorithm for blockchain [J]. arXiv preprint arxiv: 1809. 00554, 2018.

[8] HERLIHY M. Atomic cross-chain swaps [C]//Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, 2018: 245-254.

[9] 刘峰, 张嘉淏, 周俊杰, 等. 基于改进哈希时间锁的区块链跨链资产交互协议 [J]. 计算机科学, 2022, 49 (1): 336-344.

[10] 罗长远, 李伟, 邢洪智, 等. 空间网络中基于身份的分布式密钥管理研究 [J]. 电子与信息学报, 2010, 32 (1): 183-188.

[11] 张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全与隐私保护研究综述 [J]. 通信学报, 2018, 39 (3): 1-21.

[12] 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.

[13] 袁勇, 王飞跃. 区块链技术发展现状与展望 [J]. 自动化

学报，2016，42（4）：481－494.
[14] 邵奇峰，张召，朱燕超，等. 企业级区块链技术综述［J］. 软件学报，2019，30（9）：2571－2592.
[15] YANG W，AGHASIAN E，GARGS，et al. A survey on blockchain-based internet service architecture：requirements，challenges，trends，an future［J］. IEEE Access，2019（7）：75845－75872.
[16] 韩璇，袁勇，王飞跃. 区块链安全问题：研究现状与展望［J］. 自动化学报，2019，45（1）：208－227.
[17] ALI M，VECCHIO M，PINCHEIRAM，et al. Applications of blockchains in the Internet of things：a comprehensive survey［J］. IEEE Communications Surveys & Tutorials，2019（21）：1676－1717.
[18] BUTERIN V. A next-generation smart contract and decentralized application platform［R］. White Paper，2014.

（收稿日期：2024－02－27）

作者简介：

张义（1999－），男，硕士研究生，主要研究方向：区块链、网络优化。

李桐（1992－），通信作者，男，博士研究生，助理研究员，主要研究方向：移动计算、网络孪生、网络优化。E-mail：t. li@ connect. ust. hk。

王钺（1977－），男，博士，副研究员，主要研究方向：智慧城市、数据治理。

（上接第45页）

[4] 于显宁. 点云配准算法在堆叠零件拾取中的应用研究［D］. 长春：长春工业大学，2023.
[5] 侯大伟. 一种基于实例分割和点云配准的六维位姿估计方法［J］. 信息技术与网络安全，2021，40（6）：56－61.
[6] 翟红飞. 基于深度学习的机械臂抓取系统研究［D］. 南昌：南昌大学，2022.
[7] VU T，KIM K，LUU T M，et al. SoftGroup for 3D instance segmentation on point clouds［C］//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition，2022：2708－2717.
[8] 郑伟斌，练国富，张学明，等. 基于主成分分析和特征图匹配的点云配准方法［J］. 智能科学与技术学报，2023，5（4）：543－552.
[9] JIANG L，ZHAO H，SHI S，et al. PointGroup：dual－set point grouping for 3D instance segmentation［C］//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition，2020：4867－4876.
[10] CHEN S，FANG J，ZHANG Q，et al. Hierarchical aggregation for 3D instance segmentation［C］//Proceedings of the IEEE/CVF International Conference on Computer Vision，2021：15467－15476.
[11] ÇIÇEK Ö，ABDULKADIR A，LIENKAMP S S，et al. 3D U－Net：learning dense volumetric segmentation from sparse annotation［J］. arXiv preprint arXiv：1606. 06650，2016.
[12] GUO Y，WANG H，HU Q，et al. Deep learning for 3D point clouds：a survey［J］. IEEE Transactions on Pattern Analysis and Machine Intelligence，2020，43（12）：4338－4364.

（收稿日期：2024－03－11）

作者简介：

周剑（1980－），男，博士研究生，主要研究方向：三维物体识别与检测、三维重建、三维场景理解。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部