目　录

一、 背景调研

在高速发展的网络时代中，物联网、电子商务、电子医疗给社会带来非常便利的操作，其中， 如何保障网络传输中信息的隐私安全是一个亟需解决的问题。访问控制是为了防止未经授权的实体非法获取秘密资源的一种安全技术，但传统的访问控制都是集中式方案，很容易造成隐私泄露和单点瓶颈。传统的访问控制方案由于缺乏动态性和细粒度性，已不再符合当下网络的发展趋势。随着物联网（Internet of Things，IoT）的飞速发展，然而，IoT 设备的计算能力和存储能力有限，用户数据存储在一个中心化的第三方手中，具备安全隐患。

物联网等现实世界的访问控制模型多基于中央可信实体的概念构建. 去中心化的区块链技术解决了中心化模型带来的安全隐患。区块链作为一种分布式、可追溯、防篡改的技术，对于构建访问控制模型有着天然的优势，因此也出现了越来越多关于这方面的研究和探讨。但是除了已有的区块链基础设施外，想要构建多场景、高安全性下的访问控制模型，我们还可以针对特定场景结合相应的技术进行赋能。如基于智能合约制定针对电子医疗、用户健康管理数据的访问控制模型，基于边缘计算指定针对物联网海量边缘节点的访问控制方案，还有基于区块链实现域间访问控制模型，基于椭圆加密技术的智能家居访问控制方案。

我们知道传统的访问控制都是由集中式机构管控，用户无法对隐私数据进行自主管理，易泄露用户个人敏感数据和隐私信息。集中式的访问控制方案已不再符合网络发展的安全趋 势，同时在当下强实时性的网络环境下，传统的访问控制方案缺乏动态性和细粒度性。其中基于角色的访问控制（Role-based Access Control，RBAC）是将主体与权限分离，通过 为主体分发多种角色来实现访问控制，每一种角色对应一系列访问权限，RBAC 作为一种商业主导模式，它在具备多种优势的同时也存在一些缺陷：例如资源所有者无法灵活地对 自身资源进行访问控制，对于角色的分配方面无法达到细粒度分配，访问权限无法实现动态性增删改查，所以如何在分布式环境下实现动态性、细粒度的 RBAC 方案这一问题有待 研究。访问控制最终目标是实现数据共享，随着物联网（Internet of Things，IoT）的快速发 展，利用 IoT 设备或移动终端来收集用户健康信息也

越来越受欢迎，由于 IoT 设备或移动 终端的存储能力和计算能力有限，所以传统医疗方案中的用户健康信息都被存储在可信的 第三方手中或外包给云服务器，这种集中式的第三方存储一旦出现破坏，存储的用户数据 就会被泄露和损坏，用户敏感数据存在隐私安全问题，用户对于个人的健康信息无法自主管控。所以如何设计一种隐私保护、用户信息自主可控、去中心化的智能医疗体系吸 引了广大专家和学者们的关注。同时，用户的电子健康记录对于科研工作来说具有极大的科研价值，当病人向科研机构想要共享某些病历信息时，他/她通常与科研机构之间有按病历科研价值付费的交易规则。然而，病人把自己的病历信息提供给科研机构后，他们可能不信任科研机构支付的费用。同时，病人提供的共享病历信息必须有足够的科研价值，科研机构才会向病人提供科研付费操作。公平支付意味着病人只有提供的病历信息有足够科研价值的基础上才可以收到共享付款，同时病人也可以自行验证个人收到的付款与自己提 供的病例信息之间是否存在对等关系，因此如何协调病人病例信息和科研工作，实现公平支付这一问题也存在一定的研究价值。

对于物联网方面，区块链技术已被越来越多地应用于分布式物联网体系 中，以提供安全性和隐私性。它在保证数据分布式存储的 同时，确保数据的不可篡改，特别适合存储和保护重要隐私 数据，降低了物联网设备因数据中心被攻击而导致的用户个 人隐私数据泄露或大量数据丢失的风险。而区块链 3. 0 中 引入的智能合约则使得通过区块链技术解决访问控制问题 有了新的可能。目前通过区块链来解决集成边缘计算下物 联网的安全问题，大多是针对隐私保护、数据安全方 面，对物联网边缘节点的访问控制问题的研究并不多见。有部分研究只针对集成边缘计算的物联网系统中数据匿 名性和完整性问题，采用区块链技术实现安全存储 IoT 数 据。面向工业物联网下大规模数据传输存储问题， 用边缘计算处理源头数据再由区块链实现数据的安全存储 和管理。国内针对物联网安全数据访问与控制相关的研究 仍仅考虑将区块链技术与物联网所结合，国内一些研究学者提 出一种基于区块链的 IoT 访问控制框架、基于区块链的权能令牌环网来解决物联网越权访问、基于区块链的角色访问控制模型来解决对物联网 设备的安全访问。在将边缘计算与区块链集成下的研究中， 还有一部分人等

提出一种基于区块链和边缘计算的物联网数据 管理架构来实现数据的安全管理。他们忽视了边缘节点的潜在风险，默认存在的边缘节点为安全可靠，却忽视了物联 网规模扩展下，边缘节点在接入物联网时应通过可信机制加 以确认，同时也忽视了边缘计算带来的强大计算能力，即针对目前集成边缘计算的物联网体系新范式下，没有考虑边缘节点在访问控制过程中的作用。

因此总的来说，将区块链技术应用到具体场景下的访问控制模型会面临到很大的挑战和机遇。接下来也将会针对各个领域进行更加详细的分析。

二、 原理基础

2.1 区块链

区块链，是比特币的一个重要概念，它作为比特币的底层技术，本质上是一个去中心 化的链式数据库。2009 年 Nakamoto 首次提出，比特币是第一个被广泛使用的点对点无需信任的电子货币，之后又陆续出现了很多以区块链作为底层技术的加密货币。区块链技术通过将点对点网络、密码算法、分布式数据存储和去中心化的共识机制结合，为大众提供了一种安全和可溯源的方式达成的协议，用协议来商定特定的事态和记录。区块链是一系列区块，它持有一个完整的交易记录列表，区块链示例如下图所示。

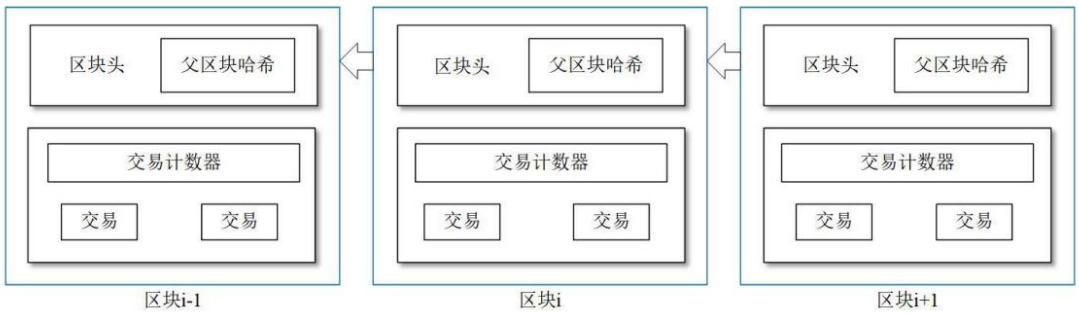

图 2-1 区块链示例

一个区块只有一个父区块，而区块链中的第一个区块被称为创世区块，它没有父区块。 区块结构如下图所示，区块头包含以下字段：

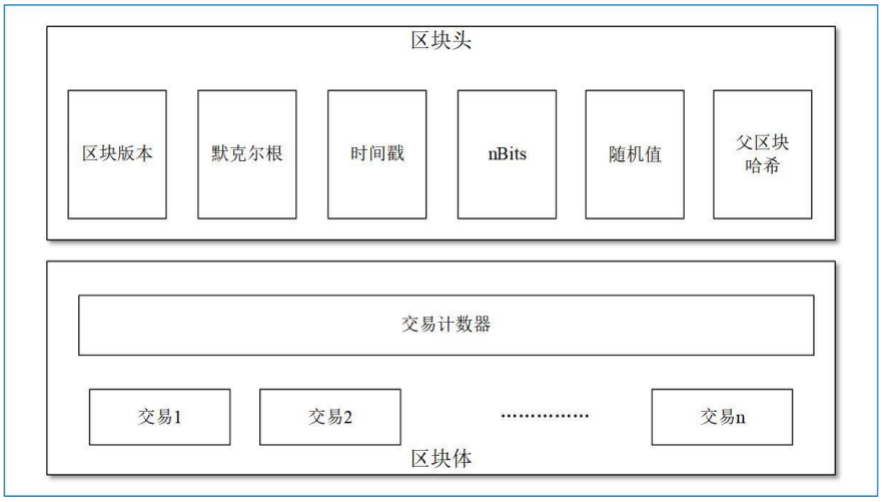

图 2-2 区块结构图

（1） 区块版本：字段指示哪一组区块验证时要遵守的规则。

（2） 默克尔根：区块中所有交易的哈希值。

（3） 时间戳：从 1970 年 1 月 1 日起，以秒为单位表示的当前时间。

（4） nBits：有效区块哈希的目标阈值。

（5） 随机值：一个 4 字节的字段，通常以 0 开头，每次哈希计算都会增加。

（6） 父区块哈希：一个指向前一区块的 256 位哈希值。 区块体由交易计数器和多个交易组成。一个区块中包含最大交易数量取决于区块大小 和每个交易的大小。

2.2 以太坊和智能合约

以太坊：以太坊是一种具有名为 Solidity 内置脚本语言的区块链平台，这类平 台支持智能合约，它提供一个抽象的图层，任何人都可以为自己的格式创建所有权规则、 交易处理和状态转换函数。以太坊的状态是由账户组成的，账户具有一个 20 字节的地址 和状态事务。“状态”一词是一种在地址和账户状态之间的映射操作。

以太坊账户：私钥控制的外部账户和合约代码控制的合约账户。以太坊账户包含四 个字段：

（1）随机值：表示从特定地址发送的交易数或帐户创建的合约数，并用于保证每个 交易只能处理一次。

（2）以太币余额：是该地址拥有的 Wei 数，Wei 表示以太币的最小单位，一个以太币 等于 1018 Wei 。以太币用于支付交易费用。

（3）合约代码哈希：合约代码哈希是账户的以太坊虚拟机（Ethereum Virtual Machine， EVM）代码的 Keccak-256 哈希，如果地址接收到消息调用，则执行该哈希。

（4）存储根：表示账户内容的 Merkle Patricia 树的根节点的 256 位哈希值。Merkle Patricia 树用于存储以太坊生态系统中的所有键值对绑定。

以太坊交易和消息：交易是以加密方式签名的单个指令。主要有两种类型的交易，分 别是消息调用的交易和创建新账户的交易。交易被定义为从外部账户发送的签名数据包， 每个交易都由消息的接收方、标识发送方的签名、发送以

太币的数量、可选数据字段、 STARTGAS 和 GASPRICE 字段组成。由于矿工在处理高 GASPRICE 的交易时会得到更多 的奖励，因此发送方必须谨慎地选择 GASPRICE 值。一个合约可以在以太坊网络中向另一 个合约发送消息，消息类似于交易，但消息是由合约生成。与交易相同，该消息会导致接 收方账户运行其代码。

以太坊状态转换函数：通过执行交易来更改发送方和接收方的状态，首先验证交易的正确性，主要进行签名有效性判断和随机值匹配，如果验证正确，将计算 STARTGAS×GASPRICE 作为交易费，从发送方的账户余额中减去相应值，并增加随机值。 同时，在交易中按字节支付费用，并将请求的以太币传输给接收方。如果收款账户不存在，创建收款账户；如果收款账户是合约，执行合约代码。如果发送方没有足够的以太币进行 交易，或者代码执行花费掉所有的 Gas，状态转换函数将还原除矿工支付费用之外的所有状态更改。

Gas：以太坊采用了一种内部定价机制，即对其上运行的所有交易使用 Gas。Gas 是一种度量交易花费计算资源量的方法。用户需要为每一笔交易支付 Gas。当交易 Gas 用尽，交易则会失败。通过 Gas 机制，以太坊能够更好地分配资源和缓解网络上的垃圾邮件。

智能合约：Nick Szabo 于 1994 年引入“智能合约”这个概念，将智能合约定义为“执行合约的一种计算机化交易协议”。在区块链定义中，智能合约是存储在链上的脚本，大致过程可以认为类似于关系式数据库管理系统的存储过程。因为存储在链中，所以智能合约有一个独特的地址，节点通过发送寻址交易来触发智能合约[46]。每个交易根据触发中包含的数据独立执行，网络中每个节点以规定的方式自动交易，意味着在一个智能合约支持的区块链中，每个节点都运行一个虚拟机 EVM，而该区块链网络充当一个分布式虚拟机的角色。

智能合约最突出的框架是以太坊，在以太坊中，智能合约被视为计算机程序，最常用 的以太坊智能合约编程语言是 Solidity 语言。Solidity 是一种类似 JavaScript 的脚本语言，合约是一个类，具有封装构造、合约继承和许多其他特性。以太坊的共识协议指定对等网络的节点如何扩展区块链，主要目标是确保合约的正确执行。

2.3 传统访问控制模型

传统的访问控制模型有很多种方式，最早的是自主访问控制模型

（Discretionary Access Control，DAC）和强访问控制模型（Mandatory Access Control，MAC）。随着技术的 发展，这两种访问控制模型已经无法满足当时的社会需求，随之出现基于角色的访问控制 模型（Role-Based Access Control，RBAC）和基于属性的访问控制模型（Attribute-Based Access Control，ABAC）等一些更适合当代系统安全。

- 自主访问控制

DAC 根据用户的身份和授权（或规则）来管理用户对信息的访问，这些授权（或规则） 为系统中的每个用户和对象（或用户组和对象组）指定允许用户访问对象的访问模式（例 如，读、写或执行），用户访问对象的每个请求都会根据指定的授权进行检查。如果存在 一个授权，说明用户可以在指定模式下访问对象，并授予访问权限，否则拒绝访问。 DAC 的灵活性使其适用于各种系统和应用，被广泛应用于各种实现，特别是在商业和 工业环境。然而，DAC 的缺点是不能对系统中的信息本身提供真正的保证，易躲避通过授 权声明的访问限制。例如，能够读取数据的用户可以在所有者不知情的情况下将数据传递 给其他无权读取数据的用户。DAC 不会对用户获得信息后的信息使用施加任何限制，信息的传播不受控制。

- 强制访问控制

相比之下， MAC 可以通过防止存储在高级对象中的信息流入低级对象来控制信息的 传播。

MAC 根据系统中主体和客体的分类来管理访问，系统中的每个用户和每个对象都被 分配一个安全级别。与对象相关联的安全级别反映对象中包含信息的敏感性，即未经授权 的信息泄露可能导致的潜在损害。与用户相关联的安全级别，也称为许可证，反映已授权 用户不向未授权用户披露敏感信息的可信度。在最简单的情况下，安全级别是分层有序集 的一个元素。在军事和政府领域，等级集通常由最高机密（TS）、机密（S）、机密（C） 和非机密（U）组成，其中 TS>S>C>U。每个安全级别都控制着自己及其下面所有其他级 别。只有在与某个对象相关的安全级别之间满足某种关系（取决于访问类型）时，才能授予主体对客体的访问权限。

然而 MAC 没有涵盖许多现实需求，MAC 使用于严格的军事环境，无法满足大多数商业企业的需求。

- 基于角色的访问控制

RBAC 是根据用户在系统中执行的活动来管理用户对信息的访问。RBAC 模型中存在 用户、角色和权限三种组件。RBAC 需要识别系统中的角色，角色可以定义为与特定工作 活动相关的一系列行动和职责，系统不再指定每个用户可以执行的所有访问操作，而是为 角色指定对象上的访问授权，用户则是被授予采用角色的权限。

允许拥有角色的用户执行该角色授权的所有访问。一般来说，用户可以在不同的场合 获取不同的角色，同样的角色也可以由多个用户同时拥有。RBAC 已被广泛采用，并提供 管理和安全方面的优势，RBAC 有如下几方面优点：

（1） 授权管理：RBAC 通过将任务分为两部分，一部分将角色分配给用户，另一部分将客体的访问权限分配给角色，从指定用户授权的逻辑独立性中获益，大大简化安全管理。

（2） 层次化角色：在许多应用程序中，角色有一个基于熟悉的泛化和专业化原则且 自然的层次结构。分层角色进一步简化了授权管理。

（3） 最小权限：角色允许用户以手头特定任务所需的最小权限行使。直到实际需要 这些权限之前，被授权担任强大角色的用户不需要行使这些权限，这样可以最大限度地减少由于疏忽错误或冒充合法用户的入侵者造成的损害。

（4） 职责分离：职责分离是指任何用户都不应被赋予足够的权限，自行滥用系统的 原则。职责分离既可以静态执行，即通过取消角色关联也可以动态执行，即在访问时强制控制。

（5） 客体分类：RBAC 根据用户执行的活动对用户进行分类，因此，应该为客体提供 分类，使授权管理更加容易和更好控制。此外，在每个客体上授权的访问是根据客体的类 型自动确定的，而不需要在每个客体创建时指定授权。

然而，RBAC 也存在一些缺陷：在用户角色分发方面缺乏细粒度；没有提

供操作顺序的管控机制；实施成本高昂，而且无法实现以适应作为访问控制参数的实时环境状态。

- 基于属性的访问控制

ABAC 是一种更新、更简单的访问控制模型，并且能够容纳实时的环境状态，通过评 估实体、操作和与请求相关的环境属性来控制对客体的访问。ABAC 系统能够同时实施 DAC 和 MAC 概念，支持精确的访问控制，允许访问控制决策中的更多离散输入，提供这 些变量更大的组合可能性。

ABAC 的基本思想不是直接在主体和客体之间定义权限，而是使用它们的属性作为授 权的基础。对于主体，属性可以是静态的，也可以使用动态的，如年龄、位置等。对于客 体，可以使用元数据属性。

ABAC 特别适合于开放和分布式系统中的授权和访问控制。它是对 RBAC 的扩展。相较于 RBAC，ABAC 提供了一种灵活、动态、细粒度的访问控制。它将角色或身份抽象为一组由属性授权机构发布的属性，使用一组属性上的布尔公式描述的访问策略来定义有效 和授权的访问，无须为系统中的每个角色分配角色或创建访问控制列表。相反，属性权限 只需要管理系统中定义的每个属性，并将它们分发给适当的用户。这样，由于系统中的属性数远小于系统中的用户数，可以有效地简化访问管理。

三、 模型方案

本章主要是对上面列举到的多个基于区块链和其他新兴技术结合实现访问控制的具体解释和探讨。

3.1 智能家居认证与访问控制方案

下图所示是该章节所构造的系统模型，由用户、移动 APP、终端 设备、网关、边缘服务器（edge sever，ES）组成，其中用户指智能家居的家庭成员，移动 APP 是用户用来与区块链网络进行交互的设备，终端设备如智能灯泡、智能电表（smart meter，SM）、 智能监控、传感器等，是一些轻量级设备，可以充当区块链网络的轻节点。

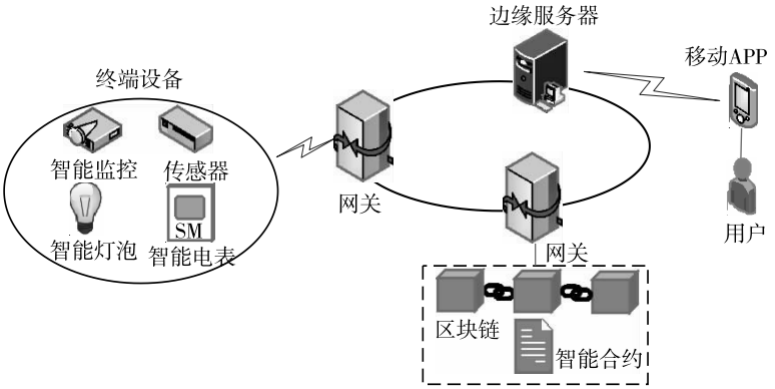

图 3-1 智能家居系统模型

这些传感器和设备通过智能家居中配置的各种异构物联网收集和监控智能家居网络环境中的数据。网关和边缘服务器都是能力设备，它是指具有足够的计算、存储和通信 资源的设备，作为区块链网络的全节点，可以进行交易的创建、验证以及查询等操作。网关存储设备层生成的数据，并根据需要提供给用户。边缘服务器充当边缘云，可以处理大量运算。

授权访问过程如图 2 所示，用户通过认证之后，要想进行访问，需要有设备的权能令牌，设备的权能令牌存储在网关中。用户需要检查设备 DUID 以获取他／她应该连接到哪个网关，并联系该网关，向网关请求相应设备的权能令牌，这一过程需要调用区块链上的智能合约（获取令牌算法，即算法 1）用以获取设

备 权能令牌，验证通过后，该网关会将设备权能令牌发送给用户。用户再向网关请求设备服务访问，再次调用区块链上的智能合约（验证令牌服务算法，即算法 2），验证令牌以检查存储在相应 的链上凭证中被授予的访问控制权限，返回验证结果，网关根据 验证结果将所需的设备服务 API 和手册转发给用户，为用户提 供设备服务访问，用户此时可以对终端设备进行访问操作。

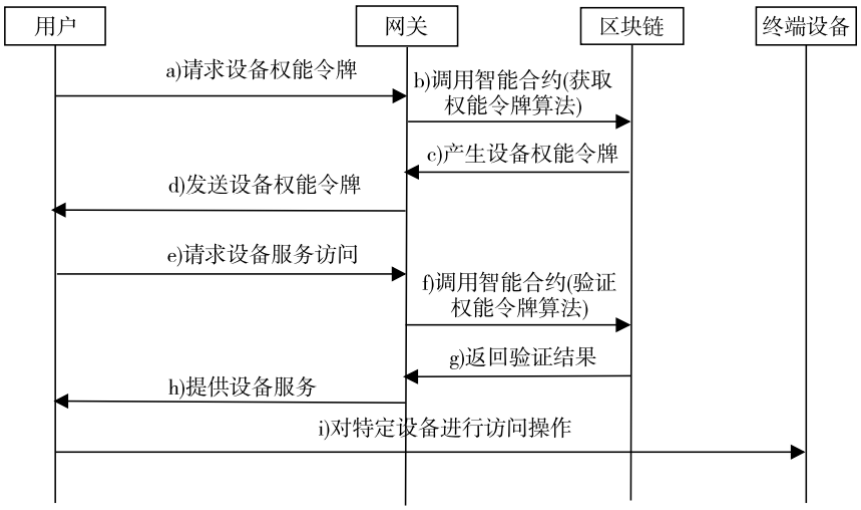

图 3-2 授权访问

算法 1 为向通过认证的用户发送设备的权能令牌。

Algorithm 1 获取令牌算法
a）从网关中获取服务列表 b）接受服务名称作为输入，并确定相应的服务 ID c）传递服务 ID 和设备 ID 给“ / fetchToken”路径去请求一个令牌 如果响应为否定 打印错误消息并退出 否则 转到步骤 d） d）获取数据 如果响应是“无效令牌” 从服务器请求新令牌并转到步骤 e） 否则打印收到的数据并返回到菜单 e）获取数据 如果响应是“无效令牌” 打印错误消息并退出

算法 2 为验证用户是否有对设备的访问控制权限。

Algorithm 2 验证令牌服务算法
a）如果请求设备没有被注册 返回错误 否则 转到步骤 b） b）如果服务不受支持 返回错误 否则 转到步骤 c）

c）查询具有设备 ID 和服务 ID 的智能合约的访问权限 如果设备不允许访问所请求的服务 返回错误 否则 转到步骤 d）

d）如果所请求的服务存在已缓存的令牌 转到步骤 e） 否则 转到步骤 f）

e）如果缓存的令牌已过期 从身份验证服务器获取新令牌，缓存并返回 否则 返回缓存的令牌

f）从身份验证服务器获取新令牌，缓存并返回

系统中的每个参与者（即用户和物联网设备）被一个唯一 的 UID 识别，并且特定设备服务的访问控制权限由权能令牌 确定。与其他方案相比，基于权能的访问控制相对更轻量，因 为它只需要描述主体的访问权限，并通过令牌授予权限。 对于未获得相应权限的设备，每次处理访问请求时被访问 设备都会创建访问交易记录。如果全节点发现该设备存在超 出可接受阈值的异常行为时，会将该设备从设备列表中清除， 同时从区块链中查询所有该设备的权能令牌，调用各个令牌管 理合约的令牌撤销接口冻结该异常节点的所有访问令牌。

3.2 基于智能合约的属性访问控制模型

基于属性的访问控制（Attribute-Based Access Control， ABAC）模型的访问结构由｛主体，客体，操作，环境｝构成。 它通过在对应环境下主体向客体的操作是否包含正确的属 性来确定是否向主体提供访问权限。

在物联网环境中，由于属性是每个主体、客体、操作和环 境所固有的，将每种设备和资源的属性与访问权限关联，使得 ABAC 模型适合管理物联网的简单设备和广泛数据。但对于异构设备的动态接入管理，ABAC 采用属性发现机制， 并不能按｛属性，权限｝对接入设备进行精确合适的权限分 配。而这会限制异构设备对数据的正常访问和实时处理，给 存在边缘节点的场景带来了挑战。因此本文针对异构设备的动态接入，基于 ABAC 提出 SC-ABAC 的访问控制模型，将智能合约与 ABAC 相结合，通过 ABAC 对资源和节点进行权限划分，并基于智能合约来确 保对应操作的正确执行。

在 SC-ABAC 中，主体和客体被视为相同对象，这是因为在物联网中每个设备都可以成为为其他设备提供资源的客 体，或作为主体从其他设备访问资源。每个物联网设备第一次接入时需通过边缘服务器向区块链注册信息，并通过其固有属性获得对应权限；为了设备自身的安全，将权限与椭圆曲线加密（Elliptic

Curve Cryptography，ECC）获得的公钥进行绑定，并在之后的访问和数据传输过程中采用私钥进行加密。而属性的判断则基于智能合约进行实现，并将每次的访问请求和判断结果存入区块链中实现同步。

智能合约是一种直接控制区块链内部数据的人为编写 的程序脚本［18］，由区块链内的多个用户共同参与实施，在没 有第三方的情况下也能控制交易的行为。智能合约可采用 调用自定义函数来执行相关命令：如发送某一节点的访问请 求或返回结果。

基于 SC-ABAC，本文设计了管理合约（Manager Contract， MC）{地址，属性，权限 }、判 断 合 约（Judeg Contract， JC） {编号，主体，主体权限，资源，资源权限，结果，时间 }、惩 罚 合 约（Punish Contract，PC）{编号，JC 结果，结果，时间 }和访问控制合约（Access Contral Contract，ACC）{编号，主体，资源，JC 结果，PC 结果，时间}。

1）MC 用于管理相关策略，主体为访问发起人，由对应 的 MAC 地址代替，属性为该对象所固有的特性，权限是以数 值进行描述的可操作行为，权限依次提高为读取、写入、管理 等。其中自定义函数有：

- ManageAdd() 用于添加某一对象的权限信息
- ManageUpdate() 用于更新某一对象的权限信息
- ManageDelete() 用于删除某一对象的权限信息
- QueryData (Hash) 用于通过 Hash 来获取某一对象的信息

2）JC 用于对某一对象申请对某一资源进行操作时的判 断，通过对主体权限和资源权限的比较得出结果，包括允许 所有操作、可读写、可读和非法访问等。其中自定义函数有：

- JudgeFromMC() 用于向 MC 中获取对象的权限信息
- JudgeToPC() 用于向 PC 发送判断结果
- JudgeToACC() 用于向 PC 发送判断结果

3）PC 用于对 JC 发送的结果进行处理，如对访问越权数据 的设备实施惩罚机制，或是对正常访问、发送数据的设备提供 奖励机制，以达到分配动态权限的目的。其中自定义函数有：

- PublishToACC() 用于向 ACC 发送惩罚结果

4）ACC 用于实现对设备和资源进行最终的访问控制， 通过 JC 结果向主体返回判断结果，通过 PC 结果向 MC 进行 主体和资源的函数操作：

- ACCAnswer() 将 JC 结果返回给主体以完成对资源的访问控制
- ACCSetMC() 通过 JC 结果调用 MC 中的函数对对象权限进行修改

基于区块链的访问控制管理机制具体流程如下图所示：

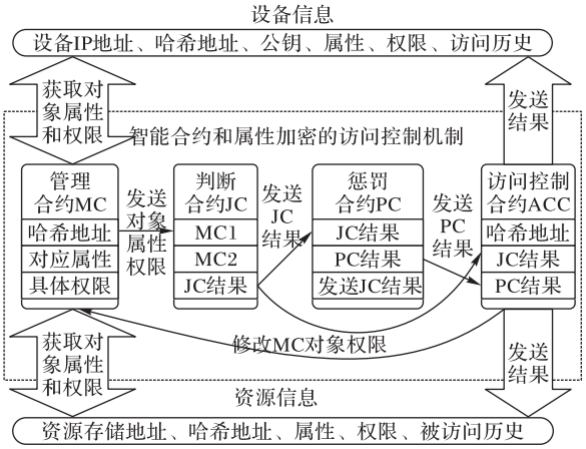

图 3-3 基于 SC-ABAC 的智能合约实现流程

3.3 基于智能合约的动态、细粒度的 RBAC 改进机制

本章节通过研究现有发展的局限性，主要介绍一种基于智能合约的动态、细粒度的 RBAC 改进机制 DF-RBAC。

（1）在解决角色分配细粒度和角色安全验证问题方面，将 RBAC 方案与 IBS 和 FH-CP-ABE 两种技术进行结合，利用一个层次访问结构对角色集合进行加密操作，只有 当满足部分或全部层次访问结构时，用户才能获得相应的角色信息，进一步利用 IBS 签名 完成对角色的安全验证操作。

（2）在解决用户、角色和权限三者之间动态性增删改查操作，本方案利用智能合约 进行算法设计，合约函数调用成功之后，会自动触发相应的函数事件，通过链上的事件记录实现安全审计功能。

文章中的实验结果表明这一访问控制方案适用于智慧医疗方面。下面将详细介绍。

模型方案主要包含四个组件，分别是资源所有者 DO，资源请求者 DR，区块链和智能 合约。

（1）资源所有者 DO：DO 是资源的拥有者，DO 可以自定义访问策略来管理自己的 资源信息；

（2）资源请求者 DR：DR 是对资源的请求者，当 DR 向 DO 发送角色请求时，只有 满足 DO 自定义的访问策略的 DR 才可以获得请求的角色信息，再利用角色进行进一步的资源访问。

（3）区块链：区块链主要是用来实现安全的可审计功能。智能和与合约函数调用成 功之后，会触发相应的事件，这些事件会以交易的形式存储在区块链中，保证访问控制的 各个环节安全可审计。

（4）智能合约：智能合约主要是用来实现用户、角色和权限三者之间动态性增删改 查操作，合约是由 DO 来进行部署。

模型方案流程如下图所示，主要分为 7 个步骤。

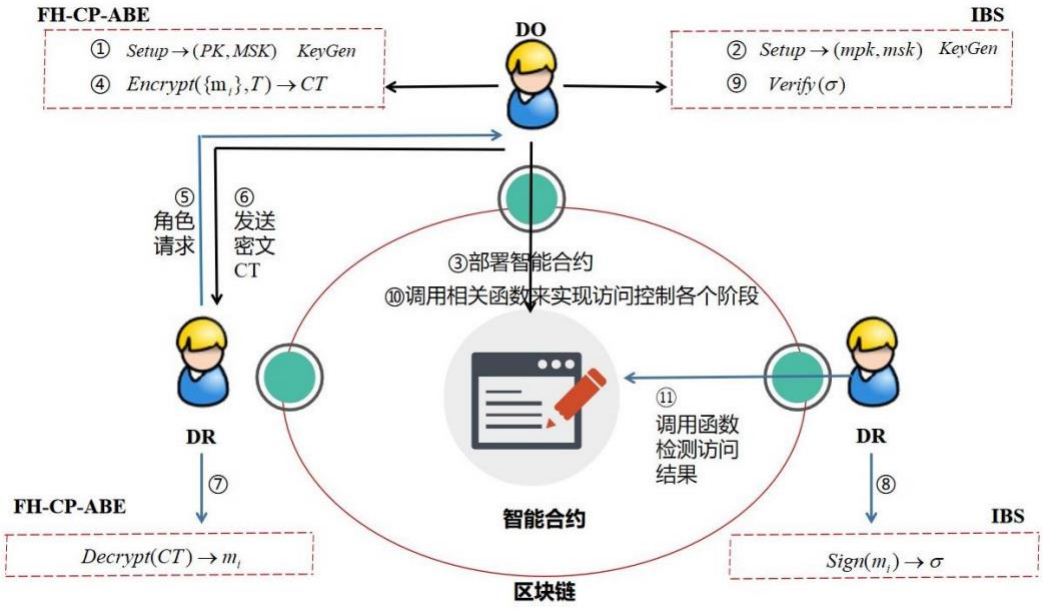

图 3-4　DF-RBAC 机制图

（1）初始化阶段：资源所有者 DO 执行 FH-CP-ABE 方案中的 SetupFH –CP–ABE 和 KeyGenFH –CP–ABE 算法，进行初始化操作，为各个用户生成相对应的属性密钥，之后执行 IBS 方案中的 SetupIBS 和 KeyGenIBS 算法，为各个用户生成相对应的身份密钥。之后 DO 在区块 链上部署智能合约，具体操作如图 3.1 中①②③。

（2）加密阶段：DO 自定义访问结构，利用一个层次访问结构树 T 来对角色哈希集合 进行加密，得到密文 CT，如图 3.1 中④。

（3）解密阶段：DR 首先会向 DO 发送角色请求，DO 接收到 DR 的角色请求，将密 文 CT 发送给 DR，DR 执行 DecryptFH –CP–ABE 算法，只有满足部分或全部 T 的 DR 才可以进 行解密操作，最终获得相对应的角色哈希，如图 3.1 中⑤⑥⑦。

（4）签名阶段：DR 利用身份密钥对解密获得的角色哈希执行 Sign 算法，生成对应的 签名 σ ，如图 3.1 中⑧。

（5）验证阶段：DR 执行完 Sign 算法之后，将得到的签名 σ 和角色哈希发送给 DO，DO 执行 Verify 算法来验证签名 σ 的有效性。如果该签名 σ 被验证是有效的，DO 会调用智 能合约中相应的函数进行授权用户的注册、角色的授予和权限的分配，具体操作如图 3.1 中⑨⑩。

（6）访问阶段：DO 调用智能合约函数成功后，即 DR 在区块链上监测上相应的事件 后，DR 可以调用访问函数进行访问判断，如果调用成功，在区块链上监测到相应的事件， 则证明 DR 拥有此权限；否则 DR 无权限执行此操作。

3.4 域间访问控制模型

先介绍域间网络结构, 如下图所示：

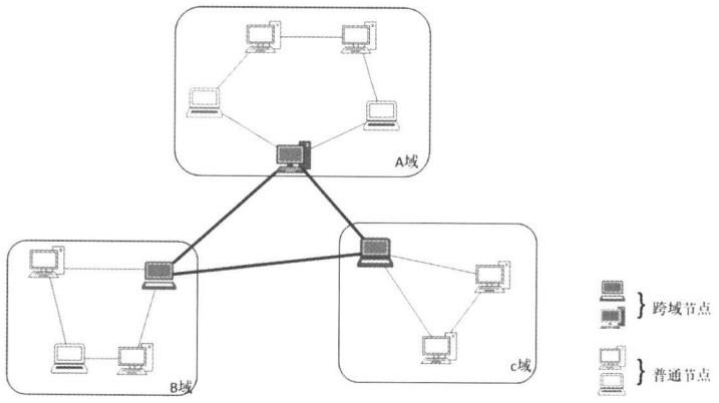

图 3-5 域间网络结构

区块链由各个安全域共同维护。该区块链由 A 域、B 域、C 域中的某一个域内节点作为跨域节点，所有安全域的跨域节点共同组成区块链中的网络节点，共同维护域问区块链的正常运行，其中，

- 跨域节点既是安全域中的网络节点，又是域问区块链的网络节点，主要负责本域和其他域的通信联系， 维护区块链服务的正常运行。安全域中，跨域节点最多只有 1 个。
- 普通节点是安全域中的普通网络节点，主要负责维护本域中的数据。某

一个普通节点由安全域指定为本域的跨域节点，若跨域节点宕机，则由新指定的跨域节点通过区块链网络进行同步获得链上数据。

因为各域是分布式位于不同位置，由各域的某些节点共同组成区块链并对其进行维护，符合资源的分布式 特点，各域对于资源请求的授权与否都由各域独自决定而无需增加“资源汇聚机制”，这令各安全域在资源共享过程中更加自主。

再介绍模型架构，本章节介绍的模型分为 3 层，自下而上分别为提供数据存储的数据层、提供区块链服务的服务层、提供各种功能的应用层，其架构如下图所示。

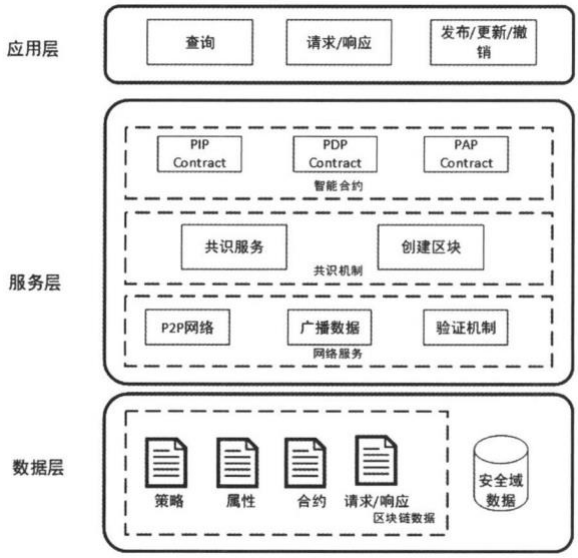

图 3-6 模型架构

1) 数据层：各安全域存储的数据资源和区块链存储的访问控制策略、属性和属性关系、智能合约以及 数据请求或响应操作等，这些数据在区块链中都以事务的形式存储。
2) 服务层：各安全域共同组成并维护的区块链，为域间交互提供访问控制服务。
   - 网络服务：为域间交互提供 P2P 网络、数据广播以及数据验证机制服务。域问数据资源请求或者 响应，属性和策略的创建、更新、撤销等操作，均通过区块链网络在域间广播。链上各节点负责验 证这些消息的合法性，合法继续传播，否则停止。
   - 共识机制：通过各种共识算法保证区块链节点间各类数据的一致性

和可信性，以此在各域间达到 稳定共识。

- 智能合约：ABAC 所需要的访问控制模块，在区块链中使用智能合约替代这些模块进行逻辑功能 操作，包括：PIP Contract，用于查询实体属性和属性关系；PDP contract，用于访问控制请求判断； PAP Contract，用于访问控制策略管理。

3) 应用层：主要提供各种功能应用，比如查询操作，请求数据资源和响应请求操作，属性和属性关系、访问 控制策略的发布、更新、撤销等操作。

介绍完上述之后，就要引出本模型了。是将区块链和 ABAC 访问控制模型结合，对 ABAC 进行一定的改造，其框架如下图所示：

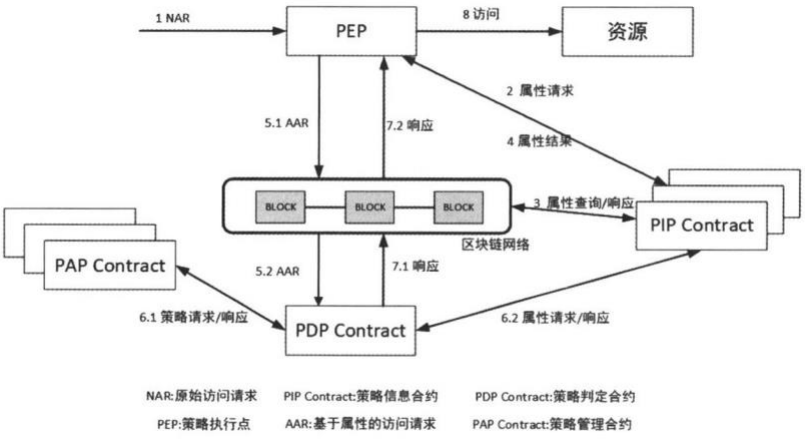

图 3-7 域间访问控制框架

在 ABAC 中，主要由 PEP、属性权威(attribute authority, 简称 AA)、策略管理点(point administration point， 简称 PAP)、策略决策点(policy decision point，简称 PDP)以及策略信息点(policy information point，简称 PIP)这 5 个核心部分组成。在本文框架中，AA 由区块链替代，属性信息在区块链中存储，保证属性信息的真实可信；PAP，PDP，PIP 分别由 PAP Contract，PDP contract，PIP Contract 这 3 种智能合约替代，智能合约由区块链存储，区块链中的节点可以调用合约来实现相应的功能；各安全域的跨域节点作为 PEP，接收访问请求并执行策略判定结果。

具体来讲，PEP 接收原始访问请求 NAR，然后根据 NAR 调用 PIP Contract 查询在区块链中存储的相关属性信息，用来构建一个基于属性的访问请求(AAR)，AAR 描述了主体、资源、操作和环境属性，如果不希望公开请求，那

么 PEP 会将 AAR 用资源拥有域的公钥加密封装成请求事务，然后通过区块链网络广播，区块链网络中的节点负责验证该事务的合法性并将其继续传播，资源拥有域收到该事务后调用 PDP contract，PDP contract 会分别调用 PAP contract，PIP contract，通过 PAP contract 和 PIP contract 获取策略集和属性信息，对 AAR 进行判定，并将判定结果和资源访问地址用请求域的公钥加密后封装成响应事务，通过区块链网络广播。PEP 收到响应事务后执行此访问，判定结果。

访问控制策略存储在区块链中，防止中心化策略判决不透明，保证策略按照资源拥有域的意图判定，即策略信息以及策略执行结果对于区块链中的各个安全域是公开透明、可验证、可追溯、不可篡改的．如果未进行加密处理，那么维护区块链的所有安全域均可以对策略信息和策略执行结果进行公开验证；如果对 AAR 进行了加密处理，那么请求域(作为请求方的安全域)可以对策略信息和策略执行结果进行公开验证，保障访问控制过程和结果的可信性。使用区块链网络作为各种事务的传播方式，对于请求域来说，区块链服务处理过程是完全透明的，请求域可以使用资源拥有域的公钥对请求进行加密处理，在充分利用区块链网络特点的同时，有效地防止请求域隐私泄露。保障在公开的域间区块链网络中的隐私安全。

四、 总结与探讨

4.1 总结

经过上面针对多种基于区块链技术所实现的访问控制模型和方案的介绍，我们对其有了进一步清晰的认识。我们也从各自对应的方面来进行总结和探讨。

智能家居方面给人们带来了舒适便捷的生活环境，但网络通信传输安全问题不容乐观，人们的隐私安全正在遭受威胁。对于本文介绍的基于区块链的智能家居认证与访问控制方案，该方案结合区块链与密码学技术，保护用户身份和设备信息，同时引入边缘计算保证高效的访问控制。用户和设备都有自己的唯一标志符，不需要额外的身份注册。因此，该方案可以解决用户身份管理困难的问题。安全性分析表明本文方案具有数据防窜改、 机密性、完整性和可扩展性等特点。原文的实验结果表明，该方案与传统方案相比具有更快的响应时间，能够提供服务的可用性。 由于智能家居系统本身还有许多难题需要解决，所以该方案具体实施还需要一段时间，可以为以后的智能家居研究作参考。

属性访问控制方面结合区块链技术设计了一种通过物联网边缘节点对终端设备和资源的访问控制模型，旨在为目前处理边缘计 算和区块链在物联网安全体系下访问控制研究的不足提供新的解决思路。基于原有的集成边缘计算的物联网体系，设 计出集成边缘计算的访问控制架构，将区块链中的智能合约与基于属性的访问控制相结合，提出了 SC-ABAC 模型。考虑到安全性能，基于 ECC 和 ECDSA 实现了基于区块链的访问控制管理机制，并通过实验来验证模型与架构的安全可靠性。对于未来的工作，考虑到本研究只针对边缘物联网下数 据的访问控制进行研究，对于数据本身存在的环境及个人隐私信息未作相应的处理，下一步将试图结合基于属性的加密 来构建高效且保护隐私的边缘物联网环境。

本文介绍了针对智慧医疗而利用区块链和密码学技术进行传统 RBAC 方案的改进。在医疗方面，提出一种公平支付、隐私保护、用户健康数据自主 管理的多链智能医疗数据共享方案，具体总结如下： 针对于传统 RBAC 存在的三

种问题：单点失效、用户角色分配的粗粒度性和用户、角 色和权限三者分配的静态性，设计出一种去中心化、细粒度的角色分配和动态性用户、角 色和权限分配的访问控制机制 DF-RBAC，利用区块链和密码学技术实现去中心化和细粒度的角色分配问题，利用智能合约来实现用户、角色和权限三者之间的动态性增删改查操作。通过与已有的工作进行安全性分析和成本开销对比，本文提出的方案具有更为广阔的 应用价值，此方案是实际可行的。 针对于传统医疗存在这些问题：集中式、用户对健康数据和诊断结果缺乏自主管理和 健康信息资源的浪费，提出一种具有去中心化、隐私保护、用户健康数据自主管理、公平支付的多链智能医疗数据共享方案。通过与传统的医疗方案进行仿真对比，该方案更符合现下大数据和智能背景，方案同样也是实际可行的。

对于域间访问控制模型，本文介绍将区块链和 ABAC 相结合，基于 Hyperledger Fabric 实现域间访问控制。一方面，充分发挥了区块链“共享”的特点；另一方面，通过细粒度的访问控制，对各域资源进行有效的控制管理。本文的核心思想是：使用区块链作为访问控制策略的载体，利用区块链的特点将“中心化”策略决策方式改为由智能合约自动化进行，策略执行过程和结果公开且可验证：区块链由各安全域维护，进一步提高策略执行的可信性，同时，策略由各域根据自身需要制定，且对权限授予与否拥有最终决定权，进一步提高资源拥有者的自主性，保障资源的访问权由资源拥有者决定；本文所述访问控制模型基于 ABAC 模型，并提出了对属性信息和访问控制策略标准化的概念，在更加准确地描述策略的同时，增加对整个动 态系统管理的灵活性；使用非对称密钥对隐私信息进行加密处理，有效地保障各安全域的隐私安全、本文所述模型在新型计算环境下能有效地保障域间访问和数据的共享安全，同时增强了用户的自主性，提高了系统的灵活性、扩展性和可管理性。因此，本模型具有广泛的应用价值。

总的来说，本文介绍的四个模型在其各自的领域都解决了所面临的特有的问题，在安全性，效率，便捷度上相较传统访问控制方案均有了显著的提升，但也面临落地难，不通用，耗资源等实际问题，因此要做到广泛应用还需要很长的路要走。

4.2 探讨与发展

首先，在讲述技术难点之前，我们需要了解区块链技术的基本原理。区块链是一种分布式账本技术，它通过对数据进行加密和分组，在不同的节点之间进行复制和储存，从而实现数据的安全存储和共享。这些被加密并分组的数据称为“区块”，而这些区块按照时间顺序组成的链称为“区块链”。

那么，基于区块链实现访问控制的技术难点主要有以下几点：

1. 数据存储的安全性。在区块链系统中，数据是通过加密和分组的方式储存的，因此具有较高的安全性。但是，区块链系统也存在一定的安全漏洞，如“51%攻击”、“中间人攻击”等，这就要求我们在设计区块链系统时要注意加强数据存储的安全性。
2. 权限管理的复杂性。在区块链系统中，由于数据是分布式存储的，因此权限管理相对比较复杂。例如，在区块链系统中，我们可能需要为不同的用户设置不同的访问权限，这就要求我们在设计区块链系统时，要考虑如何实现对用户访问权限的管理。
3. 数据同步的复杂性。在区块链系统中，数据是通过多个节点进行复制和储存的，因此在数据更新时，需要对所有节点进行数据同步。这就要求我们在设计区块链系统时，要考虑如何实现数据同步的机制。

除了技术难点之外，基于区块链实现访问控制的发展方向也是一个值得关注的问题。目前，区块链技术已经被广泛应用于金融、物流、医疗等领域，而在未来，区块链技术在访问控制领域的应用也将得到进一步拓展。

例如，在数字版权管理领域，区块链技术可以通过对数字内容进行加密和分组，并通过区块链的不可篡改性，实现对数字版权的保护。在智能合约领域，区块链技术也可以用于实现自动执行的合同，通过对合同内容进行加密和分组，并通过区块链的不可篡改性，实现对合同的执行。

此外，区块链技术在访问控制领域的应用也可以拓展到更多的领域，例如：

- 在数字身份管理领域，区块链技术可以用于实现数字身份的认证和管理，通过对用户信息进行加密和分组，并通过区块链的不可篡改性，实现对用户身份的认证。

- 在数据隐私保护领域，区块链技术也可以用于实现数据隐私的保护，通过对数据进行加密和分组，并通过区块链的不可篡改性，实现对数据隐私的保护。

最后，基于区块链实现访问控制的意义也是值得我们深入思考的。区块链技术的出现，为我们提供了一种新的数据存储和共享方式，可以有效地解决传统数据存储方式存在的安全性、可靠性等问题。而基于区块链实现访问控制，可以进一步保证数据的安全性和可靠性，并且可以有效地实现对数据访问的控制，避免数据被恶意访问或篡改。

总的来说，基于区块链实现访问控制具有重要的意义，它不仅可以为我们提供一种安全、可靠的数据存储方式，还可以有效地保证数据的安全性和可靠性，并且在未来还有广阔的发展空间。因此，我们应该继续探索基于区块链实现访问控制的技术，以更好地为我们的数据安全保驾护航。

最后非常感谢崔永泉老师在课上的教导，让我能够顺利完成这篇报告！

五、 参考文献

【1】张建标，张兆乾，徐万山，等. 一种基于区块链的域间访问控制模型[J]. Journal of Software, 2021, 32(5).

【2】史锦山，李茹. Survey of Blockchain Access Control in Internet of Things[J]. Journal of Software, 2019, 30(6): 1632-1648.

【3】何俊杉. 基于区块链的访问控制技术与应用研究[D]. 北京邮电大学, 2021.

【4】张杰，许姗姗，袁凌云. 基于区块链与边缘计算的物联网访问控制模型[J]. 计算机应用, 2022, 42(7): 2104.

【5】张利华，张赣哲，曹宇，等. 基于区块链的智能家居认证与访问控制方案[J]. 计算机应用研究, 2022.