

基于区块链技术的网络用户隐私信息安全防护

肖荣旺¹, 付莹莹²

1. 南昌大学共青学院, 江西 九江 332020

2. 睢宁经济开发区高级中学, 江苏 徐州 221200

DOI: 10.61369/SDME.2025300013

摘 要 : 抖音、微博和微信等社交媒体的飞速发展给人们的生活带来了便利, 但无形中增加了网络用户隐私信息泄露、窃取的风险, 容易给用户带来不可估量的损失。区块链技术具有去中心化、不可篡改和加密认证等特点, 有利于加强对网络用户隐私信息防护, 更好地保障用户财产安全和信息安全。本文分析了区块链技术特点, 分析了区块链在网络用户隐私信息安全防护的应用场景, 从网络隐私数据匿名化、权限管理与访问控制、检测和响应网络攻击、构建区块链安全协议四个方面进行阐述, 从而提高网络用户隐私信息安全防护效果。

关 键 词 : 区块链; 网络隐私; 信息安全; 防护措施

Security Protection of Network Users' Privacy Information Based on Blockchain Technology

Xiao Rongwang¹, Fu Yingying²

1. Gongqing College of Nanchang University, Jiujiang, Jiangxi 332020

2. Suining Economic Development Zone Senior High School, Xuzhou, Jiangsu 221200

Abstract : The rapid development of social media platforms such as Douyin, Weibo and WeChat has brought great convenience to people's lives, yet it has inadvertently increased the risks of leakage and theft of network users' privacy information, which is likely to cause inestimable losses to users. Blockchain technology features decentralization, immutability and encrypted authentication, which is conducive to strengthening the protection of network users' privacy information and better safeguarding users' property and information security. This paper analyzes the characteristics of blockchain technology and its application scenarios in the security protection of network users' privacy information, and elaborates on four aspects including the anonymization of network privacy data, authority management and access control, detection and response to network attacks, and the construction of blockchain security protocols, so as to improve the effectiveness of security protection for network users' privacy information.

Keywords : blockchain; network privacy; information security; protection measures

引言

数字经济时代下, 社交媒体、电商平台、智慧医疗和电子政务平台的应用越来越广泛, 用户数量飞速增长, 用户隐私信息泄露风险也在日益加剧。传统网络用户隐私防护体系以“中心化存储+边界防护”的架构模式为主, 存在过度收集用户隐私数据、中心化服务器难以抵御黑客攻击、二次售卖用户数据等问题, 侵犯了用户隐私数据。这一背景下, 区块链技术在网络用户隐私信息安全防护的应用成为主流趋势, 可以有效对网络用户隐私数据进行匿名化处理、加强用户数据权限管理与访问控制, 并对用户网络环境进行检测, 及时预警和防范网络攻击, 从而更好地保障网络用户隐私信息。

一、区块链技术特点分析

(一) 去中心化

去中心化是区块链技术最鲜明的特征之一。区块链网络由众多节点组成, 把用户数据存储在各个节点上, 确保每个节点可以独立运行、独立存储数据, 避免由于某个节点故障而影响整个网

络运行, 从而更好地保护用户数据^[1]。同时, 区块链技术支持协同验证, 对各个节点数据进行验证与保护, 通过去中心化功能重构数据信任关系, 便于用户在区块链上生成唯一的 DID 标识, 简化线上身份验证环节, 降低用户隐私数据泄露的风险。

(二) 安全性

区块链技术安全性更强, 通过非对称加密算法为用户生成唯

一的公钥和私钥，其中公钥可以帮助用户在数据交互中使用匿名标识；私钥可以帮助用户进行身份认证和数据签名，确保用户数据访问权限的唯一性，加强对用户隐私数据、线上交易数据的保护。此外，区块链技术可以把用户数据存储在点对点网络的各个节点上，并对用户线上数据交互过程进行监测，防范用户隐私数据被泄露或篡改^[2]。

（三）不可篡改性

区块链技术具有不可篡改性。首先，区块链所有节点上的数据交互、修改等操作过程都会被记录，通过哈希算法为用户生成唯一的身份标识，一旦网络黑客试图篡改用户数据会导致哈希值变化，无法通过区块链各个节点验证，从而避免用户隐私数据被篡改或窃取。其次，区块链可以对用户数据进行全流程追溯，对用户所有数据、使用过程进行监测，并由多个节点对用户身份进行认证，一旦监测到某个节点数据被异常访问或受到攻击，能够及时阻断外部攻击，从而更好地保护用户数据安全^[3]。

二、基于区块链的网络用户隐私信息安全防护应用场景

（一）政务服务领域

我国电子政务平台逐步普及，为群众提供了便捷的线上服务，促进了政府跨部门协作，但是会大量搜集用户身份证号、手机号码、户籍和社保卡等隐私信息，这给用户隐私信息安全防护带来了不小的挑战。区块链可以帮助政府部门加强用户隐私信息安全防护，通过去中心化技术为公民建立数字身份证，加强公民隐私数据访问权限的管理，建立跨部门联盟链网络，从而提高政府数据的安全性，避免公民隐私数据被泄露或窃取^[4]。此外，区块链技术可以帮助政府部门建立智能合约体系，便于公民线上授权相关政府部门访问个人隐私数据，既可以保证公民隐私数据的安全性，又可以提高政务办理效率。例如市民可以在电子政务平台上申请更换新的机动车驾驶证，填写身份证号、驾驶证号码等个人信息，授权交管部门、车辆管理所等部门访问个人信息，足不出户办理新的机动车驾驶证。

（二）医疗健康领域

区块链技术可以帮助医院、医疗机构建立医疗隐私防护体系，对患者病历信息、基因数据和诊疗记录等进行管理，避免公民医疗健康数据被窃取。医疗隐私防护体系采用“区块链+分布式存储”的架构，对患者医疗健康数据进行加密处理，将其分布式存储在医疗系统中，并对患者健康数据访问记录、更改记录进行完整记录，明确医院各部门数据访问权限。患者可以通过私钥设置医疗健康数据访问权限，例如允许医院、医保局等部门访问个人社保卡、就诊记录等数据，避免个人健康数据被其他医疗机构或个人非法获取。例如京津冀地区建立了医疗数据共享平台，推进患者医学影像检查、病历信息和就诊记录等数据的共享，利用区块链技术加强患者隐私信息管理，减轻患者就医经济负担，保证患者隐私信息安全^[5]。

（三）电子商务领域

数字经济时代下，网络购物成为消费新时尚，虽然给消费者

带来了便捷的服务，但也存在过度采集网络用户隐私数据的问题。区块链技术可以加强电子商务领域用户隐私信息安全管理，对用户收货地址、手机号码、购物记录和支付信息等进行加密保护，在用户完成身份认证后允许其匿名登录电商平台，避免用户在交易过程中二次填写身份信息，最大限度降低用户隐私信息泄露的风险。电商平台利用非对称加密技术对用户隐私信息进行加密处理，只允许交易双方查看用户收货地址、支付信息等敏感数据，并通过智能合约明确店家对用户隐私数据的使用权限，允许用户授权平台访问个人数据，避免用户隐私信息被过多收集或二次售卖^[6]。例如某跨境电商平台利用区块链技术搭建了用户隐私数据安全防范体系，根据用户填写的身份证、手机号等信息进行海关信息核验，提高了通关身份检验工作效率，身份核验合格的订单才可以发货，并为订单设置虚拟电话号码，既可以让快递员联系用户，又可以避免用户隐私数据泄露或二次售卖。

三、区块链技术在网络用户隐私信息安全防护中的应用路径

（一）对网络用户隐私数据进行匿名化处理

区块链技术采用分布式数据存储架构，划分为许多节点，可以对网络用户隐私信息进行匿名化处理，例如对用户身份证、手机号码等隐私信息进行变形处理，避免隐私信息被识别，从而降低用户隐私信息被过度收集、泄露的风险。基于区块链技术的网络用户隐私信息安全防护离不开数据加密技术、数据变形和脱敏技术，一方面可以把用户隐私信息存储在不同节点上，设置不同级别密码，避免过度获取用户隐私信息；另一方面可以对网络用户敏感信息进行脱敏和变形处理，有效保护网络用户敏感信息^[7]。数据匿名化处理在医疗健康、电子商务和电子政务等领域有着广泛应用，可以加强对用户健康、教育、金融等信息的保护，避免网络用户隐私信息被滥用或“二次售卖”。

（二）加强对网络用户隐私信息权限管理与访问控制

区块链技术可以帮助政府部门、医疗机构、电商平台和企业加强对网络用户隐私信息安全防护建设，通过设置访问权限控制相关部门、企业对用户隐私信息的访问行为，只有通过授权的相关账号、网络IP地址才可以访问用户隐私数据，从而保证用户隐私信息的安全性和整个区块链数据库的完整性和安全性。例如学校可以利用区块链技术对师生隐私信息进行管理，实现对教职工个人信息、学生学籍信息和科研信息等的分布式权限管理，根据各部门工作需要设置师生隐私信息访问权限，避免师生隐私信息被滥用；通过智能合约技术设定多层次的师生隐私信息访问权限，满足教研室、档案室和教务处等部门查询需求，规范师生隐私信息使用流程，进一步保障师生隐私信息安全性^[8]。

（三）智能化检测和响应网络攻击

区块链技术在网络用户隐私信息安全防护中发挥着巨大作用，不仅可以通过共享安全事件日志监测用户隐私信息访问情况，自动识别是否受到网络黑客或计算机病毒攻击；还可以通过共识机制对各个节点数据进行验证，进一步提高用户隐私信息安

全防护效果。基于区块链技术的智能合约机制可以对用户所使用的无线局域网、网络流量进行监测,自动监测用户网络流量是否异常、是否遭受网络黑客攻击。一旦检测到用户网络存在异常,区块链技术可以自动开启防护模式,对可疑流量进行拦截,通知管理员对网络环境进行检测,及时拦截网络黑客或计算机病毒攻击,从而确保网络用户隐私信息的安全性^[9]。此外,区块链可以全程、实时记录网络用户数据访问和使用情况,确保信息不被篡改,即使某个节点的信息受到网络攻击,也可以避免其他节点数据被攻击或篡改,从而确保网络用户隐私信息的真实性和安全性。

(四) 构建区块链网络安全协议

技术人员要根据用户需求设计区块链网络安全协议,从共识协议、身份认证协议和数据传输协议等方面对区块链网络环境进行监测,保护区块链网络信息安全。首先,共识协议可以保证区块链网络数据的完整性和一致性,通过 Proof of Work (PoW)、Proof of Stake (PoS)、Delegated Proof of Stake (DPoS) 等共识机制对区块链网络内的用户隐私数据进行保护,提高区块

链网络抗攻击性和安全性。其次,区块链采用分布式数据存储方式,把用户隐私数据储存在不同节点中,通过身份认证协议可以防止恶意节点攻击和欺诈行为,可以采用数字签名、私钥等技术对用户进行身份认证,避免用户数据被窃取^[10]。

四、结语

总之,区块链技术为网络用户隐私信息安全防护提供了新的技术支持,在电子政务、医疗健康、教育教学和电子商务等领域都有着广泛运用,有效提高了用户隐私信息安全性、完整性和真实性,保证了网络用户的合法权益,为促进数字经济发展奠定了良好基础。未来,技术人员要积极促进人工智能、云计算等新技术和区块链技术的融合,构建完善的网络用户隐私信息安全防护体系,满足不同类型用户信息安全防护需求,让消费者安心网购、让学校安全开展线上教育、促进数字金融产业发展,为我国数字经济发展奠定良好基础。

参考文献

- [1] 李亦佳. 基于 APCO 模型的匿名提问平台用户隐私披露行为影响机制研究 [D]. 上海外国语大学, 2024.
- [2] 刘斯远, 王博琼. 基于区块链技术的网络用户隐私信息安全防护研究 [J]. 信息记录材料, 2024, 25(01): 20-22.
- [3] 文莅莅. 抖音短视频用户网络隐私信息保护行为影响因素研究 [D]. 河北大学, 2023.
- [4] 冯亚飞, 孙永强. 社交网络平台用户共有信息披露中的集体隐私应对行为研究 [J]. 图书情报工作, 2023, 67(11): 25-38.
- [5] 李英. 基于区块链的网络用户隐私信息加密系统 [J]. 信息与电脑 (理论版), 2022, 34(13): 221-224.
- [6] 单孟丽, 付文婧, 张思光. 网络用户数据素养、隐私关注与隐私信息披露意向 [J]. 河南科学, 2022, 40(04): 666-674.
- [7] 褚晓璇. 区块链技术驱动下的社交网络用户隐私保护行为研究 [D]. 天津大学, 2022.
- [8] 李会东. 网络信息隐私关注与网络隐私保护行为的探讨 [J]. 电子元器件与信息技术, 2022, 6(02): 253-254.
- [9] 贾若男, 王晰巍, 范晓春. 社交网络用户个人信息安全隐私保护行为影响因素研究 [J]. 现代情报, 2021, 41(09): 105-114+143.
- [10] 刘裕, 周毅, 农颜清. 网络信息服务平台用户个人信息安全风险及其治理——基于 117 个 APP 隐私政策文本的内容分析 [J]. 图书情报工作, 2022, 66(05): 33-43.