区块链技术在计算机网络安全中的实践研究

宋彦芳，高晨，李英 *

郑州大学第三附属医院，河南 郑州 450000

摘　　要： 互联网广泛普及背景下，计算机网络技术逐渐渗透到社会生产生活各个角落，加快社会进步和发展的同时，却也带来了一系列的风险和挑战。由于计算机网络的开放性特点，如何保障计算机网络安全逐渐成为人们重点关注的一个问题，而区块链技术作为一项时代前沿技术，在实际应用中能够净化网络环境，有效防范计算机网络安全风险，对于保障用户数据信息安全具有重要意义。文章主要围绕计算机网络安全中心区块链技术的应用情况进行分析，期待为相关工作展开提供参考和支持。

关 键 词： 计算机网络安全；区块链技术；网络环境；网络攻击

Practical Research on Blockchain Technology in Computer Network Security

Song Yanfang, Gao Chen, Li Ying*

Zhengzhou University Third Affiliated Hospital, Zhengzhou, Henan 450000

Abstract: In the context of the widespread popularity of the Internet, computer network technology has gradually penetrated into every corner of social production and life, accelerating social progress and development, but also brought a series of risks and challenges. Due to the open nature of computer networks, how to ensure the security of computer networks has gradually become a key concern for people. As a cutting-edge technology of the times, blockchain technology can purify the network environment and effectively prevent computer network security risks in practical applications, which is of great significance for ensuring the security of user data information. The article mainly analyzes the application of blockchain technology in the computer network security center, hoping to provide reference and support for related work.

Keywords: computer network security; blockchain technology; network environment; network attack

当前时代背景下，计算机网络技术不断更新迭代，计算机网络系统中，通常是采用防护、响应、检测和恢复等技术形成动态的安全防护体系，用于识别和防控网络安全问题，但仍然存在一定的欠缺和不足。区块链技术最初主要是在数字货币交易领域应用，随着此项技术逐步完善和创新，在计算机网络安全领域中同样展现出不俗的作用。因此，新时期进一步加强对区块链技术的研究有助于丰富理论研究成果，为技术创新发展做出更大的贡献。

一、区块链技术的特点和优势

区块链技术最初被提及，主要是在数字货币交易领域。区块链本质上属于共享数据库，实现大量数据信息的集中存储，每个区块等同于一个数据库存储单元。依托于哈希算法，区块哈希值在前一个区块信息中存储，数据信息规模随着区块数量增加而变大，通过增强各个区块之间的联系，最终形成了完整的区块链。区块链数据分布式存在，交易信息永久的留存[1]。

（一）区块链技术的特点

1. 开放性。区块链技术是依托于计算机网络诞生，区块链中的信息保持开放状态存放信息，但是隐私信息是保密的。只需要连接互联网，即可看到区块链中的双方交易记录，实现信息大范围共享。

2. 去中心化。去中心化是区块链技术的核心特点，相较于其他的现代化信息技术，区块链技术相较于独立存在，对于第三方机构依赖程度不高。因此，对于区块链而言，自身不仅可以独立存在，还可以自我验证和管理内部数据信息。

3. 安全性。区块链技术涵盖的数据信息规模大，涉及到很多交易信息，因此对于数据安全性要求较高[2]。区块链中超过半数的区块节点未掌握，自然无法获取网络整体的数据，因此区块链的内部数据存储较为安全可靠。

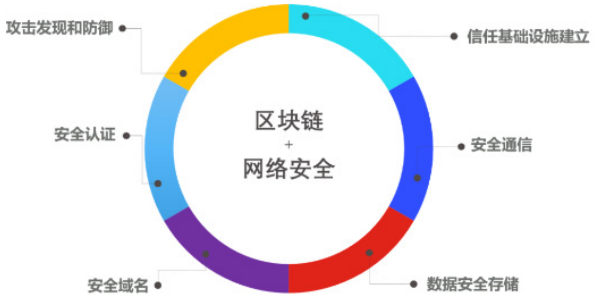
4. 匿名性。区块链技术的应用，共同规则为数据存储的基础，各节点遵循统一的规则传输和共享数据信息，不需要双方公开个人身份即可进行交易。所以，区块链技术除了保障交易顺利

通讯作者：李英

进行以外，也可以最大程度上保护个人隐私安全[3]。

（二）区块链技术的优势

一般情况下，计算机网络安全问题多是网络攻击入侵某个节点，或是恶意伪造的方式来获取信息，此种形式将不同程度上威胁到计算机网络安全[4]。反之，如果引入区块链技术手段，能够全面排查和剔除潜在的安全隐患，为计算机网络数据信息安全提供坚实保障。如图1。因此，区块链技术的优势主要表现在以下几个方面。



> 图 1 区块链的网络安全特性

1. 提高网络安全性。区块链技术内部采用共识安全机制，有机整合网络资源，共同识别和抵御个别入侵攻击行为。而且区块链技术的不可篡改、去中心化等特性，可以为网络安全提供坚实保障[5]。依托于区块链技术的分布式存储、验证机制，能够有效避免单点故障，维护数据信息真实性和可靠性。而且通过智能合约自动执行，能够显著减少人为欺诈和干预行为出现几率，最大程度上保障网络信息安全。

2. 精简身份信息验证流程。由于区块链技术的去中心化特性，区块链上的用户拥有唯一的身份标识，记录和验证用户的身份信息。此种分布式身份验证方式可以精简身份信息验证流程，提高验证的准确性，尽可能抵御非法访问行为出现。

3. 降低信任成本。传统计算机网络中，大多是依靠中心化维护和管理，但容易受到攻击，篡改信任机制，诱发信任危机。基于去中心化方式，运用区块链技术能够建立相互信任的关系，实现交易行为和数据共享安全可靠，降低信任成本[6]。

4. 推动数字化转型发展。区块链技术具有数据安全、去中心化、透明化等优势，有助于加快数字化转型和发展趋势，催生更多新兴产业发展。而且区块链技术同样具有可编程特点，能够结合用户实际需求和对象动态调整，或是同其他安全技术结合，更好地满足各个行业领域发展需求，保障计算机网络安全。

二、目前计算机网络安全面临的挑战

（一）多样化网络攻击手段

钓鱼攻击和社交工程是典型的网络攻击手段，把握人性的好奇心、信任等特点，诱骗用户泄漏敏感信息，或是自动化执行恶意操作。网络攻击手段日趋隐蔽、复杂，如，通过二维码、邮件伪装等形式快速传播，导致用户防范难度较大[7]。勒索软件是一种恶意攻击软件，通过对用户重要数据信息加密隐藏的方式，要求用户支付赎金来恢复数据访问权限。随着勒索软件持续更新，攻击范围逐渐广泛化，并且勒索软件可以联合其他攻击手段潜伏和渗透。如，联合 APT 攻击行为，实现目标长期潜伏和渗透。分布式拒绝服务（DDoS），主要是通过计算机或网络设备控制，发送大量无效请求给网络设备，以至于目标服务器资源消耗殆尽，自然难以正常提供服务。

（二）数据信息的安全保护

大数据、云计算等技术手段广泛应用下，数据信息的存储和传输安全面临着重重挑战，一旦重要的数据信息泄露，会为精准诈骗提供可乘之机，情况严重下造成重大的经济损失和负面影响。一般情况下，数据信息安全隐患超过半数以上来源于内部，如，员工操作疏忽、恶意行为或是系统漏洞等，都可能造成重大数据信息泄露，为企业数据信息安全带来严峻挑战。

（三）技术和资源限制

网络威胁不断演变发展，网络安全防护技术也在持续更新，但发展速度远远落后于网络威胁发展速度，此种情况下导致很多常规的安全防护措施无法应对新型网络威胁。另外，网络安全人员数量和资源不足，面对多样的网络威胁无法灵活有效应对，一旦安全防线失守，将造成重大的损失[8]。

三、计算机网络安全中心区块链技术的应用实践

（一）海量网络信息管理

区块链技术与之相比，拥有传统网络安全防护所不具备的共享数据库，不需要借助第三方的支持，即可借助共识系统将数据信心安全存储到区块链中，并实现对网络数据有效监督和管理。借助区块链技术的身份验证功能，用户的身份信息全部存储在区块链上，拥有授权的用户方可访问数据，即便黑客盗取了用户的账号和密码，也同样无法访问其账号内容。另外，区块链技术还拥有着数据信息灵活配置的交互功能，大范围的监控海量数据信息，实现信息良性传输和共享，避免重要数据信息被窃取、篡改[9]。例如，IBM 公司已经开始运用区块链技术，私有区块链网络中，用户允许和管理 IoT 数据。Obsidian 公司采用区块链技术保障社交媒体上用户的重要隐私信息安全，由于用户元数据在区块链系统中随机发布，用户即便攻击单一节点也是无法获取用户数据信息的，因此该公司推出的多款聊天软件深受用户喜爱。

（二）网络资产智能化管理

引入区块链技术，无论是有形资产，还是无形资产，都可以实现安全、可靠的管理。在无形资产管理方面，依托于区块链技术不可随意篡改和时间戳的功能特性，能够实现福彩管理、知识产权等监督管理，维护网络交易秩序，避免数字交易出现双重支付问题。面对有形资产管理，运用区块链技术和物联网技术可以实现资产精准标注和管理，此种方式多是在车辆、不动产等资产管理领域应用。如果某个环节如果发生异常情况，即可快速调取记录，定位异常情况出现环节，最大程度上提升产品生产线安全性[10]。

（三）网络安全通信

区块链技术采用先进加密算法，封装网络交易数据后进行传输，只有拥有私钥的用户才可以将数据揭秘访问，避免数据信息传输中被解惑、篡改，提供给网络通信高等级安全防护。另外，区块链共识机制作为保障计算机网络通信安全的基础保障，依据共识算法，对网络节点共同验证交易有效性，保障数据信息写入的一致性。如，比特币工作量证明机制，以太坊的权益证明机制，均属于共识算法范畴。借助竞争或是抵押方式，恶意节点无法攻击和篡改网络数据信息，最大程度上保障网络通信安全。

运用区块链技术通态加密、零知识证明等密码加密技术的应用，可以在不泄露信息前提下，有效验证数据信息有效性，为计算机网络信息提供高等级防护。如，医疗保健行业领域运用区块链技术，保障患者电子健康记录前提下，实现数据信息传输过程安全、可靠，避免重要数据信息泄露、滥用。伴随着物联网技术创新发展，设备安全问题随之涌现，运用区块链技术的去中心化身份验证与数据存储服务，极大地提高物联网设备安全性。如，Xage Security 公司运用区块链技术平台，有效保障网络设备隐私数据分发及认证安全，提供多形式的网络通信支持，促进物联网技术和区块链技术深度融合。

（四）防御供应链攻击

供应链攻击涉及到多个环节，由于此种攻击行为的隐蔽性和复杂性特点，安全防护难度较大。使用区块链技术，依托于分布式账本记录供应链的交易行为，实现供应链可追溯性和透明化。所有参与方能够实施查看供应链历史记录，及时发现和追踪潜在风险行为，便于企业快速响应供应链攻击，追踪风险源头，最大程度上减少损失。供应链管理中，企业运用区块链技术编写智能合约定义安全策略，组织未授权的访问，自动检测异常交易等行为，在出现异常情况下即可自动化启动安全防护措施，有效抵御供应链攻击。区块链技术同大数据、物联网等技术整合，建立实时监测和预警系统，收集节点设备数据信息，传输到区块链上，掌握供应链的具体运行状态。运用大数据分析技术，深度挖掘和分析数据信息，及时识别潜在攻击行为，系统检测到异常风险信号后，触发预警机制，通知相关人员及时处理，有效抵御供应链攻击。

四、结论

综上所述，计算机网络安全面临着多重攻击和挑战，为了保障网络信息安全，积极引入区块链技术很有必要。通过区块链技术有效应用，可以创设安全可靠的网络环境，及时发现和防控风险行为，为计算机网络数据信息安全提供坚实保障。

参考文献

[1] 张静，苏蓓蓓，黄星杰，等 . 基于区块链技术的计算机网络安全优化方法 [J]. 企业科技与发展 ,2022(3):49-51.

[2] 江荣娜 . 基于区块链技术的安全计算机网络设计与实施 [J]. 信息记录材料 ,2024,25(4):122-124.

[3] 孙卓，李辉 . 区块链技术在计算机网络安全中的应用 [J]. 计算机产品与流通 ,2022(11):58-60.

[4] 李兴福，肖仁锋 . 基于区块链技术的计算机网络安全优化分析 [J]. 数码设计 ,2023(1):32-34.

[5] 杨万纬，张彦林 . 区块链技术在计算机网络安全中的应用探索 [J]. 数字化用户 ,2024(37):137-138.

[6] 程力 . 区块链技术在计算机网络安全中的应用 [J]. 数字技术与应用 ,2022,40(9):240-242.

[7] 田帅 . 区块链技术在网络与信息安全领域的应用 [J]. IT 经理世界 ,2020,23(5):80.

[8] 徐梓容 . 大数据时代计算机网络安全技术的优化策略 [J]. 电子元器件与信息技术 ,2024,8(3):192-195,199.

[9] 熊辉，郭兴元，康娟 . 区块链技术与医疗健康大数据应用简析 [J]. 中国市场 ,2020(11):159-160.

[10] 原毅 . 大数据时代的计算机网络安全及防范措施分析 [J]. 中国新通信 ,2020,22(15):141.