基于区块链的访问控制技术研究进展

高振升，曹利峰，杜学绘
（信息工程大学，河南 郑州 450001）

摘　要：区块链技术有着去中心化、可信度高、难以篡改的特点，能够解决传统访问控制技术中存在的信任难题。通过总结现有的基于区块链的访问控制机制，分别从基于交易事务和基于智能合约两种实现方式分析了将区块链技术应用于访问控制领域的独有优势。根据区块链应用中的关键问题，从动态访问控制、链上空间优化、隐私数据保护 3 个关键技术总结了现有的研究进展。结合目前基于区块链的访问控制机制面临的挑战，提出了 5 点研究展望。

关键词：区块链；访问控制；大数据；智能合约；隐私保护
中图分类号：TP309
文献标识码：A
DOI: 10.11959/j.issn.2096−109x.2021044

Research progress of access control based on blockchain

GAO Zhensheng, CAO Lifeng, DU Xuehui
Information Engineering University, Zhengzhou 450001, China

Abstract: Blockchain technology has the features of decentralization, high credibility, non-tampering and traceability, which can address the trust problem in traditional access control technology. Based on the implementation with blockchain, the unique advantages of applying blockchain to access control are analyzed from two aspects: based on transaction and based on smart contract. Based on the key issues in blockchain application, the current research progress is summarized from three key technologies: dynamic access control, blockchain space optimization, and privacy data protection. Based on the challenges faced by the current blockchain-based access control mechanism, five research prospects are proposed.

Keywords: blockchain, access control, big data, smart contract, privacy protection

---

收稿日期：2020−09−04；**修回日期：**2020−12−19
通信作者：曹利峰，caolf302@sina.com
基金项目：国家重点研发计划（2018YFB0803603, 2016YFB0501901）；国家自然科学基金（61502531, 61702550）
Foundation Items: The National Key R&D Program of China (2018YFB0803603, 2016YFB0501901), The National Natural Science Foundation of China (61502531, 61702550)

论文引用格式：高振升, 曹利峰, 杜学绘. 基于区块链的访问控制技术研究进展[J]. 网络与信息安全学报, 2021, 7(6): 68-87.
GAO Z S, CAO L F, DU X H. Research progress of access control based on blockchain[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 68-87.

1　引言

随着物联网、云计算等技术的兴起，人们悄然进入大数据时代，与此同时，数据成为重要的经济资产[1]，成为新的生产因素渗透到各行各业。随着数据资源的广泛共享，数据资源的安全问题受到越来越多的关注，特别是对敏感数据的安全防护正面临着严峻的挑战。首先，数据资源的外包存储服务使个人的数据不受自己掌控，分布式存储数据的流通共享变得愈加复杂，这带来了潜在的安全风险。其次，利用数据挖掘技术，原有的“低价值”数据经过聚类分类能够推导出固定的用户模式，导致信息泄露。最后，由于庞大的数据量以及数据的非结构化，针对性的数据窃取、篡改、勒索等恶意攻击更难防范。实际上，相应的安全事件已经屡见不鲜，2014 年 5 月，eBay 的用户数据库遭到冒充员工的黑客的攻击，导致 1.45 亿用户的账号信息泄露；2018 年 3 月，Facebook 被曝出约 5000 万条的用户信息被第三方公司违规收集并使用；2018 年 3 月，圆通 10 亿条用户快递信息在暗网被兜售，至今未溯源到泄露原因。2018 年互联网大会上发布的《大数据安全白皮书》中指出，要在大数据平台基本组件安全的基础上为数据和应用提供安全机制保障，并在数据安全的基础上实现对个人敏感信息的安全防护[2]。

访问控制技术最早可以追溯到 20 世纪 70 年代，它的诞生是为了满足当时大型主机系统内的数据访问需求。访问控制作为一种重要的信息安全技术，它通过某种途径显式地准许或限制主体对客体访问能力及范围[3]，实现保证用户在其合法权限内访问数据，并禁止非授权用户的违规和越界操作。在大数据的环境中，访问控制技术仍是重要的数据保护手段，但大数据的 4V 特点，即 Volume（体量大）、Variety（模态繁多）、Velocity（生成快速）和 Value（价值巨大但密度低）[4]，给现有的访问控制技术带来了挑战。传统的访问控制机制无法应对大数据环境下信息共享程度高、数据流通快、分布式存储的特点，面临着上文示例的数据主权难维护、访问权限难界定、第三方泄露难防范等问题，这给访问控制技术的发展带来了“桎梏”。

区块链最早出现于 2008 年中本聪发表的 *Bitcoin: a peer-to-peer electronic cash system*[5]，而且准确地说其中只提出了“区块”（block）和“链”（chain），还没有出现“区块链”（blockchain）这个词。早期的区块链作为虚拟货币系统的底层技术，还没有引起人们的重视，直到比特币系统稳定运行三四年后，业界才渐渐关注到区块链技术去中心化、安全可信的特点，并将其拓展应用到各个领域。

区块链具有分布式、交易透明、难以篡改的特点以及无须第三方背书的可信机制，这与大数据环境下访问控制需要解决的分布式部署、审计机制、信任机制的需求不谋而合。正因如此，基于区块链的访问控制自从提出就受到了诸多学者的关注，图 1 显示了在 Web of Science 数据库中，以 blockchain 和 access control 为关键词检索得到的文献情况（截至 2020 年 12 月），可以看到目前结合区块链的访问控制机制正处在研究的上升期。在大数据背景下，诸多基于区块链的访问控制机制已经在物联网、云计算、医疗、工业自动化等多个领域被提出并应用，且仍有较大的改进空间和广阔的应用场景。

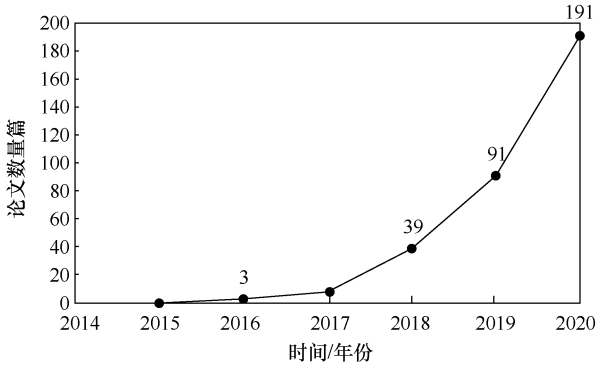


图 1　Web of Science 中检索相关论文按年份发表情况

Figure 1　Relevant papers retrieved in Web of Science published by year

2　大数据访问控制分析

2.1　大数据下的热点技术

移动互联网、物联网以及云计算等热点的崛起在很大限度上是大数据产生的原因[6]。如果将大数据比作数据分析员，那么物联网作为感知器

官，负责时时刻刻收集周边的各种信息，云计算则是大脑，负责存储海量的数据，并提供强大的计算能力以支持数据分析，而网络通信技术则作为神经器官，负责信息的传递与共享，如图 2 所示。

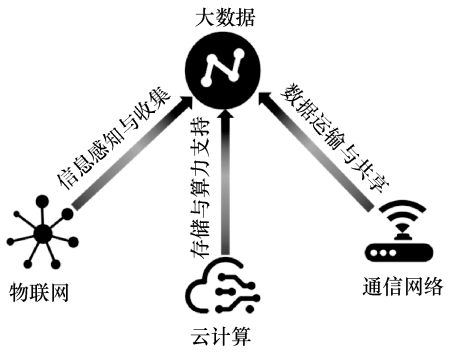


图 2　大数据与物联网、云计算、通信网络的关系

Figure 2　The relationship between big data and the internet of things, cloud computing, communication network

物联网的概念在 1999 年首次被提出，它强调在互联网的基础上实现物品与网络的互联，并在物品设备间进行信息通信和交换，形成智能化功能的网络。经过 20 多年的发展，特别是随着智能摄像头、可穿戴设备、智能汽车等设备的普及，对物联网设备的数据保护问题已经引起越来越多研究者的注意。物联网场景下数据的访问控制技术主要面临 3 个方面的挑战：① 物联网设备的部署多是分布式架构，对网络中终端设备的针对性攻击难以防范，要求访问控制机制应具备一定的容错性，避免少量虚假数据造成整个系统的瘫痪；② 数据的存储呈现分布式的特征，设计的访问控制机制应具备多地协作统一的能力；③ 物联网中存在着大量以摄像头、传感器为代表的信息采集设备，其产生的数据价值密度低但是数量巨大，如何实现对这些“数据原料”的安全防护也是需要研究的问题。

云计算依托于互联网，通过在网络上提供快速的云计算服务与数据存储服务，让用户可以使用网络上的外包数据库与计算资源，它的普及为企业和用户提供了灵活高效的数字资源管理服务。但是近些年来云平台上的数据泄密事件，让人们意识到云计算中数据安全管控的重要性。云计算场景下，对数据的访问控制技术主要面临 3 个方面的挑战：① 云计算环境中用户对个人数据难以管控，云服务商对访问权限的履行情况难以确定，导致个人敏感数据的泄露；② 云计算环境中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，制定访问控制策略，实现细粒度的数据访问控制并杜绝非必要信息的泄露也是待解决的问题；③ 云计算环境中数据资源更新速度快，数据的上传和下载影响着用户的数据状态，静态的权限授予策略有时难以应对数据的快速演变，因此设计实现动态的访问控制机制显得尤为必要。

2.2　大数据下访问控制的需求

结合 2.1 节对大数据环境下关键场景的分析，总结目前访问控制技术面临以下 6 个方面的挑战。

挑战 1：分布式架构的部署。大数据特别是物联网的兴起，引发了分布式的浪潮，大量的数据在信息共享系统的存储呈现出地理区域隔离、安全域隔离的特点。这要求访问控制系统在分布式架构下要具有协调统一的跨域管理机制，特别是在不同的数据域有着不同的安全需求时，相应的管理机制更加复杂。

挑战 2：权限管理策略。大数据环境中的访问控制主体组成复杂，信息共享频繁，数据流通管理困难。巨大的数据量、用户的多样需求和服务商的多类型业务都给权限管理带来了挑战，权限管理策略应当具有可信的授予、更新、删除机制。

挑战 3：细粒度访问控制。由于数据体量浩大和模态繁多的特点，传统的授权模式难以满足最小授权原则[7]。为了维护访问边界，禁止越权访问，需制定适宜应用场景的近似最小授权访问策略。

挑战 4：敏感数据保护。大数据环境下，包括聊天信息、购物记录、医疗数据、浏览记录等个人数据都在未经授权的情况下被第三方收集。这些看似“低价值”的数据经过挖掘，往往可以推导出用户的身份信息、喜爱偏好、健康情况等，而泄露的信息被第三方恶意使用，就会出现商品“杀熟”、虚假广告、隐私敲诈等问题，这就需要设计针对敏感数据的隐私保护机制。

挑战 5：动态访问控制。大数据环境中的数据更新速度快，用户和服务商时时刻刻都在进行数据的上传和下载，所以相应的访问控制机制也

应具有调整策略，并考虑到访问控制策略实施滞后性，部署能够灵活地根据客体属性和主体需求变化进行实时动态调整的访问控制机制。

挑战 6：权限核查。数据的体量大且模态繁多的情况下，相应的权限分配会愈加复杂，特别是在多方信息共享的情景下，不信任的双方进行通信时需要互相核查对方的身份和权限，这需要建立相应的保证机制，减少双方的审核开销。

2.3　传统访问控制机制的不足

访问控制作为数据保护的基石性技术之一，用以控制访问主体和客体之间的数据安全交互。随着计算机技术的发展，对访问控制的要求愈加细化，访问控制技术也随之得到完善和发展。目前主要的访问控制模型有基于角色的访问控制（RBAC，role-based access control）[8]、基于属性的访问控制（ABAC，attributes based access control）[9]、基于任务的访问控制（TBAC，task-based access control）[10-11]等。

基于角色的访问控制的核心思想是在用户集和权限集之间建立一层角色集，对每种角色设定一组对应的访问权限，在对用户进行授权时只需建立起用户到角色的映射，这样用户直接拥有该角色的全部权限。RBAC 的出现简化了用户的权限管理，减少了系统的操作开销，适用于企业级的数据安全管控。但是在大数据环境下，RBAC 仍面临两个问题。一是复杂的系统环境让角色的设计成为一项艰巨的挑战，角色挖掘的需求显得尤为突出。Molloy 等[12-14]致力于复杂数据集下的角色挖掘工作，这给基于 RBAC 的大数据管理带来了显著的改进，但是大数据应用中的访问权限依然难以细化到各个角色上，过度授权和授权不足的现象难以避免。二是难以实现分布式环境下的授权需求，文献[15]提出将 RBAC 与证书认证相结合，用以克服 RBAC 模型中集中式管理的缺陷，但是证书的颁发工作仍需要中心化的权威服务器执行，不能普及到节点完全对等的分布式环境中。

基于属性的访问控制核心思想是基于实体的属性来判决是否允许用户对资源的访问，其中访问控制策略可以根据属性值以及属性之间的关系灵活制定。ABAC 克服了角色身份的限制，能够通过属性对访问权限进行描述，具备实现最小授权原则的条件。例如，文献[16-17]探索了将 ABAC 应用于大数据访问控制的可能性，并提出将机器学习算法应用于复杂组织集和属性集下的访问控制策略制定，能够应对较大数据规模下的访问控制需求。但是在大数据不可信的网络环境下，ABAC 也存在着安全问题：一是访问策略由用户自定义制定，策略的执行依然依托第三方背书的权威机构，其执行结果往往用户无法跟踪，个人的数据泄露难以察觉；二是用户制定的策略存储在服务器上，也有受到黑客篡改的可能，致使数据的泄露。

基于任务的访问控制是从工作流的角度出发，通过将业务划分为多个任务，然后依据任务和任务状态对权限进行动态管理，适用于解决分布式环境下多机构参与的信息管控需求。TBAC 的访问权限与任务相绑定，任务执行完则权限被消耗，所以主体对客体的访问具有时间窗口，提升了安全性。但是 TBAC 仅关注工作流，没有设计对主体和客体的约束，不符合实际的应用情况，因此它往往作为补充机制与其他的访问控制模型结合使用。

此外，有学者将基于风险的访问控制引入大数据领域，文献[18]提出使用基于风险的访问控制来管理患者医疗数据，通过对医生的访问行为进行评估，给每位医生量化其风险，进而限制高风险医生的过度访问。文献[19]则将风险概念引入云计算中，云租户和服务商可以通过自定义的风险策略来管理自己的数据，从而适应云环境下资源和用户灵活度高、可伸缩性强的特点。总体来说，基于风险的访问控制能够适应动态性强、可扩展性高的系统，但是也存在风险量化标准难确定、风险衡量结果不可信的问题。

3　区块链技术

区块链技术是一种去中心化、去信任化的分布式数据库技术方案[20]，它并不是一项新的技术，而是革命性的技术组合。一个完整的区块链系统通过哈希算法和时间戳保证数据区块难以篡改和不可伪造；利用数字签名实现交易的确认与验证；利用对等网络上的共识机制实现各个诚实

节点记账的一致性；利用 Merkle 树实现区块数据的快速归纳和校验。区块链技术带来的颠覆性思想，让业界将其作为“价值互联网”的基础协议[21]，在访问控制领域具有天然的安全优势。

3.1　区块链架构

自 2008 年比特币诞生以来，区块链技术一直在持续地改进和发展，特别是随着以太坊、EOS 等项目的提出，让人们看到它在多种场景下的应用潜力。Swan 发表的 *Blockchain：Blueprint for a new economy* 中将区块链技术的应用分为 3 个层次，即区块链 1.0、区块链 2.0、区块链 3.0[22]。其中，区块链 1.0 架构应用于虚拟货币系统，即与支付、转账、审计相关的密码学货币的应用。区块链 2.0 架构的主要关注点在于智能合约的应用，其核心理念在于利用区块链的高可信性，把其作为一个可编程的分布式可信任基础设施，从而将其应用拓展到认证、拍卖、知识产权保护等需要建立信任机制的领域。区块链 3.0 架构还没有准确的定义，但其核心思想是在区块链 2.0 的基础上，建立起实际的分布式系统，将其应用领域再次拓展到政务、工业、医疗、艺术等领域，实现广义的可信任“资产”交易。

区块链的基础架构如图 3 所示，区块链系统可分为基础网络层、中间协议层以及应用服务层。其中，基础网络层可细分为数据层和网络层，中间协议层可细分为共识层、激励层和合约层。接下来分析架构中与基于区块链的访问控制机制相关的关键技术。

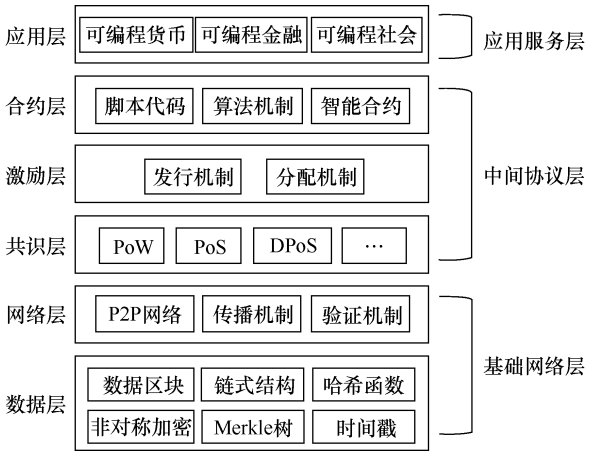


图 3　区块链的基础架构

Figure 3　Blockchain infrastructure

3.2　数据区块结构

区块链的区块结构保证了数据只增不减、难以篡改、可以溯源的特性。如图 4 所示，区块链在区块体内以 Merkle 树的形式存储交易数据，在区块头存储时间戳、区块哈希、随机数、Merkle 根等信息。Merkle 树以二叉树的结构进行哈希运算，实现交易信息的“压缩”和防篡改，达到数据校验和快速归纳的目的。时间戳用于记录当前区块数据的写入时间，它为区块数据增加了一个时间维度，增强数据的可追溯性。此外，每个区块利用哈希算法，结合随机数和 Merkle 根等信息得到其区块头的哈希值，并将其作为下一区块的目标哈希，以实现记账权的竞争机制。在此机制下，区块头的哈希值成为区块间的链接“指针”，实现了区块链的链式结构，保证了区块数据的存储可信性。

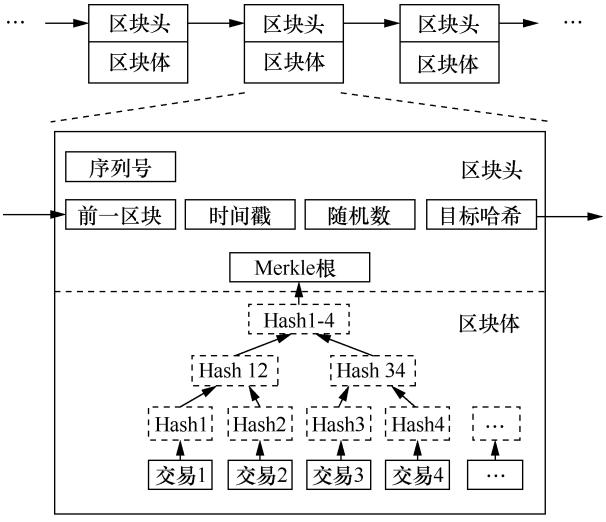


图 4　区块链的数据结构

Figure 4　Data structure of blockchain

3.3　共识机制

作为去中心化的记账系统，区块链通过共识机制来实现互不信任的分布式节点之间就交易的合法性达成一致性共识。区块链的共识机制解决了分布式记账数据库的两个问题：账本的写入权归属和节点之间的账本同步。研究者认为区块链的共识问题可被归纳为文献[23]提出的拜占庭将军问题，而文献[24]提出的 Fischer-Lynch-Paterson 定理证明：在含有多个确定性进程的异步系统中，只要有一个进程可能发生故障，就不存在协议能

保证在有限时间内使所有进程达成一致。因此，研究者根据实际的工程模型，通过附加同步性假设、时间假设等限制条件提出了许多共识算法，并根据设定的条件可分为强一致性共识和最终一致性共识两大类。

强一致性共识算法一般应用在节点数较少且具备节点准入机制的联盟链和私有链环境中，如实用拜占庭容错机制（PBFT）和 Raft 机制等。而目前应用比较广泛的工作量证明机制（PoW）、权益证明机制（PoS）以及股份授权证明（DPoS）都属于最终一致性共识算法，它们多应用在节点数量巨大的公开链环境中。通过查阅相关资料以及参考文献[25]的工作，将常见的共识机制归纳如表 1 所示。

3.4　智能合约

智能合约可以被看作一种计算机程序，是开发者根据已经制定好的合约条款转换成的运算逻辑，它会时刻监督用户的数据状态和行为信息，并根据已经制定好的逻辑规则，保证合约的顺利执行。智能合约的概念在 1994 年被提出，并将其描述为“由计算机处理的、可执行合约条款的交易协议”[26]，但由于当时的技术不成熟以及安全机制不完善，这个概念难以应用落地。而区块链有着难以篡改、公开透明、安全可信的特点，能够为智能合约提供高可信度的存储和执行环境，使智能合约重新受到许多研究者的重视，得以快速发展。特别是在以以太坊为代表的区块链架构 2.0 下，智能合约成为其核心关键组件，已经成为未来互联网合约的重要研究方向，有着广泛的应用空间。智能合约的工作机制可划分为智能合约的部署和智能合约的执行两个部分。

以以太坊为例，如图 5 所示，智能合约的部署首先由开发人员按照预定的协议编写智能合约代码，再编译为字节码后通过 geth 客户端上传至区块链网络，包含有该合约的区块在经过全网验证后会被写入每个节点管理的区块链上，一段时间后通过记账节点完成智能合约上链。在完成智能合约的部署后，智能合约以账户的形式保存在区块链上，用户通过该账户的地址订阅智能合约。如图 6 所示，智能合约会定期检查用户是否满足触发条件，在条件触发后通过一笔事务调用合约，合约代码会在本地的以太坊智能合约虚拟机（EVM）上执行，之后再对执行结果打包、广播、验证，在其他节点确认无误的情况下将执行结果上传到区块链上。

4　基于区块链的访问控制机制分析

区块链具有分布式、交易透明、难以篡改的特点以及无须第三方背书的可信机制，这与大数据环境下访问控制需要解决的分布式部署、审计机制、信任机制的需求不谋而合，区块链技术与访问控制技术结合有以下 6 点优势。

1) 策略和权限可信任。由于区块链难以篡改的特点，访问权限数据以及部署的智能合约在经过共识机制存储到区块之后将无法删除和更改，这避免了针对性的权限篡改、删除等恶意攻击，

表 1　常见的共识机制对比

Table 1　Comparison of consensus mechanisms

共识机制	优点	缺点	适宜场景	代表项目
PoW	完全去中心化，节点容纳量大，允许节点动态加入删除，可信度高	消耗大量算力和电力，共识达成时间长，存在 51% 攻击	无许可准入机制的公开链	比特币
PoS	允许节点动态加入删除，与 PoW 相比资源消耗少，缩短了共识达成时间	记账权易受富裕节点支配，去中心化程度随着时间的推移降低，存在 Nothing-at-Stake 攻击漏洞	无许可准入机制的公开链	未来币
DPoS	秒级验证，大幅缩短共识达成时间	代表节点验证机制牺牲了去中心化，降低了安全性	无许可准入机制的公开链	EOS
PBFT	共识达成时间快，能够解决拜占庭故障	实现机制复杂，节点数较多时效率降低，1/3 记账者受攻击时系统就会瘫痪	带许可准入机制的公开链	Hyperledger
Raft	秒级验证，大幅缩短共识达成时间，节点间通信复杂度低	实现机制复杂，去中心化程度低，属于多中心化机制	可信环境，如私有链	Quorum

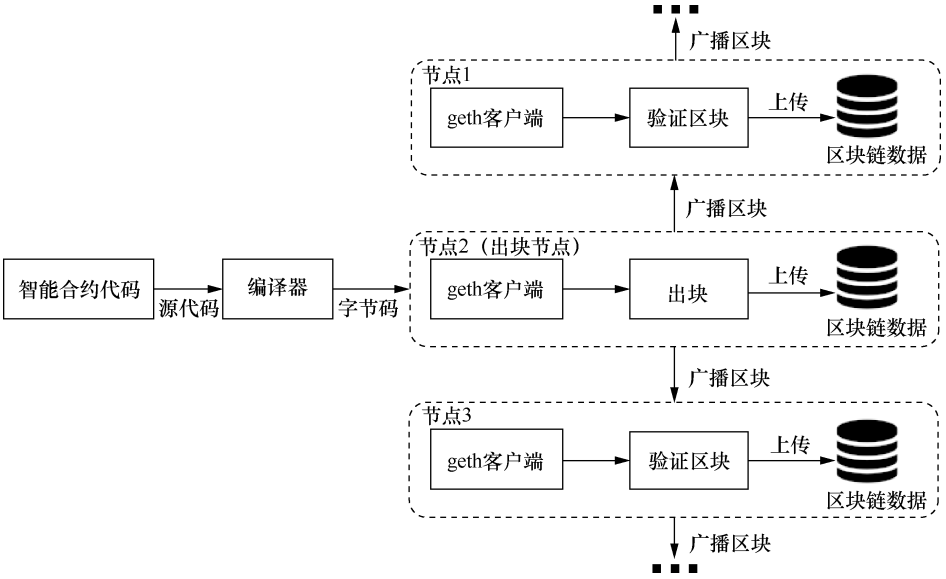


图 5　智能合约的部署流程
Figure 5　Deployment process of smart contract

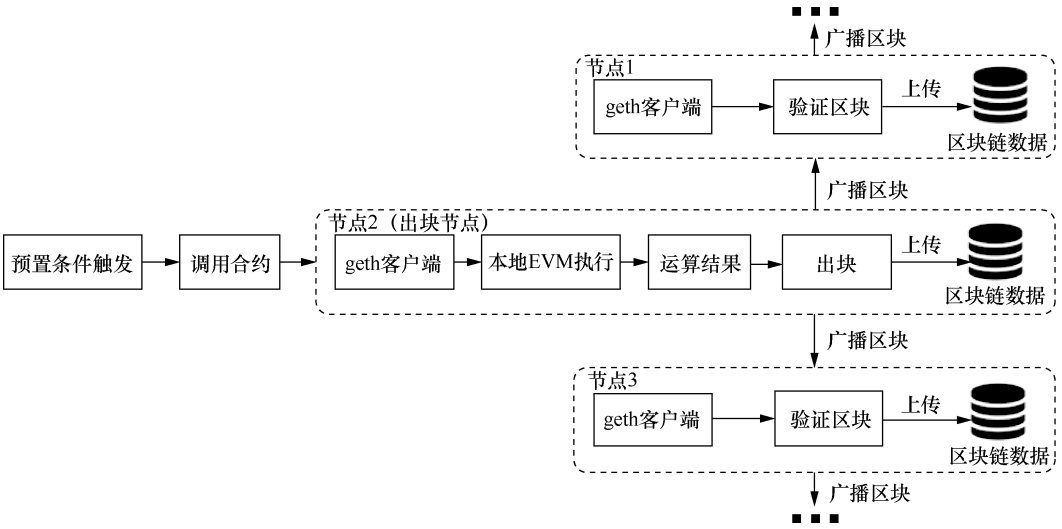


图 6　智能合约的执行流程
Figure 6　Execution process of smart contract

为权限管理机制提供了安全保障。

2) 策略和权限可核查。区块链上的数据公开可查询，这在多方信息共享系统中有着重要作用。策略的透明建立起了参与方对系统安全的信任，避免“后门”问题。权限透明且难以篡改，使通信双方可以在无须第三方背书的情况下建立起信任机制，简化了交易流程，降低了信任成本。

3) 分布式账本。区块链去中心化的思想与大数据时代的分布式环境相符合，区块链中的P2P(peer-to-peer)网络、共识算法和分布式数据库等机制适合应用于分布式架构的系统。同时区块链中的账本分布式地存储各个节点上，增强了系统的健壮性，网络中部分节点出现故障不会影响系统的运行或者造成数据的丢失，也避免了集中式管理带来的针对性攻击问题。

4) 访问策略自动化实现。用户可以根据需求，自定义智能合约并将其部署在区块链上，当有访问请求时，系统会根据智能合约的逻辑策略并依据请求者的属性、角色等信息自动化地判决，且无人工干预。

5) 细粒度访问控制。用户个人数据的访问权限可以通过主体−客体对的形式存储在区块链上，

具备对用户数据进行细粒度划分的能力，访问者被局限在规定的访问边界内，防止了服务商对用户数据的过度收集。链上的信息公开、客体的所有权明确，方便服务商直接对主权方发出请求，同时服务商的操作信息能够以只增不减的方式记录在区块链上，越权访问、泄露数据等行为能够经过日志分析发现，实现安全、透明、高效的数据资源共享。

6) 数据流通可溯源。现有的针对区块链溯源的研究，主要是面对商品或代币的全周期追踪记录。同样可以借鉴这种思想，将用户的数据看作商品，利用链上访问权限和链下的访问日志，结合时间戳和签名信息，联合分析用户数据的全周期流通过程，掌握数据的演变历程，从而溯源越权访问等违规操作。

4.1　基于区块链的访问控制实现机制

目前基于区块链的访问控制技术的主要实现方式有两种：基于交易的访问控制机制和基于智能合约的访问控制机制。

基于交易的访问控制机制核心思想是借助区块链的可信存储特性，将区块链作为访问控制系统内的存储单元，用户通过事务交易（transaction）实现访问权限的授予和撤销，系统通过查询链上的交易能够判断是否允许其他用户的访问。同时可以将访问控制策略、主体和客体信息以及管理员操作日志等数据打包，然后以事务交易的形式存储到区块链上，保证信息的公开透明和不被篡改。

基于智能合约的访问控制机制基本原理是借助区块链的可信计算特性，用户将其访问控制策略转化为智能合约代码上传至区块链，在访问主体满足合约预置的条件时，自动化地赋予其对客体的访问权限，并以交易事务的形式存储在区块链上。进一步拓展，用户可以利用智能合约控制访问主客体之间所有的数据交互过程，实现对主体和客体的属性状态、权限授予溯源信息、策略更新历史记录等所有数据的监督和管理。

4.1.1　基于交易的访问控制机制

基于交易的访问控制机制在区块链研究的早期被提出，是访问控制技术与区块链技术融合的开始。Zyskind 等[27]针对移动应用的数据访问控制需求，提出将访问控制策略以用户与服务商的联合身份 $\mathrm{Compound}_{u,s}^{\mathrm{public}}$ 发布，并将联合身份表示为 $\mathrm{Compound}_{u,s}^{\mathrm{public}}=(\mathrm{pk}_{\mathrm{sig}}^{u,s},\mathrm{pk}_{\mathrm{sig}}^{s,u})$（其中 $\mathrm{pk}_{\mathrm{sig}}^{u,s}$ 代表用户的公钥，$\mathrm{pk}_{\mathrm{sig}}^{s,u}$ 代表服务商的公钥）。该机制的原理如图 7 所示，由于区块链只增不减的特性，规定联合身份最新发布的交易为有效交易，这样通过查找最近的权限交易 T_{access} 就可以实现权限的授予、更改和撤销。通过数据交易 T_{data} 提交服务商的访问请求，并同时将数据的访问操作记录在区块链上，保证访问操作可溯源。该机制巧妙地引入联合身份的概念，使得用户可以针对不同的服务商实现不同类型数据的访问控制策略，同时使用访问控制列表（ACL，access control list）的策略描述方式，适宜低复杂度的访问控制策略、较小数据量的个人数据保护需求。

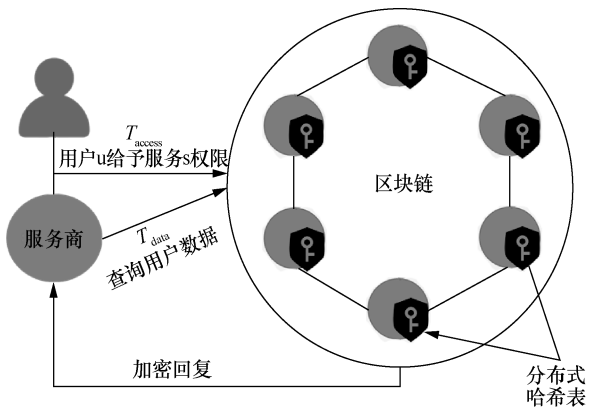


图 7　Zyskind 机制原理
Figure 7　Principle of Zyskind mechanism

文献[28]探索了在物联网背景下，使用多条区块链分类别存储主客体信息和权限决策信息，以实现灵活自动的访问控制决策机制。如图 8 所示，作者提出的 ControlChain 机制规定使用关系链（relationship blockchain）存储主体和客体之间的关系数据，使用上下文链（context blockchain）存储传感器数据、处理后的数据和人为输入的数据。并定义解码器（decoder）用于在自定义的访问控制模型下（RBAC、ABAC、OrBAC 等），将主客体的属性角色数据和关系链中的数据等自动转换为访问控制模块可以直接识别的数据结构类型（ACL 等），并最终将授权决策信息存储在责任链（accountability blockchain），以实现授权的

溯源和问责制度。该机制实现了传统访问控制模型和区块链的融合，可以在用户自定义的访问控制模型下完成访问控制决策。

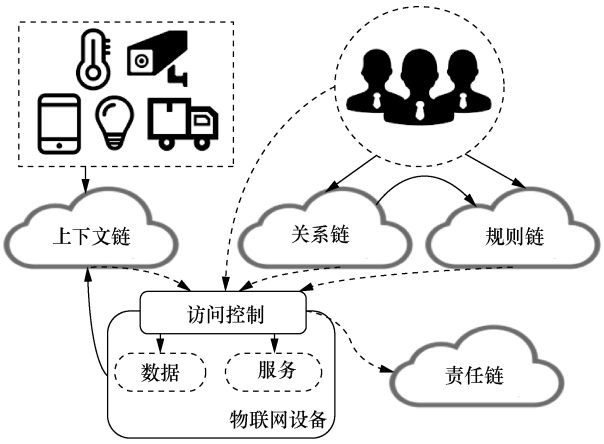


图 8　ControlChain 机制框架
Figure 8　Architecture of ControlChain mechanism

文献[29]提出在链上以交易的形式完成访问控制策略和访问权限的创建、更新和撤销。作者定义了两种类型的交易：一是策略创建交易（PCT，policy creation transaction），用于实现策略的创建；二是权限转移交易（RTT，right transfer transaction），用于实现主体间权限的更替。为了在只增不减的区块链上实现策略的更新和撤销，作者利用区块链的代币机制，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，即每次交易的输入是先前的策略信息和一定的交易费用（比特币），输出是新的策略信息和交易后剩下的费用。同时作者又规定数据操作权限的拥有者 RT（right holder）在进行 RTT 交易时，可以将原有的访问控制策略限制得更加严格，只有在交易方满足条件时才给予其操作权限并完成交易。文献[29]提出的系统模型 Maesa 机制原理如图 9 所示，可以看到区块链在该系统中作为存储组件，通过与策略管理点（PAP）交互，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控制用户与数据资源的交互。该系统通过利用区块链上的交易机制，实现了 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，在数据规模较大时也能满足细粒度的访问控制需求。

总的来说，目前基于交易的访问控制机制通过利用区块链可信存储的特性，可分为以下 4 个方面。

1) 存储访问权限。文献[27, 30]利用区块链公开透明和数据可信的特性，在链上存储访问权限，使得权限的信息公开可查询，可以在无第三方背书的情况下建立信任。同时由于区块链只增不减的特性，链上的权限数据只能以覆盖的方式修改而无法撤回，保证了请求者不能私自越权访问，授权者也不能反悔抵赖。其中文献[30]引入虚拟链（virtualchain）[31-32]的概念，提出通过虚拟链将高级的数据存储功能转化为基础的逻辑存储单元，以实现在不修改区块链数据结构的基础上，将云存储系统的数据以虚拟链的形式有序上链。

2) 存储访问控制策略。文献[33-35]分别提出

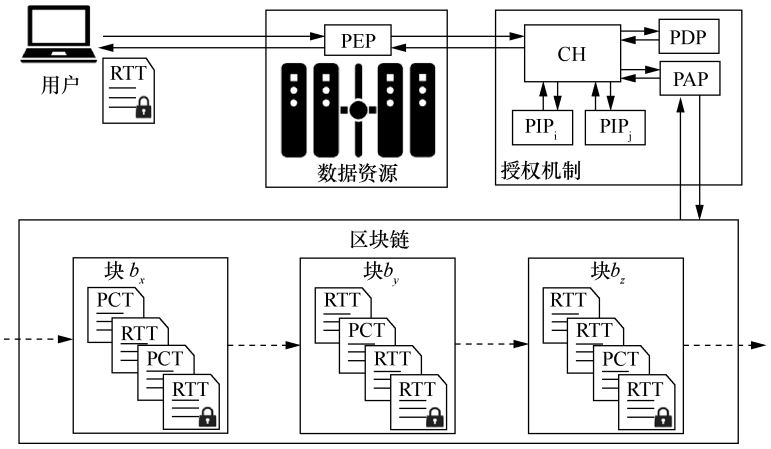


图 9　Maesa 机制原理
Figure 9　Principle of Maesa mechanism

在物联网、云联盟和云存储的环境下将访问控制策略放在区块链上，使得策略公开透明，保证访问控制策略的可信任性，避免存在利用“后门”等暗箱操作的行为。Maesa 等[29]还考虑到访问控制策略的存储空间问题，提出使用自定义的符号映射表，将各类属性映射为固定长度的数值，以实现策略的压缩存储和高效拓展。

3) 存储关键敏感数据。文献[36]利用区块链难以篡改和不可删除的特性，在医疗数据分享中应用区块链技术，保证用以研究的数据真实可靠，不被恶意篡改。Pinno 等[28]则利用区块链分布式特性，在物联网中搭建专门用来存储数据的上下文链（context blockchain），存储分布的传感器数据和人工输入数据。文献[37]提出了一种利用区块链技术实现的防篡改的数据存储管理框架，利用哈希指针树型索引结构实现数据的高效查询。但值得注意的是，考虑到链上信息全透明，在某些需要隐私保护的情景下必须通过某些机制实现“信息隐匿”。同时，由于区块链的共识机制和竞争记账机制，在链上存储大规模数据开销较大，因此多数的基于区块链访问控制系统往往在链下存储原始数据，而在链上只维护数据的分布式哈希表（DHT，distributed hash table）[27, 38]或地址指针等简略信息，以达到在节省链上空间同时保证数据完整性的目的。

4) 存储访问控制操作记录。利用区块链可查、可信、可溯源的特性，建立审计追责系统，实时记录主体的操作记录，以监察授权者的不当授权和操作者的违规操作，同时能够逐级溯源，实现相应的按级惩戒。文献[39]以互联网租车作为背景，提出将租车平台对用户数据的访问记录存储在区块链上，在用户发现个人隐私泄露时，可以此为依据进行溯源，实现对互联网租车软件平台的追责机制。乔蕊等[40-41]则针对动态数据的安全问题，设计了基于区块链的动态数据安全存储机制。以云计算为代表的数据存储技术，有着数据流通快、更新快的特点，带来了攻击行为难界定、数据伪造难发现、数据篡改难定责的问题，乔蕊等首先在文献[40]中提出了动态数据存储体系，通过改进区块链共识机制杜绝攻击者对数据账本的非授权篡改。之后在文献[41]中针对物联网下的数据安全问题引入动态数据存储体系，并将所有的动态操作永久地记录在区块链上，通过双联盟链实现多维授权和动态数据存储，通过冯 • 诺依曼–摩根斯坦效用评估节点的操作收益，并以此为依据结合链上的操作日志找寻攻击节点，实现动态数据攻击溯源。

上述代表性的机制汇总如表 2 所示。

4.1.2　基于智能合约的访问控制机制

随着以太坊上图灵完备的链上脚本的出现，智能合约的应用也得以落地。作为区块链 2.0 架构的核心模块，智能合约使得区块链的应用由“虚拟货币”拓展到更广泛的“交易平台”。在访问控制领域，智能合约通过区块链提供的分布式信用基础设施，将数据的交互作为主体之间的“交易”，这样通过自定义的脚本语言就可以实现可信、细粒度、无人为干预的访问控制机制。

文献[42]提出了使用智能合约的基于角色访问控制框架（RBAC-SC）。该框架利用以太坊平台的智能合约技术，提出跨组织的质询–响应身份验证协议，解决了在跨组织情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

表 2　基于交易的访问控制机制代表文献汇总

Table 2　Summary of representative literature on access control mechanisms based on transaction

文献	核心思想	应用方向	应用场景
[27]	用户与服务商以联合身份发布权限交易，控制权限的授予、更改和撤销	在链上存储访问权限	小数据量的个人数据防护
[28]	使用多条区块链分类别存储主客体信息和权限决策信息，以实现灵活自动的访问控制决策机制	在链上存储访问控制策略以及关键敏感数据	具有多种类型设备的物联网数据防护
[29]	将区块链与 ABAC 模型相结合，利用区块链的代币机制，实现链上的策略和权限的更新	在链上存储访问控制策略与访问权限	大规模数据防护
[41]	通过双联盟链存储访问权限和访问控制操作日志，具备对攻击节点的溯源功能	在链上存储访问权限与访问控制操作日志	物联网中的动态数据防护

色管理和验证机制。作者的思想是利用区块链可信、公开、透明的特点，让用户都通过以太坊上的账户地址或者系统分配的公钥表示，并允许组织可以发布带有签名的角色管理合约。这样跨组织的其他用户就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用户的角色身份，从而实现了跨组织的角色验证。

Zhang 等[43]提出了一种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（如图 10 所示）。

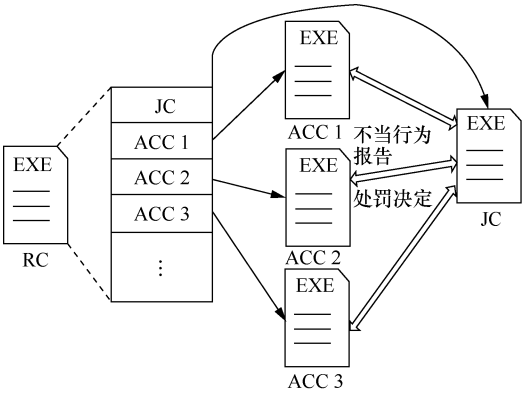


图 10　Zhang Y 机制框架结构
Figure 10　Architecture of Zhang Y mechanism

该框架包含了多个访问控制合约（ACC，access control contract），每一个都实现了访问控制策略中一个主客体对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，judge contract）用以接收不当行为报告并确定相应的惩罚。而注册合约（RC，register contract）则用来管理 JC 和 ACC 并提供它们的简略汇总信息。该机制通过将访问控制策略拆分为多个访问控制合约，可以细化主客体交互行为，有利于访问控制策略的细粒度实现。

在医疗数据保护领域，Azaria 等针对患者数据碎片化严重、交流渠道少、共享效率低、隐私保护机制不完善等问题，提出了 MedRec 框架[44-45]。作者的思想是利用智能合约让病人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。如图 11 所示，作者设计注册合约来管理患者信息，并将患者账户与其汇总合约绑定；汇总合约（SC，summary contract）则用来关联患者的数据权限及其状态；而医患关系合约（PPR，patient provider relationship）负责患者数据的查询及访问权限管理。通过 MedRec 机制，患者在数据库中的数据都被附上相应的操作权限信息，并在患者的 SC 地址上可以查询到相应的 PPR 的状态，这样患者的医疗数据就被严格地控制在患者手中，违法的操作都会因为权限不足而被拒绝。而出于研究目的的医疗数据访问者也可以通过查询 RC 上公开的患者账户地址，向相应的患者提

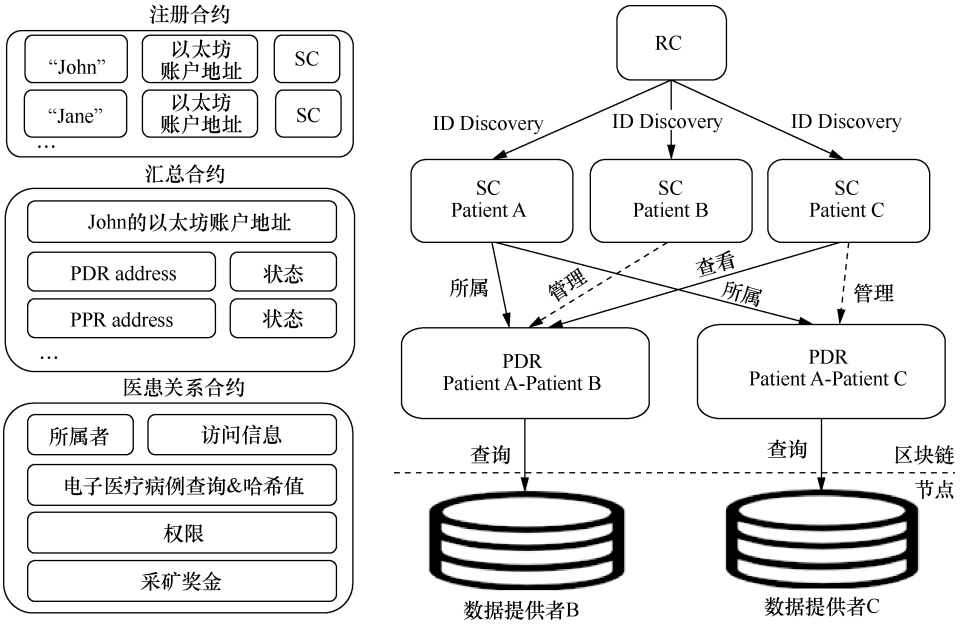


图 11　MedRec 框架结构
Figure 11　Architecture of MedRec

出申请，在经过患者同意后方可访问。同时可以注意到由于区块链的匿名性，虽然链上的数据都是公开的，但患者的身份是通过以太坊账户表示的，而且隐私的医疗数据存储在链下，只有操作权限是公开可查的，这样就在保护了患者隐私的前提下提高了数据的共享率。

文献[46]提出了一种针对大数据资源的访问控制机制 BBAC-BD。作者结合大数据资源的特点，以分布式访问控制需求和访问控制动态性需求为着眼点，利用区块链事务实现访问控制策略的全流程分布式管理，利用智能合约实现策略的自动化判决，利用 ABAC 模型实现基于请求者属性的动态访问控制，有利于大数据资源的灵活管控和安全共享。该机制的工作原理如图 12 所示。

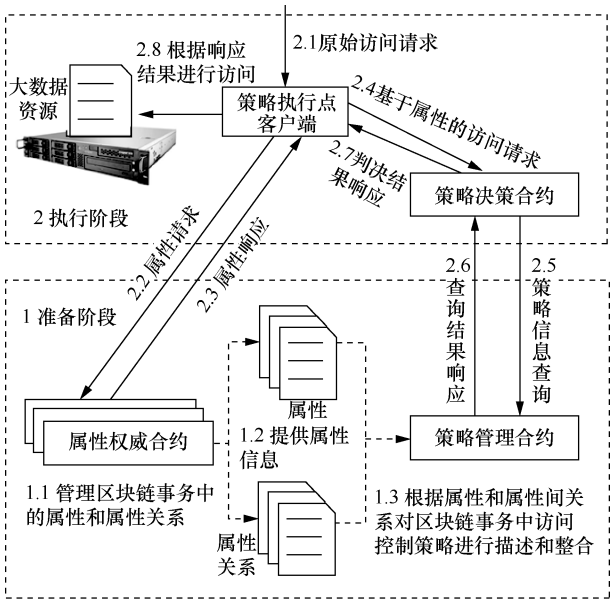


图 12　BBAC-BD 机制原理框架
Figure 12　Architecture of BBAC-BD mechanism

BBAC-BD 工作流程如下。

Step 1　在准备阶段，由属性权威（AA，attribute authority）合约预先收集区块链事务的属性信息，并提供给策略执行点（PEP，policy enforcement point）和策略管理点（PAP，policy administration point）。

Step 2　在 PAP 上的智能合约结合属性信息收集整合区块链事务中的访问控制策略。

Step 3　进入执行阶段，当 PEP 上的代理收到资源操作请求后，根据从 AA 合约得到的信息生成基于属性的访问控制请求（AAR）并将其发往策略决策点（PDP，policy decision point）。

Step 4　PDP 上的智能合约根据从 PAP 合约响应返回的访问控制策略集对操作是否允许进行判决，并将结果发往 PEP。

Step 5　PEP 代理根据判决结果对资源进行操作。

可以看到，该机制中的属性收集与整合、策略管理、访问权限决策都是通过智能合约自动、透明、公开地执行，而且无须第三方背书，降低了信用成本，有利于大数据下主体间资源的高效共享。同时考虑到大数据环境中数据变化快、主体身份复杂的特点，作者对 BBAC-BD 进行了仿真测试，在访问控制策略设计得当的情况下，该系统的判决时延能够满足动态性的需求。

文献[47]针对企业间的数据共享需求，提出了一种基于联盟链的、利用属性基加密（ABE）[48]进行改进的企业级访问控制模型，同样采用了智能合约来实现基于属性的访问控制策略。作者设计利用企业的诚信值来实现共识机制，在降低了企业间的信任成本的同时起到违规惩戒作用。

总体来说，目前基于智能合约的访问控制机制通过利用区块链可信计算的特性，可分为以下 5 个方面。

1) 用户信息管理。文献[42, 44, 49]都是利用智能合约管理系统内的用户，以不可篡改的方式记录用户信息，并将用户与其以太坊地址、公钥等信息绑定，在无第三方背书的情况下保证用户身份的可信任。此外，将主体以以太坊地址或公钥的形式表示，也有利于惩戒机制的追根溯源。

2) 链上数据管理。利用智能合约管理链上的数据，实现包括访问控制策略集、主体访问权限集、主客体属性信息等数据的增添、更新和删除。文献[44]设计的医患关系合约（PPR）针对医疗数据的权限管理问题，将数据所属方、数据请求方、数据指针和访问权限绑定，用户通过改写合约内的属性值，自定义地控制访问控制策略，管理链下存储在数据库内的数据。文献[50]提出的 FairAccess 机制，通过向访问请求方账户发送带有签名的授权令牌的形式进行权限管理，由授权令牌规定能够访问对应的资源，权限的撤销由令牌上的时间戳和约定的失效时间控制。而授权令牌的管理则是通过链上脚本，也就是智能合约进

行。作者在文献[51]中详细地介绍了 FairAccess 框架中如何通过智能合约将访问控制策略转化为授权令牌，并探讨了这一方案的可行性和安全性。

3) 数据整合与查询。区块链上的数据公开透明，任何用户都可以查询链上的访问控制策略，但在数据量较大或者访问控制策略较复杂的情景下，人工在链上查询收集数据的工作量大且效率低，所以可以利用智能合约自动化地整合和归纳链上数据。例如，文献[43]设计的注册合约（RC）将细化的访问控制合约（ACC）汇总，并与法官合约交互（JC），提供了各个 ACC 的接口，自动化地维护着策略实施列表和不当行为惩罚列表，实现了策略和权限的高效查询。文献[44, 49]都设计了具有归纳汇总功能的智能合约，它们通过指针、关键字的形式将患者拥有的所有医疗数据汇总，便于患者直观地了解所有数据的权限授予情况。文献[46]考虑到大数据下访问控制策略分布式存储后查询效率低的问题，提出了基于 Bloom Filter[52]的策略管理合约，通过哈希函数将属性值映射为二进制向量，进而用二进制向量来描述数据集合，根据资源属性的二进制向量是否与策略事务数据块匹配，达到快速筛选关联策略集的目的，整个查询过程通过部署的智能合约进行，公开透明。

4) 违规行为监测。区块链上的数据只增不减，可以通过时间戳、用户签名等方式溯源，这保证了在区块链上运行监视组件和存储访问日志不会被破坏和篡改，因此基于区块链的监测机制可以监察违规行为，并通过惩戒机制的反馈来完善访问控制系统。Ferdous 等[53]针对云环境下的分布式访问控制系统节点的安全性难以保证、访问控制组件易被攻击的问题，提出一种基于区块链的分布式访问控制系统实时监控方案 DRAMS。它通过在分布式访问控制系统节点上搭建数据探针、日志记录合约和行为分析合约，可以在运行时通过智能合约来记录访问行为，并分析其是否符合规定的访问控制策略，并且考虑到存储在链上的日志内可能包含用户的某些敏感信息，存储的日志通过 AES-256 算法加密。

5) 访问权限判决。利用智能合约根据访问请求者的身份、角色、属性等信息判断其是否满足访问控制策略的约束，返回允许、拒绝或者无法判决的结果，整个过程无人工干预，无须第三方背书，依靠在 EVM 中的合约代码执行，为资源拥有者和请求者双方都建立起高信任度。例如文献[46]提出的策略判决合约根据访问请求者的属性集是否满足与其关联的访问控制策略集，将自动化判决并返回允许、拒绝、属性信息不足或策略集不匹配的任一结果。

上述具有代表性的机制汇总如表 3 所示。

4.1.3　基于区块链的访问控制实现机制总结

基于交易的访问控制机制利用区块链可信存储的特性，可从存储访问权限、访问控制策略、关键敏感数据以及访问控制操作记录 4 个方面进行划分。该机制将区块链作为可信存储实体，与传统的访问控制模型结合，解决用户间的信任问题，通用性与移植性较好。同时链上数据公开透明，有利于授权操作的查验与审计。但是该机制依然依赖中心授权服务器发布权限交易，没有完全解决访问控制单点化的问题。

表 3　基于智能合约的访问控制机制代表文献汇总

Table 3　Summary of representative literature on access control mechanism based on smart contract

文献	核心思想	应用方向	应用背景
[42]	利用智能合约管理用户角色，通过合约规定的接口实现对角色身份的查验	利用智能合约实现用户信息管理	具有跨组织数据访问需求的数据防护
[44-45]	设计三种智能合约管理用户信息、医疗数据状态以及访问权限，保证用户可以实时监管个人医疗数据	利用智能合约实现用户信息管理和链上数据管理	用户隐私的个人电子医疗数据防护
[46]	结合 ABAC 模型，利用智能合约实现属性收集与整合、策略管理以及访问权限决策，并实现基于 Bloom Filter 的策略查询功能，能够满足动态访问控制需求	利用智能合约实现数据整合与查询与访问权限判决	具有分布式、动态访问控制需求的数据防护
[53]	通过在区块链节点上搭建数据探针、日志记录合约和行为分析合约来监测用户的数据访问行为	利用智能合约实现违规行为监测	具有访问行为溯源审计需求的分布式访问控制系统

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，从用户信息管理、链上数据管理、数据整合与查询、违规行为监测以及访问权限判决 5 个方面的需求出发，通过开发智能合约，实现自动化、无干预的访问控制操作，其摆脱了对中心授权服务器的依赖，具备更高的安全性。但是该机制下如何实现访问控制策略向智能合约代码的转化，是开发者需要面临的挑战，因此，如何提高该机制的通用性是待解决的问题。

4.2　关键技术分析

基于区块链的访问控制技术有着广泛的应用空间和巨大的应用潜力，但是由于大数据的 4V 特性，目前针对大数据资源的访问控制需求仍存在诸多挑战。基于 2.2 节提出的大数据下访问控制现有的需求，结合目前的研究现状，本文将从动态访问控制、数据存储空间优化和隐私数据保护 3 个方面对现有研究成果进行分析。

4.2.1　动态访问控制

大数据时代，数据动态演变性强且资源流通速度快，静态的访问控制机制无法适应主客体的快速变化，往往会出现控制策略失效或者不匹配的问题，因此解决访问控制的动态性需求显得至关重要。而动态的访问控制机制主要体现在两个方面：一是灵活性，即能够跟随主客体的属性变化，及时准确地制定出适宜的访问控制策略；二是低时延，即在收到访问请求后，能够在一定的时间窗口内完成策略的决策并实行。

文献[54]基于 FairAccess 机制，提出使用机器学习算法改进访问控制策略，通过反馈信息鼓励代理选择更安全的访问控制方法，并将相关信息更新到智能合约上。机器学习组件的调用不依赖访问控制模型，反馈信息基于客体数据是否收到损坏，因此能够应用于多种访问控制框架，实现动态优化和自调整的安全策略。刘敖迪等[46]则着手于大数据下的动态访问控制需求，使用 ABAC 模型以适应大数据下资源种类繁多、主客体属性变化快的特点，资源拥有者根据资源属性制定访问控制策略，提高访问控制的适应性和灵活性。同时为了提高系统的响应速度，利用智能合约实现基于 Bloom Filter 的访问控制策略管理机制，以允许低概率的误差为代价减少存储空间，同时提高查询的效率以降低检索的时延。Decker 等[55]引入区块链中微支付通道的概念，提出在链下构建用户之间的低时延传输通道，区块链只在通道的设置和关闭时对双方进行交易保障，从而实现用户间链下动态交易以及链上资产担保，但是该机制下用户交易的数据必须是提前经过区块链确认锁定的。

除此之外，改进区块链的共识机制以更快速地达成共识和完成记账也是降低系统时延的有效手段。根据 3.3 节的分析，区块链的共识机制决定了链上权限交易的写入和验证速度，选择适用的共识协议，能够在符合安全需求的限定条件下达到权限信息快速记账并确认的目的，从而提升整个系统的响应速度。

薛腾飞等[56]提出的 MDSN 框架通过使用 DPoS 共识机制，并将其与具备信誉机制的医疗和审计服务器联盟结合，减轻了节点的计算压力，有效提升了访问控制系统的响应速度。此外，闵新平等[57]针对区块链共识机制中存在的算力消耗大、交易时延高、数据吞吐量低的问题，提出许可链多中心动态共识机制(PBCM)。作者首先构建主从多链结构，其中，从链负责存储交易数据，主链负责维护已经确认的交易的摘要，同时提出了基于 PBFT 机制改进的多主节点 PBFT 协议（MPBFT），利用该协议实现构成多链的多节点之间的共识。PBCM 机制有效克服了 PoW 等机制存在的时延高，能耗大的问题，在具备动态响应需求的数字资产存储、管理、保护领域有着独有的优势，但是该机制局限于许可链，只能在具备一定可信度的环境下才能应用，具有一定的局限性。共识协议达成共识的速度与区块链的抗攻击能力是矛盾的，更快地达成共识意味着数据的验证过程更加简化，因此基于区块链的访问控制系统在选择共识协议组件时，必须结合实际的应用场景，在安全阈值内选择适用的共识机制。

4.2.2　数据存储空间优化

区块链作为只增不减的分布式账本，账本的多副本特性需要大量的额外存储空间[58]，上链的数据不仅要通过共识协议消耗巨大算力，实现一致性记账，还要永久地存储在区块上增加维护成本，因此如何在受限的存储空间内高效安全地完

成权限交易的记录成为重要的研究问题。尤其是在物联网等资源受限的场景下，存储空间的优化显得至关重要。

目前主流的解决思路有两个：一是通过提前规定的数据格式或者字符映射，实现数据的压缩存储；二是将原始数据存储在链下，链上只存储必要的简略信息或关键字。文献[29]提出了一种自定义的编码格式用来压缩存储到区块链上的访问控制策略数据，它通过字符映射表将复杂的策略数据、属性名称和操作信息表示为定长的字符码，在实现压缩存储的同时实现基于关键字的高效查询。而文献[27, 37-38, 44]则是选择将包含大量数据的访问控制事务存储在链外，仅向区块链上传指向链外的哈希值。这个解决方案的好处是可以有效减少链上的数据量，但缺点是链外的数据不再受区块链技术保护，数据的存储由本地的数据库单点负责，不再具有分布式账本的可靠性，在发生单点故障时会导致指针失效，影响整个访问控制系统的正常运行。Poon 等[59]在微支付通道的基础上提出的闪电网络，其核心思想是在用户间构建链下支付通道，链上只存储简略信息保证双方的可信性，从而大大提高用户间交易的吞吐量。该机制的思想同样可以应用于访问控制系统中用户间策略数据的交换，通过用户间“私信”的方式实现低开销的数据存储交换，但是其安全性也相应地减弱。

除此之外，有学者从数据区块的结构着手，通过增加区块的数据量来缓解存储压力。Eyal 等[60]提出的 Bitcoin-NG 区块链架构，增加了微区块的概念，选举出的首领节点可以在预先划分的时间窗口内向区块链附加多个微区块，从而提高单位时间内区块链的存储空间。如图 13 所示，其中正方形表示的是关键区块，圆形表示的是微区块，微区块使用与关键区块的公钥相对应的私钥签名，在规定的时间内以恒定的速度产生。该机制通过关键区块选举首领节点，它的产生仍需要 PoW 机制，但是微区块的产生只需首领的签名，所以微区块并不会增加区块链的重量，增强了区块链的存储能力。但是微区块上数据的准确性仅由其首领节点负责，首领的选举过程显得至关重要，因此更适用于具备许可准入机制的联盟链环境中。此外，文献[61]提出的 GHOST 规则通过改进区块链节点构建方式，以重建区块链的方法提高了交易的吞吐量。

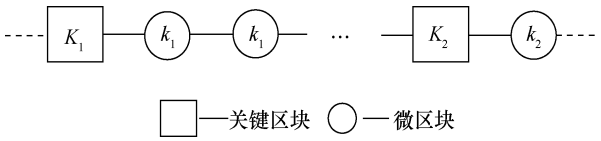


图 13　Bitcoin-NG 区块链架构
Figure 13　Architecture of Bitcoin-NG

4.2.3　隐私数据保护

区块链是完全公开透明的系统，链上的交易和智能合约暴露给所有的用户，这在增强系统公信度的同时给用户的隐私带来了隐患。虽然区块链具有匿名性，但是实际情况下攻击者可以根据链上公开的交易信息，通过数据挖掘的方式获得用户的各种特征，从而锁定用户身份，文献[62-63]证明了通过分析加密货币的交易图结构进行去匿名攻击的可行性。除此之外，对用户敏感数据的管理，更要求系统具有隐私保护的功能，如文献[44-45, 49, 64]等针对医疗数据共享的研究，系统具有完善的隐私保护机制是用户选择使用此系统并提高数据共享率的必然要求。因此，此方面的研究也受到了诸多学者的关注。

Zyskind 等[38]针对区块链数据的隐私安全管理，将哈希指针与安全多方计算（MPC，multi-party computation）相结合，提出了分布式的数据管理框架 Enigma。针对不同的隐私保护需求，Enigma 将数据的管理分为 Public ledger、DHT 和 MPC 共 3 种类型，其中链上 Public ledger 的数据对全部用户公开，而 DHT 和 MPC 的数据只在链上存储数据的哈希指针。DHT 的数据具有一定的隐私保护，它只在链上存储对数据的引用，同时通过哈希函数校验链下数据是否被篡改。而 MPC 的数据通过使用安全多方计算[65]、数据的查询以分布式进行，数据被分割到不同的节点进行处理，没有任何一方能够访问全部数据，从而在无须第三方背书的情况下实现敏感数据的存储和运算。

Kosba 等[66]同样针对区块链的隐私保护问题，提出了智能合约开发平台 Hawk。与 Zerocash 类似，Hawk 采用 zk-SNARK 零知识证明技术[63]，用来保证在验证过程中矿工可以在不知道交易的具体信息的情况下判定交易的有效性，从而实现

对交易中敏感信息的隐私保护。Hawk 平台原理架构如图 14 所示，Hawk 借鉴了 Zerocash 中的 mint（铸币）和 pour（消费）操作，用户可以通过这两个操作来隐匿智能合约中的交易地址。根据数据的敏感性，用户将负责交易数据的智能合约划分为公开部分和私密部分，通过编程人员开发的编译器自动转化为“秘密合约”。代理人则作为用户的代理，在不透露用户身份的前提下代替用户进行交易。

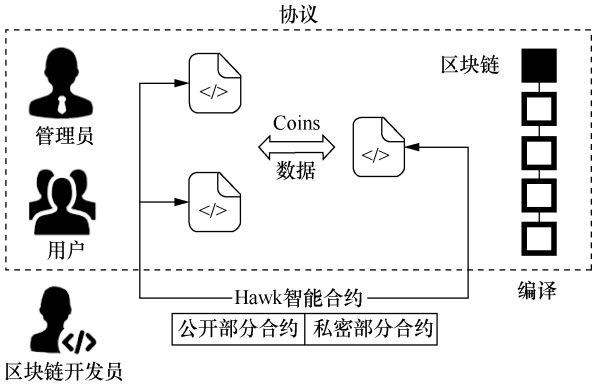


图 14　Hawk 平台原理架构
Figure 14　Principle of Hawk platform

此外，有学者利用密码学技术对区块链数据进行加密，实现用户的隐私保护。Le 等[67]则将密码加密技术与区块链结合，提出了针对物联网设备隐私保护需求的 CapChain 框架。它采用 FairAccess 机制中授权令牌的形式对物联网设备进行权限管理，同时采用密码学知识，通过公钥地址、一次性地址和域地址进行交易，来预防针对用户交易地址的关联分析。文献[68]同样将密码学知识与区块链结合，提出了通过多密钥生成中心(KGC)的群签名隐匿交易节点身份信息，实现链上用户的匿名保护，但目前该机制是以联盟链为基础，无法拓展到完全公开的公共链。李少卓等[69]提出了一种基于 RSA 的区块链按需披露隐私保护机制（PPM-ODB），通过 Quorum 链实现了隐私信息持有者和知情者间的密钥分发，支持知情者的匿名分析、隐私信息的加密解密以及数据的流通追溯。

属性基加密（ABE）作为一种新兴的加密技术，实现了一对多的通信加密，适用于解决分布式环境的数据保护需求，可以解决区块链的隐私保护问题。ABE 以属性为公钥，将密文和用户私钥与属性关联，能够灵活地表示访问控制策略，可以低开销地实现密文的加解密。田有亮等[70]基于 Waters 的 CP-ABE 方案[71-72]，提出基于属性加密的区块链数据溯源算法，针对溯源信息难以动态共享这一问题，通过改进的属性加密算法完成对交易的隐私保护，该数据加密方式具有通用性，同样可以应用在其他区块链系统。邱云翔等[73]同样提出了一种基于 CP-ABE 算法的区块链数据访问控制方案，并结合超级账本平台上原有的 Fabric CA 模块支持密钥的管理工作，实现了用户属性私钥的安全分发。

将上述不同需求下的代表文献及其核心思想总结如表 4 所示。

表 4　不同访问需求下的代表文献总结
Table 4　Summary of representative literature under different access requirements

访问控制需求	核心思想	文献
动态访问控制	利用机器学习算法动态调整访问控制策略	[54]
	基于 ABAC 模型，利用 Bloom Filter 降低策略查询时延	[46]
	提出使用微支付通道，允许用户在线下交换动态数据	[55]
	改进共识算法以达到更快的决策速度，降低时延	[56-57]
存储空间优化	使用自定义的编码格式压缩数据集	[29]
	使用链下存储，链上摘要的方式减少数据量	[27,37-38,44]
	利用微支付通道直接交易数据，不在链上占据空间	[59]
	改进数据区块结构和共识算法，达到在单位时间内产生更多数据区块的目的	[60-61]
隐私数据保护	敏感数据存储在链下、链上根据哈希值校验是否被篡改	[27,44,49]
	结合多方安全计算，在不泄露秘密的前提下将数据集分割后处理	[38]
	利用零知识证明技术，在不泄露敏感信息的前提下确认交易有效性	[66]
	利用密码学知识，加密用户信息	[67-70,73]

5　基于区块链的访问控制技术研究展望

（1）提升通用性与可移植性

访问控制技术经过几十年的发展，提出了诸多优良的访问控制模型，并且经过应用证明其访问控制机制的可行性，同时已经广泛应用在现有的系统上。若能对已有的访问控制系统进行改进，使区块链技术与其结合，在保证原功能的基础上实现数据上链，便能利用区块链分布式存储、透明公开、难以篡改的特性，增强系统的安全性和可信性。因此，如何设计区块链系统使其拥有较好的通用性，能够通过接口与现有的访问控制系统互联，并对各类访问控制模型都拥有完善的处理机制，成为研究的一个重点内容。

此外，如何实现可拓展访问控制标记语言（XACML）向智能合约代码的转化也是值得研究的一个方向。XACML 作为一种通用的访问控制策略定义语言，标准化地描述各个系统间的访问控制策略和过程。如果实现了 XACML 向智能合约代码的高效转化机制，那么就能实现基于 XACML 框架的访问控制系统向区块链的迁移，而且标准化的描述语言还能保证迁移后的系统仍具备与其他系统的互操作性。

（2）跨域与跨链访问

大数据环境下，网络中存在诸多各自封闭的可信域，如何利用区块链公开可信的技术，“链通”各个可信域，建立起低成本的信任机制，满足用户的跨域访问控制需求，也是研究的重点方向。目前针对单链的跨域认证与访问控制，已经取得一定的研究进展[74-77]。但是，在大数据庞大的数据管理需求下，只通过一条区块链实现所有的数据管理是不现实的，必然需要多条链并行运作实现各个组织下的数据管理机制。如何链接起多条区块链，解决访问控制策略冲突、用户身份重复、智能合约不通用等问题，也是实现跨链的协同数据管理需要解决的难题。

（3）访问控制性能优化

区块链诞生的最初目的是作为比特币的底层技术，服务于电子货币的，其挖矿机制并不适宜访问控制需求，同样在以太坊平台上也面临着区块产生过慢、数据存储开销过大的问题，这直接制约了基于区块链的访问控制系统的性能。同时，根据 Seth 等提出的 CAP 理论[78]，区块链在满足分区容错性的前提下，必须在一致性和可用性之间进行权衡，即必须在安全性和高效性之间进行取舍。因此，如何改进区块链的共识机制、记账机制和存储结构等，使其适宜访问控制需求也是未来必须解决的一个问题。

（4）数据隐私保护

区块链作为公开的账本，在应用中必须考虑对敏感关键数据的隐私保护，虽然已有研究者提出通过同态加密、属性基加密等机制实现对链上交易信息的保护，但是这些加密算法的引入带来了计算开销，必然会引起额外的响应时延。如何设计适用于区块链的分布式密码协议，是解决这一性能瓶颈的研究重点。此外，区块链上共识机制要求相关验证节点能够获取到交易信息，恶意节点虽然无法影响共识的达成，但是依旧可以获取所有的账本数据，虽然零知识证明可以避免这个问题，但是其也需要较大的算力支持，在现有的 ZCash 平台上这一过程需要 30~40 s，并且其安全性未得到证实，这也是需要继续进行研究的方向。

（5）区块链+人工智能

将人工智能引入基于区块链的访问控制机制中，可以在减少开发员工作量的同时进一步提升系统的安全性。首先可以利用深度学习算法改进访问控制策略，优化授权范围，解决访问策略冲突问题。其次可以利用人工智能算法对开发的智能合约代码进行漏洞分析，保证合约执行结果的可靠性和完备性。最后可以研究基于人工智能的共识机制，利用机器学习算法分配计算资源，加快共识达成速度，减少授权请求响应时间。

6　结束语

大数据环境下信息流通快，存在着数据主权难维护、访问权限难界定、第三方泄露难防范等问题，给现有的访问控制机制带来了挑战。而基于区块链的访问控制机制利用区块链公开透明、可信度高、难以篡改的特点，能够实现去中心化的访问控制管理。本文从基于区块链实现机制出发，总结了现有的基于交易和基于智能合约的访

问控制机制，重点分析了动态访问控制、链上空间优化和隐私数据保护 3 个关键技术，并结合现有的研究展望，基于区块链的访问控制技术面临的挑战，以期对未来的研究提供参考与启发。总体而言，目前国内基于区块链的访问控制机制仍处于研究的初步阶段，尚未形成统一的技术标准与成熟的技术方案，在云租户数据管理、物联网数据保护、医疗信息共享、企业数据管理等领域仍有广阔的研究空间。

参考文献：

[1] 李昊, 张敏, 冯登国, 等. 大数据访问控制研究[J]. 计算机学报, 2017, 40(1): 72-91.
LI H, ZHANG M, FENG D G, et al. Research on access control of big data[J]. Chinese Journal of Computers, 2017, 40(01): 72-91.

[2] 信息通信研究院. 大数据安全白皮书[EB]
China Academy of Information and Communications Technology. White paper of big data security[EB].

[3] 沈海波, 洪帆. 访问控制模型研究综述[J]. 计算机应用研究, 2005, 22(6): 9-11.
SHEN H B, HONG F. Survey of research on access control model[J]. Application Research of Computers, 2005, 22(6): 9-11.

[4] 李国杰, 程学旗. 大数据研究：未来科技及经济社会发展的重大战略领域——大数据的研究现状与科学思考[J]. 中国科学院院刊, 2012, 27(6): 647-657.
LI G J, CHENG X Q. Research status and scientific thinking of big data[J]. Strategy & Policy Decision Research, 2012, 27(6): 647-657.

[5] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB].

[6] 方巍, 郑玉, 徐江. 大数据: 概念、技术及应用研究综述[J]. 南京信息工程大学学报(自然科学版), 2014, 6(5): 405-419.
FANG W, ZHENG Y, XU J. Big data: Conceptions，key technologies and application[J]. Journal of Nanjing University of Information Technology (Natural Science Edition), 2014, 6(5): 405-419.

[7] 张锐卿, 汤泰鼎, 万可. 大数据环境下细粒度的访问控制与审计管理[J]. 信息安全研究, 2017, 3(6): 509-516.
ZHANG R Q, TANG T D, WAN K. Fine-grained access control and audit management in big data environment[J]. Journal of Information Security Research, 2017, 3(6): 509-516.

[8] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[9] YUAN E, TONG J. Attributed based access control (ABAC) for web services[C]//IEEE International Conference on Web Services (ICWS'05). 2005.

[10] THOMAS R K, SANDHU R S. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management[M]//Database Security XI. Berlin: Springer. 1998: 166-81.

[11] 邓集波, 洪帆. 基于任务的访问控制模型[J]. 软件学报, 2003, 14(1): 76-82.
DENG J B, HONG F. Task-based access control model[J]. Journal of Software, 2003, 14(1): 76-82.

[12] MOLLOY I, HONG C, LI T, et al. Mining roles with multiple objectives[J]. ACM Transactions on Information & System Security, 2010, 13(4): 1-35.

[13] MOLLOY I, LI N, YUAN Q, et al. Mining roles with noisy data[C]//Proceedings of the 15th ACM Symposium on Access Control Models and Technologies. 2010: 45-54.

[14] MOLLOY I, CHARI S. Generative models for access control policies: applications to role mining over logs with attribution[C]//Proceedings of the 17th ACM Symposium on Access Control Models and Technologies. 2012: 45-56.

[15] 聂伯敏, 熊桂喜. 分布式环境下基于角色访问控制的实现[J]. 计算机工程, 2002, 28(8): 181-183.
NIE B M, XIONG G X. Implementation of role-based access control in distributed environment[J]. Computer Engineering, 2002, 28(8): 181-183.

[16] LONGSTAFF J, NOBLE J. Attribute based access control for big data applications by query modification[C]//IEEE Second International Conference on Big Data Computing Service and Applications (BigDataService). 2016: 58-65.

[17] BHATT S, PATWA F, SANDHU R. ABAC with group attributes and attribute hierarchies utilizing the policy machine[C]//Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control. 2017: 17-28.

[18] 惠榛, 李昊, 张敏, 等. 面向医疗大数据的风险自适应的访问控制模型[J]. 通信学报, 2015, 36(12): 190-199.
HUI Z, LI H, ZHANG M, et al. Risk-adaptive access control model for big data in healthcare[J]. Journal on Communications, 2015, 36(12): 190-199.

[19] SANTOS D R D, WESTPHALL C M, WESTPHALL C B. A dynamic risk-based access control architecture for cloud computing[C]//IEEE Network Operations and Management Symposium (NOMS). 2014: 1-9.

[20] 何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述[J]. 计算机科学, 2017, 44(4): 1-7, 15.
HE P, YU G, ZHANG Y F, et al. Survey on blockchain technology and its application prospect[J]. Computer Science, 2017, 44(4): 1-7, 15.

[21] 邹均, 张海宁. 区块链技术指南[M]. 北京: 机械工业出版社. 2017.
ZOU J, ZHANG H N. Blockchain technology guide[M]. Beijing: Machinery Industry Press. 2017.

[22] SWAN M. Blockchain: blueprint for a new economy[M]. O'Reilly Media, Inc, 2015.

[23] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3): 382-401.

[24] FISCHER M J, LYNCH N A, PATERSON M S. Impossibility of distributed consensus with one faluty process[J]. ACM Tocs, 1985, 32(2): 374-382.

[25] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//IEEE International Congress on Big Data (BigData Congress). 2017: 557-564.

[26] TAPSCOTT D, TAPSCOTT A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world[M]. Penguin, 2016.

[27] 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.

[28] PINNO O J A, GRéGIO A, BONA L C E D. ControlChain: blockchain as a central enabler for access control authorizations in the IoT[C]//Globecom IEEE Global Communications Conference. 2017: 1-6.

[29] 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.

[30] SHAFAGH H, BURKHALTER L, HITHNAWI A, et al. Towards blockchain-based auditable storage and sharing of IoT data[C]//Proceedings of the 2017 on Cloud Computing Security Workshop. 2017: 45-50.

[31] ALI M, NELSON J, SHEA R, et al. Blockstack: a global naming and storage system secured by blockchains[C]//2016 USENIX Annual Technical Conference. 2016: 181-194.

[32] NELSON J, ALI M, SHEA R, et al. Extending existing blockchains with virtualchain[C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.

[33] DORRI A, KANHERE S S, JURDAK R, et al. Blockchain for IoT security and privacy: The case study of a smart home[C]//IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). 2017: 618-623.

[34] ALANSARI S, PACI F, SASSONE V. A distributed access control system for cloud federations[C]//IEEE 37th International Conference on Distributed Computing Systems (ICDCS). 2017: 2131-2136.

[35] JEMEL M, SERHROUCHNI A. Decentralized access control mechanism with temporal dimension based on blockchain[C]// IEEE 14th International Conference on e-Business Engineering (ICEBE). 2017: 177-182.

[36] JIE Z, XUE N, XIN H. A secure system for pervasive social network-based healthcare[J]. IEEE Access, 2016, 4(99): 9239-9250.

[37] 焦通, 申德荣, 聂铁铮, 等. 区块链数据库:一种可查询且防篡改的数据库[J]. 软件学报, 2019, 30(9): 2671-2685.
JIAO T, SHEN D R, NIE T Z, et al. BlockchainDB: querable and immutable database[J]. Journal of Software, 2019, 30(09): 2671-2685.

[38] ZYSKIND G, NATHAN O, PENTLAND A. Enigma: decentralized computation platform with guaranteed privacy[J]. arXiv preprint arXiv:150603471, 2015.

[39] 章宁, 钟珊. 基于区块链的个人隐私保护机制[J]. 计算机应用, 2017, 37(10): 2787-2793.
ZHANG N, ZHONG S. Mechanism of personal privacy protection based on blockchain[J]. Journal of Computer Applications, 2017, 37(10): 2787-2793.

[40] 乔蕊, 董仕, 魏强, 等. 基于区块链技术的动态数据存储安全机制研究[J]. 计算机科学, 2018, 45(2): 57-62.
QIAO R, DONG S, WEI Q, et al. Blockchain based secure storage scheme of dynamic data[J]. Computer Science, 2018, 45(2): 57-62.

[41] 乔蕊, 曹琰, 王清贤. 基于联盟链的物联网动态数据溯源机制[J]. 软件学报, 2019, 30(6): 1614-1631.
QIAO R, CAO Y, WANG Q X. Traceability mechanism of dynamic data in Internet of things based on consortium blockchain[J]. Journal of Software, 2019, 30(6): 1614-1631.

[42] CRUZ J P, KAJI Y, YANAI N. RBAC-SC: role-based access control using smart contract[J]. IEEE Access, 2018, 6: 12240-12251.

[43] 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.

[44] AZARIA A, EKBLAW A, VIEIRA T, et al. Medrec: using blockchain for medical data access and permission management[C]//2016 2nd International Conference on Open and Big Data (OBD). 2016: 25-30.

[45] EKBLAW A, AZARIA A, HALAMKA J D, et al. A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data[C]//Proceedings of IEEE Open & Big Data Conference. 2016.

[46] 刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654.
LIU A D, DU X H, WANG N, et al. A blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654.

[47] 王秀利, 江晓舟, 李洋. 应用区块链的数据访问控制与共享模型[J]. 软件学报, 2019, 30(6): 1661-1669.
WANG X L, JIANG X Z, LI Y. Model for data access control and sharing based on blockchain[J]. Journal of Software, 2019, 30(6): 1661-1669.

[48] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2005: 457-473.

[49] DAGHER G G, MOHLER J, MILOJKOVIC M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cities & Society, 2018, 39: 283-297.

[50] OUADDAH A, ABOU ELKALAM A, AIT OUAHMAN A. FairAccess: a new Blockchain-based access control framework for the Internet of Things[J]. Security & Communication Networks, 2016, 9(18): 5943-5964.

[51] OUADDAH A, EL KALAM A A, OUAHMAN A A. Harnessing the power of blockchain technology to solve IoT security & privacy issues[C]//Proceedings of the ICC. 2017.

[52] BLOOM B H. Space/Time trade-offs in hash coding with allowable errors[J]. Ipsj Magazine, 1970, 12(7): 422-426.

[53] FERDOUS M S, MARGHERI A, PACI F, et al. Decentralised runtime monitoring for access control systems in cloud federations[C]//IEEE 37th International Conference on Distributed Computing Systems (ICDCS). 2017: 2632-2633.

[54] OUTCHAKOUCHT A, HAMZA E, LEROY J P. Dynamic access control policy based on blockchain and machine learning for the Internet of Things[J]. Int J Adv Comput Sci Appl, 2017, 8(7): 417-424.

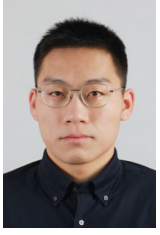
[55] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]// Symposium on Self-Stabilizing Systems. 2015: 3-18.

[56] 薛腾飞, 傅群超, 王枞, 等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报, 2017, 43(9): 1555-1562.
XUE T F, FU Q C, WANG Z, et al. A medical data sharing model via blockchain[J]. ACTA Automatica Sinca, 2017, 43(9): 1555-1562.

[57] 闵新平, 李庆忠, 孔兰菊, 等. 许可链多中心动态共识机制[J].

计算机学报, 2018, 41(05): 1005-1020.
MIN X P, LI Q Z, KONG L J, et al. Permissioned blockchain dynamic consensus mechanism based multi-centers[J]. Chinese Journal of Computers, 2018, 41(5): 1005-1020.
[58] 蔡振华, 林嘉韵, 刘芳. 区块链存储：技术与挑战[J]. 网络与信息安全学报, 2020, 6(5): 11-20.
CAI Z H, LIN J Y, LIU F. Blockchain storage: technologies and challenges[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 11-20.
[59] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[R]. 2016.
[60] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//Usenix Conference on Networked Systems Design and Implementation. 2016: 45-59.
[61] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in bitcoin[C]//International Conference on Financial Cryptography and Data Security. 2015: 507-527.
[62] RON D, SHAMIR A. Quantitative analysis of the full bitcoin transaction graph[C]//International Conference on Financial Cryptography and Data Security. 2013: 6-24.
[63] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy. 2014: 459-474.
[64] QI X, SIFAH E B, ASAMOAH K O, et al. MeDShare: trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5(99): 14757-14767.
[65] YAO C C. How to generate and exchange secrets[C]//27th Annual Symposium on Foundations of Computer Science (SFCS 1986). 1986: 162-167.
[66] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//IEEE Symposium on Security and Privacy (SP). 2016: 839-858.
[67] LE T, MUTKA M W. CapChain: a privacy preserving access control framework based on blockchain for pervasive environments[C]//IEEE International Conference on Smart Computing (SMARTCOMP). 2018: 57-64.
[68] 杨亚涛, 蔡居良, 张筱薇, 等. 基于SM9算法可证明安全的区块链隐私保护方案[J]. 软件学报, 2019, 30(6): 1692-1704.
YANG Y T, CAI J L, ZHANG X W, et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software, 2019, 30(6): 1692-1704.
[69] 李少卓, 王娜, 杜学绘. 按需披露的区块链隐私保护机制[J]. 网络与信息安全学报, 2020, 6(3): 19-29.
LI S Z, WANG N, DU X H. Privacy protection mechanism of on-demand disclosure on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 19-29.
[70] 田有亮, 杨科迪, 王缵, 等. 基于属性加密的区块链数据溯源算法[J]. 通信学报, 2019, 40(11): 101-111.
TIAN Y L, YANG K D, WANG Z, et al. Algorithm of blockchain data provenance based on ABE[J]. Journal on Communications, 2019, 40(11): 101-111.
[71] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]//International Workshop on Public Key Cryptography. 2011: 53-70.
[72] SAHAI A, SEYALIOGLU H, WATERS B. Dynamic credentials and ciphertext delegation for attribute-based encryption[C]//Annual Cryptology Conference. 2012: 199-217.
[73] 邱云翔, 张红霞, 曹琪, 等. 基于 CP-ABE 算法的区块链数据访问控制方案[J]. 网络与信息安全学报, 2020, 6(3): 88-98.
QIU Y X, ZHANG H X, CAO Q, et al. Blockchain data access control scheme based on CP-ABE algorithm[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 88-98.
[74] 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案[J]. 电子学报, 2018, 46(11): 2571-2579.
MA X T, MA W P, LIU X X. A cross domain authentication scheme based on blockchain technology[J]. Chinese Journal of Electronics, 2018, 46(11): 2571-2579.
[75] 周致成, 李立新, 李作辉. 基于区块链技术的高效跨域认证方案[J]. 计算机应用, 2018, 38(2): 316-320, 326.
ZHOU Z C, LI L X, LI Z H. Efficient cross-domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications, 2018, 38(2): 316-320, 326.
[76] LI C, WU Q, LI H, et al. Trustroam: A novel blockchain-based cross-domain authentication scheme for wi-fi access[C]//International Conference on Wireless Algorithms, Systems, and Applications. 2019: 149-161.
[77] YAO Y, CHANG X, MIŠIĆ J, et al. BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. IEEE Internet of Things Journal, 2019, 6(2): 3775-3784.
[78] GILBERT S, LYNCH N. Perspectives on the CAP Theorem[J]. Computer, 2012, 45(2): 30-36.

[作者简介]



高振升（1995– ），男，河南洛阳人，信息工程大学硕士生，主要研究方向为信息安全、区块链。

曹利峰（1981– ），男，河南禹州人，信息工程大学副教授，主要研究方向为网络安全、信息安全。

杜学绘（1968– ），女，河南新乡人，博士，信息工程大学教授、博士生导师，主要研究方向为大数据安全、云计算安全、信息系统多级安全。