区块链技术支持视角下的计算机数据安全与保护研究

Bo Li, Shi Li*

重庆理工大学　重庆

【摘要】网络时代，数据量激增，很多数据信息具有高密度、高价值的信息属性，这也使得数据安全保护问题凸显。社会的持续关注。基于数据保护的目的，人们开始从区块链技术支持的角度探讨数据安全保护措施，希望通过区块链技术的发展与应用，降低数据信息交换过程中的受损风险，加速信息数据的共享，实现信息本体价值的边缘化处理，从而最大限度地提高信息传输的稳定性，保障信息安全。本研究首先从区块链技术支持的角度探讨了计算机数据安全与保护问题，然后明确了安全保护的具体措施以及区块链技术在计算机数据安全中的应用价值，最后为计算机数据安全与保护提供一定的理论研究支持。

【关键词】区块链技术；电脑；数据安全；保护应用

【收稿日期】2025 年 5 月 6 日　　【出刊日期】2025 年 6 月 10 日　　【DOI】10.12208/j.bta.20250001

Research on computer data security and protection from the perspective of blockchain technology support

*Bo Li, Shi Li**

Chongqing University of Technology, Chongqing

【Abstract】In the network era, the amount of data has surged, and a lot of data information has high density and high value information attributes, which also makes the problem of data security protection arouse the continuous attention of the society. Based on the purpose of data protection, people began to discuss the data security protection measures from the perspective of blockchain technology support. It is hoped that the development and application of blockchain technology can reduce the risk of damage in the process of data information exchange, accelerate the sharing of information data, and realize the marginalized processing of information ontology value, so as to maximize the stability of information transmission and ensure information security. This work first discussed the problem of computer data security and protection from the perspective of blockchain technology support, then clarified the specific measures of security protection and the application value of blockchain technology in computer data security, and finally provided certain theoretical research support for computer data security and protection.

【Keywords】Blockchain technology; Computer; Data security; Protection applications

1 简介

区块链技术作为一项新兴技术，正处于快速发展阶段，为高效的数据处理提供了多重支撑。它不仅驱动数据共享和传输，还能提高数据共享效率，凸显数据价值，实现计算机数据的有效保护和深度利用[1]。区块链技术被称为数据利用的“保护伞”，其保护原理也相对简单， 强化了点对点数据的去中心化，深化了以往数据的可追溯性，建立了无信任关系的交易体系。基于密码学、分级存储等信息技术，形成了新的数据处理体系。这样，对称加密、非对称加密等算法为计算机数据安全提供了多重保障，数据安全保护效果更佳[2]。

2 区块链技术及应用特点

区块链技术作为一项新兴技术，有着广阔的应用空间和光明的应用前景，它被普遍认为是一种具有分布式功能的数据存储载体， 区块链技术以各类精准算法、共识技术和传输技术为支撑。在区块链技术的实际应用过程中，其选择去中心化的数据处理模式，完成底层的优化设计，并借助密码学及各类加密技术及时提取

*通讯作者：Shi Li

注：本文于 2023 年发表在 Advances in Computer and Communications 期刊 4 卷 2 期，为其授权翻译版本。

数据块的价值，实现对数据信息各类属性的精确度量。综上所述，区块链技术有三大特点：第一，区块链技术可追溯。这意味着区块链技术可以追踪有价值的信息或数据在网络系统中的全过程，实现不同数据节点的可追溯处理。第二，区块链技术具有高度的不可逆性[3]。它以数据传输属性为核心，体现不同网络节点呈现的数据信息与时间点的关联属性，并自动锁定数据传输的路径，因此不存在数据覆盖和修改的风险，提高了数据传输的稳定性和安全性。第三，区块链技术具有开放性。在实现过程中，区块链技术被认为是一种基于分布式框架的自动化数据传输和集成。 它可以确保信息本体在传输过程中性能稳定，保证结构和计算符合范式要求，从而实现对数据价值属性的精准阐述。区块链技术的开放性还能有效保证数据传输的接收方和发送方同步明确数据信息的演化模式，增强数据处理和传输的安全性。基于这些特性，借助区块链技术加强计算机数据的安全防护是可能且必要的。

3 区块链技术支持视角下的计算机数据安全与保护性能

3.1 数据去中心化函数

数据去中心化功能是区块链技术的基本功能，在基础数据处理中发挥着重要作用。利用区块链技术，分布式系统可以有效地进行批量数据处理，既包括数据完整性的存储，也包括中心化的数据序列更新，从而构建一个无中心依赖的信任体系。区块链技术构建的技术环境使得外部因素无法攻击系统节点，区块链网络的整体运行免受任何干扰。在利用区块链技术去中心化功能时，应加强应用三方合作，以分布式运算能力完成去中心化任务，从而提高数据处理的效率和准确性[4]。

3.2 开放数据记录

区块链技术具有面向全网节点的数据处理功能，可选择先进的数据处理方式，记录并动态替换数据。区块链技术可以为计算机操作者提供分布式账本的使用支持，分布式的视角使得数据存储更加完备。当计算机网络各环节的程序处于开放状态时，网络运行程序、网络架构规则、网络节点接入形式等共同构成一个可信的区块链信任框架。在相应的区块链信任框架中，应发挥数据存储功能，记录用户操作信息，确保节点所有数据统计的全面准确。

3.3 信息篡改困难

除了数据去中心化的功能外，还可以借助其分布式存储单元模式，在计算机的任意程序中设置数据存储节点。当各节点对数据存储达成共识后，数据类型便得到标准化和维护。一般而言，当区块链技术的运行框架规模较大时，节点数量也会相应增加，节点分布也会形成较大的规模。因此 它将构成全网行为管控联动体系，保障全网各节点数据存储的监管效果，大幅降低数据篡改的可能性。基于对量化节点数据类型达成共识，区块链数据能够在短时间内高效更新。从理论层面来看，当至少一半节点的控制完成时， 在区块链技术的支持下，可以实现对全网节点的有效统一管控，降低信息被篡改的可能性 并降低数据安全成本。

3.4 匿名方案

当区块链技术有序运作时，它还能以匿名的形式驱动数据交换，促进数据交易。节点间进行数据交换时，可以通过固定的算法预测交易双方，预测的主体是计算机的地址。即使不公开交易双方身份，数据交易也能完成。 这意味着更少的信任确认和更简单的流程。

4 基于区块链技术的计算机数据安全与保护模型构建

4.1 基于区块链的私密通信网络构建

基于区块链技术的计算机数据安全保护模型主要由通信基础设施设备、上层通信网络和注册安全中心部分组成。其中，通信基础设施是基本工作单元，每个独立的通信基础设施对应一个区块链轻节点。上层通信网络是一个软件定义的去中心化网络通信结构，包括由不同区域选举产生的节点组成的区块链网络、卫星网络、基站通信网络。借助上层通信网络，不同地理位置的节点之间可以实现有效通信，形成可信通信网络管理中心，进行证书注册、认证和签发。信息验证通过后，最终连接到各个区域的区块链网络。综上所述，基于区块链的私有通信网络的构建，实现了注册认证模型的分布式节点网络认证，建立了相应的认证机制，构建了 P2P 分布式通信网络，进而设计了抗破坏多路由方案，通过节点路由存储和备份提供相应的路由元素[5]。

4.2 生存目标路由设计

私有通信网络的具体应用过程中，数据交换往往由网络节点间的合作驱动。在同一个区块链网络中，通信发起节点与终止节点进行数据传输时，节点需要通过算法选择路由后再进行数据传输。然而，考虑到网络受不可控因素的影响，可能无法形成链路，从而影响数据传输。因此，在一些特殊的网络数据通信场景中，在执行上线操作后，需要在不同的小型局域网（LAN）之间高效地选择可信代理节点，并在认证节点中复用。代理路由网络根据节点拥有的账本信息生成路由，更不易

受到外界干扰，使网络通信更加稳定。目前主要的防丢路由方案是在节点信息交互过程中通过账本信息和路由算法生成稳定的路由，并通过代理节点进行信息转发，从而使网络信息传输更加安全稳定。

4.3 网络节点的安全通信

在安全网络节点通信方面，重点在于有效构建通信应用场景。常规网络节点通信主要包括通信专网、内部通信和跨区域网络通信。在实际通信网络中，可以利用区块链去中心化的特性，充分发挥其点对点传输的优势，优化基于区块链的专用通信网络设计方案。网络本质上是分层网络[6]。第一层网络是基于 SDN 的软件定义的去中心化网络通信结构，包括由不同区域选举产生的各类节点构成的区块链网络、卫星网络、基站通信等网络。第二层网络由不同区域的多个通信基础设施和区域层级构成，区块链网络也被称为“小型通信网络”。

5 基于区块链技术的计算机数据安全模型应用效率

5.1 抗破坏性

利用区块链技术，充分利用共识算法和账本特性，在一定时间内进行存活节点的检测和节点信息账本的更新，使网络中的节点拥有更多的备选方案，避免通信节点故障或损坏，网络依然存在尝试性广播的问题。当不可抗力导致网络中部分节点故障时，节点可以根据已有信息快速构建路径，保障网络的抗干扰传输。

5.2 防重放

重放攻击主要发生在身份认证过程中，它将接收到的数据包发送至目标主机，破坏目标机器的认证正确性。因此，该方案在进行选举记录时，通过添加时间戳和随机数进行判断。节点只需在短时间内保存所有随机数，接收方通过验证数据包中的时间戳和随机数来判断是否受到重放攻击。在区块链中使用时间戳和随机数的优势在于随机数占用的数据空间不高，并且时间戳同步不需要精确，可以大大减少网络开销。

5.3 可追溯性和不可否认性

当节点加入网络时，可以通过注册中心生成并分发的公钥进行身份识别，只有拥有相应私钥的节点才能进行数据操作，因此在通信中可以通过公钥追溯节点身份，从而使数据包具有不可否认的特性[7]。

5.4 匿名性

在数据传输中，该方案结合代理的特点，可以保证节点传输的匿名性，当前节点只能解密前一跳和最后一跳的地址，而无法获得源节点和目的节点的完整通信路径，从而可以相对隐蔽地实现私有通信网络中各个节点之间的传输。

6 区块链背景下数据安全共享机制研究

6.1 区块链技术网络数据安全共享机制

从目前数据安全共享平台的建设成果来看，区块链技术被认为是实现网络中数据节点区域划分、逐步实现数据信息真实性检测的关键技术。区块链技术基于区域网络节点的属性分析，对整个数据承载区域进行标记，使得安全区域内的数据传输类型能够被即时检测，并支持记录各种数据传输模式的时间节点。这不仅可以减少外界因素的干扰，降低数据传输风险，还能降低数据信息处理的成本。区块链技术的实现过程可以理解为固有数据域内的 PKI 信任值，以整个系统所承载的服务模式为切入点，通过认证机制、身份识别机制和用户体系，确定不同区域数据在合理访问空间内的衍生效应，借助区域属性的精准对接，实现基于信任度的数据传输。这样，数据信息在确认后，将独立于整个传输域，并且数据信息本身的传输属性会被打上信用值。在实际的数据交易过程中，可以从用户端和接收端进行跨域认证，使数据信息传输更加稳定安全，防范整体网络架构和数据共享平台的风险漏洞。

6.2 实现区块链技术网络数据的安全共享

从技术角度来看，区块链技术应用于全网数据安全共享平台时，采用精准算法，并结合数据结构对标区块顶层设计。在此过程中，为了确保共享框架内各类数据信息传输的安全性，需要明确整体信息主体，进而对不同结构中信息节点呈现的数据进行标记和授权，以保障后续任务在运行过程中的请求机制。从数据传输的角度看，用户在定义各类信息时，从自身需求出发，通过数据信息所呈现的属性定义不同用途或信息的传输路径[8]。区块链技术通过用户的指令实现相关数据的授权处理，并以可识别、可追溯的方式确保整体信息在网络架构内的传输，从而对数据进行确认。在此模式下，数据信息可以在内网或整个广域网中同步存储和传输。同时，区块链技术的认证功能在于实现基于分布式结构的不同网络体系的区域化构建。通过整个数据安全范畴的信息共享和传输方式，可以确保每一种传输结构和网络结构都有区块链技术的支持，形成云服务器或计算机网络服务器的有效整合。

7 结论

通过分析区块链技术的特点及其在计算机数据安全保护中的作用，不难看出，积极推广区块链技术，发挥其在计算机数据安全保护中的价值十分必要。需要加

大区块链技术的研发和应用力度，加强基于区块链技术的数据安全技术融合，随着区块链技术的深入应用，提升计算机数据的安全性。通过多措并举，营造更加安全的数据传输和共享应用环境，才能真正凸显区块链技术在信息安全保护中的价值，也为该技术的推广提供一定的理论支撑。

参考文献

[1] Zeng, Z., Li, Y., Cao, Y., Zhao, Y., Zhong, J., Sidorov, D., & Zeng, X. (2020). Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application. Energies, 13(4), 881.

[2] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208.

[3] Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications, 154, 223-235.

[4] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.

[5] Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22, 14743-14757.

[6] Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H., & Boshkoska, B. M. (2019). Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. Computers in industry, 109, 83-99.

[7] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3.

[8] Khan, M. A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M. I., ... & Ali, A. (2020). A machine learning approach for blockchain-based smart home networks security. IEEE Network, 35(3), 223-229.

版权声明：©2025 作者与开放获取期刊研究中心(OAJRC)所有。本文章按照知识共享署名许可条款发表。
https://creativecommons.org/licenses/by/4.0/
OPEN ACCESS