

**认证与访问控制结课论文**

**题目：基于区块链实现访问控制**

**专业班级： 信安XXXX班**

**学 号： U2021XXXXX**

**姓 名： MTX。**

**指导教师： 崔永泉**

**报告日期： 2024.1.1**

**网络空间安全学院**

**目 录**

[摘 要 3](#_Toc155390498)

[1 引言 4](#_Toc155390499)

[2 访问控制与大数据 6](#_Toc155390500)

[2.1 大数据相关技术 6](#_Toc155390501)

[2.2 大数据下访问控制的需求 7](#_Toc155390502)

[2.3 传统访问控制的不足 8](#_Toc155390503)

[3 区块链技术 10](#_Toc155390504)

[3.1 区块链架构 10](#_Toc155390505)

[3.2 区块数据结构 12](#_Toc155390506)

[3.3 共识机制 13](#_Toc155390507)

[4 基于区块链的访问控制机制分析 14](#_Toc155390508)

[4.1 基于交易的访问控制机制 14](#_Toc155390509)

[4.2 基于智能合约的访问控制机制 17](#_Toc155390510)

[4.3 基于区块链的访问控制实现机制总结 19](#_Toc155390511)

[5 基于区块链的访问控制技术研究展望 20](#_Toc155390512)

[参考文献 21](#_Toc155390513)

**基于区块链实现访问控制**

# 摘 要: 区块链技术具备去中心化、高度可靠和难以篡改的特性，本文对基于此技术的访问控制进行了深度探讨和分析。借助区块链的无中心化特性和智能合约的自动化执行功能，我们有能力创建一个更加安全且高效的访问控制体系，从而为信息系统的安全管理开辟出新的途径。伴随着区块链科技的持续进步，未来基于区块链的访问管理可能会变成信息安全行业的主流方向。

# 关键词:区块链；访问控制；去中心化；大数据；隐私保护

**Implementation of Access Control Based on Blockchain Technology**

**Abstract:** Blockchain technology possesses the characteristics of decentralization, high reliability, and tamper resistance. This article delves into an in-depth exploration and analysis of access control based on this technology. Leveraging the decentralized nature of blockchain and the automated execution capability of smart contracts, we have the ability to create a more secure and efficient access control system, thereby paving the way for enhanced security management of information systems. With the continuous advancement of blockchain technology, access management based on blockchain may become the mainstream direction in the field of information security.**Keywords:**Blockchain,Access Control,Decentralization,Big Data,Privacy Protection

# 1 引言

随着信息技术的不断发展，数字化社会中对数据的存储、传输和共享需求日益增加。然而，这也伴随着对数据安全性和隐私保护的日益关切。在各行各业，访问控制作为一项关键的安全机制，扮演着保护敏感信息免受未经授权访问的重要角色。

传统的访问控制方法往往集中在中心化的身份验证和授权管理上，然而，这种模式面临着单点故障和容易受到攻击的风险。区块链技术的崛起为解决这一问题提供了新的思路。作为一种分布式账本技术，区块链通过其去中心化、不可篡改的特性，为建立更加安全、透明的访问控制机制提供了可能性。

区块链技术最早是由中本聪（Satoshi Nakamoto）在2008年提出的。中本聪通过发布一篇名为《比特币：一种点对点的电子现金系统》的白皮书，详细描述了区块链的设计和实现。该技术最初的应用是比特币（Bitcoin），一种基于区块链的加密数字货币。

区块链技术具有以下几个主要技术特点：

1）去中心化（Decentralization）：区块链采用分布式的节点网络，不存在中央权威机构，每个节点都有权参与网络的维护和决策，从而消除了单点故障和中央控制。

2）分布式账本（Distributed Ledger）：区块链通过将交易数据以区块的形式存储在每个节点上，形成一个共享的分布式账本。这使得每个节点都有完整的交易记录，增加了数据的透明性和可追溯性。

3）不可篡改性（Immutability）：区块链中的每个区块都包含前一区块的哈希值，形成链式连接。一旦一个区块被添加到链上，就无法修改，确保了交易的不可篡改性，增强了数据的安全性。

4）智能合约（Smart Contracts）：区块链可以支持智能合约，这是一种自动执行合约条款的计算机程序。智能合约的执行依赖于预先定义的规则，可以在没有中介的情况下自动执行，提高了合同执行的效率。

5）共识算法（Consensus Mechanism）：区块链网络通过共识算法来解决节点间的信任问题。常见的共识算法包括工作量证明（PoW）、权益证明（PoS）等，确保节点对账本的一致性，防止恶意篡改。

6）匿名性和隐私保护（Anonymity and Privacy）：区块链网络中的参与者可以使用加密技术保护其身份，提高了交易的匿名性。同时，一些区块链平台还提供隐私保护技术，确保敏感信息不被公开。

7）开放性和互操作性（Openness and Interoperability）：区块链技术是开放的，任何人都可以参与。此外，一些区块链标准的制定和采用促进了不同区块链系统之间的互操作性，使它们能够更好地协同工作。

这些技术特点使区块链成为一种安全、透明、可信赖的分布式账本技术，广泛应用于金融、物联网、供应链管理、医疗保健等领域。 访问控制技术的起源可以追溯到早期的计算机系统，其最初的目的是确保只有授权用户可以访问系统资源。随着信息技术的发展，访问控制逐渐演化并融入各种应用和网络环境中。传统的访问控制方法包括基于身份验证和授权的机制，但随着信息系统的复杂性和互联性的增加，传统方法面临一些挑战，如单点故障和中心化管理。其技术特点如下：

1）身份验证（Authentication）：身份验证是访问控制的第一步，用于确认用户或系统实体的身份。常见的身份验证方式包括用户名密码、生物特征识别（如指纹、虹膜扫描）、智能卡等。成功的身份验证是访问控制的前提。

2）授权（Authorization）：授权确定经过身份验证的用户或系统实体能够访问哪些资源和执行哪些操作。授权通常基于用户的角色、权限或其他属性进行定义。例如，系统管理员可能具有对系统所有资源的完全控制权限，而普通用户可能仅能访问特定文件夹。访问策略（Access Policies）：访问策略是定义在系统或网络中的规则和规定，用于指导访问控制的实施。访问策略可以基于最小权限原则，即用户或实体只被授予完成任务所需的最小权限。

3）强制访问控制（Mandatory Access Control，MAC）：MAC 是一种严格的访问控制机制，通过强制规则、标签或等级来控制用户对系统资源的访问。在这种模型下，用户不能自行更改资源的访问权限，权限由系统或安全管理员预先定义。

4）自主访问控制（Discretionary Access Control，DAC）：DAC 是一种灵活的访问控制模型，它允许资源的所有者决定谁能够访问资源以及如何访问。资源的所有者具有授予权限的自主权。角色基础访问控制（Role-Based Access Control，RBAC）：RBAC 是基于用户角色的访问控制模型，用户被分配到不同的角色，每个角色有一组特定的权限。这种模型简化了权限管理，提高了系统的可维护性。

5）审计和监控（Auditing and Monitoring）：访问控制系统通常包括审计和监控功能，用于记录用户的活动和访问尝试。审计日志可以用于事后审查、故障排除和安全事件响应。

6）单点登录（Single Sign-On，SSO）：SSO 允许用户通过一次身份验证访问多个相关系统。这提高了用户体验，并减少了需要记住多个凭证的负担。

访问控制是信息安全的基石之一，有效的访问控制机制可以帮助组织防范潜在的威胁，确保系统和数据的安全性。在现代计算环境中，访问控制也不断演化和创新，以适应日益复杂和多样化的安全挑战。

本论文旨在探讨基于区块链技术的访问控制方法。通过将区块链的去中心化和分布式特性与访问控制需求相结合，我们可以构建更加强大和鲁棒的访问控制系统。通过区块链的智能合约机制，我们能够实现更为灵活和自动化的权限管理，减少中间环节的风险。

在接下来的章节中，我们将深入研究区块链技术在访问控制领域的应用，分析其优势和挑战，并提出一种基于区块链的访问控制框架，以应对数字化社会中不断增长的安全挑战。这一框架有望为信息安全领域带来新的思路和解决方案，推动访问控制领域的创新和发展。

# 2 访问控制与大数据

## 2.1 大数据相关技术

大数据的兴起主要源于移动互联网、物联网和云计算等热点技术的发展。大数据、物联网和云计算之间存在紧密的关系。物联网中的设备生成大量的数据，这些数据被传输到云平台进行存储和处理。云计算提供了强大的计算和存储能力，以支持大数据的处理和分析。大数据分析可以从物联网数据中提取有价值的信息和洞察力，帮助用户做出更明智的决策和改进业务。同时，物联网设备的连接和通信也可以通过云计算进行管理和控制。大数据、物联网和云计算三者相互依存、相互促进，共同构建了一个以数据为核心的智能化技术体系，为各行各业带来了巨大的创新和发展机遇，如图1所示。

物联网概念于1999年首次提出，是指将各种物理设备（如传感器、智能设备、机器等）通过互联网连接起来，实现设备之间的通信和数据交换。随着智能摄像头、可穿戴设备、智能汽车等设备的普及，物联网设备的数据保护问题受到了关注。在物联网的大环境中，数据的访问控制主要面对如下的三个问题：

1）分布式部署：物联网设备分布广泛，难以完全防范针对性的攻击，因此访问控制机制需要具备一定的容错性。

2）分布式存储：数据存储呈现分布式特征，访问控制机制需要协作统一的能力。

3）设备安全：大量信息采集设备存在，如摄像头、传感器等，对这些设备的数据进行安全防护也是一个需要研究的问题。

云计算依托于互联网，是一种通过互联网提供计算资源和服务的模式。它基于虚拟化技术和分布式计算，将计算资源（如计算能力、存储空间和应用程序）以服务的形式提供给用户。云计算提供了可伸缩性、灵活性和经济性等优势，用户可以根据需要按需获取和使用计算资源，而无需购买和维护自己的物理硬件和软件。云计算还提供了丰富的数据存储、处理和分析工具，以支持大数据和物联网应用。在云计算环境中，数据的访问控制面临以下挑战：

1）用户数据管控困难：在云计算模式下，用户将数据存储在云服务提供商的基础设施上，这可能导致用户对自己的数据失去直接的所有权和完全的控制权。用户需要明确了解云服务提供商的数据使用政策和条款，以确保他们对自己的数据仍然拥有一定程度的控制权。

2）多样性的数据类型：用户来源广泛且数据类型多样，如何在满足用户数据分享需求的前提下，制定细粒度的访问控制策略，防止非必要信息泄露是一个待解决的问题。

3）快速数据更新：云计算环境中数据资源更新速度快，因此设计实现动态的访问控制机制变得尤为重要。

需要注意的是，为了保护大数据和云计算中的数据安全，不断进行研究和改进访问控制技术是至关重要的。这样可以确保在允许合法访问的同时，防止未经授权的数据泄露和滥用。

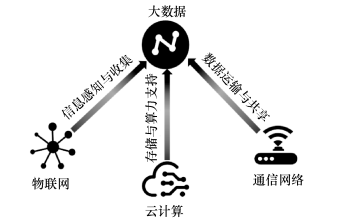


图1 大数据相关技术关系示意图

在信息安全领域，访问控制和身份认证是保护系统安全的两大关键要素。访问控制旨在确保只有经过授权的用户或系统实体能够访问敏感资源，从而防止未经授权的访问。这一机制涵盖了多种类型，如基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）、强制访问控制（MAC）、自主访问控制（DAC）等，每种类型都在不同场景中发挥着关键作用。

与此同时，身份认证则聚焦于确认用户或系统实体所声称的身份是否合法。在这个过程中，采用多种认证方式，如用户名和密码认证、多因素身份认证、生物特征认证等。这有助于确保用户确实是其声称的身份，提高了整体系统的安全性。

这两者的结合为建立强大的安全框架提供了坚实基础。通过在身份认证阶段验证用户身份，系统随后可以通过访问控制机制根据用户的权限级别对其资源访问进行精细化控制。这种综合应用不仅有助于减少潜在的安全威胁，还提升了整体系统的鲁棒性和可维护性。因此，访问控制和身份认证的协同作用在确保信息系统安全性方面起到了不可替代的作用。

## 2.2 大数据下访问控制的需求

当涉及到大数据环境下的访问控制时，一些关键的需求变得尤为重要。大数据环境下的数据集通常是大规模、多样化并且快速增长的，其中包含了各种类型的敏感商业信息、个人隐私数据以及关键的业务数据。因此，确保对这些数据的访问进行有效的控制和保护就显得尤为重要。

首先，数据保密性是一个关键需求。大数据中包含了商业机密信息、知识产权、个人身份信息等敏感数据。因此，访问控制机制需要能够限制只有经过授权的用户或角色才能访问敏感数据。这可能涉及加密技术、身份验证和授权机制的应用。通过加密数据可以确保即使数据被盗或泄露，也无法被未经授权的人员访问和解读。

其次，数据完整性也是一个重要的需求。在大数据环境中，确保数据的完整性是至关重要的。数据完整性涉及防止数据的篡改、损坏或未经授权的修改。访问控制机制需要能够验证数据的完整性，并提供机制来检测和防止任何未经授权的修改。例如，使用数字签名技术可以确保数据在传输和存储过程中不被篡改，并能够验证数据的完整性。

另一个重要的需求是数据的可用性。大数据的价值在于能够以高效和可靠的方式访问和查询数据。因此，访问控制机制需要确保数据的可用性，即授权用户能够在需要时快速、高效地访问数据。这可能涉及到灵活的权限管理和高性能的数据访问机制。访问控制机制需要考虑到数据集的规模、数据请求的并发性以及数据访问的延迟等因素，以确保数据的及时可用性。

角色和权限管理也是大数据环境下访问控制的重要需求之一。在大数据环境中通常存在多个用户、多个角色和复杂的组织结构。因此，访问控制机制需要能够支持灵活的角色和权限管理。用户可以根据其角色和职责来访问不同的数据集和功能。这种细粒度的访问控制可以确保数据只被授权人员访问，并防止未经授权的数据访问和操作。

实时监控和审计是大数据环境下另一个重要的访问控制需求。访问控制机制需要能够记录和跟踪用户对数据的访问和操作，包括谁访问了哪些数据、何时访问的、访问的目的等信息。通过实时监控和审计，可以及时发现和应对任何异常访问行为或安全事件。

此外，跨组织和跨平台的访问控制需求也需要考虑。在大数据环境中，涉及多个组织和参与方的情况较为普遍。访问控制机制需要能够支持跨组织和跨平台的访问控制。这意味着不同组织之间可以分享和访问特定的数据，同时保持数据的安全和隐私。通过建立信任框架和合作机制，可以实现安全跨组织数据共享和访问控制。

最后，弹性和可扩展性也是大数据环境下访问控制的重要需求。大数据环境通常具有高度的弹性和可扩展性要求。访问控制机制需要能够适应不断变化的数据规模和增长，以及应对高并发的数据访问需求。这可能涉及到水平扩展的访问控制解决方案，以确保在大规模数据处理和访问的情况下能够提供高性能和可靠的访问控制服务。

综上所述，大数据环境下的访问控制需求包括数据保密性、数据完整性、数据可用性、角色和权限管理、实时监控和审计、跨组织和跨平台的访问控制，以及弹性和可扩展性。通过满足这些需求，可以确保大数据环境中的数据安全和隐私，并提供高效、可靠的数据访问和查询服务。

## 2.3 传统访问控制的不足

传统访问控制方法在应对现代复杂的信息系统和网络环境中的安全挑战方面存在着一些不足之处。这些不足主要涉及到访问控制的刚性、缺乏上下文感知、无法处理动态权限管理、缺乏细粒度控制、以及难以应对内部威胁等方面。

首先，传统访问控制方法往往是基于静态的权限规则和策略。这种刚性的访问控制机制无法适应现代复杂的信息系统和网络环境中的动态变化。例如，当用户的角色或职责发生变化时，传统访问控制方法需要手动调整权限配置，导致管理和维护的工作量加大，并且容易出现错误和遗漏。此外，对于临时访问权限的授权和撤销也存在困难，无法灵活地应对临时性的访问需求。

其次，传统访问控制方法缺乏上下文感知能力。它们通常只依赖于用户的身份信息或角色来做访问决策，而忽视了其他重要的上下文因素，如用户的位置、时间、设备状态、行为模式等。这种缺乏上下文感知的访问控制机制容易受到伪冒身份、恶意行为和内部威胁的攻击。例如，如果一个合法用户的账号被黑客盗用，传统访问控制方法很难检测到异常行为，因为黑客使用了合法用户的身份信息。

第三，传统访问控制方法无法有效处理动态权限管理。在现实世界中，用户的权限需求通常是动态变化的。传统访问控制方法往往只能在静态的权限配置基础上进行访问控制，无法及时响应用户权限需求的变化。例如，当一个员工从一个部门调动到另一个部门时，他的访问权限需要相应地进行调整。然而，传统方法往往需要手动的、耗时的操作来更新权限，难以满足快速变化的权限管理需求。

第四，传统访问控制方法往往缺乏细粒度的控制能力。在许多情况下，用户可能只需要访问某个数据集中的一部分或者执行某个操作的一部分，而不是全部。然而，传统的访问控制方法通常只能基于整个数据集或整个操作来进行权限控制，缺乏细粒度的控制能力。这可能导致用户获得了不必要的权限，增加了数据泄露和滥用的风险。

最后，传统访问控制方法难以应对内部威胁。内部威胁是指来自组织内部的恶意行为或滥用访问权限的威胁。传统访问控制方法通常将重点放在外部威胁的防御上，而对于内部威胁的检测和防范相对较弱。例如，一个有恶意意图的内部员工可能利用自己的合法访问权限窃取敏感数据或者篡改数据，而传统访问控制方法往往难以识别和防止这样的行为。

针对这些传统访问控制方法的不足，现代的访问控制技术提出了一些解决方案。例如，基于上下文感知的访问控制技术可以综合考虑用户的身份、位置、时间、设备状态等上下文因素，从而更准确地做出访问决策。这些技术可以通过引入智能算法和机器学习模型来分析和识别异常行为，以提高系统对内部威胁的检测和防范能力。另一个解决方案是引入动态权限管理机制。这些机制可以根据用户的实际权限需求和上下文情况，动态地调整和分配权限。例如，基于角色的访问控制可以通过将权限与用户的角色解耦，实现更灵活的权限管理。另一种方法是使用属性基础访问控制（Attribute-Based Access Control，ABAC），它允许根据用户的属性和策略规则来动态决定访问权限。

细粒度访问控制技术也得到了广泛的研究和应用。这些技术可以将权限控制到更具体的数据和操作级别，从而实现更精细的访问控制。例如，基于标签的访问控制（Label-Based Access Control，LBAC）可以为数据集中的每个对象分配标签，并根据标签来控制用户的访问权限。另一种方法是使用策略语言和规则引擎来定义和执行细粒度访问控制策略。此外，新兴的访问控制技术还包括基于身份管理的访问控制（Identity-Based Access Control，IBAC）、基于属性的访问控制（Attribute-Based Access Control，ABAC）和基于行为分析的访问控制（Behavior-Based Access Control，BBAC）等。这些技术通过整合不同的访问控制维度和引入更高级的策略和机制，为信息系统提供了更灵活、更智能和更安全的访问控制能力。

总结而言，传统访问控制方法在应对现代复杂的信息系统和网络环境中的安全挑战方面存在一些不足之处。这些不足主要涉及到访问控制的刚性、缺乏上下文感知、无法处理动态权限管理、缺乏细粒度控制以及难以应对内部威胁等方面。为了解决这些问题，现代的访问控制技术提出了一些解决方案，包括基于上下文感知、动态权限管理、细粒度控制和智能分析等技术。这些新兴技术为信息系统提供了更灵活、更智能和更安全的访问控制能力，有助于应对日益复杂的安全挑战。

# 3 区块链技术

区块链是一种分布式账本技术，它以去中心化、安全性和透明性为特点。通过将交易记录按照时间顺序链接成一个不可篡改的区块链，区块链技术为数据交换和记录提供了一种可信的方式。区块链最初是作为比特币的底层技术而引入的，但现在已经被广泛应用于金融、供应链管理、物联网、医疗保健等领域。以下是对区块链技术的起源、技术特点和应用场景的详细介绍。首先，区块链的起源可以追溯到2008年，当时一个名为中本聪（Satoshi Nakamoto）的匿名个体发表了一篇题为《比特币：一种点对点的电子现金系统》的论文，这标志着区块链技术的诞生。中本聪提出了一种去中心化的数字货币系统，其中的核心机制就是区块链。区块链通过将交易记录按照时间顺序链接在一起，并通过共识算法使网络上的节点达成一致，从而实现了去中心化的信任机制。

区块链的技术特点之一是去中心化。传统的中心化系统依赖于中央机构来验证和记录交易，而区块链技术通过将数据和交易记录存储在网络中的各个节点上，消除了中央机构的需求。每个节点都可以参与到区块链的维护和验证过程中，从而实现了去中心化的数据管理和交易确认。其次是安全性。区块链使用密码学技术来保护交易数据的安全性。每个区块都包含有关前一个区块的哈希值，这样一旦区块链中的一个区块被篡改，整个区块链的哈希值都会发生变化，从而易于检测到篡改行为。此外，区块链的共识算法确保了网络上的节点达成一致，防止了恶意节点的攻击和数据篡改。最后是透明性。区块链中的交易记录是公开可见的，任何人都可以查看和验证交易数据。这种透明性有助于建立信任，特别适用于一些需要公开透明的领域，如供应链管理和公共部门的管理。

区块链技术具有广泛的应用场景。首先，金融领域是区块链技术应用最为广泛的领域之一。区块链可以用于实现去中心化的数字货币系统，改变传统金融机构的支付和结算方式。此外，区块链还可以应用于股票交易、借贷、风险管理等金融业务，提高交易的效率和安全性。其次，供应链管理也是区块链技术的重要应用领域之一。通过将供应链上的交易和物流信息记录在区块链上，可以实现供应链的透明化和可追溯性，提高供应链的效率和管理水平。区块链技术可以帮助解决供应链中的信息不对称和欺诈问题，从而提高整个供应链的可信度。物联网是另一个适合应用区块链技术的领域。物联网涉及大量的设备和传感器，这些设备之间需要进行安全的通信和数据交换。区块链可以提供一种安全可靠的机制，确保物联网设备之间的通信和数据交换的可信度。通过将物联网设备生成的数据记录在区块链上，可以实现数据的不可篡改和可追溯，从而增加物联网系统的安全性和可靠性。

总结而言，区块链技术是一种去中心化、安全、透明的分布式账本技术。它的起源可以追溯到比特币的诞生，而现在已经被广泛应用于金融、供应链管理、物联网、医疗保健等领域。区块链的技术特点包括去中心化、安全性和透明性，这些特点使得区块链成为一种可信的数据交换和记录方式。未来，随着区块链技术的不断发展和完善，相信它将在更多的领域发挥重要作用。

## 3.1 区块链架构

自从2008年比特币诞生之后，区块链技术就进入了人们的视野之中，不断迭代更新，特别是随着以太坊、EOS等项目的提出，人们看到了它在多方面的经济价值和巨大的未来潜能。在Swan发表的论文Blockchain：Blueprint for a new economy中将区块链技术的应用分为3个层次 [1]，如图2所示。

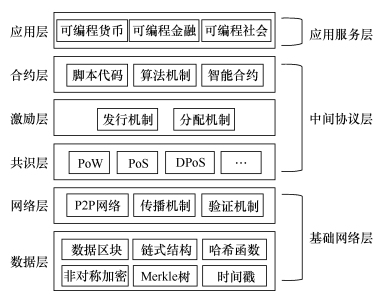


图2 区块链的架构

应用层：应用层是区块链系统的最上层，它包括了基于区块链技术构建的各种应用和服务。这些应用可以是数字货币、智能合约、供应链管理、电子投票等。应用层的设计和功能由具体的区块链应用决定，它们使用底层的协议层提供的功能来实现特定的业务逻辑和交互。

协议层：协议层是区块链系统的中间层，它定义了区块链网络的规则和协议。协议层包括共识算法、网络协议、数据验证规则等。共识算法用于确保网络中的节点达成一致，保证区块链的安全性和一致性。常见的共识算法包括工作量证明（Proof of Work，PoW）、权益证明（Proof of Stake，PoS）等。网络协议定义了节点之间的通信规则，确保区块链网络的稳定和可靠。数据验证规则用于验证交易和区块的有效性，防止恶意行为和数据篡改。

数据层：数据层是区块链系统的最底层，它包括了区块链的数据结构和存储方式。区块链使用链式结构来组织交易记录，每个区块包含了一批交易和指向前一个区块的哈希值。这种链式结构使得区块链的数据是按照时间顺序链接在一起的，并且一旦区块链中的一个区块被篡改，整个区块链的哈希值都会发生变化，从而易于检测到篡改行为。数据层还包括了区块链的存储方式，可以是分布式存储或者共享存储，确保数据的安全性和可靠性。

这是一个基本的区块链架构，不同的区块链系统可能会有一些差异和扩展。例如，有些区块链系统可能会在架构中加入智能合约层，用于执行和管理可编程的自动化合约。另外，随着区块链技术的发展，也出现了一些区块链的改进和扩展，如侧链、闪电网络等，这些技术可以进一步提高区块链的性能和扩展性。

总之，区块链的架构由应用层、协议层和数据层组成。应用层提供具体的区块链应用和服务，协议层定义了区块链网络的规则和协议，数据层则负责区块链的数据结构和存储。这种三层架构使得区块链系统能够实现分布式、去中心化的交易记录和信任机制。

## 3.2 区块数据结构

区块链的区块结构确实具有数据只增不减、难以篡改和可溯源的特性，如图3所示。

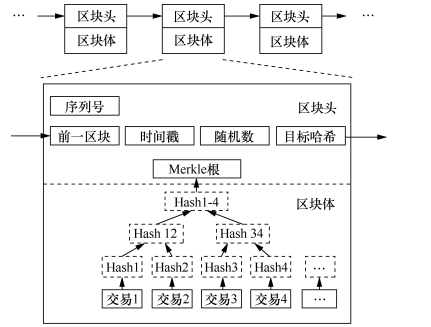


图3 区块数据结构

下面对图中所示的区块结构进行解释：

区块体（Block Body）：区块体存储了一组交易数据，通常使用Merkle树的形式来组织这些交易数据。Merkle树是一种二叉树结构，通过对交易数据进行哈希运算，构建一个树形结构，其中每个叶子节点是一个交易的哈希值，而非叶子节点是其子节点的哈希值。通过Merkle树，可以实现对交易数据的高效验证和快速归纳，同时也可以防止数据的篡改，因为任何一个交易的更改都会导致其哈希值的改变，从而影响到根节点的哈希值。

区块头（Block Header）：区块头是区块链中每个区块的元数据和摘要信息。它包含了版本号、前一个区块的哈希、梅克尔根、时间戳、难度目标和随机数等字段。这些字段经过哈希运算后生成区块头哈希，用于验证区块的有效性和链接区块链中的不同区块。区块头在区块链中起着重要的作用，它帮助验证区块的顺序和完整性，调整网络的运行状态，并实现安全和稳定的区块生成。随机数（Nonce）是一个随机值，用于参与哈希计算的过程，以满足共识算法的要求。Merkle根（Merkle Root）是指Merkle树的根节点的哈希值，它是区块体中交易数据的摘要，用于验证区块中的交易数据的完整性。

区块链接（Block Linkage）：每个区块通过哈希算法，结合随机数和Merkle根等信息，计算出其区块头的哈希值，并将其作为下一个区块的目标哈希。这样，每个区块的区块头哈希值成为了链式结构中下一个区块的指针，将前一个区块和后一个区块连接在一起，形成了区块链。通过这种链接机制，保证了区块链的连续性和完整性，使得区块链中的数据无法随意篡改，同时也实现了去中心化的记账权竞争机制。

总结而言，区块链的区块结构利用Merkle树、区块头和区块链接等关键技术，实现了数据的不可篡改性、可溯源性和链式结构，确保了交易数据的安全性和可信性。

## 3.3 共识机制

共识机制（Consensus Mechanism）是区块链系统中用于解决分布式环境下参与者之间达成一致的算法和规则。它是保证区块链网络中的节点就交易的有效性、顺序和状态达成共识的关键机制。以下是一些常见的共识机制：

工作量证明（Proof of Work，PoW）：PoW是比特币所采用的共识机制，也是最早应用于区块链的共识算法之一。在PoW中，节点需要通过解决一个复杂的数学难题，即挖矿问题，来竞争记账权。解决问题的过程需要大量的计算能力和电力消耗，而且难题的难度会根据整个网络的算力进行调整。第一个成功解决问题的节点将获得记账权，并获得一定数量的奖励。PoW机制的优点是安全性高，但它也需要大量的计算资源和能源消耗。

权益证明（Proof of Stake，PoS）：PoS是另一种常见的共识机制，它根据参与者持有的加密货币数量来决定记账权的分配。在PoS中，持有更多加密货币的节点有更大的概率被选为记账节点。通过抵押一定数量的加密货币作为"权益"，节点可以参与记账的竞争，并有机会获得记账权和相应的奖励。PoS机制减少了对计算资源的需求，降低了能源消耗，但也引发了一些潜在的问题，如富者愈富的现象。

权益证明与工作量证明混合机制（Proof of Stake and Proof of Work Hybrid，PoS/PoW Hybrid）：一些区块链系统采用PoS和PoW的混合机制，结合两种方式的优点。例如，以太坊的Casper协议就是采用PoS/PoW混合机制，通过PoS来选择验证者，而PoW则用于区块的生成。这种混合机制旨在提高安全性和可扩展性，减少能源消耗。

权威证明（Proof of Authority，PoA）：PoA是一种基于信任节点的共识机制，其中一组被信任的节点拥有记账权。这些节点通常是通过身份验证和授权过程来确定的，因此具有较高的可信度。PoA机制适用于私有链或联盟链等特定场景，其中对节点的身份和可信度要求较高。

这些共识机制各有优缺点，适用于不同的区块链应用和场景，选择合适的共识机制是根据具体需求和目标来决定的。

# 4 基于区块链的访问控制机制分析

基于区块链的访问控制技术总体上分为两部分：一是基于交易的访问控制机制，二为

基于智能合约的访问控制机制。

基于交易的访问控制机制利用区块链的可信存储特性，基于交易的访问控制机制利用区块链的可信存储特性，提供了一种安全而可靠的数据访问控制解决方案。区块链是一种分布式、去中心化的数据库，其中的数据以交易的形式被记录和存储。通过将访问控制规则和权限信息作为交易记录在区块链上，可以实现对数据的细粒度控制和完全可追溯的访问历史。在基于交易的访问控制机制中，每个数据访问请求都需要通过生成一笔交易来进行授权和验证。数据所有者可以创建授权交易，指定特定的访问规则和权限，并将其记录在区块链上。当用户发起数据访问请求时，系统会验证用户身份，并根据区块链中的交易记录检查用户是否有权限进行访问。这种机制确保了数据的安全性和可信度，因为区块链的不可篡改性和分布式共识机制使得任何未经授权的访问尝试都会被拒绝。

基于智能合约的访问控制机制利用区块链的可信计算特性。基于智能合约的访问控制机制利用区块链的可信计算特性，提供了一种安全、可靠的数据访问控制解决方案。区块链是一种分布式、去中心化的技术，而智能合约则是在区块链上执行的自动化合约代码。通过将访问控制规则和权限信息编写为智能合约，可以实现对数据的细粒度控制和可验证的访问逻辑。在基于智能合约的访问控制机制中，访问请求必须通过智能合约进行验证和授权。智能合约包含了访问控制规则和权限设置，以及对请求方身份的验证逻辑。当用户发起数据访问请求时，该请求会被提交到区块链上的智能合约进行验证。智能合约会检查用户身份、访问权限和其他相关条件，并根据预先设定的规则判断是否授权该访问请求。这种机制确保了访问的安全性和可靠性，因为智能合约的执行是透明的、不可篡改的，并且在整个网络中具有共识。

## 4.1 基于交易的访问控制机制

基于交易的访问控制机制最早在区块链研究中被提出，标志着访问控制技术与区块链技术的结合的开端。Zyskind等人[2]针对移动应用中的数据访问控制需求，提出了一种基于联合身份发布的访问控制策略。该策略的原理如图4所示，利用区块链的特性，规定最新发布的联合身份交易为有效交易，通过查找最近的权限交易（Taccess）来实现权限的授予、更改和撤销。同时，通过数据交易（Tdata）提交服务商的访问请求，并将访问操作记录在区块链上，以实现可溯源的访问操作。

这种机制巧妙地引入了联合身份的概念，使得用户可以为不同的服务商实现不同类型数据的访问控制策略。同时，它使用了访问控制列表（ACL，access control list）的策略描述方式，适用于低复杂度的访问控制策略和个人数据保护需求较小的情况。这种方法为用户提供了更多灵活性和可定制性。

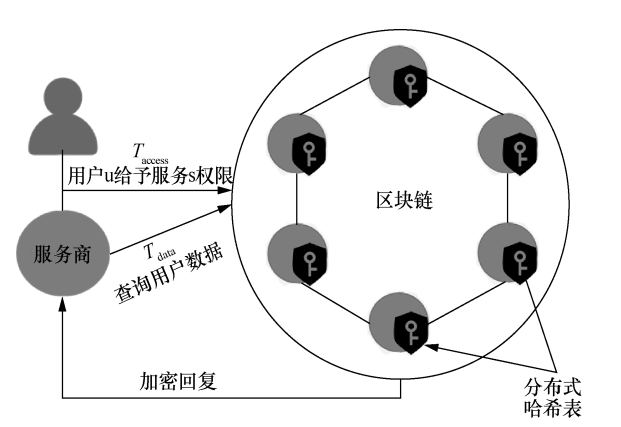


图4 Zyskind机制原理

文献[3]的提出，他们引入了一种基于交易的访问控制策略和权限管理机制。该机制通过链上的交易完成访问控制策略和权限的创建、更新和撤销。作者定义了两种类型的交易：策略创建交易（PCT，policy creation transaction）用于策略的创建，权限转移交易（RTT，right transfer transaction）用于权限的更替。为了实现策略的更新和撤销，作者利用了区块链的代币机制，规定在进行更新和删除的PCT交易时，必须花费该策略先前的交易输出。每次交易的输入包括先前的策略信息和一定的交易费用（比特币），输出则是新的策略信息和交易后剩余的费用。

此外，作者还规定了数据操作权限的拥有者（RT，right holder）在进行RTT交易时，可以对原有的访问控制策略进行更严格的限制。只有在交易方满足特定条件时，才会获得操作权限并完成交易。文献[3] 提出的系统模型Maesa机制原理如图5所示，其中区块链作为存储组件，在与策略管理点（PAP）进行交互后，为授权系统提供访问控制策略的全周期信息。然后，策略执行点根据授权系统的处理结果来控制用户与数据资源的交互。

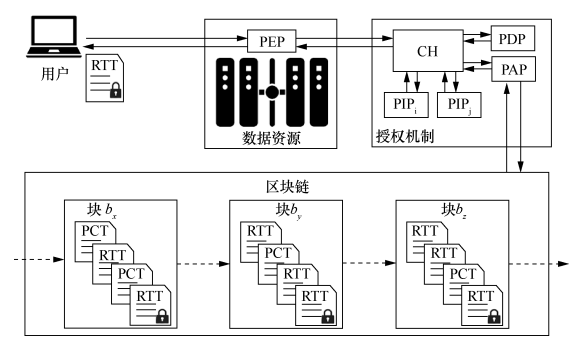
通过利用区块链上的交易机制，该系统实现了基于属性的访问控制（ABAC）模型下的安全可信、修改灵活、全周期溯源的访问控制机制。即使在大规模数据的情况下，该机制也能满足对细粒度访问控制的需求。

图5 Maesa机制原理

基于交易的访问控制机制是一种利用区块链交易记录来管理和控制访问权限的方法。在这种机制下，访问主体通过发送特定的交易到区块链网络，来请求对某个客体的访问权限。这些交易会被记录在区块链的交易历史中，并可以被所有参与者验证和审计。

这种机制的关键在于交易的内容和属性。通过在交易中包含访问请求的相关信息，如访问主体的身份标识、客体的标识以及访问权限的要求，系统可以根据交易的内容来判断是否授予访问权限。当交易被区块链网络确认并添加到区块链上时，访问主体将获得相应的访问权限。

基于交易的访问控制机制具有一些优势。首先，由于交易记录被保存在区块链上，具备不可篡改和可追溯的特性，使得访问控制过程具备高度的透明性和可验证性。任何人都可以审计和验证交易历史，确保访问权限的合法性和正确性。

其次，基于交易的访问控制机制还具备灵活性和可扩展性。通过定义不同类型的交易和交易属性，可以满足各种复杂的访问控制需求。例如，可以定义不同的交易类型来表示不同的访问权限级别或者访问控制策略。交易的属性也可以根据具体需求进行扩展和定制，以支持更多的访问控制规则和条件。

此外，基于交易的访问控制机制还可以与其他智能合约和应用程序进行集成，实现更加复杂的访问控制逻辑和功能。通过与智能合约的交互，可以实现更加灵活和智能化的访问控制策略，例如基于时间、地点、属性等的动态访问控制。

综上所述，基于交易的访问控制机制利用区块链交易记录来管理和控制访问权限。它具备透明性、可验证性、灵活性和可扩展性等优势，为访问控制领域带来了新的解决方案，并在各种应用场景中展现了广阔的前景。通过合理设计和使用交易的属性和交易类型，可以实现高效、安全和可信的访问控制管理。

## 4.2 基于智能合约的访问控制机制

随着以太坊等具备图灵完备链上脚本的区块链平台的出现，智能合约的应用逐渐成为现实。作为区块链2.0架构的核心组件，智能合约将区块链应用从仅限于虚拟货币扩展到更广泛的交易平台。在访问控制领域，智能合约利用区块链提供的分布式信任基础设施，将数据交互视为主体之间的"交易"。通过自定义的脚本语言，实现了可信、细粒度、无人为干预的访问控制机制。

文献[4] 提出了基于智能合约的角色访问控制框架（RBAC-SC）。该框架利用以太坊平台的智能合约技术，提出了一种跨组织的质询-响应身份验证协议，解决了跨组织场景下的角色利用问题，为基于角色的访问控制提供了安全高效的角色管理和验证机制。作者的思路是利用区块链的可信、公开和透明特性，通过以太坊上的账户地址或系统分配的公钥来表示用户，并允许组织发布带有签名的角色管理合约。其他组织的用户可以通过该组织发布的智能合约查询接口，查询该组织内访问控制系统中用户的角色身份，从而实现跨组织的角色验证。Zhang等人[5] 提出了基于智能合约的框架，通过多个访问控制合约、一个法官合约和一个注册合约实现了分布式可信的访问控制。这个框架的具体实现如图6所示。

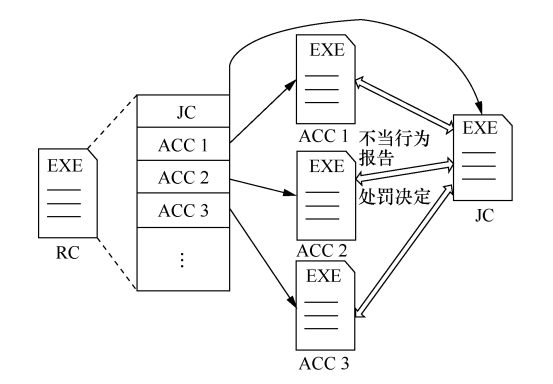


图6 Zhang Y机制框架结构

该框架包括多个访问控制合约（ACC），每个合约实现了访问控制策略中不同主体之间的具体访问控制方法，并同时维护着策略实施列表和不当行为惩罚列表。法官合约（JC）用于接收不当行为报告并确定相应的惩罚。注册合约（RC）用于管理法官合约和访问控制合约，并提供它们的摘要信息。通过将访问控制策略拆分为多个访问控制合约，可以更细粒度地实现主体之间的交互行为。

在医疗数据保护领域，Azaria等人提出了MedRec框架，针对患者数据碎片化、交流渠道有限、共享效率低和隐私保护机制不完善等问题。该框架利用智能合约使患者能够管理自己的数据访问权限，并通过区块链实现跨组织的访问控制。作者设计了注册合约来管理患者信息，并将患者账户与其摘要合约绑定。摘要合约用于关联患者的数据权限和状态。医患关系合约负责患者数据的查询和访问权限管理。通过MedRec机制，患者的数据在数据库中附有相应的操作权限信息，并且可以通过患者的摘要合约地址查询到相关医患关系合约的状态。这样，患者的医疗数据严格受控制在患者手中，违法操作因权限不足而被拒绝。研究目的的医疗数据访问者可以通过查询注册合约上公开的患者账户地址向相应的患者提出申请，在获得患者同意后才能访问数据。

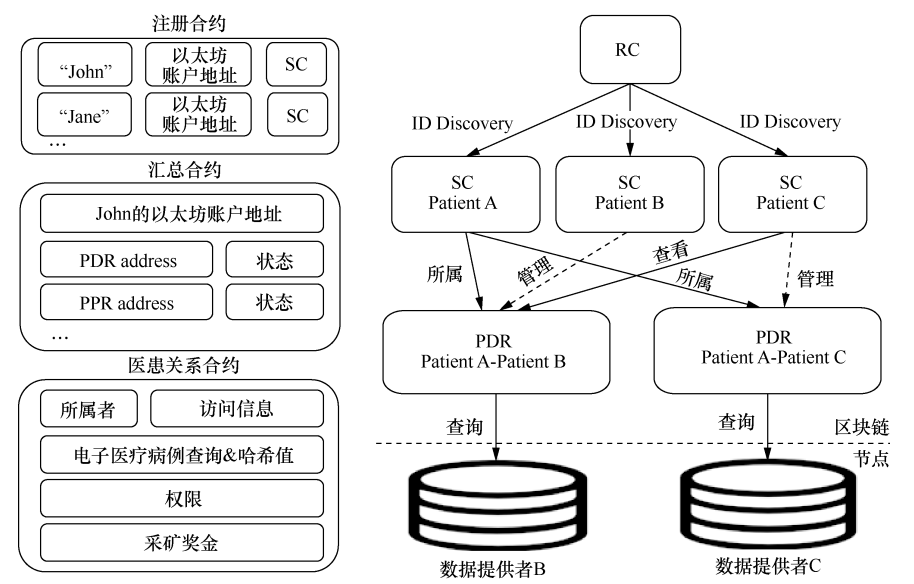
需要注意的是，由于区块链的匿名性，尽管链上数据是公开的，但是患者的身份是通过以太坊账户表示的。此外，患者的隐私医疗数据存储在链下，只有操作权限是公开可查的。这样一来，在保护患者隐私的前提下，数据的共享率得以提高。

图7 MedRec 框架结构

基于智能合约的访问控制机制是一种应用区块链技术的创新方法。该机制的基本原理是将访问控制策略转化为智能合约代码，并上传到区块链网络中。在这种机制下，当访问主体满足智能合约预设的条件时，系统会自动赋予其对客体的访问权限，并将此操作以交易事务的形式存储在区块链上。这种机制的优势之一是借助区块链的可信计算特性，使得访问控制过程更加透明、可验证和不可篡改。智能合约作为可编程的自动执行代码，可以确保访问控制策略的准确执行，消除了传统访问控制机制中由于人为因素导致的错误和滥用的可能性。

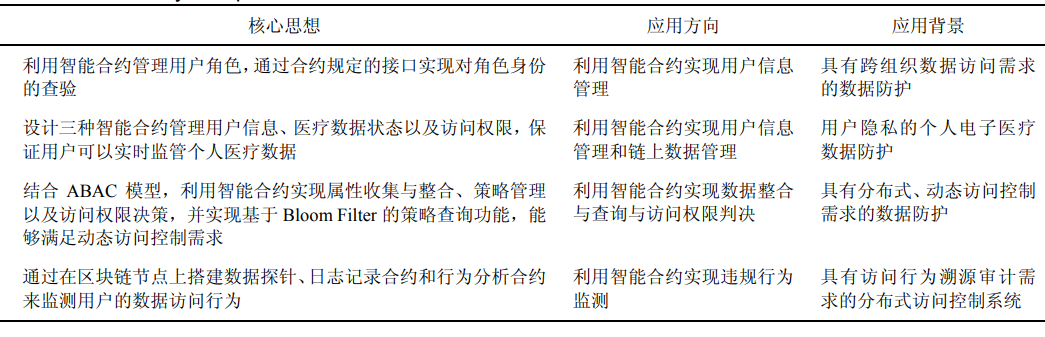
此外，基于智能合约的访问控制机制还具备灵活性和可扩展性。智能合约可以根据实际需求进行编写和部署，从而满足各种复杂的访问控制需求。例如，可以定义灵活的权限授予条件和访问规则，实现细粒度的权限管理。同时，智能合约的可编程性还使得访问控制机制能够与其他智能合约和应用程序进行集成，实现更加复杂的访问控制逻辑和功能。

基于智能合约的访问控制机制还具备监督和管理的能力。通过智能合约，可以对访问主体和客体之间的所有数据交互过程进行监督和管理，包括属性状态、权限授予溯源信息以及策略更新历史记录等。这种综合性的数据监督和管理能力可以增强访问控制系统的安全性和可信度，更好地满足复杂的访问控制需求。

综上所述，基于智能合约的访问控制机制借助区块链技术的可信计算特性，通过智能合约代码实现对访问权限的自动化管理和控制。它具备透明性、可验证性、灵活性和监督管理能力等优势，为访问控制领域带来了新的解决方案，并在各种应用场景中展现了广阔的前景。

## 4.3 基于区块链的访问控制实现机制总结

表1 基于智能合约的访问控制机制汇总



基于交易的访问控制机制利用区块链可信存储的特性，可以从存储访问权限、访问控制策略、关键敏感数据以及访问控制操作记录这四个方面进行划分和实现。

1）存储访问权限：区块链可以作为一个分布式的可信存储，存储访问权限的相关信息。通过区块链技术，可以记录和验证用户的身份和角色，并将其与特定资源的访问权限关联起来。每个参与者都可以在区块链上查找和验证其他参与者的权限，并确保只有授权用户才能访问特定的数据或资源。

2）访问控制策略：基于交易的访问控制可以建立在智能合约上。智能合约是在区块链上执行的可编程代码，可以定义访问控制策略和规则。通过智能合约，可以实现灵活的访问控制规则，例如基于角色的访问控制、多重签名控制等。参与者可以根据智能合约中定义的策略来验证和执行访问请求。

3）关键敏感数据：区块链可以用于存储关键敏感数据，如个人身份信息、医疗记录等。通过访问控制机制，只有经过授权的用户才能访问和修改这些敏感数据。区块链的不可篡改性和去中心化特性确保数据的安全性和可信性，防止未经授权的访问和篡改。

4）访问控制操作记录：所有的访问控制操作可以被记录在区块链上，形成不可篡改的操作记录。这些记录可以用于审计和追踪访问行为，确保访问的可追溯性和透明性。参与者可以通过查看区块链上的操作记录，验证访问控制操作的合法性，并发现任何未经授权的访问行为。

通过基于交易的访问控制机制，区块链可以提供更可信、安全和透明的访问控制方式，保护存储在区块链上的数据和资源的安全性和私密性。

基于智能合约的访问控制机制利用区块链可信计算的特性，可以满足以下五个方面的需求：

1）用户信息管理：智能合约可以作为区块链上的可编程代码，用于管理和验证用户的身份信息。通过智能合约，可以实现用户注册、身份认证和权限分配等功能。用户的身份信息可以被存储在区块链上，确保数据的安全性和可信性。

2）链上数据管理：智能合约可以定义访问控制策略，确保只有授权的用户能够访问链上的数据。通过智能合约，可以限制对数据的读取和修改权限，并记录每个访问行为。这种机制可以保护数据的完整性和隐私性，防止未经授权的访问和篡改。

3）数据整合与查询：区块链可以用于存储和管理多个数据来源的数据。智能合约可以定义数据整合和查询的规则，确保只有合法的查询请求能够访问和获取数据。通过智能合约，可以实现跨链数据的整合和查询，提高数据的可访问性和可用性。

4）违规行为监测：智能合约可以定义违规行为的规则和条件，并监测链上的操作行为。通过智能合约，可以检测和记录违规行为，如未经授权的数据访问、篡改数据等。这种机制可以提供实时的监测和警报，保护数据的安全性和合规性。

5）访问权限判决：基于智能合约的访问控制机制可以根据事先定义的规则和条件判定访问权限。通过智能合约，可以自动执行访问权限的判决过程，确保只有合法的用户能够访问受限资源。这种机制可以提供高效、准确的访问权限管理，减少人为错误和滥用访问权限的风险。

基于智能合约的访问控制机制结合区块链的可信计算特性，可以实现安全、可靠的访问控制，保护数据的安全性和隐私性，以及监测和防止违规行为的发生。

# 5 基于区块链的访问控制技术研究展望

基于区块链的访问控制技术目前已经取得了一定的研究成果，但仍然存在一些挑战和问题。在未来，可以望见以下几个方向的研究和发展：

1）提高性能和可扩展性：目前区块链的性能和可扩展性是制约其应用的主要问题之一。为了实现在大规模访问控制场景下的高效率和低延迟，需要进一步研究和改进区块链的共识机制、存储结构、网络传输等方面的技术，以提高整体性能和可扩展性。

2）强化隐私保护：隐私保护一直是访问控制技术的重要方面。基于区块链的访问控制技术需要解决用户身份隐私、数据访问隐私等问题。未来的研究可以探索匿名身份验证、零知识证明、同态加密等隐私保护技术在区块链访问控制中的应用，以提供更好的隐私保护机制。

3）引入多方参与模式：传统的访问控制模式通常是由中心化的授权机构来管理和控制。未来的研究可以考虑引入多方参与的模式，通过智能合约和去中心化的机制来实现更加民主、去信任的访问控制系统。这将有助于提高系统的可信度和抗攻击性，并促进用户间的直接交互和合作。

4）融合人工智能技术：人工智能技术在访问控制领域有着广泛的应用前景。未来的研究可以探索将人工智能技术与区块链相结合，例如利用机器学习和深度学习来实现智能的访问控制策略推荐、异常检测和风险评估等功能，以提高系统的智能化和自适应性。

5）跨链互操作性：随着区块链技术的发展，不同的区块链网络相互之间的互操作性成为一个重要的问题。在访问控制领域，需要研究如何实现不同区块链网络之间的访问控制策略和权限的互通，以实现更广泛的应用场景和跨组织的合作。

总的来说，未来基于区块链的访问控制技术的研究将继续关注性能和可扩展性、隐私保护、多方参与模式、人工智能技术的应用以及跨链互操作性等方面的问题。这些研究将推动区块链访问控制技术的进一步发展和应用。

# 参考文献

1. SWAN M. Blockchain: blueprint for a new economy[M]. O'Reilly Media, Inc, 2015
2. ZYSKIND G, ZEKRIFA D M S, ALEX P, et al. Decentralizing privacy: using blockchain to protect personal data[C]//IEEE Security & Privacy Workshops. 2015: 180-184.
3. MAESA D D F, MORI P, RICCI L. Blockchain based access control[C]//IFIP International Conference on Distributed Applications and Interoperable Systems. 2017: 206-220.
4. CRUZ J P, KAJI Y, YANAI N. RBAC-SC: role-based access control using smart contract[J]. IEEE Access, 2018, 6: 12240-12251.
5. ZHANG Y, KASAHARA S, SHEN Y, et al. Smart contract-based access control for the Internet of Things[J]. IEEE Internet of Things Journal, 2018, 6(2): 1594-1605.