doi:10.11835/j.issn.1000-582X.2026.06.009
引用格式:韩永征,胡春强 . 基于区块链的体域网动态信任委托访问控制研究[J]. 重庆大学学报, 2026,49(6): 93-102.

基于区块链的体域网动态信任委托访问控制研究

韩永征[1],胡春强[2]
(1. 重庆城市管理职业学院 大数据与信息产业学院 重庆 401331; 2. 重庆大学 大数据与软件学院,重庆 400044)

摘要:传统访问控制模型在体域网环境中面临单点故障、权限僵化及动态授权困难等挑战。针对这些挑战,文中提出一种基于区块链的体域网动态信任委托访问控制模型。该模型设计了轻量级双层区块链架构,通过主链管理全局策略与子链处理具体业务分离,有效降低存储与计算开销;构建了多智能合约协同的访问控制逻辑,实现委托授权的自动化管理与执行;引入动态信任评估机制,融合身份可信度、行为历史及实时生理上下文,实现权限的动态调整。通过实验分析,该模型能显著降低权限验证与紧急访问的延迟,提升委托操作成功率,并有效减少存储开销,从而为资源受限的体域网环境提供安全、高效且灵活的访问控制支持。

关键词:体域网;区块链;访问控制;委托授权;动态信任评估;智能合约
中图分类号:TP393.08 **文献标志码:**A **文章编号:**1000-582X(2026)06-093-10

Blockchain-based dynamic trust delegation access control for body area networks

HAN Yongzheng[1], *HU Chunqiang*[2]
(1. School of Big Data and Information Industry, Chongqing City Management College, Chongqing 401331, P. R. China; 2. School of Big Data & Software Engineering, Chongqing University, Chongqing 400044, P. R. China)

Abstract: In body area network (BAN) environments, traditional access control models face challenges such as single points of failure, rigid permission structures, and limited support for dynamic authorization. To address these challenges, this study proposes a blockchain-based dynamic trust delegation access control model for BANs. To effectively reduce storage and computational overhead, a lightweight two-layer blockchain architecture is designed, in which global policy management is maintained on the main chain, while specific service operations are processed on the subchain. In addition, a multi-smart-contract access control framework is developed to enable the automated management and execution of delegated authorization. To support dynamic permission adjustment, a trust evaluation mechanism integrating identity credibility, behavioral history, and real-time physiological context is further introduced. Experimental results show that the proposed model significantly reduces permission verification delay and emergency access latency, improve the success rate of delegation operations, and effectively reduce storage overhead. Overall, the model provides secure, efficient, and flexible access control support for

收稿日期:2025-12-02
基金项目:重庆市教委科学技术研究项目(KJQN202303301);重庆城市管理职业学院校级项目(2022NDXM08)。
Supported by Scientific and Technological Research Project of Chongqing Municipal Education Commission (KJQN202303301) and School-level Project of Chongqing City Managemcnt College (2022NDXM08).
作者简介:韩永征(1984—),男,硕士研究生,主要从事区块链和访问控制方向研究,(E-mail) hanyongzheng@cqc.edu.cn。

resource-constrained body area network environments.

Keywords: body area network; blockchain; access control; delegated authorization; dynamic trust evaluation; smart contract

随着体域网[1](body area network,BAN)技术的快速发展,其在远程医疗、慢性病管理和紧急救援等场景中发挥着越来越重要的作用。然而,BAN环境固有的资源受限性、拓扑动态变化性以及医疗数据的高敏感性,使得传统基于中心化服务器的访问控制模型面临单点故障、权限僵化及动态授权困难等挑战。

传统的基于角色或属性的访问控制模型依赖于中心化授权服务器,存在可信性不足和灵活性差的问题。近年来,区块链技术以其去中心化、不可篡改和可追溯的特性[2],为构建分布式信任体系提供了新的解决方案。智能合约作为自动执行的代码,能够将访问策略编码为可自动执行的逻辑,实现权限管理的自动化与去中介化。同时,区块链在结合生物特征进行身份认证与交易安全增强方面也展现出潜力[3],并在数据完整性审计与安全去重等存储安全领域得到进一步探索[4-9],这些研究为BAN中融合多模态认证与轻量级数据安全机制提供了重要参考。

在体域网安全与访问控制领域,He等[10]提出轻量级密码学BAN认证协议,通过优化椭圆曲线运算降低计算开销,但该方案在访问控制动态性与灵活性上存在不足,跨域委托与紧急授权缺乏有效支撑。李旭辉等[11]将区块链应用于电子医疗隐私保护,采用Merkle树验证节点合法性,结合混合签名算法保障数据安全完整,为BAN设备认证提供了参考,但其访问控制策略较静态,未充分适配BAN环境动态特性与复杂委托需求。

在医疗数据管理领域,已有诸多研究探索区块链的应用。Zhang等[12]提出了基于区块链的医疗数据共享框架,通过智能合约实现细粒度访问控制。Li等[13]设计了基于属性的加密方案,结合区块链实现医疗数据的安全共享。然而,这些方案在面向资源高度受限的BAN环境时,仍存在存储开销大、能耗高、访问策略与实时生理上下文融合不够等问题。Xia等[14]提出联盟链电子健康记录共享系统,通过智能合约实现数据访问自动化管理。王威雄等[15]设计智能合约电子病历访问控制委托框架,借助委托、访问控制和请求判断3类合约,实现权限灵活委托与异常访问检测,其多合约协同设计思想对本研究颇具启发。

在委托授权与动态信任评估领域,Wang等[16]提出区块链跨域访问控制方案,通过智能合约实现域间权限委托,为链上细粒度、可追溯访问控制的实现提供重要参考。Liu等[17]提出上下文感知访问控制模型,综合用户行为与环境因素实现动态权限调整,其动态评估思路可为BAN中基于生理上下文的权限管理提供借鉴。此外,人体姿态识别技术的研究进展[18],为BAN融合行为感知与上下文理解的动态访问控制提供了技术启发。

现有研究在区块链应用于委托访问控制方面已取得进展,但在面向资源受限、场景多变的BAN环境时,仍存在以下不足:1)缺乏对BAN设备资源约束的深度优化;2)访问控制策略静态,未与实时生理上下文深度融合;3)紧急场景快速、安全授权机制不完善。

针对上述挑战,文中提出一种基于区块链的体域网动态信任委托访问控制模型(blockchain-based trust-delegation dynamic access control model for BAN,BTDAC-BAN)。文中的主要贡献包括:设计轻量级双层区块链架构以降低资源消耗;提出动态信任评估机制实现权限的细粒度调整;构建多智能合约协同的访问控制逻辑;提出优化的验证算法提升系统效率。

1 BTDAC-BAN模型设计

1.1 系统架构

BTDAC-BAN系统架构如图1所示,包含5大核心组件:

1)感知层:由各类生物医学传感器节点(心电、脑电、血糖传感器等)构成,负责采集原始生理数据并初步加密。这些传感器节点资源极端受限,无法直接参与区块链共识。

2）网关层：通常为智能手机或专用智能设备，负责汇聚传感器数据、进行本地预处理，并作为区块链轻节点管理与区块链网络的交互。网关设备具备相对较强的处理能力与存储空间。

3）区块链层：采用双层架构设计，包括主链和子链。主链负责全局权限策略、委托关系与审计日志等元数据管理；子链针对不同医疗场景（如心血管监测、糖尿病管理）独立设计，存储加密医疗数据哈希值。实际医疗数据存储在链外分布式系统中。

4）存储层：采用星际文件系统（interplanetary file system，IPFS）等分布式存储系统，存储加密后的原始生理数据，仅返回内容标识符（content identifier，CID）至区块链层。这种设计显著降低了链上存储开销。

5）应用层：包括医生、护士、研究人员、急救人员等数据使用者，通过客户端应用发起数据访问请求。

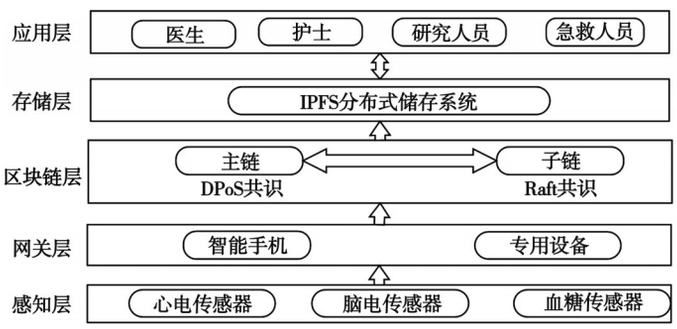

图 1　BTDAC-BAN 系统架构

Fig. 1　BTDAC-BAN system architecture

1.2　双层区块链架构

传统区块链的单链架构在资源受限的BAN环境中存在明显效率瓶颈。一是全局共识开销大，每次请求都需所有节点验证，导致延迟高、网络压力大；二是数据存储负担重，若将所有日志、策略和数据哈希都放在一条链上，会使网关等轻节点同步困难，难以满足轻量化要求。为此，文中提出图2所示的双层区块链架构。该架构通过主链维护更新频率较低的全局信任信息，而将高频、细粒度的业务交由独立子链处理。这样既避免了局部业务对全局共识的干扰，也允许子链针对不同医疗场景定制轻量级共识与存储结构，从而有效提升BAN环境下的系统性能。

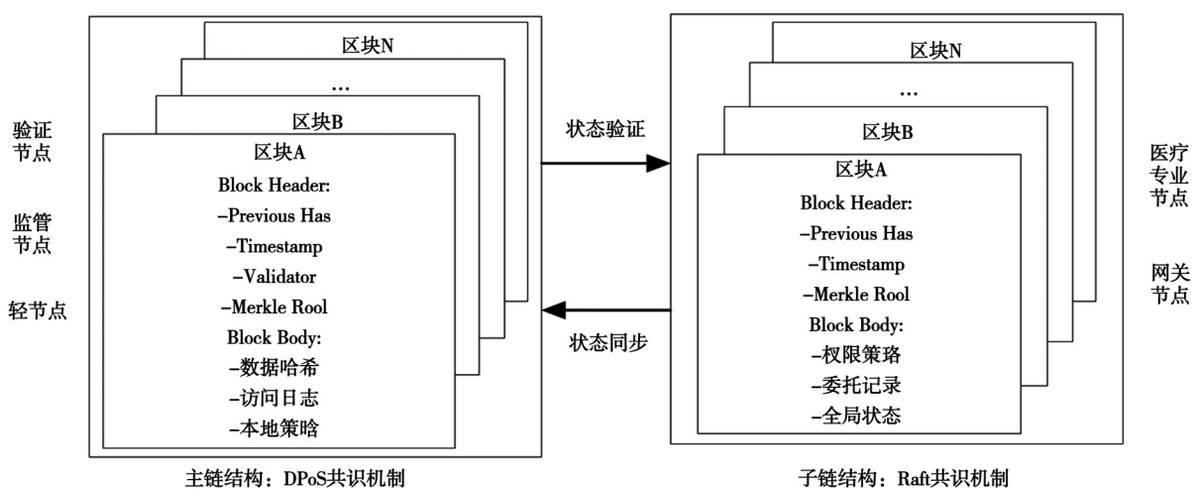

图 2　双层区块链架构

Fig. 2　Double-layer blockchain architecture

1.2.1　主链设计

主链作为系统全局信任核心，负责维护统一的权限策略、委托关系等关键记录，保障跨场景访问控制的一致性。为适配BAN资源约束，主链采用改进DPoS共识机制，通过选举有限可信节点参与共识，降低能耗

并提升吞吐量。

主链节点分为3类:验证节点由医疗管理机构、知名医院等可信实体担任,负责区块生成与验证;监管节点由卫生监管部门担任,监督系统运行并参与仲裁;轻节点部署于网关,仅同步区块头信息并完成简易验证,以控制资源占用。

1.2.2 子链设计

子链针对特定医疗场景定制,实现数据隔离与专业化优化。采用"链上-链下"分级存储:链上存储权限策略、委托关系、访问日志等元数据;链下通过分布式存储系统保存加密原始医疗数据,借助密码学哈希建立链上链下关联。

共识机制采用改进Raft算法,通过减少共识节点、优化心跳机制、支持节点动态增减,降低计算与通信开销,适配BAN特性。

1.3 智能合约设计

BTDAC-BAN模型构建了3类协同联动的智能合约:委托管理合约负责权限静态传递与委托关系生命周期维护;情境感知合约结合实时环境与用户状态,动态注入信任评估结果;审计追踪合约记录所有权限操作,保障全过程可追溯。该解耦协同架构使委托授权流程自动化执行,相较于单一合约或简单叠加方案,在扩展性与执行效率上更具优势。

1.3.1 委托管理合约

委托管理合约(delegation management contract,DMC)负责委托创建、验证、撤销的全生命周期管理,采用Merkle Patricia Trie结构维护委托记录状态树,确保可信管控与快速查询。合约核心功能通过标准化API实现,主要API如表1所示。

表1 委托管理合约的主要API

Table 1 Main APIs of the delegation management contract

API	输入参数	输出结果	功能描述
createDelegation	被委托者地址、资源ID、操作列表、有效期、最大深度	委托ID	创建新的委托关系,仅资源所有者可调用
verifyDelegation	访问者地址、资源ID、操作类型	布尔值	验证指定委托关系是否存在且有效
revokeDelegation	委托ID	无	撤销指定的委托关系,仅委托创建者可调用
getDelegationInfo	委托ID	委托详细信息	查询指定委托的详细信息

当用户发起访问请求时,DMC通过遍历委托状态树来验证委托链的完整性和有效性,确保权限传递的可信性。

1.3.2 情境感知合约

情境感知合约(context-aware contract,CAC)是本系统的决策中心,负责集成动态信任评估并做出最终的访问控制决策。该合约通过综合身份信任、行为信任和上下文信任,实现智能化的权限判定。情境感知合约中的信任评估因素如表2所示。

表2 情境感知合约的信任评估因素

Table 2 Trust evaluation factors of context-aware contracts

信任维度	评估指标	权重系数	数据来源
身份信任	数字证书等级、生物特征强度	α	CA机构、生物传感器
行为信任	历史访问成功率、恶意行为次数	β	审计日志、行为分析
上下文信任	生理危急度、位置接近度、时间相关性	γ	BAN传感器、环境上下文

通过动态调整权重系数,CAC能够适应不同场景的需求。在紧急情况下,可提高上下文信任的权重,使急救人员快速获得访问权限。

1.3.3　审计追踪合约

审计追踪合约(audit trail contract,ATC)提供不可篡改的审计日志服务,记录所有关键访问控制事件。该合约通过结构化的数据存储,为系统提供完整的安全审计能力。表3为审计追踪合约中审计记录的数据结构。

表3　审计记录数据结构

Table 3　Data structure of audit record

字段名称	数据类型	描述	示例
访问者标识	地址	发起访问请求的用户地址	0x742d35Cc…
资源标识	字节32	被访问资源的唯一标识	ECG_001
时间戳	整数256	访问请求发生的时间	1728000000
访问结果	字符串	访问控制决策结果	“GRANTED”
交易哈希	字节32	对应区块链交易标识	0x8f3a9b2c…

所有审计记录一旦写入便无法修改,为责任追溯和安全分析提供可靠依据。通过优化存储结构,ATC在保证完整性的同时最小化链上存储开销。

2　动态信任评估机制

在体域网环境中,传统的静态访问控制模型难以适应复杂的医疗场景需求。患者的生理状态、医疗人员的可信度以及环境因素都处于持续变化中,这就要求访问控制系统具备动态调整权限的能力。BTDAC-BAN提出的融合实时生理上下文的动态信任评估机制,将动态变化的生理危急度(如心律失常、血氧骤降)作为关键信任因子纳入量化评估模型,实现了访问控制策略与患者实际生命状态的深度绑定,是实现情境感知权限动态调整的核心。

2.1　信任评估模型

在BAN环境中,访问者的可信度是一个动态变化的指标,它受到生理上下文、行为历史和环境因素的共同影响。BTDAC-BAN提出的多维信任评估模型,通过建立完善的量化指标体系,实现对访问请求实时可信度的精确评估。

2.1.1　身份信任 T_{id}

身份信任是信任评估的基础维度,基于数字证书、生物特征等强认证方式建立。在医疗环境中,不同身份级别的医疗人员被赋予不同的基础信任值。计算公式为

$$T_{id} = W_a \cdot A_a + W_b \cdot A_b, \tag{1}$$

式中:A_a、A_b分别代表机构认证和生物特征认证强度;W_a和W_b为对应权重。

2.1.2　行为信任 T_{bh}

行为信任反映了访问者的历史行为模式,是基于长期观察建立的信任维度。通过分析访问者的历史操作记录,系统能够识别出行为特征并预测其未来的可信度。计算公式为

$$T_{bh} = \frac{\sum_{i=1}^{N}(S_i \cdot w_i) - \sum_{j=1}^{M}(B_j \cdot \lambda_j)}{\sum_{k=1}^{P} A_k}, \tag{2}$$

式中:w_i为第i类成功访问的权重;λ_j为第j类恶意行为惩罚因子;S_i为第i类成功访问行为的次数;B_j为第j类恶意或异常行为的次数;A_k为第k次访问记录,所有成功与失败的访问尝试;N为成功行为类别总数;M为恶

意行为类别总数；P为总访问次数。

2.1.3 上下文信任T_{ctx}

上下文信任是动态性最强的信任维度，基于实时采集的生理数据与环境信息计算得出，能够使系统快速适配紧急救援等特殊场景的权限需求，其计算公式为

$$T_{ctx}=f(P,\ L,\ T,\ E), \tag{3}$$

式中：P为生理危急度，基于BAN传感器采集的心率变异性、血氧饱和度、血压等关键生理参数计算得出，当检测到患者生命体征出现异常时，系统会自动提升急救人员访问请求的信任权重；L为位置接近度，通过GPS、Wi-Fi定位及蓝牙信标技术实现精准定位，当访问者与患者物理位置接近时，相应提高其信任度，契合医疗急救的实际场景需求；T为时间相关性，主要考量访问时间与正常诊疗时段、预约就诊时间的匹配程度，在正常工作时间或预约时段内发起的访问请求将获得较高基础信任值；E为环境因素，包含网络安全状态、设备完整性等技术环境指标，用于保障访问过程的安全性与可靠性。

2.2 动态权限调整

基于实时计算得出的信任值$T(V)$，系统采用动态权限调整策略，实现细粒度访问控制，既满足医疗场景的紧急性需求，又能有效保障患者数据的安全。计算公式为

$$T(V)=\alpha\cdot T_{id}+\beta\cdot T_{bh}+\lambda\cdot T_{ctx}, \tag{4}$$

式中，$\alpha+\beta+\lambda=1$，权重系数根据具体场景动态调整。

1）在常规医疗场景中，采用标准权重配置$\alpha=0.5$、$\beta=0.3$、$\gamma=0.2$，强调身份信任的基础地位。

2）在紧急医疗情况下，系统自动调整权重配置$\alpha=0.3$、$\beta=0.2$、$\gamma=0.5$，大幅提升上下文信任的权重，使急救人员能够快速获得必要的访问权限。

3）对于科研数据访问场景，采用严格权重配置$\alpha=0.4$、$\beta=0.4$、$\gamma=0.2$，加强行为信任的考察，确保数据使用的规范性。

3 核心算法设计

3.1 基于改进MPT的轻量级权限验证算法

传统Merkle Patricia Trie (MPT)验证路径较长，在资源受限的BAN环境中效率不高。本算法通过压缩共享前缀和缓存高频访问路径进行优化，核心是利用访问局部性。网关本地维护带TTL的缓存，优先响应高频请求。若缓存未命中，则向链上合约查询。合约不仅返回验证结果，还附上一个精简的Merkle证明。网关只需结合已知的区块根哈希校验该证明，即可在无需同步全状态的情况下确认结果有效性。这一设计将耗时的链上遍历转化为一次轻量级证明验证，显著降低了网关的计算与通信开销。

算法1 改进的MPT权限验证算法

输入：访问者地址V_addr，资源ID R_id，操作Action

输出：验证结果true/false

1. 从网关本地缓存中查找 (V_addr, R_id, Action) 对应的预验证结果
2. if 缓存命中且未过期 then
3. 返回缓存结果
4. end if
5. // 缓存未命中，执行链上验证
6. 构建查询键 Key=Keccak256(V_addr || R_id || Action)
7. 从区块链获取当前状态树的根哈希 Root_hash
8. 调用DMC.verifyDelegation(V_addr, R_id, Action)（该函数内部会遍历MPT）

9. 获取验证结果 Result 和 Merkle 证明 Proof

10. if Result == true then

11. 验证 Proof 与 Root_hash 是否一致

12. if 验证成功 then

13. 将 (Key, Result, TTL) 存入本地缓存

14. 返回 true

15. else

16. 返回 false//证明无效

17. end if

18. else

19. 返回 false

20. end if

该算法通过本地缓存与批量验证显著减少链上操作次数,降低网络开销与验证延迟,特别适合资源受限的 BAN 环境。

3.2　紧急访问快速共识算法

为应对急救场景下分秒必争的需求,设计了紧急访问快速共识算法,其核心逻辑是基于多源可信证据的加权决策,而非传统的计算密集型共识。当网关收到紧急请求时,会实时核验地理位置、急救资质、患者生理信号等多类证据,并依据预设权重进行快速积分。若总分超过安全阈值,则自动签发短期访问令牌,并同步更新访问策略。这一过程无需全网节点同步确认,事后再将操作日志异步上链存证,在确保安全底线的同时,实现了秒级应急响应,为抢救争取了关键时间。

算法 2　紧急访问快速共识算法

输入:紧急请求者 E,患者 P,紧急类型 Type

输出:临时访问令牌 Token 或 null

1. //多源信息收集与验证

2. Evidence_Set = ø

3. if E 的地理位置 near P 的已知位置 then

4. 添加证据 E_geo = “Location_Proximity” 到 Evidence_Set

5.end if

6. if E 持有有效的、在期的急救资质证书 (链上存哈希) then

7. 添加证据 E_cred = “Valid_Credential” 到 Evidence_Set

8. end if

9. if 从 P 的 BAN 传感器检测到生命体征异常 then

10. 添加证据 E_physio = “Critical_Physio”到 Evidence_Set

11. end if

12. if E 所在的机构(如医院)与 P 有诊疗关系 then

13. 添加证据 E_affil = “Trusted_Affiliation”到 Evidence_Set

14. end if

15. //快速共识决策

16. Trust_Score = 0
17. for each evidence in Evidence_Set do
18. Trust_Score += getWeight(evidence) //为不同证据赋予权重
19. end for
20. if Trust_Score ≥ Emergency_Threshold then
21. Token = GenerateEmergencyToken(E, P, Type, Short_Validity)
22. CAC.overrideAccessPolicy(P, E, Token) //临时更新策略
23. ATC.logEmergencyAccess(E, P, Type, Token)
24. 返回 Token
25. else
26. 返回 null
27. end if

该算法通过多源证据验证与快速共识决策,在保障安全前提下实现紧急权限的快速授予,为急救场景争取宝贵时间。

4 实验与性能分析

4.1 实验环境设置

为验证文中所提的BTDAC-BAN模型的综合性能,搭建了模拟体域网测试环境。实验采用RPi 4B模拟体域网网关设备,使用Arduino Uno模拟资源极端受限的传感器节点。服务器节点采用配置Intel Core i7-12700 H处理器与32 GB内存的PC机进行模拟。

区块链网络基于以太坊Geth客户端搭建私有联盟链,共设置4个共识节点,采用PBFT共识算法。主链与子链采用差异化共识参数,其中主链区块间隔设置为2 s,子链区块间隔为500 ms。

智能合约使用Solidity 0.8.x版本编写,并通过Remix集成开发环境进行部署。测试数据来源于PhysioNet数据库中的生理信号数据,采用MIT-BIH心律失常数据库模拟实时体域网数据流。测试期间共生成约100 000条访问请求,涵盖正常访问、委托访问及紧急访问等多种典型场景。

4.2 性能指标测试

4.2.1 权限验证延迟

测试不同并发请求数下的平均响应时间。如表4所示,在低并发(10请求)下,中心化RBAC方案凭借其简单架构略有优势(28 ms)。但随着并发量增至100,中心化方案出现明显瓶颈,而文中所提BTDAC-BAN得益于分布式验证与缓存机制,延迟稳定在150 ms左右。当并发请求数达到200时,本方案延迟为225 ms,仍保持可用性,优于对比的文献[15]方案(395 ms)。这证明了双层架构与轻量级验证算法的有效性。

表4 权限验证延迟对比

Table 4 Comparison of permission verification delay ms

并发请求数	文中所提BTDAC-BAN	传统RBAC-中心化	文献[15]方案
10	48	28	65
50	105	115	158
100	150	超时/性能骤降	242
200	225	超时/性能骤降	395

4.2.2 委托操作成功率

对委托创建、验证、撤销操作进行1 000次重复测试。结果显示如表5所示,操作成功率均高于97.5%,表明智能合约的原子性与区块链网络稳定性提供了可靠保障。少数失败主要源于瞬时网络拥堵导致的Gas不

足或超时,通过优化Gas定价策略与重试机制可进一步提高成功率。平均延迟方面,委托验证因涉及缓存优化而最快(142 ms),委托创建与撤销因需更新链上状态而稍慢。

表5　委托操作成功率

Table 5　Success rate of delegation operations

操作类型	成功率/%	平均延迟/ms	主要失败原因
委托创建	99.3	335	Gas不足,网络拥堵
委托验证	97.5	142	缓存不一致
委托撤销	98.8	298	权限验证失败

4.2.3　存储开销对比

比较运行一段时间后,各组件数据存储量如表6所示,传统的将全部数据上链的方案需要1 100 MB链上存储。通过采用“链上存哈希,链下存密文”的协同策略,文中所提BTDAC-BAN将链上存储压缩至仅68 MB,较文献[15]方案(125 MB)降低约45.6%。网关本地缓存虽增加了约12 MB的少量存储开销,但换取了验证性能的显著提升。总存储开销约为600 MB,在保证数据可验证性的同时,极大缓解了BAN网关的存储压力。

表6　存储开销对比

Table 6　Storage overhead comparison　　MB

方案/组件	链上存储	网关本地存储	链下存储	总存储
传统全链存储	1 100	—	—	1 100
文献[15]方案	125	18	520	663
文中所提BTDAC-BAN	68	12	520	600

4.2.4　紧急访问响应时间

测试紧急访问流程从发起请求到获得令牌的平均时间如表7所示。可知,文中所提BTDAC-BAN通过紧急访问快速共识算法实现了秒级紧急授权,远快于传统人工审批方式,为急救争取宝贵时间。在标准急救流程下,平均响应时间为190 ms;在极端危急场景(如患者生命体征危急)下,系统通过简化验证流程进一步缩短响应时间至165 ms。本方案为抢救赢得了宝贵的时间窗口。

表7　紧急访问性能

Table 7　Emergency access performance

场景	文中所提BTDAC-BAN	传统人工授权	改进幅度/%
标准紧急流程	190 ms	数分钟至数十分钟	>99
极端紧急情况	165 ms	不可用	100

5　结束语

针对体域网在智慧医疗场景中面临的资源受限、拓扑动态变化及数据高敏感等核心问题,设计了基于区块链的动态信任委托访问控制模型。该模型整合了轻量级双层区块链架构、融入实时生理上下文的动态信任评估机制,以及多智能合约协同工作的优化算法体系,成功解决了BAN环境下数据安全、隐私保护、动态访问控制与设备资源受限之间的核心矛盾。此外,在追求高性能的同时,本研究也充分考虑了模型的安全边界。例如,为提升紧急场景下的响应效率,模型采用了简化验证流程,这可能带来潜在安全风险,对此设计了多层次的安全防御机制,通过多源证据交叉验证、严格遵循最小权限原则并设置短期有效权限,再配合完整

的事后审计追溯功能，有效管控了潜在安全风险。从实验测试结果来看，BTDAC-BAN的综合性能表现突出，尤其在权限验证延迟、委托操作成功率、存储资源占用以及紧急场景响应时间等核心指标上优势明显，为构建安全、高效且具备场景感知能力的BAN数据共享系统，提供了一条切实可行的技术方案。

参考文献

[1] Shi Q F, Yang Y Q, Sun Z D, et al. Progress of advanced devices and Internet of Things systems as enabling technologies for smart homes and health care[J]. ACS Materials Au, 2022, 2(4): 394-435.

[2] Okegbile S D, Cai J, Alfa A S. Practical Byzantine fault tolerance-enhanced blockchain-enabled data sharing system: latency and age of data package analysis[J]. IEEE Transactions on Mobile Computing, 2024, 23(1): 737-753.

[3] Bisogni C, Iovane G, Landi R E, et al. ECB2: a novel encryption scheme using face biometrics for signing blockchain transactions[J]. Journal of Information Security and Applications, 2021, 59: 102814.

[4] Zhang K, Guo Z R, Wang L L, et al. Revocable certificateless Provable Data Possession with identity privacy in cloud storage [J]. Computer Standards & Interfaces, 2024, 90: 103848.

[5] Tan X, Xie Q, Han L D, et al. Proof of retrievability with flexible designated verification for cloud storage[J]. Computers & Security, 2023, 135: 103486.

[6] Xu Y L, Jin C H, Qin W Y, et al. BDACD: Blockchain-based decentralized auditing supporting ciphertext deduplication[J]. Journal of Systems Architecture, 2024, 147: 103053.

[7] Miao Y P, Miao Y, Miao X X. Blockchain-based transparent and certificateless data integrity auditing for cloud storage[J]. Concurrency and Computation: Practice and Experience, 2024, 36(27): e8285.

[8] Tian G H, Hu Y H, Wei J H, et al. Blockchain-based secure deduplication and shared auditing in decentralized storage[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(6): 3941-3954.

[9] Miao Y, Gai K K, Zhu L H, et al. Blockchain-based shared data integrity auditing and deduplication[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 3688-3703.

[10] He D B, Kumar N, Khan M K, et al. Efficient privacy-aware authentication scheme for mobile cloud computing services[J]. IEEE Systems Journal, 2018, 12(2): 1621-1631.

[11] 李旭辉, 柳毅 . 基于区块链的电子医疗隐私保护与数据存储[J]. 计算机应用与软件, 2025, 42(8): 86-93.
Li X H, Liu Y. Electronic medical privacy protection and data storage based on blockchain[J]. Computer Applications and Software, 2025, 42(8): 86-93. (in Chinese)

[12] Zhang A Q, Lin X D. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain[J]. Journal of Medical Systems, 2018, 42(8): 140.

[13] Li M, Yu S C, Zheng Y, et al. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1): 131-143.

[14] Xia Q, Sifah E, Smahi A, et al. BBDS: blockchain-based data sharing for electronic medical records in cloud environments[J]. Information, 2017, 8(2): 44.

[15] 王威雄, 朱晓军, 赵涓涓, 等 . 基于智能合约的电子病历访问控制委托框架[J]. 计算机工程与设计, 2024, 45(7): 2220-2227.
Wang W X, Zhu X J, Zhao J J, et al. Smart contract based access control delegation framework for electronic medical records[J]. Computer Engineering and Design, 2024, 45(7): 2220-2227. (in Chinese)

[16] Wang S P, Zhang Y L, Zhang Y L. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. IEEE Access, 2018, 6: 38437-38450.

[17] Liu J K, Au M H, Huang X Y, et al. Fine-grained two-factor access control for web-based cloud computing services[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(3): 484-497.

[18] Ali M A, Hussain A J, Sadiq A T. Human body posture recognition approaches: a review[J]. Aro-the Scientific Journal of Koya University, 2022, 10(1): 75-84.

（编辑 侯 湘）