doi:10.6041/j.issn.1000-1298.2026.12.028

基于区块链的土壤资源数据可信访问方法

张　新[1]　帅博宇[1,2]　钱建平[2]　赵峙尧[1]　肖鹏南[2]　许继平[1]　于家斌[1]
(1.北京工商大学计算机与人工智能学院,北京 100048;2.中国农业科学院农业资源与农业区划研究所,北京 100081)

摘要:土壤资源数据具有量大、多源异构且敏感性高特点,在保障数据安全的同时实现高效访问与合理利用是核心挑战。针对现有土壤信息系统中存在的数据安全性不足、权限管理不完善和共享效率低等问题,本文构建了基于区块链的土壤资源数据可信访问模型,并进行系统测试。首先,在土壤资源数据特性分析与分级的基础上,构建基于主从多链架构和 PKI 框架的土壤资源数据可信访问模型。然后,结合用户身份证书分级管理和用户访问行为,设计了节点综合信誉值排序机制,并以此设计了跨域信息交互机制和 RSPBFT 共识机制。最后,使用 Hyperledger Fabric 平台设计并开发了土壤资源数据可信访问原型系统,并进行实验验证及系统应用案例分析。实验结果表明,跨域交互计算耗时为 15.43 ms + $10T_0$(每次通信所需时间),相较现有方案计算开销平均降低约 30%;在高并发场景下,RSPBFT 共识算法系统吞吐量较 PBFT 算法提升约 16.2%,并且访问控制等核心操作平均响应时延均控制在可接受范围内,体现出良好的可扩展性与实用性。综上所述,所提方法在安全性、性能和可扩展性方面具备良好表现,能够为土壤信息系统提供更加安全、高效、可控的数字化身份管理方案,在隐私保护与身份认证等方面具有广泛应用前景。

关键词:土壤资源数据;区块链;可信访问;主从多链;PKI 框架;信誉排序机制
中图分类号:TP311.11　　**文献标识码**:A　　**文章编号**:1000-1298(2026)12-0296-14　　**OSID**:

Trusted Access Method of Soil Resource Data Based on Blockchain

ZHANG Xin[1]　SHUAI Boyu[1,2]　QIAN Jianping[2]　ZHAO Zhiyao[1]　XIAO Pengnan[2]　XU Jiping[1]　YU Jiabin[1]
(1. *School of Computer and Artificial Intelligence*, *Beijing Technology and Business University*, *Beijing* 100048, *China*
2. *Institute of Agricultural Resources and Regional Planning*, *Chinese Academy of Agricultural Sciences*, *Beijing* 100081, *China*)

Abstract: Soil resource data are characterized by large volume, multi-source heterogeneity, and high sensitivity. Achieving secure, efficient access and rational utilization while ensuring data security is therefore a core challenge. To address the issues of insufficient data security, imperfect permission management, and low sharing efficiency in existing soil information systems, a blockchain-based trusted access model for soil resource data and conducts system testing was proposed. Firstly, based on the analysis and classification of soil resource data characteristics, a trusted access model for soil resource data was constructed by using a master-slave multi-chain architecture and a PKI framework. Then by integrating hierarchical management of user identity certificates with user access behaviors, a comprehensive node reputation-based ranking mechanism was designed, upon which a cross-domain information interaction mechanism and an RSPBFT consensus mechanism were developed. Finally, a prototype system for trusted access to soil resource data was designed and implemented on the Hyperledger Fabric platform, followed by experimental validation and application case studies. Experimental results showed that the cross-domain interaction computation time was 15.43 ms + $10T_0$ (where T_0 was the time required for a single communication), reducing the average computational overhead by about 30% compared with that of existing schemes. Under high-concurrency scenarios, the system throughput of the RSPBFT consensus algorithm was about 16.2% higher than that of PBFT, while the average response latency of core operations such as access control remained within an acceptable range, demonstrating good

收稿日期:2025-02-14　修回日期:2025-05-14
基金项目:国家重点研发计划项目(2022YFF1101103)、中国农科院科技创新工程项目(CAAS-CSAL-202402)、国家自然科学基金项目(62402020)、中央级公益性科研院所基本科研业务费专项(Y2025YC82)和北京市教育委员会“市属高校分类发展-北京工商大学数字商学新兴交叉学科平台建设”项目
作者简介:张新(1989—),男,副教授,主要从事区块链和 AI 融合应用研究,E-mail:zhangxin@btbu.edu.cn
通信作者:钱建平(1979—),男,研究员,主要从事数字土壤研究,E-mail:qianjianping@caas.cn

scalability and practicality. Overall, the proposed method performed well in terms of security, performance, and scalability, which can provide a safer, more efficient, and controllable digital identity management solution for soil information systems, with broad application prospects in privacy protection and identity authentication.

Key words: soil resource data; blockchain; trusted access; master-slave multi-chain; PKI framework; reputation ranking mechanism

0　引言

土壤资源数据是通过观测、监测、实验或模型模拟等方式获取的，能够系统描述土壤属性、分布、质量及其动态变化的各类数据集合，具有多源异构、时空关联性强、层级分布复杂及敏感性高等特点。正在开展的第三次全国土壤普查[1]将产生包括外业调查采样、内业测试化验等海量数据，是土壤资源数据的重要组成部分。安全、合理地利用土壤资源数据有助于实现耕地资源的合理配置和高效利用[2-4]。然而，土壤资源数据的高敏感性，若缺乏精细化权限管理机制，可能导致用户身份认证不严、访问权限分配不清等问题，从而在数据共享过程引发信息泄露、数据滥用等安全隐患。在确保数据安全的前提下，合理分配用户身份[5-7]，推进数据高效访问与合理利用，是发挥土壤资源数据价值的关键。

传统数据访问机制大多存在用户身份易被篡改、数据中心化存储、透明度不够等问题[8-10]；区块链技术通过去中心化和分布式设计，实现了数据共享的隐私保护，结合密码学和共识机制，确保数据安全、完整且不可篡改，为实现可信访问提供了有效方法。随着区块链技术的普及，农业领域对区块链技术也正在逐渐开展研究[11-14]。基于区块链构建农业信息可信共享系统，有助于增强农业信息的安全性与可靠性，为数据提供可信的信息共享机制，保障数据的深度挖掘与价值实现[15-18]。但由于区块链自身特点可能会导致浪费资源、效率较慢、存储困难等问题，学者对数据安全共享模型进行了多角度研究。近年来，研究人员开始将区块链与多方计算(MPC)、同态加密等技术相结合，提升数据处理的可信性与隐私保护能力[19]。LOU 等[20]将区块链与 IPFS 结合，并采用代理重加密机制，有效提升了加密密钥的分发效率。LIANG 等[21]引入可链接环签名机制，通过隐藏证书签发者身份，提高了系统的安全性与吞吐能力。针对多链环境下共识效率问题，也有学者引入信誉监督机制优化共识算法，提升系统安全性与认证效率[22]。随着这些技术的不断发展，越来越多研究开始聚焦于区块链在农业场景的落地应用。张新等[23]构建了基于多链的果蔬管理模型，针对不同类型数据进行了分级权限控制，解决了企业间数据共享的安全性问题。此外，结合自我主权身份(SSI)与可验证凭证方案，实现了农业物联网中用户间可信共享与风险信息访问[24]。也有研究将公钥基础设施(PKI)引入食品供应链，增强系统的信任机制[25]。然而，这些方法在面对复杂身份验证场景时，仍存在效率瓶颈。为此，VANGALA 等[26]构建了基于区块链的智能农业身份认证方案，引入基于投票机制的改进方案，提升了系统运行效率。综上所述，当前已有大量研究围绕区块链在农业数据可信访问中应用展开，提出了多种通用的数据共享与安全访问模型，在提升农业数据透明度和安全性的同时，为推动农业数字化提供了重要支撑。

已有通用数据访问模型，无法满足土壤资源数据可信访问的安全需求，也难以兼顾数据共享与安全防护间的平衡，进而可能导致访问风险与管理漏洞。为实现土壤数据的高效利用，必须在保障安全可控的前提下，提升访问效率与透明度，从而充分发挥数据价值。因此，亟需构建一个既能有效防止数据泄露，又能深度适配土壤资源特性、保障数据安全可信的访问模型，以支撑精准农业与智慧耕地的发展需求。本文以区块链技术为支撑，以实现土壤资源数据的安全高效访问为目标。通过对 PKI 框架和身份权限认证研究，构建基于主从多链的土壤资源数据可信访问模型。对访问用户的访问行为和用户等级进行综合信誉值评估，并以此提出土壤资源安全高效共识机制。设计并开发土壤资源数据可信访问系统，以实现对土壤资源数据的安全高效访问目标，提供一种与土壤资源深度适配的数字化身份认证方法。

1　土壤资源数据可信访问模型

1.1　土壤资源数据分析与分级

土壤资源数据种类繁多，可能会发生数据在不同地域等级中数据敏感性也不同的情况，根据数据重要性、影响范围等因素将土壤资源数据敏感度分为高敏感(Ⅰ)、中敏感(Ⅱ)、低敏感(Ⅲ)。同时，将 3 个敏感度等级与访问用户身份等级和地域等级结合，建立更加安全、可信的用户身份分级标准，使满足规定等级的用户可以查看对应数据。根据信息敏感度对数据访问者身份进行限定，数据资源以土

壤属性数据和用户隐私信息数据为例，用户地域等级与数据类型敏感度分级关系如表 1 所示。

表 1 土壤资源数据分级

Tab. 1 Soil resource data grading

地域等级	数据敏感度分级		
	Ⅰ级	Ⅱ级	Ⅲ级
省级	省级 A_1、省级 A_2、实验人员身份信息 B_1	省级 A_3、省级 A_4	省级 A_5
市级	市级 A_1、市级 A_2	市级 A_3、实验人员身份信息 B_2	市级 A_4、市级 A_5
县级	县级 A_1	县级 A_2、县级 A_3	县级 A_4、县级 A_5、实验人员身份信息 B_3

表 1 中集合 A_1 = {土壤有机质含量，土壤有效铜含量，土壤有效锌含量，土壤有效硼含量，土壤有效钼含量}；A_2 = {土壤有效铁含量，土壤有效锰含量}；A_3 = {土壤阳离子交换量、土壤容重、土壤有效硫含量}；A_4 = {砾石含量，土壤质地，黏粒含量，砂粒含量，粉粒含量}；A_5 = {土壤酸碱度、土壤全氮含量，土壤全磷含量，土壤全钾含量，土壤有效磷含量，土壤速效钾含量，耕层厚度}。其中，B_1 为省级隐私信息，B_2 为市级隐私信息，B_3 为县级隐私信息。

不同地域等级用户访问其地域范围内数据等级分类存在差异，需对不同地域数据进行详细的敏感度分级，设计安全访问控制策略。

省级用户可访问数据包含集合 A_1 和集合 B_1，均属于高敏感数据；市级用户可访问数据包含集合 A_1 和集合 A_2，其中 B_2 属于中敏感数据，集合 A_3 属于低敏感数据；县级用户可访问数据包含集合 A_2，其中 B_3 属于低敏感数据。

同一地域等级中，用户根据访问需求不同，分为 3 个等级：低级用户、中级用户和高级用户。低级用户身份需提供真实姓名和手机号作为可被验证的法定属性和通信属性；中级用户身份在低级用户基础上外加进行线上身份核验；高级用户在中级用户基础上加上人脸识别进行身份核验。

1.2 基于主从多链的土壤资源数据可信访问模型

在土壤资源数据特性分析下构建基于区块链的土壤资源数据可信访问模型，如图 1 所示。将土壤资源数据按省级行政区通过多链隔离技术构建若干条局部区块链，不同省级行政区的用户在各自局部链中记录数据，省级主链作为全局调度与管理链，负责对各从链的数据访问状态进行协调与认证，各条从链通过跨域身份信息交互可进行消息互联互通。访问用户发起请求后，根据其证书等级、信誉值及目标数据敏感度，调用链上智能合约进行访问权限控制。土壤资源数据存储在链下数据库，仅访问摘要信息在链上存证，保障了土壤资源数据在多地域环境下可信访问与安全共享。

根据土壤资源数据需求上链数据分为隐私数据

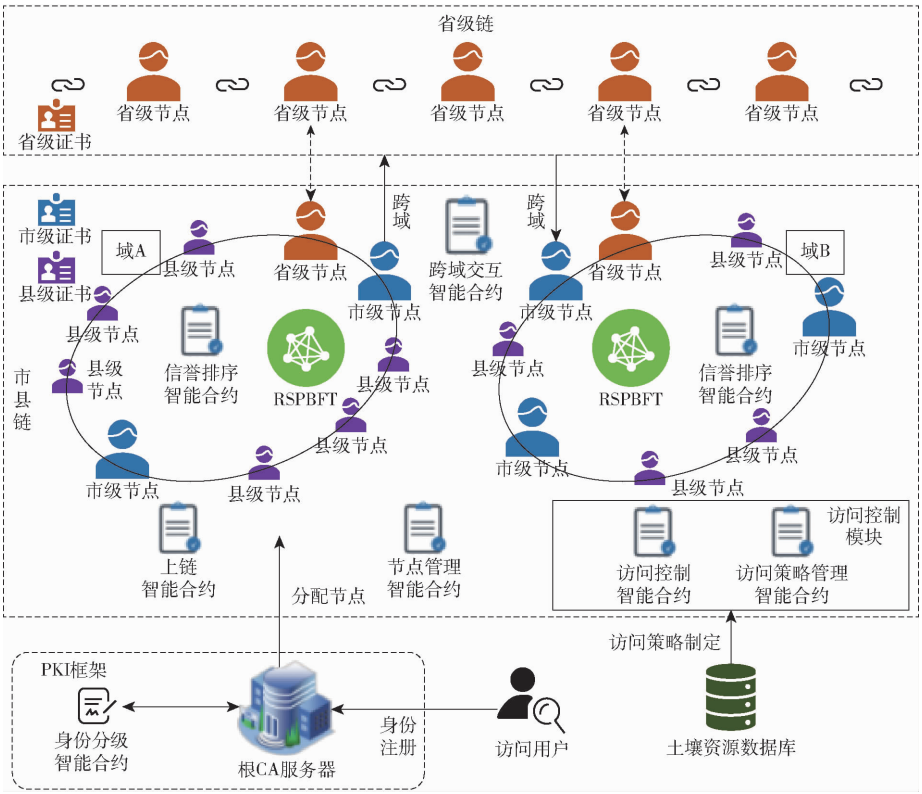

图 1 基于主从多链的土壤资源数据可信访问模型

Fig. 1 Trusted access model for soil resource data based on master-slave multi-chain

和访问请求数据。各条从链存储隐私数据，访问请求数据经主链处理后在对应从链中存储。隐私数据是指在一个访问节点进行身份认证过程所产生的证书、身份信息等数据，与土壤资源数据的安全性直接挂钩。合理使用和监管数据，是可信访问土壤资源数据的前提。访问请求数据是指节点在访问过程待与证书验证是否匹配的数据，该数据会直接影响用户是否能看到对应土壤资源数据，高效地验证并处理访问请求数据，是挖掘土壤资源数据价值的关键。

1.3　基于主从多链的 PKI 框架构建

PKI(Public key infrastructure)是一种基于公钥密码学算法解决数字身份认证问题的常见技术，在传统 PKI 中，CA 是一切认证的起点，只有当 CA 本身是可信的，所颁发的证书才可信。针对传统 PKI 面临根 CA(Root certificate authority, RCA)服务器单点故障的问题，设计了基于主从多链的 PKI 框架对身份进行安全、高效的认证，框架结构如图 2 所示。

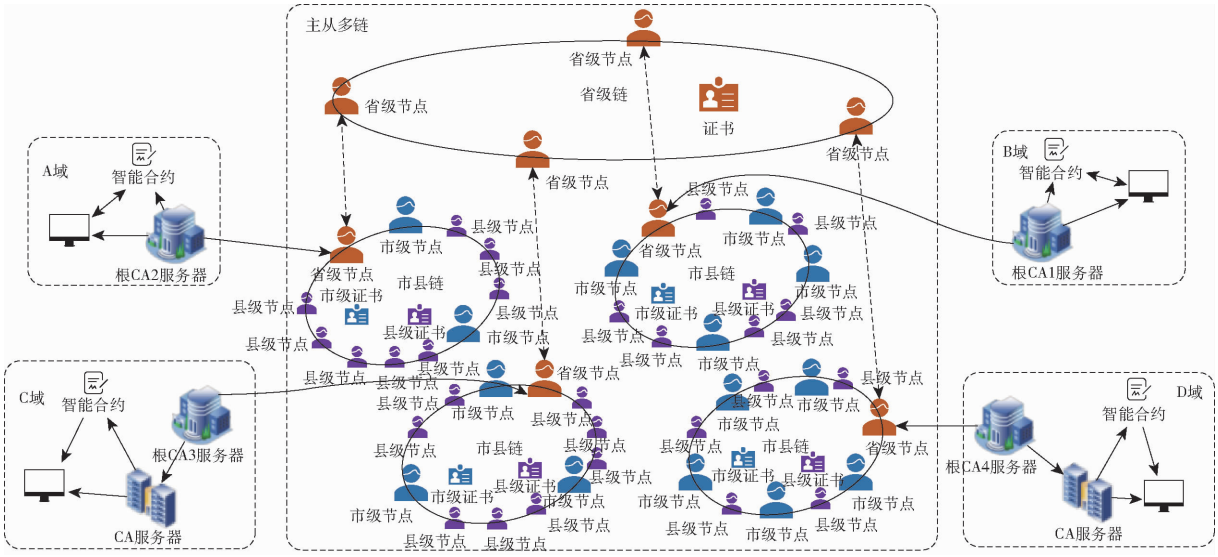

图 2　基于主从多链的 PKI 框架

Fig. 2　Master-slave multi-chain PKI framework

主链由省级节点组成，各条从链由对应省份的下级市、县节点构成。市县链内部进行基于信誉排序的实用性拜占庭容错(Reputation sorting practical Byzantine fault tolerance，RSPBFT)，省级链进行 POA(Proof of authority)共识。该模型将每条从链分为不同的域，在链上以 CA 节点形式将不同域的信息进行交互、共识，共同维护区块链网络。根 CA 与省级节点对应，每个域内配置 1 个根 CA 服务器，负责本域整体的证书管理工作；CA 是 RCA 下级，由上级 CA 颁发证书，一般与市级节点对应，子 CA 也可以给应用服务商和用户以及域服务器颁发证书，负责证书日常管理工作。

经过上述方法引入区块链技术，实现多 CA 协同签名的主从多链 CA 结构，由于 RCA 在颁发证书时是经过区块链网络中多个域 CA 节点达成共识的，从源头上解决了传统 PKI 框架中存在单点故障的问题。

2　数据交互和权限控制机制

在构建土壤资源数据可信访问模型的基础上，构建了融合 PKI 框架的信誉值排序机制，并基于此设计跨域信息交互机制和 RSPBFT 共识机制，实现用户身份的动态评估与分级管理，保障访问过程的身份可信与权限可控，提升数据访问安全性、协同效率与共识性能。

2.1　融合 PKI 框架的用户信誉值排序机制

土壤资源数据隐私度高、数据量庞大，为保证数据访问过程数据的安全性，需对用户行为进行区分，同时需符合土壤资源用户分级规定，因此提出一种融合 PKI 框架的用户信誉值排序机制。根据访问节点的历史访问行为和由 PKI 框架产生的证书等级计算访问节点的综合信誉值。当访问节点进行恶意访问时，用户信誉值就会降低。

(1)初始信誉值

访问节点初始信誉值计算参数包括用户成功访问次数(S_i)和用户恶意访问次数(F_i)。用户初始信誉值 C_{origin} 计算式为

$$C_{\text{origin}} = \sum_{i=1}^{m} \frac{\alpha_i S_i + \beta_i F_i}{m} \tag{1}$$

其中　　$\sum \alpha_i = 1$　　$\sum \beta_i = 1$

式中　m——数据等级总类别数

α_i——针对不同等级用户成功访问计算权重

β_i——针对不同数据等级用户恶意访问计算权重

(2)历史信誉值

访问节点获得初始授权后,会产生历史信誉值。随着时间推移和用户授权次数增加,用户信誉值需随时间变化而调整。历史信誉值 C_{History} 计算式为

$$C_{\text{History}} = \frac{\sum_{i=1}^{n} (C_{\text{Current}} t_i)}{\sum_{i=1}^{n} t_i} \tag{2}$$

式中 t_i——访问节点从提出访问请求到策略匹配完成授权的总时间

n——访问节点的历史访问次数

C_{Current}——访问节点每次结束访问的信誉值

(3)PKI 信誉值

PKI 信誉值根据访问节点身份认证产生,在土壤资源数据可信访问系统中按地域划分共分为 3 个地域等级用户(A_i),分别为省级用户、市级用户和县级用户,在每个用户地域等级中分为 3 个等级用户(B_i),分别为高级用户、中级用户和低级用户。

PKI 信誉值 C_{PKI} 计算式为

$$C_{\text{PKI}} = \gamma_i A_i + \delta_i B_i \tag{3}$$

式中 γ_i——地域等级计算权重

δ_i——用户等级计算权重

(4)综合信誉值

综合信誉值 C_{Final} 计算式为

$$C_{\text{Final}} = aC_{\text{origin}} + bC_{\text{History}} + cC_{\text{PKI}} \tag{4}$$

其中 $a + b + c = 1$ 且 $c > a > b$

式中 a——初始信誉值权重

b——历史信誉值权重

c——PKI 信誉值权重

综合信誉值与信誉等级映射如表 2 所示。将信誉值划分为 3 个区间,保证信誉值可以区分访问用户是否为良好用户,同时满足严格的用户等级规定,防止出现低等级用户信誉值比高等级用户信誉值高的情况。对每个信誉等级设定不同访问控制策略,从而实现对访问者进行授权。

表 2 综合信誉值与信誉等级映射

Tab. 2 Comprehensive reputation score and reputation rating mapping

C_{Final}	信誉等级
(80,100]	C1
(60,80]	C2
(0,60]	C3
(−∞,0]	禁止访问

(5)信誉惩罚

针对综合信誉值小于或等于 0 的用户,使用访问策略控制用户暂时不能访问数据资源,但随着时间推移,不良访问记录造成的影响会被历史信誉值进行稀释,综合信誉值此时会大于 0,从而恢复用户访问权限。

2.2 跨域身份信息交互机制

设计跨域身份信息交互机制,保证主从多链 PKI 框架在分布式分发证书过程的信息一致性,完成不同从链间的信息互联互通,跨域身份信息交互机制如图 3 所示。

以 Issuer*A* 所辖域 Do_A 中的 C 县由主链审核后匹配到 Issuer*B* 所辖域 Do_B 中的 E 县进行跨域身份信息交互为例描述本机制,如图 3 所示(C 县已完成身份注册流程)。Issuer 节点表示从链,Master 表示主链,Request*I* 表示跨域身份交互请求正文,Sign*I* 表示加密正文后的请求密文,Identity*C* 表示节点 C 身份原信息,Cert*J* 表示节点证书,Sk*J* 表示节点私钥,Pk*J* 表示节点公钥,InstructionAgree 表示同意跨域交互请求指令,SignCert*E* 表示请求跨域交互节点 C 使用 Sk*J* 对交互节点 E 证书签名的证书,SignCert*C* 表示交互节点 E 使用 Sk*E* 对请求跨域交互节点的证书进行签名后的证书,I 表示信息交互过程,J 表示节点。

跨链身份信息交互机制具体算法:

算法 1:

输入:节点 C 身份原信息、请求信息、证书、公钥以及私钥

输出:更新后节点 C 证书

1. Function 〈 Cross-domain interactions 〉([〈 IdentityC 〉, 〈 RequestC 〉, 〈 CertC 〉, 〈 PkC 〉, 〈 SkC〉])

2. Begin

3. SignRequestC ← Sign(RequestC, SkC) # 节点 C 对请求进行签名

4. SendToMaster (IdentityC, RequestC, SignRequestC, CertC, PkC) # 节点 C 发送匹配跨域验证节点请求

5. End

6. If Verify(CertC, IdentityC, PkC) Or Verify(RequestC, SignRequestC, PkC) # 主链验证节点 C 证书和身份原信息一致性,请求和签名一致性

7. TrustedNodes ← GetTrustedNodesByReputation(C1) # 获取 C1 信誉等级的可信节点

8. Sort(TrustedNodes, ByDescendingReputation) # 按信誉值从高到低排序

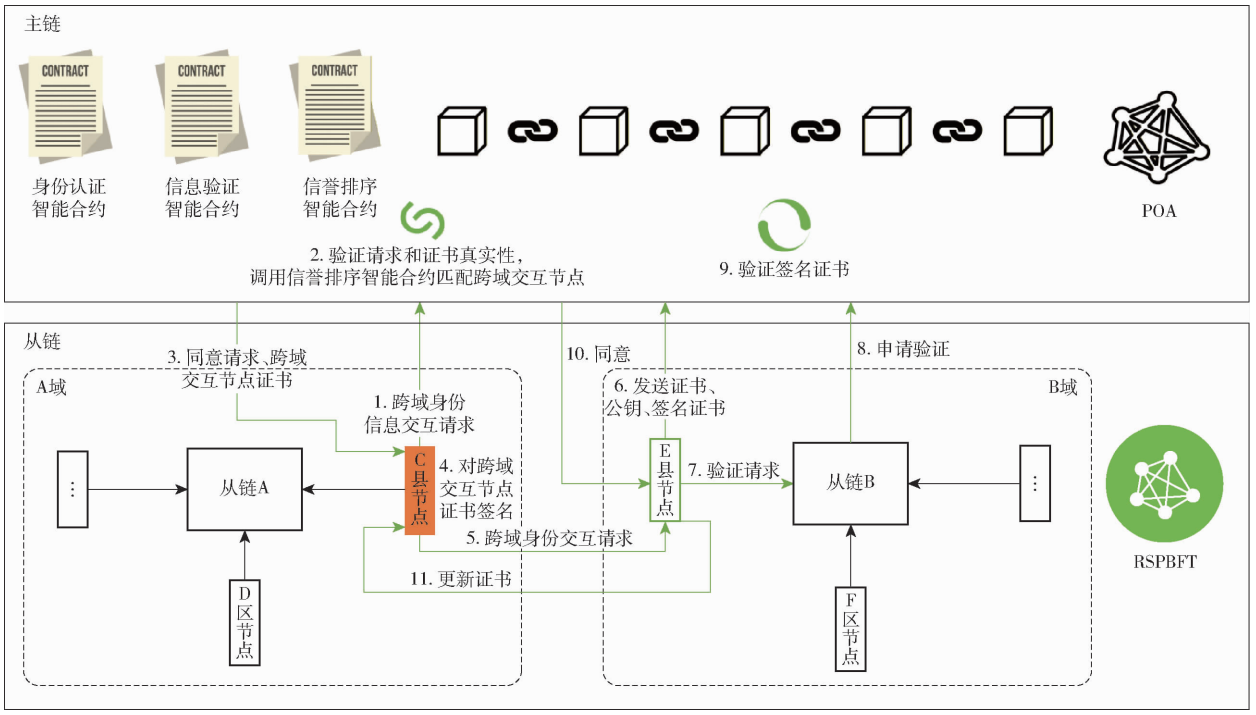

图 3　跨域身份信息交互机制

Fig. 3　Cross-domain identity information interaction mechanism

9. MatchedNode ← SelectBestNode(TrustedNodes) # 选择信誉值最高节点

10. MatchedNodeCert ← GetNodeCertificate(MatchedNode) # 调取匹配的验证节点 E 证书

11. SendToNodeC(CertE, InstructionAccept) # 将匹配节点 E 证书和指令返回给节点 C

12. End

13. SignCertE ← Sign(CertE, SkC) # 节点 C 对证书进行签名

14. SendToNodeE(SignCertE, RequestC, PkC) # 节点 C 发送跨域请求并签名

15. End

16. If Verify(SignCertE, CertE, PkC) Or Verify(RequestC, CertC, PkC) # 节点 E 验证签名证书与原证书一致性,请求和签名一致性

17. SignCertC ← Sign(CertC, SkE) # 节点 E 用私钥签名

18. SendToMaster(SignCertC, PkE) # 将签名证书和节点 E 公钥发送至主链

19. SendToIssuerB({RequestE → IssuerB, SignE → IssuerB, PkE}) # 节点 E 向从链 B 发送验证请求

20. End

21. If Verify(SignE→IssuerB, RequestE→IssuerB) # 从链验证请求一致性

22. RequestVerified ← ForwardRequestToMaster(RequestE→IssuerB) # 从链 B 验证后发至主链

23. End

24. If Verify(SignCertC, CertC, PkE) # 主链收到从链 B 请求后验证节点 C 证书和签名证书一致性

25. SendInstructionToNodeE(InstructionAgree) # 发送同意跨域验证指令给节点 E

26. End

27. NewCert ← GenerateNewCert() # 节点 E 生成新证书

28. SendToNodeC(NewCert) # 发送至节点 C

29. End

30. UpdateCert(CertC, NewCert) # 节点 C 更新证书

31. End

32. End

2.3　土壤资源数据访问权限共识研究

基于信誉值排序机制对 PBFT 共识机制进行改进,解决性能瓶颈问题。并构建访问控制模型,制定访问控制策略,保证用户访问土壤资源数据的可信性、真实性。

2.3.1　RSPBFT 共识机制设计

PKI 框架提高了用户身份认证的安全性,但由于繁琐的信息交互过程,导致效率受到影响,因此通过使用一种快速、安全的共识机制平衡系统效率。PBFT 具有速度快、安全性高,且适用于主从链的特点,但随访问土壤资源数据的用户节点逐渐增加,只使用 PBFT 共识算法面临性能瓶颈问题,例如,在网络中出现恶意节点时,会在共识过程消耗额外算力,在主节点故障时,无法将故障节点在下轮竞选中有效剔除。

在基于主从多链的土壤资源数据可信访问模型中,主链采用 POA 进行共识,各条从链则引入 RSPBFT 机制,以提升共识效率和安全性。

RSPBFT 在传统 PBFT 共识机制的基础上,结合节点综合信誉值排序机制,通过分级选取主节点和共识节点,优化共识流程。具体而言,综合信誉值为 C1 等级可以参与主节点选举,C2 等级以上节点参与共识过程,C3 等级节点只负责记录共识结果不参与共识(图 4)。这种信誉值驱动的选举机制符合土壤资源数据对节点分级的要求,确保主节点优先从高级用户节点中选取,从而提高系统稳定性和数据访问安全性。

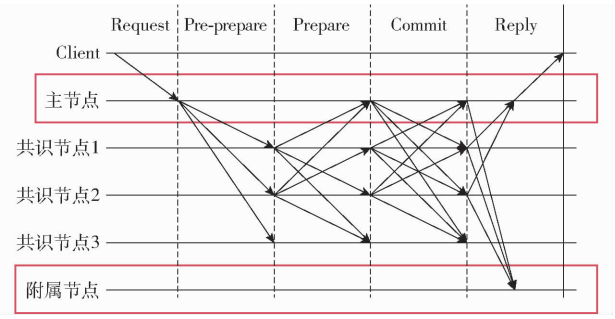

图 4 RSPBFT 共识过程

Fig. 4 RSPBFT consensus process

根据上述共识算法,提出基于 RSPBFT 算法的共识协议,以证书签发操作为例,算法协议流程如图 5 所示。

(1)用户 U 向域内根 CA 发送证书申请请求。

(2)根 CA 验证用户 U 信息,之后签发数字证书并将信息发送给主节点。

(3)主节点验证证书和交易信息的合法性,之后打包广播 Pre-prepare 消息给共识节点。

(4)共识节点在收到 Pre-prepare 消息,验证消息后,发送 Prepare 消息至主节点并将消息写入交易日志。

(5)若主节点收到来自全部节点的消息反馈是一致的,则共识达成,主节点向客户端发送结果,并在区块链网络中广播,从链中所有节点同步区块;若不一致,执行一致性协议共识算法,执行步骤(6)。

(6)共识节点收到 Pre-prepare 消息,验证消息后进入准备阶段,互相广播 Prepare 消息,并将消息写入交易日志。

(7)当共识节点和主节点收到 $2f$ 个 Prepare 消息与 Pre-prepare 消息一致,互相广播 Commit 消息。

(8)节点收到 $2f+1$ 个相同的 Commit 消息后,将 Reply 消息发给主节点和附属节点并同步区块。

(9)主节点收到 $2f+1$ 个 Reply 消息后发送给根 CA。

(10)RSPBFT 共识协议至此完成,根 CA 将证书签发结果返回给用户。

RSPBFT 通过在特定区域的动态主节点选举,提高了主节点安全性、稳定性。并且只选取中高信誉值节点进行共识,可以将通信复杂度从原来的 $O(i^2)$减小为 $O(j^2)$,$j \ll i$(j 为参与共识节点数量,i 为全部节点数量),提高区块链网络中节点数量众多时性能,适用于土壤资源快速、可信访问需求。

2.3.2 基于综合信誉值的访问控制策略制定

基于区块链 PKI 生成的证书,根据土壤资源数据敏感度等级、用户身份属性和节点综合信誉值进行访问控制,结合智能合约实现安全、高效的访问控制。土壤资源数据库或者用户隐私信息数据拥有者根据数据敏感度等级设定访问控制策略,通过智能合约方式存储到区块链,经过后续一系列的访问控制策略,完成对本次访问请求的判定。

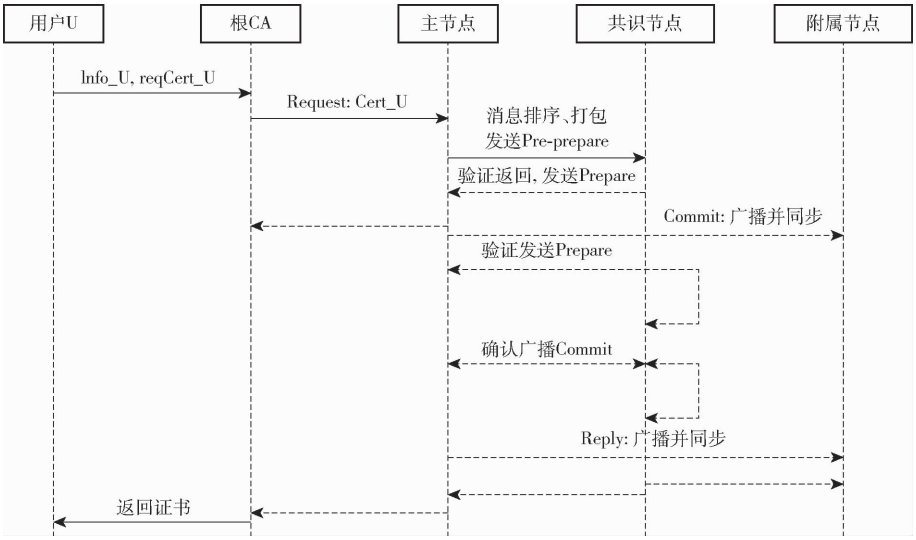

图 5 基于 RSPBFT 共识算法的协议流程

Fig. 5 Protocol flow based on RSPBFT consensus algorithm

根据用户节点的综合信誉值进行综合信誉值判定规则制定，用户综合信誉值与土壤资源数据敏感度关系如表 3 所示。

表 3　综合信誉值与可访问土壤资源数据关系

Tab. 3　Relationship of comprehensive reputation scores and accessible soil resource data

综合信誉值		Ⅰ	Ⅱ	Ⅲ
高级用户	C1	√	√	√
	C2		√	√
	C3			√
中级用户	C1		√	√
	C2		√	√
	C3			√
低级用户	C1			√
	C2			√
	C3			√

注：√表示该等级用户访问权限。

在同一地域内分为高级用户、中级用户和低级用户，同一等级用户分为 C1、C2、C3，3 个不同综合信誉值等级。以高级用户为例说明综合信誉值与土壤数据资源的关系：C1 级高级用户可访问该地域内Ⅰ、Ⅱ、Ⅲ级数据资源；C2 级高级用户可访问该地域内Ⅱ、Ⅲ级数据资源；C3 级高级用户可访问该地域内Ⅲ级数据资源。

根据上述综合信誉值判定规则结合用户身份证书代表的地域等级制定省、市、县 3 种可信访问控制策略。

3　实验验证与系统实现

3.1　实验验证

测试环境基于 Hyperledger Fabric 2.5.10 搭建，使用 VMware 的 Ubuntu 20.04.6 虚拟机，Docker 版本为 27.3.1。硬件配置为：16 GB 内存、AMD Ryzen 7 8745H with Radeon Graphics 3.80 GHz 处理器，系统为 Windows 11。

3.1.1　土壤资源数据可信访问流程

对用户进行可信访问过程进行描述。访问节点通过身份注册后加入到区块链网络，可信访问时需在链上完成访问请求与身份证书验证。基于区块链的土壤资源数据可信访问流程如图 6 所示。

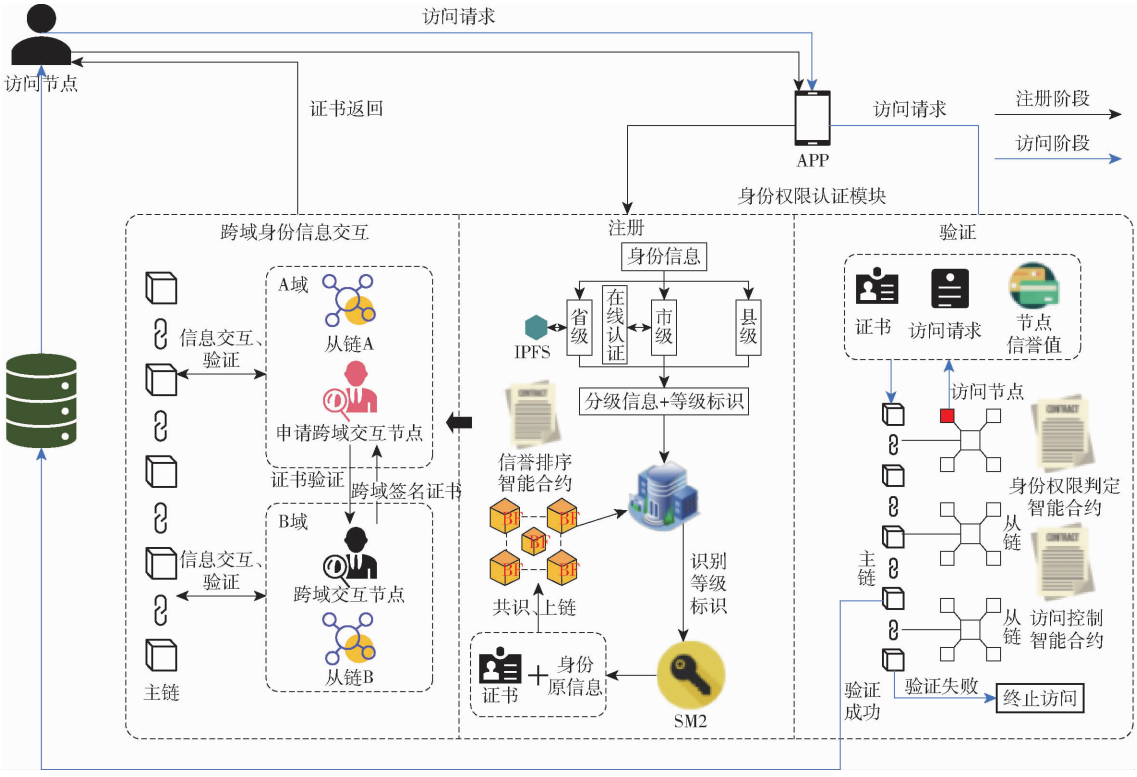

图 6　基于区块链的土壤资源数据可信访问流程

Fig. 6　Blockchain-based trusted access process for soil resource data

（1）身份注册

用户通过 APP 端完成对身份认证；县级需提供本人手机号和真实姓名；市级在前一等级基础上加入在线认证；省级在前一等级基础上进行人脸识别。考虑到隐私安全问题，省级人脸识别信息将存入 IPFS 中并生成地址；经过身份信息填写无误后在信息上加入各等级标识，将身份信息上链存储到该节点区块上。

（2）证书申请、签发与跨域交互

用户申请数字证书，需向当前域根 CA 发出证

书申请请求。根 CA 接收用户发来的证书申请请求,查询当前节点的存储区块,从区块链网络上获取相关人员的信息数据,用户信息验证通过后将用户的调用操作记录存储在对应从链上。一旦用户信息查询验证通过,便生成数字证书。证书由 SM2 国密算法生成私钥对身份信息数据进行加密产生,之后将身份原信息等信息和产生的证书在全网通过 RSPBFT 和 POA 共识算法达成共识。主节点和参与共识的节点将该节点证书用公钥进行解密并与原信息等信息进行对比,若该证书合法,则区块链网络通过智能合约通知根 CA 服务器,将证书返回给该节点。节点收到证书后,在区块链网络中完成跨域身份信息交互,并生成新的签名证书,各节点同步更新本地区块链,以达到操作公开透明且不可篡改,实现区块链网络中不同域间的信息互联互通。

(3)身份权限认证

用户节点完成上述步骤,将根据证书等级赋予节点综合信誉值作为节点实时状态的描述。区块链网络中通过智能合约的方式随时对节点信誉值和身份证书进行共识,同时在用户进行访问时也会根据信誉值和身份证书并结合访问请求信息完成对身份权限的访问控制。

(4)访问验证

访问请求直接发送到主链,同时访问节点将节点证书和当前信誉值发送到主链,主链在收到信息后,通过智能合约完成对本次访问请求的验证,若对访问请求的结果评定为成功,则可以访问。反之,视为恶意访问并终止访问。

3.1.2 加密算法对比

对 SM2 国密算法与 RSA 非对称加密算法、AES 对称加密算法在加解密过程的安全性和效率进行对比。非对称加密算法采用 RSA2048 位算法进行实验。分别对 SM2、RSA 和 AES 算法进行 10 次加密长度为 100 字符的加密和解密过程测试平均耗时,如表 4 所示。

表 4 加密算法效率

Tab. 4 Efficiency of encryption algorithms ns

算法	1	2	3	4	5	6	7	8	9	10	平均值
AES 加密	90 922	86 784	126 890	115 071	68 053	70 613	106 495	82 559	176 767	68 735	99 289
AES 解密	554 752	487 338	1 772 286	480 255	516 906	408 959	477 610	385 151	1 023 529	423 167	652 995
RSA 加密	569 642	134 826	2 773 907	339 839	92 629	107 989	141 183	135 381	140 330	125 994	456 172
RSA 解密	3 199 702	1 441 790	15 735 197	21 189 656	2 733 651	1 651 753	1 883 518	3 592 274	2 085 758	4 150 652	5 766 395
SM2 加密	113 824	33 676	479 317	67 867	22 389	27 993	27 430	24 614	29 481	27 198	85 379
SM2 解密	639 913	357 958	2 736 532	4 237 873	547 892	426 938	327 919	624 743	478 384	830 132	1 120 828

由表 4 可知,在加密和解密过程 SM2 算法平均耗时相较 RSA 算法基本提升 5 倍,略低于 AES 算法。RSA 算法密钥长度为 2 048 位,而 SM2 算法仅有 256 位,且要达到相同的安全等级,SM2 算法所需公私钥长度比 RSA 算法短很多。使用 SM2 算法进行数据加密以及身份认证比 RSA 算法耗时更短且更安全。

3.1.3 计算开销测试

与其他跨域交互方案在计算开销方面进行了测试,忽略与跨域过程无关的因素,主要体现在加解密次数、签名与验证次数、双线性运算次数、哈希运算次数 4 类计算资源上。假设所有方案使用相同的加解密算法,使用同一算法情况下可从图 7 直观地体现各方案计算开销。

在加解密次数中,本文只在生成证书时使用加解密算法对身份原信息进行计算,后续在跨域身份认证过程全部使用各节点证书进行信息交互。本文相较于其他方案[27-29]加解密次数大幅降低,其他方案在跨域过程需涉及隐私数据表明身份,而本文方案证书本身即可代表身份信息。本文方案与其他方案签名与验证次数基本持平。由于本文使用 SM2 算法不涉及双线性运算,可以在保证安全性的同时保持效率。本文方案哈希运算次数最多,但计算开销远小于其他 3 类计算资源。

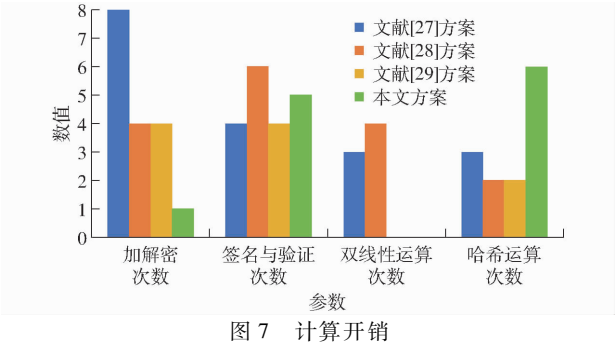

图 7 计算开销

Fig. 7 Calculated cost

使用 SM2 算法测试 4 类计算资源平均耗时可知,加密耗时 T_{AE}、解密耗时 T_{AD}、签名耗时 T_{AS}、验签耗时 T_{AV}、双线性运算耗时 T_P、哈希运算耗时 T_H 分别为 1.35、1.26、1.06、1.48、9.64、0.02 ms。并

对各跨域方案具体步骤进行数值分析(表 5)，T_0 表示每次通信交互所需时间，假设各方案中每次 T_0 时间相同。由表 5 可知，本文方案耗时较短，由于本文使用主从多链结构，在通信交互的次数上最多，但还不会影响整体效率，相较现有跨域交互方案计算开销平均降低 30%。总之，本文所提出的跨域身份认证方案在计算开销和计算耗时方面具有一定优势。

表 5　计算量与耗时

Tab. 5　Computation and time

方案	计算量	耗时/ms
文献[27]	$8(T_{AE}+T_{AD})+4(T_{AS}+T_{AV})+3T_P+3T_H+6T_0$	$60.02+6T_0$
文献[28]	$4(T_{AE}+T_{AD})+6(T_{AS}+T_{AV})+4T_P+2T_H+5T_0$	$64.28+5T_0$
文献[29]	$4(T_{AE}+T_{AD})+4(T_{AS}+T_{AV})+2T_H+4T_0$	$20.64+4T_0$
本文	$T_{AE}+T_{AD}+5(T_{AS}+T_{AV})+6T_H+10T_0$	$15.43+10T_0$

3.1.4　共识性能测试

通过 Hyperledger Caliper 工具对 RSPBFT 算法与 PBFT 算法在不同情况下进行了性能和安全性分析。

(1)理论分析

PBFT 算法在选举主节点的过程采用全节点随机选举，而 RSPBFT 算法根据信誉值排序机制划分出 1 个高信誉值区域进行主节点选举，可以有效提高系统安全性、鲁棒性与性能。RSPBFT 算法通过动态调整综合信誉值，主节点选举偏向高信誉值节点，能够减少主节点发生故障的概率，从而降低重新选举的开销。存在作恶节点时，RSPBFT 可以根据节点行为调整节点信誉值，快速将作恶节点踢出主节点选举过程，而 PBFT 无法在共识过程有效遏制节点的恶意行为，会使系统消耗额外的算力。

(2)实验分析

区块链网络中系统吞吐量即系统每秒可处理事务的数量(Transaction per second，TPS)，该指标是衡量共识算法性能的重要依据。分别测试 RSPBFT 和 PBFT 在节点数量不同时处理相同请求次数时的吞吐量变化，以及在节点数量相同处理不同请求次数时的吞吐量变化，同时在实验中随机加入节点的恶意行为。

将请求次数设置为 400 次，分别对节点数量为 12、16、20、24、28、32 时对共识算法的吞吐量进行测试，实验结果如图 8 所示。

将节点数量设置为 32 个，请求次数分别为 10、50、100、200、400、800 时进行测试，实验结果如图 9 所示。

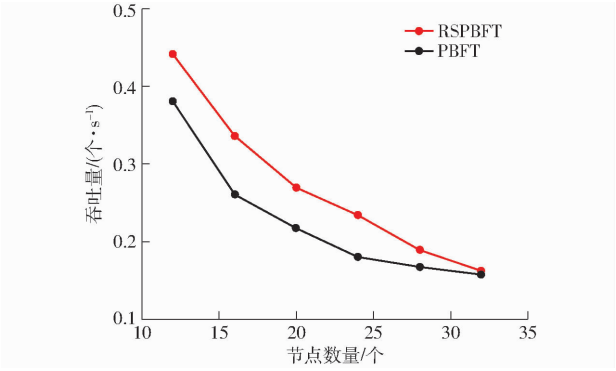

图 8　不同节点数量下吞吐量变化曲线

Fig. 8　Throughput variation curves for different numbers of nodes

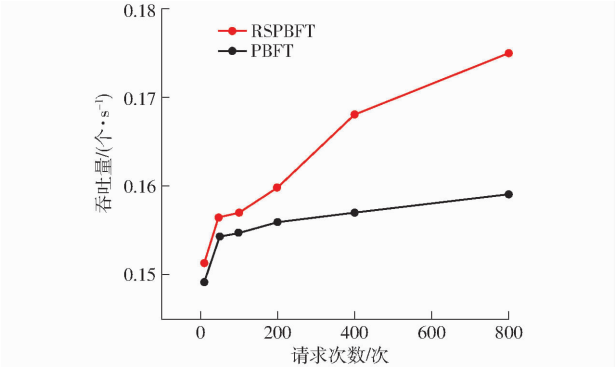

图 9　不同请求次数下吞吐量变化曲线

Fig. 9　Throughput variation curves for different number of requests

在不同请求负载与节点规模条件下，RSPBFT 算法均优于 PBFT 算法。综合统计结果表明，RSPBFT 整体平均吞吐量提升约 16.2%，在中等规模网络条件下最高可达 28%，在高并发场景下提升超过 12%，表明 RSPBFT 算法在网络扩展与高负载环境中具有更好的性能优势。

3.2　系统设计与实现

3.2.1　系统架构设计

提出基于区块链的土壤资源数据可信访问系统结合土壤资源数据对安全性、可信性的需求，采用主从多链架构和 PKI 框架，保障隐私数据安全交互、身份权限可信认证。系统架构如图 10 所示，分为物理层、共识层、数据层、合约层、网络层、应用层。

物理层通过网闸将访问请求指令交给土壤资源数据库处理信息，采用数据切片技术和非对称加密算法调用数据，并制定数据等级规定以严格控制用户访问，提升系统可信性和安全性。数据层包括证书数据库、身份信息库、节点日志记录和数字签名等链上数据，由根 CA 根据用户身份信息和等级分发证书，同时通过节点交易行为判定综合信誉值。共

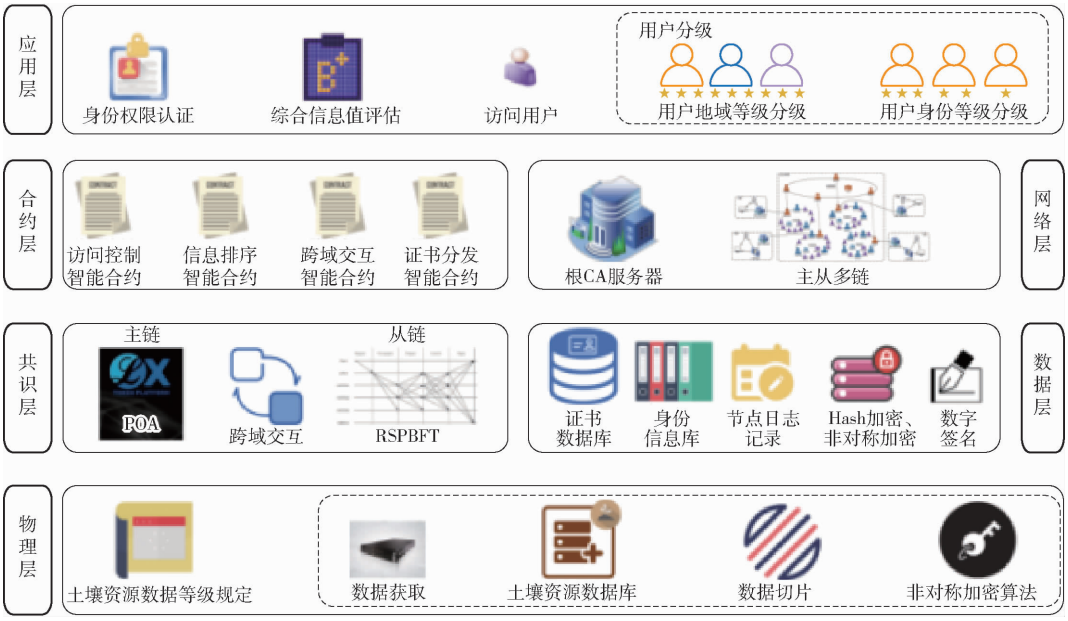

图 10 系统架构设计

Fig. 10 System architecture design

识层采用省级链内的 POA 共识机制、市县链内的 RSPBFT 共识机制,以及链间跨域交互机制,完成用户身份权限的可信认证,提高共识效率和安全性。网络层通过根 CA 服务器及主从多链架构对用户身份信息进行密码学处理,利用身份证书实现快速、安全的身份信息交互,避免信息泄露。合约层包括访问控制、信誉排序、跨域交互和证书分发等智能合约,将相关法律条例嵌套其中,实现用户身份规范化管理。应用层根据用户需求提供身份权限认证、综合信誉值评估及用户分级等服务,为用户提供安全可信的身份认证、实时身份状态评估和分级服务支持,实现土壤资源数据的高效、安全访问。

基于系统架构设计,构建土壤资源数据可信访问系统。系统功能划分为四大核心应用模块:身份管理、可信访问、访问记录管理和信誉值管理。身份管理模块负责用户注册、身份认证、权限分级以及证书申请和发放,将用户身份信息和权限等级上链存储;访问记录管理模块实现访问记录查询,确保对用户操作记录的链上监管和实时溯源;可信访问模块基于用户的综合信誉值和智能合约,对访问请求进行权限判定,并支持跨域数据访问和访问记录的不可篡改存储;信誉值管理模块对用户行为和系统运行状态进行实时监控,通过信誉值评估识别恶意用户并限制权限,同时提供访问行为审计和安全告警功能。

3.2.2 系统实现

在可信访问模型构建的基础上,开发了基于区块链的土壤资源数据可信访问系统。系统采用 B/S 服务器系统架构,利用 TCP/IP 协议实现网络通信。系统后端主要使用 Java 和 Go 开发,前端采用 Vue 框架构建,后端服务基于 Gin 框架实现,链下土壤资源数据库采用 MySQL 数据库。

系统采用 Hyperledger Fabric 区块链网络作为底链基础,支持多个组织、多节点部署。每个组织包括若干 Peer 节点、1 个 CA 节点和 1 个 Orderer 节点,其中 CA 节点负责管理证书分发与验证。区块链网络中交易和区块信息以哈希形式存储,确保数据的完整性和抗篡改性。如图 11 所示,系统在底链交易详情包含交易类型、背书签名、读写集等关键信息。



图 11 底链交易详情

Fig. 11 Bottom chain transaction details

如图 12 所示,在系统中访问用户通过身份注册后,会根据证书中反映的组织信息(省、市、县)和身份等级(高级、中级、低级)自动计算 PKI 信誉值。之后,在用户每次发起访问请求时,系统会依据用户的数字身份等级、信誉值以及数据敏感度级别,对访问权限进行严格控制,只有满足访问控制策略的用户才能成功访问数据,如图 13 所示。访问成功后,系统会将该次访问的记录上链,如图 14 所示。系统



图 12　系统查询用户信息界面

Fig. 12　System user information query interface

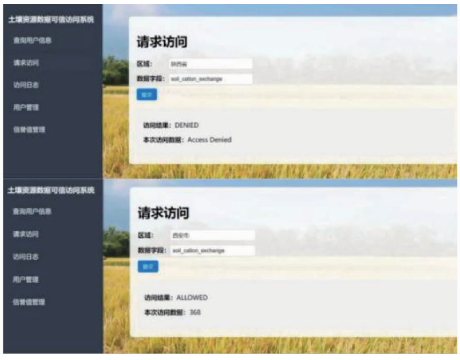

图 13　系统请求访问界面

Fig. 13　System requests access interface



图 14　系统访问记录查询界面

Fig. 14　System access record query interface

内置信誉值管理模块，当用户访问时，系统会根据访问结果（成功或失败）对用户信誉值进行动态调整，并记录详细的信誉值变动日志（包括变动时间、加分或减分情况、最终信誉值等信息），如图 15 所示，确保访问行为的可追溯性和数据安全。



图 15　系统信誉值管理界面

Fig. 15　System reputation value management interface

3.2.3　系统性能测试

为验证提出的可信访问模型在实际场景中可行性与有效性，结合土壤资源数据的地域性与敏感性特征，构建完整系统并开展性能测试。通过对可信访问系统核心功能模块的响应效率与安全保障能力进行评估，全面验证所提模型在实际环境下适用性与稳定性。

为评估本系统在多用户同时访问场景下响应性能，基于 Hyperledger Fabric 区块链网络及后端服务环境，使用 Apifox 工具模拟不同数量用户并发请求，测量“请求访问”“访问记录查询”“信誉值变动”等核心操作的响应时延，实验结果如图 16 所示。

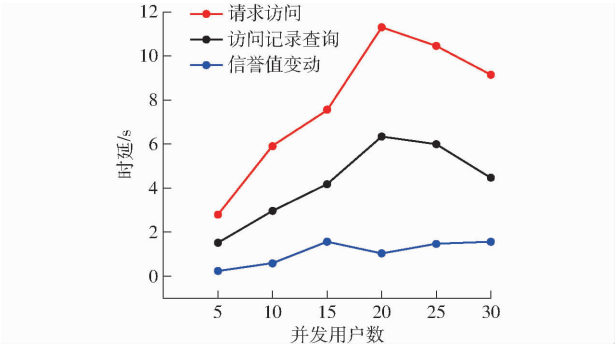

图 16　系统核心操作性能测试结果

Fig. 16　Performance testing of core system operations

由图 16 可知，在并发用户数从 5 逐步增加至 30 过程中，系统 3 类核心操作平均响应时延总体呈现平稳可控的增长趋势，体现出系统在并发负载下良好响应性能与处理能力。在并发用户数达到 20 以上时，时延降低，说明系统具备一定的负载调节与资源优化能力。整体结果验证了本系统具备适应高并发访问场景的可用性和响应稳定性，适用于土壤资源数据的可信访问需求。

此外，实验所使用的访问请求、访问控制逻辑及链下数据库均基于真实的土壤资源数据构建。数据库涵盖了不同地域的土壤资源信息，并根据行政区划和数据敏感度进行分级。访问控制策略根据用户证书等级与信誉值设定，模拟实际土壤信息平台中用户访问权限的动态判定过程。链下数据库真实存储了访问数据，而链上仅记录访问请求摘要和用户身份信息，在保证数据真实性的同时，保证了系统整体架构具备实际适应性与可部署性。

3.3　系统方案

表 6 为本文方案与其他文献方案在功能性与安全性方面的表现，重点分析分布式认证、跨域交互、节点信誉评估、匿名性、抵御 DDoS 攻击以及抗中间人攻击等关键特性。由表 6 可知，相比其他方案，本文方案在实现分布式认证、跨域交互和匿名性的基础上，进一步增强了抵御 DDoS 攻击以及抗中间人攻击的能力，可以保障系统在恶意攻击下的稳定性。同时，通过节点信誉评估机制，本文方案能够动态评估节点的行为和信誉，优化共识过程，提高整体框架的安全性和效率。与其他方案相比本文方案在土壤资源数据的可信访问场景中具有更强的适用性和可靠性。

然而，本研究仍存在一些值得进一步探索的问

表 6 土壤资源数据可信访问方案功能与安全性

Tab. 6 Functions and security of trusted access scheme for soil resource data

方案	文献[23]	文献[30]	文献[31]	文献[32]	本文方案
分布式认证	√	√	×	√	√
跨域交互	×	√	×	√	√
匿名性	√	√	√	√	√
抵御 DDos 攻击	×	×	×	×	√
抗中间人攻击	×	×	×	√	√
节点信誉评估	×	×	×	×	√

注:√表示该方法可以实现对应功能,×表示方法无法实现对应功能。

题:①智能合约优化:探索智能合约在土壤数据访问控制、授权管理等方面的应用,结合零知识证明、多方安全计算等隐私保护技术,提升数据共享的安全性和合规性。②AI 驱动的智能监管:结合人工智能技术,利用深度学习模型对链上数据进行异常检测,自动识别潜在的违规操作或数据篡改,提高系统的智能化水平和实时风险防范能力。

4 结束语

针对土壤资源数据安全可信访问需求,对土壤资源数据进行多维度特性分析与分级,构建基于主从多链架构和 PKI 框架的土壤资源数据可信访问模型,解决土壤资源数据访问安全性不足等问题,根据地域等级制定主从多链架构,通过省级节点作为主链实现全局管控,保障数据访问的安全性和可信性。设计了信誉排序机制,并以此为基础设计跨域信息交互机制和身份权限共识,提高了数据访问的效率与安全性。基于上述理论为基础结合 Hyperledger Fabric 平台,构建土壤资源数据可信访问系统整体架构,并进行系统实现。相关测试结果表明,本文方法在安全性、性能及计算开销方面均能满足土壤资源数据访问需求,相较于传统身份认证系统,具备更高的安全性和可靠性,为土壤资源数据的安全共享与高效利用提供了可行方案,有助于促进土壤资源数据的价值挖掘和智慧农业的发展。

参 考 文 献

[1] 第三次全国土壤普查工作方案[J]. 中国农业综合开发,2022(3):4 - 8.

[2] WANG J, ZHEN J, HU W, et al. Remote sensing of soil degradation: progress and perspective[J]. International Soil and Water Conservation Research,2023,11(3):429 - 454.

[3] 张忠学,尹致皓,余佩哲,等. 黑土区坡耕地水土保持耕作措施对土壤理化性状的影响[J]. 农业机械学报,2024,55(1):282 - 293.
ZHANG Zhongxue, YIN Zhihao, YU Peizhe, et al. Effects of soil and water conservation measures on soil physical and chemical properties in slope farmland in black soil region[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(1):282 - 293. (in Chinese)

[4] 张甘霖,史舟,王秋兵,等. 新时代土壤地理学的发展现状与趋势[J]. 土壤学报,2023,60(5):1264 - 1276.
ZHANG Ganlin, SHI Zhou, WANG Qiubing, et al. Development of soil geography in the new era and its future[J]. Acta Pedologica Sinica, 2023,60(5):1264 - 1276. (in Chinese)

[5] FANG L, LI Y, YUN X, et al. THP: a novel authentication scheme to prevent multiple attacks in SDN-based IoT network[J]. IEEE Internet of Things Journal, 2020, 7(7): 5745 - 5759.

[6] OGUNDOYIN S O, KAMIL I A. Secure and privacy-preserving D2D communication in fog computing services[J]. Computer Networks, 2022,210:108942.

[7] ZHANG C, LIAN Z, HUANG H, et al. PCIDS: permission and credibility-based intrusion detection system in IoT gateways [J]. IEEE Internet of Things Journal, 2024, 11(1): 904 - 913.

[8] WANG W, HUANG H, YIN Z, et al. Smart contract token-based privacy-preserving access control system for industrial Internet of Things[J]. Digital Communications and Networks, 2023, 9(2): 337 - 346.

[9] 郝亚丽. 农业物联网轻量级身份认证策略的研究[D]. 张家口:河北北方学院,2023.
HAO Yali. Research on lightweight identity authentication strategy for agricultural Internet of Things[D]. Zhangjiakou: Hebei North University, 2023. (in Chinese)

[10] BUCCAFURRI F, ANGELIS D V, LAZZARO S, et al. Enforcing security policies on interacting authentication systems[J]. Computers & Security,2024,140:103771.

[11] 许继平,王健,张新,等. 区块链驱动的稻米供应链信息监管模型研究[J]. 农业机械学报,2021,52(5):202 - 211,101.
XU Jiping, WANG Jian, ZHANG Xin, et al. Information supervision modeling of rice supply chain driven by blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(5):202 - 211,101. (in Chinese)

[12] 刘晓辉,罗娜,邢斌,等. 基于属性可搜索加密的农产品区块链追溯隐私数据访问控制方法[J]. 农业机械学报,2024,55(10):433 - 443.
LIU Xiaohui, LUO Na, XING Bin, et al. Attribute-based searchable encrypted agricultural blockchain traceability private data access control method[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(10):433 - 443. (in Chinese)

[13] 高官岳,孙传恒,罗娜,等.基于区块链的农产品供应链溯源数据多条件查询优化方法研究[J].农业机械学报,2024,55(3):362 - 374.
GAO Guanyue, SUN Chuanheng, LOU Na, et al. Blockchain-based multi-condition query optimization method for traceability data of agricultural product supply chain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024,55(3): 362 - 374. (in Chinese)

[14] 李馥娟,马卓,王群.区块链系统身份管理机制研究综述[J].计算机工程与应用,2024,60(1):57 - 73.
LI Fujuan, MA Zhuo, WANG Qun. Survey on identity management in blockchain systems[J]. Computer Engineering and Applications, 2024, 60(1):57 - 73. (in Chinese)

[15] PATEL N, SHUKLA A, TANWAR S, et al. KRanTi: blockchain-based farmer's credit scheme for agriculture-food supply chain[J]. Transactions on Emerging Telecommunications Technologies, 2024, 35(4):e4286.

[16] 王少华,孙传恒,罗娜,等.面向预制食品溯源的隐私数据加密共享方法研究[J].农业机械学报,2024,55(5):405 - 418.
WANG Shaohua, SUN Chuanheng, LUO Na, et al. Privacy data encryption sharing method for prepared food traceability[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(5):405 - 418. (in Chinese)

[17] VERN P, PANGHAL A, MOR R S, et al. Unlocking the potential: leveraging blockchain technology for agri-food supply chain performance and sustainability[J]. The International Journal of Logistics Management, 2024: 35(7):103.

[18] ZHU L, LI F. Agricultural data sharing and sustainable development of ecosystem based on block chain[J]. Journal of Cleaner Production, 2021,315:127869.

[19] ZHOU J, FENG Y, WANG Z, et al. Using secure multi-party computation to protect privacy on a permissioned blockchain [J]. Sensors, 2021, 21(4):1540.

[20] LOU J, BHAT S A, HUANG N. Blockchain-based privacy-preserving data-sharing framework using proxy re-encryption scheme and interplanetary file system[J]. Peer-to-Peer Networking and Applications, 2023, 16(5):2415 - 2437.

[21] LIANG W, YOU L, HU G, et al. LRS_PKI: a novel blockchain-based PKI framework using linkable ring signatures[J]. Computer Network, 2023, 237:110043.

[22] 任守纲,何自明,周正己,等.基于 CSBFT 区块链的农作物全产业链信息溯源平台设计[J].农业工程学报,2020,36(3):279 - 286.
REN Shougang, HE Ziming, ZHOU Zhengji, et al. Design and implementation of information tracing platform for crop whole industry chain based on CSBFT - Blockchain[J]. Transactions of the CSAE, 2020, 36(3): 279 - 286. (in Chinese)

[23] 张新,刘崇宣,许继平,等.基于多链的果蔬全程全息信息管理模型构建与系统化实现[J].农业机械学报,2024,55(6):365 - 379.
ZHANG Xin, LIU Chongxuan, XU Jiping, et al. Construction and systematic implementation of multi-chain-based management model for fruits and vegetables in a full-process and information scheme[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(6):365 - 379. (in Chinese)

[24] MANOJ T, KRISHNAMOORTHI M, NARENDRA V. A trusted IoT data sharing and secure oracle based access for agricultural production risk management[J]. Computers and Electronics in Agriculture, 2023, 204:107544.

[25] AZEVEDO P, GOMES J, ROMAO M. Supply chain traceability using blockchain[J]. Operations Management Research, 2023, 16(3):1359 - 1381.

[26] VANGALA A, SUTRALA A K, DAS A K, et al. Smart contract-based blockchain-envisioned authentication scheme for smart farming[J]. IEEE Internet of Things Journal, 2021, 8(13):10792 - 10806.

[27] SINGH P, MASUD M, HOSSAIN M S, et al. Cross-domain secure data sharing using blockchain for industrial IoT[J]. Journal of Parallel and Distributed Computing, 2021, 156:176 - 184.

[28] 谭琛,陈美娟,ACKAH Amuah Ebenezer. 基于区块链的分布式物联网设备身份认证机制研究[J].物联网学报,2020,4(2):70 - 77.
TAN Chen, CHEN Meijuan, ACKAH Amuah Ebenezer. Research on distributed identity authentication mechanism of IoT device based on blockchain[J]. Chinese Journal on Internet of Things, 2020, 4(2):70 - 77. (in Chinese)

[29] 赵平,王赜,李芳,等.主从区块链容错异构跨域身份认证方案[J].计算机工程与应用,2022,58(22):79 - 88.
ZHAO Ping, WANG Ze, LI Fang, et al. Master-slave blockchain fault-tolerant heterogeneous cross-domain identity authentication scheme[J]. Computer Engineering and Applications, 2022, 58(22):79 - 88. (in Chinese)

[30] LUO F, HUANG R, XIE Y. Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks[J]. Journal of King Saud University-Computer and Information Sciences, 2024, 36(2):101946.

[31] GEORGE W, AI-ANSARI T. GM-ledger: blockchain-based certificate authentication for international food trade[J]. Foods, 2023, 12(21):3914.

[32] SHEN M, LIU H, ZHU L, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(5):942 - 954.