基于区块链的网络安全技术研究

高　杰
浙江侨创通讯股份有限公司　浙江　杭州　310000

摘　要：随着近年来我国经济的快速发展，我国互联网的迅猛发展已经超越了西方发达国家。虽然我国互联网的起步较晚，但是它的技术发展速度非常快。截至目前，我国已经拥有超过10亿的互联网用户。互联网起源于美国，最初被用于军事领域。随着社会的进步，它已渗透到各个行业中，成为人们不可或缺的工具。但是，互联网也带来了安全隐患，甚至危及人们的生命和财产安全。本文对基于区块链的网络安全技术进行了深入研究。

关键词：区块链；网络安全技术；分析

引言

在区块链技术的背景下，网络安全管理必须以高安全系数的网络环境为主要基础，充分利用区块链技术的优势，加强互联网的安全防护能力。此外，重点管理信息质量，维护信息系统的安全系数，并自觉关注网络维护，提升网络技术水平，以确保网络正常运行。

1 区块链结构构造

1.1 数据层

在这个领域，重要的是确保互联网具有可审计性，以侧面保障数据的安全性。因此一般会使用数据库对数据进行存储。由于区块链应用的不同，其结构也会有所不同，但其应用方式大致相同，包括头部区域和数据区域。当节点形成区块时，中间节点能够连接节点的数据，形成Hash值，并将其与其他相关数据组合形成头部区域，形成默克尔树作为数据区域。

1.2 网络层

该层面为区块链去中心化提供支持，通过在区块链节点之间传播数据来实现该目标。目前，区块链使用对等网络对网络层进行组网，需要在每个节点中使用P2P协议，使节点能够建立更多的关系，从而促进网络层的发展。这样做可以保证节点之间的信息共享，并在数据传播到每个节点时构建出网络层，实现去中心化的区块链体系，并进行定期维护。

1.3 共识层

在这个层面上，主要是为了确保区块链系统搭建的数据安全性，保证其不会遭受篡改，同时在分布式节点的网络环境下，实现了数据一致性的定义。也就是说，在区块链数据共享的背景下，即使部分节点数据被恶意篡改，其他节点的数据依然正确，确保数据不会被篡改。就当前的互联网现况而言，共识协议涵盖了权益证明（PoS）和工作量证明（PoW）等算法。在计算过程中，节点会优选领导节点发送数据到其他节点，从而获得区块的哈希值和其他关键数据，并进行验证计算，验证成功后的区块才能被添加到区块链中。

2 网络安全的主要威胁

在互联网应用过程中，安全问题一直是个不容忽视的问题，各种互联网恶意攻击如黑客、木马、网络病毒等层出不穷，给人带来持续的压力。随着互联网信息技术的不断发展与应用范围的扩张，安全问题备受关注，相关管理人员已加强了安全管理工作。然而，我们也不得不承认，随着互联网信息技术的发展和普及程度的提高，安全问题仍需引起足够的重视，不仅提升了技术人员的信息技术水平，而且黑客技术水平也得到重要提升。因此，人们应该时刻警惕，认真防范黑客和病毒的攻击，以便及时发现问题并解决，从而保障客户的上网信息安全，最大程度地减少危害。通过研究互联网防御领域的现状，我们发现，为了提高信息安全性，现阶段采用了两种技术方法，即分级配置管理和集中控制。然而，要想实现零损失的目标，仅依靠这些方法是不够的。在面对复杂的病毒、木马程序和网站漏洞时，必须高度重视安全问题。随着互联网科技的蓬勃发展，互联网的应用范围越来越广泛。网络安全问题关系到我们日常生活和工作的方方面面，因此我们需要加强安全管理能力，提升网络安全技术水平，最大程度地降低网络安全风险，从而确保人们在使用网络的过程中得到充分的安全保障。

3 区块链应用于网络安全技术的方法

3.1 提升数据存储及共享能力

随着我国网络技术的不断推进，网络已成为各行业发展中的重要工具。然而，由于其开放性特征，网络使用中存在许多安全问题，这些问题威胁了网络的安全性。为此，在实际工作中，需要以区块链技术为基础构

建网络安全技术体系，通过一体化的工作模式，对网络中存在的安全漏洞进行有效应对，进一步提高网络安全技术的使用效果，凸显区块链技术在网络安全方面的优势。在区块链技术网络安全管理的生成过程中，需更加重视计算机网络安全管理，特别是储存和共享管理数据。减少问题发生，避免数据泄露，并提高安全管理效果。为了提高计算机网络的安全等级，需要加强网络安全数据的科学保护，并确保基本的共享能力。在传输数据时需进行加密，以实现公开分享。同时，利用区块链技术完善现有的安全管理功能，全面提升技术的使用效率。在运用区块链技术时，应加快信息共享速度，同时提升安全保障级别，以满足不同数据安全管理阶段需求。进一步加强审计和监管模式，使网络安全系统更加科学化。

我国科技日新月异，计算机已成为各行业不可或缺的重要工具。然而，单一环节的偏差也可能导致信息篡改和资源盗窃。为此，我们需要加强安全措施，确保信息和资源的安全，为保证数据的快速传递、稳定性和安全性，我们需要充分利用区块链技术的优点，建立高度完整性的安全防护模块，降低节点间数据的依赖度，以减少对数据管理的影响。为保证网络安全管理，需要在技术方案实施过程中进行全面监督和管理，及时有效地解决所产生的问题，确保网络安全达到预期要求，进一步保障网络数据储存共享能力正常发挥，提升网络安全管理水平。

3.2 构建完备的网络安全防护系统

实际工作中，必须改进基础设施的保护力度，以为区块链技术创造稳定的实时环境。若计算机出现去中心化故障，则信息传递存在诸多不安全因素，甚至导致网络瘫痪。因此，应利用区块链技术优势，构建安全网络体系，修补既有网络安全管理问题，并按照安全隐患发生位置，科学使用区块链技术加强防护，避免安全隐患扩散至其他基础设施，确保网络安全系数。在这个过程中，必须记录关键信息，灵活应对网络安全管理中的问题，分析异常情况，制定行之有效的对策和管理方案，确保网络安全达到预期要求，保护网络安全使用。

技术使用还需要借助区块链构建结构化网络系统。在运行过程中，由于信息交互和共享突出，尽管网络监管下能基本通行，但部分数据资料易在漏洞高网络中暴露，若网络系统遭遇黑客攻击某一环节，将造成系统严重瘫痪。因此，为解决以往使用中的矛盾，用户需提高安全意识，发挥区块链技术优势。借助分布式的使用体系，搭建完整性更强的网络系统。如此一来，用户可迅速获取所需数据并在发生安全问题时精准定位，再掌握相应安全防护模块，全面保障区块链技术应用并大幅提升网络安全。

3.3 加强物联网网络保障

随着我国科技水平的提高，物联网被广泛使用，并成为计算机网络发展的关键。然而网络安全问题突出，妨碍了网络的正常运行。因此，我们需要利用区块链技术来满足整体的安全管理要求，使其融合现代化发展方向，从而全面提高工作效率。需要注意的是，若要长期发展物联网，应充分发挥区块链技术的价值，确保互联网安全。为此，加强数据保密、完整性是必要的。在使用区块链技术时，需科学选用加密方式，全面强化网络数据安全。为增强系统自我保护功能，应根据网络特点对各节点数据进行有效加密。此外，需利用系统防护措施，降低恶意篡改和拦截的风险，以满足系统使用要求，提高安全级别。区块链技术是一种完整性较强的数据结构，可很好地记录历史数据并报告，有效提高计算机的安全性。在实际工作中，需要利用该技术更好地储存数据并加强防护机制，减少安全问题的发生，以提升使用效果和安全管理水平。

4 区块链技术应用推广建议

4.1 设立国家级区块链试验中心

目前，各个区块链实验室，比如中科院、达摩院和一些互联网企业，分化且难以满足全国性和主要行业领域的区块链技术需求。因此，就需要加强对区块链技术研发的顶层设计，建立国家级的区块链实验室，集中研究资源，以推动区块链技术的突破、普及，同时自主掌握可控制的区块链技术，以便加速产品的研发，抢占区块链技术标准制定的制高点和主动权。在国家级区块链实验室打下坚实的研发基础后，更多的市场主体可以在主要领域充分利用区块链技术的具体应用。这将为我国推动“区块链+产业”新格局的形成提供坚实的技术支撑。通过掌握区块链技术国际标准制定权，我国产业科技的全球化发展将受益，为“一带一路”建设注入科技的力量。

4.2 实施区块链监管沙盒测试制度推广行业应用

由于区块链技术被广泛应用于金融、税务、公共管理、教育以及党建等领域，安全问题备受关注，因此应考虑将即将推向市场的基于该技术的各种场景应用产品纳入监管沙盒框架。即需要建立一个专业化的、全面针对区块链技术及应用的监管沙盒。监管沙盒可以及时检测和纠正不同领域中区块链技术的安全问题。另外，监管沙盒通过对技术进行测试和认证，可以避免因信息不

对称而导致的欺诈风险，有助于市场认可和推广成熟的区块链技术和安全的应用场景，维护整个行业的健康发展。只有经过监管沙盒的测试和认证的区块链技术和应用才能被广泛应用于主要领域。

4.3 保障数据完整性，预防数据篡改

保障数据完整性就是确保数据在输入和传输过程中未被非法修改或篡改，保证数据的一致性和安全性。分布式账本技术是数据仓库中一项重要的区块链技术，它可使每个节点能够存储所有数据，通过商定的机制实现数据的监管和保护，确保储存的数据不会被恶意攻击。不能仅对节点进行数据记录，以免恶意管理。单元电路技术应用后，数据统一存储于单一电路结构中，修改需同时更改所有单元的指针，以确保数据不被随意篡改[5]。此外，采用分散式存储，每个节点均存储数据的备份以避免集中存储的单点故障。区块链可应用于数据验证，协议机制虽可防止黑客攻击，但在防御恶意篡改方面的成本较高，黑客可攻击所有节点。除此之外，还能够采用非对称加密的方式，以保证信息摘要的安全性。即有所有者使用私钥将收到的信息摘要进行加密并加上数字签名，附在原始信息上以表明信息的真实性，类似于手写签名无法被仿冒。

结语

区块链背景下的网络安全技术的应用，通过采用新颖的安全防护技术，转变了以往的技术使用方式，建立了操作性强的信任机制和安全防护模式，稳定地储存和管理网络数据，并实现数据的可靠共享。一体化的系统应用模式保障了系统运行的安全性，突显了区块链技术的可利用价值。

参考文献

[1]周宗平,李军.区块链在网络安全技术中的应用浅析[J].中国信息化,2020(07):76-77.

[2]孟维成.区块链技术在网络安全中的应用[J].电子技术与软件工程,2020(14):238-239.

[3]陈伟利，郑子彬.区块链数据分析：现状、趋势与挑战[J].计算机研究与发展，2018，55（09）：1853-1870.

[4]贺宏伟,李晨光.基于区块链技术的网络安全分析[J].网络安全技术与应用,2022(09):23-25.

[5]王利军,赫巍,尚秋明.基于区块链的网络安全技术分析[J].网络安全技术与应用,2021(04):7-8.