基于区块链的医院网络安全框架设计与实现

于翠梅

（山东省菏泽市郓城县妇幼保健院，山东 菏泽 274700）

摘 要 区块链技术是一门新兴的技术，主要通过无人的信用委托平台，实现互联网互相信任的问题，通过加密数据信息，保障数据存储的安全，也可以使数据的记录更加透明与准确。本文阐述了区块链技术的相关知识，分析了区块链技术在医院网络安全中出现的问题，探讨了基于区块链的医院网络安全架构设计与实现策略。

关键词 区块链；医院；网络安全；框架设计

中图分类号：TP393.08 **文献标识码**：A **文章编号**：2097-3365(2024)03-0022-03

医院作为重要的公共服务机构，拥有大量患者的个人隐私信息与医疗数据，因此，保护医院网络安全十分重要。而传统的网络安全防护措施，通常难以应对日益复杂的网络攻击手段，而区块链作为一种新型的技术具有许多优势，为医院网络安全提供了新的解决方案。

1 区块链技术概述

1.1 区块链的概念

区域链是一种应用模型，在模型中能够实现两点之间的功能传输，还可以对加密算法等相关功能进行运算，使不同节点形成数据信任，从而获得相应的权益。从概念出发，区块链技术通常被人们认为是一种数学算法。从广义角度来说，对区块链技术进行理解，该技术就是通过一些跨链式的结构进行数据的验证与传输，并运用自动化的脚本代码，达到智能合约的目的，再进行后续的操作。从狭义角度来说，分析区块链技术，可以认为此技术标准是参考时间的先后顺序，利用链接的方法形成链式数据的结构。

1.2 区块链的技术原理

数据的产生形式通常会通过一连串的密码学方法构建数据块，最终形成分布式的账簿系统，也就是区块链的技术原理。区块链技术包括链接与数据块，数据块属于数据结构，这种数据结构能够记录交易。挖矿记录或被验证的转账记录是交易记录，对数据块而言，它肩负着系统内加密的数据信息，同时这些数据信息需要在一定的时期内进行存储，对于验证的有效性与次生区块的形成具有一定的作用。链接就是区块和区块间的关系，最终形成的区块链。对于区块单元而言，它包括三个部分，分别是交易信息、随机数等，交易信息中有双方交易的数量与交易时形成的电子货币数字签名与双方的私钥等，这些交易信息也是区块需要承担的任务。数字签名是一个证明数据的机制与依据。它对数学机制的所有权进行证明，数字签名包含诸多内容，比如发送者的私钥等，从而确定发送方式，通过确认签名发出消息，此外，还包括确定整个数据或信息的完整性[1]。

1.3 区块链技术的特征

区块链技术属于分布式的数据库技术，它能够使数据之间实现共享，同时具有一些基本的特征，比如集体维护、去中心化、可靠数据库等，去中心化的主要特征就是在运营中没有中心化的硬件或管理机构，每一个节点的权利与任务都是平等的。若在其中有任何一个节点没有工作，都不会对整个运行系统造成影响。去信任就是在区块链技术运营中，数据库的运作与数据都是公开的，在各节点执行交易时不需要信任，因此叫做去信任，也就是在系统所规定的范围与时间内，不同节点是不能欺负彼此的。集体维护的特征就是在系统中，每个节点都是受到维护的，每个节点都参与到系统的维护中，可靠数据库就是在运营系统中，所参与的节点都是完整的信息。因此，对某个节点的数据库进行修改是不能实现的，系统会通过自己的判断，将频率最多且出现相同的记录认定为真实。对于其安全性而言，整个节点的参与度与计算能力成正比。参与度的高低直接决定计算能力的强弱，同时也代表了系统数据的安全性。

2 区块链技术在医院网络安全中出现的问题

2.1 数据存储空间不足

在区块链技术应用中，数据库是一个重要的数据集合，每笔交易都在数据库中存储，因此，所有参与的节点都需要下载与更新存储的数据，并下载与记录

自始至终的数据。在医院网络安全中，拥有数字化技术数据存储量在不断地攀升。若在医院网络安全技术中应用区块链技术，它将承载大量的医院信息与患者的数据，这就需要大量的数据库资料存储空间。若想使每个节点的数据达到同步，就需要庞大的区块链数据存储空间，这也是在众多领域中区块链技术应用的关键。对医疗系统来说，其对医疗系统工作快速开展与医患数据的准确性具有直接的影响[2]。

2.2 大规模交流下的抗压问题

随着医院内部与外部信息交流不断增加，区块链技术的应用也随之扩展。然而，当大量数据同时传输时，区块链网络可能面临严重的抗压问题。医院网络中的交流可能涉及大量的医疗数据，比如，患者的病历、医疗记录与医嘱等。这些数据的传输需要高速与稳定的网络连接，但区块链技术的分布式特性可能导致传输速度较慢，从而影响医院网络的正常运行。大规模交流下的抗压问题还涉及网络的带宽和存储容量。区块链技术需要大量的存储空间来存储交易数据和区块链的历史记录。当医院网络中的交流数据量过大时，可能会导致网络带宽和存储容量不足的问题，从而影响数据的传输与存储。区块链技术的网络节点数量也可能影响到网络的抗压能力。在医院网络中可能存在大量的节点参与区块链的验证和交易确认过程。当节点数量过多时，可能会导致网络拥堵和延迟，从而影响到医院网络的正常运行[3]。

2.3 医院网络安全缺乏实践经验

尽管区块链技术被认为是一种安全且去中心化的解决方案，但在医院网络环境中应用时仍然面临一些挑战。医院网络安全意识的欠缺是导致问题出现的主要原因，由于医疗工作人员对区块链技术并不熟悉，缺乏对网络安全威胁的认识和理解，这会导致区块链系统在使用与管理时出现漏洞，从而使医疗数据容易受到攻击。由于医院网络环境的复杂性，区块链技术的实施也会面临一些难题，医院网络通常包含多个终端设备、传感器、服务器等，这些设备之间的数据交互需要高度的安全性，然而，区块链技术的部署与配置对于医院网络来说可能是一项复杂的任务，需要采用专业技术对医院进行管理。医院网络中的潜在安全漏洞也十分令人担忧，由于医院网络常常连接到外部网络，如互联网等，因此，存在被黑客攻击的风险[4]。

2.4 隐私与安全问题

尽管区块链技术本身被认为是安全的，但其应用在医院网络中仍然存在一些风险。由于区块链是一个公开的分布式账本，其中的交易信息是可追溯的，这可能导致患者隐私泄露的风险。虽然区块链数据是匿名的，但患者的身份信息仍然可能通过其他方式与其相关联。区块链技术的去中心化特性，使得数据存储在多个节点上，这增加了网络攻击的潜在目标。黑客可能通过攻击这些节点来窃取敏感的医疗信息，从而对患者的隐私和安全造成威胁。由于区块技术是基于密码学的，一旦密码被破解，整个网络的安全性将受到威胁。区块技术还具有可扩展性，由于每个节点都需要存储完整的区块链数据，就会导致数据量的快速增长，从而对网络的带宽与存储资源提出挑战。

3 基于区块链的医院网络安全框架设计与实现策略

3.1 建立分布式的网络结构

基于区块链的医院网络安全架构设计需要建立一个分布式的网络结构，传统的网络结构中存在着集中式的服务器，一旦服务器被攻破，整个系统的安全性就会受到威胁。而区块链的分布式结构使得数据存储在多个节点上，没有单一的中心服务器，从而降低了被攻击的风险。同时，区块链的去中心化特点也增加了系统的抗攻击能力，即使某一节点被攻破，其他节点仍然能够运行正常，保证了数据的安全性与可靠性。建立分布式网络结构，可以减少单点故障的风险。分布式网络结构将数据与计算资源分散在多个节点上，即使某个节点发生故障，其他节点仍能正常运行，保证医院网络的连续性和可靠性。分布式网络结构还可以增加网络的安全性，其每个节点只存储部分数据与计算任务，大大降低了黑客获取全部数据的难度，同时，基于区块链的分布式账本技术可以确保数据的不可篡改性与透明性，使得医院网络更加安全可信。同时，还可以提高网络的性能与可扩展性，实现并行计算与负载均衡，提高网络的处理能力和响应速度。伴随医院规模的不断扩大，可以方便地添加新的节点来扩展网络的容量与覆盖范围[5]。

3.2 引入智能合约

智能合约是一种合约的进化形式，它利用人工智能与机器学习的技术，使合约能够自动学习和适应不断变化的网络环境。智能合约是区块链中的一种自动执行的合约，可以确保数据的安全和一致性。医院可以通过智能合约实现数据的自动验证与控制，确保只有授权的用户才能访问与修改数据。同时，智能合约

还可以记录和追踪数据的变更历史，任何人都无法篡改数据，保证了数据的完整性和可追溯性。智能合约在医院网络安全中的应用是为了提高网络的自我防御能力，通过对网络流量进行实时监测与分析。智能合约可以识别异常行为与潜在的威胁，并自动采取相应的应对措施，比如，当发现有可疑的网络攻击行为时，智能合约可以立即启动防御机制，如封锁攻击源 IP 地址或限制访问权限，以保护医院网络的安全。智能合约还可以进行自我学习与优化。通过不断分析与整理医院网络的安全日志与历史数据智能合约，能够识别出网络的漏洞与弱点，并提出改进的方案。这种自我学习与优化的过程，使得医院网络安全架构能够不断适应新的威胁与攻击方式，保持较高的安全性与可靠性。

3.3 加强身份认证与访问控制

基于区块链的医院网络安全架构设计需要加强身份认证和访问控制。传统的网络安全系统往往通过用户名和密码来进行身份认证，但这种方式容易被攻击者破解，而区块链技术可以通过公钥和私钥的加密方式来进行身份认证，只有拥有私钥的用户才能访问和修改数据。区块链技术的去中心化特性为医院提供了更加安全和可信的身份验证机制。通过使用区块链，医院可以建立一个分布式的身份认证系统，确保其有被授权的用户可以访问敏感的医疗信息。医院可以将所有医护人员的身份信息存储在区块链上，这些身份信息包括医生、护士和其他医疗人员的资质、执业证书与许可证等，每个医务人员都有一个唯一的身份标识符，该标识符被记录在区块链上，并与其身份信息进行关联。当医务人员需要访问医疗信息时，他们需要使用其身份标识进行身份验证。区块链技术可以确保这些身份信息的真实性与安全性，防止身份欺诈和冒名顶替。加强访问控制也是保护医疗网络安全的重要手段。医院可以实现细粒度的访问控制，确保只有授权的用户可以访问特定的医疗信息。同时，基于区块链的访问控制，可以将权限管理的过程透明化，确保只有授权人员才能进行敏感操作，提高了系统的安全性[6]。

3.4 加强数据隐私保护

基于区块链的医院网络安全架构设计，需要加强数据隐私保护。患者个人隐私信息和医疗数据的泄露，将对患者造成严重的损害，区块链技术可以通过加密算法和匿名化技术来保护数据的隐私性，确保只有授权的用户才能访问和使用数据，同时，区块链的不可篡改性，也可以防止数据被篡改或删除，保护数据的完整性与可信度。通过使用区块链技术语言，可以实现匿名化的数据存储和传输。区块链是一种分布式账本技术，每个参与者都可以验证和记录交易，而不需要透露个人身份信息，这意味着患者的个人身份和健康数据可以被加密，只有授权的参与者才能解密与访问，这将大大降低患者隐私被泄露的风险，并增加医院网络的安全性。区块链的不可篡改性是提高数据隐私保护的关键特性之一，一旦数据被写入区块链，就无法被删除或修改，只能添加新的交易记录。这确保了患者健康数据的完整性与真实性，防止任何未经授权的篡改。通过这种方式患者可以更加信任医院网络，并且对他们的个人数据的安全性与隐私保护有更多的控制权。同时，采用智能合约，也可以加强数据隐私保护，智能合约可以在区块链上执行。通过编写智能合约，医院可以定义与实施严格的访问控制策略，确保只有经过授权的参与者，才能访问患者的健康数据。

4 结论

基于区块链的医院网络安全架构设计，可以有效提升医院网络的安全性与可靠性。通过建立分布式的网络结构，引入智能合约、加强身份认证与访问控制以及加强数据隐私保护，可以有效防止网络攻击和数据的泄露，保护患者的个人隐私信息与医疗数据的安全。然而，区块链技术也存在一定的挑战与限制，因此，在实际应用中需要进一步研究与改进。

参考文献：

[1] 刘惠明，潘珺瑜 . 医疗区块链技术运用的法律规制探究 [J]. 卫生软科学 ,2023,37(12):28-33.
[2] 朱春伦，唐玲，邵维君，等 . 基于区块链的异地医疗信息共享试点项目实践 [J]. 中国数字医学 ,2024,19(01):29-33.
[3] 姚尧，袁骏毅，岑星星 . 基于区块链的电子病历安全共享方案 [J]. 医学信息学杂志 ,2023,44(11):84-89.
[4] 秦余腾，王秀娟，扈蕴琨，等 . 一种基于区块链的医院病历档案系统 [J]. 中国科技信息 ,2023(22):76-80.
[5] 沈益督 . 基于区块链技术的医院网络安全应用探究 [J]. 电脑知识与技术 ,2023,19(30):78-80.
[6] 郑荣，雷亚欣，张默涵，等 . 基于联盟区块链的多源个人健康信息协同共享模式研究 [J]. 图书情报工作 ,2023,67(20):79-92.