区块链技术在计算机通信安全中的应用与挑战

李军
民航空管技术装备发展有限公司
DOI:10.12238/acair.v1i4.6796

[摘　要] 随着网络通信技术的飞速发展,通信安全问题日益凸显。为了保障通信安全,将区块链技术应用于网络通信具有重要的现实意义。区块链技术具有信息去中心化和信用去中心化特点,将其应用于计算机通信安全,有助于提高通信安全性和防止信息数据被窃取、篡改或损坏。区块链技术的核心优势在于其去中心化特性,这使得数据传输和存储过程中无需通过第三方机构,从而降低了数据被篡改的风险。此外,区块链技术采用加密算法对数据进行加密和验签,确保数据传输的安全性和完整性。通过将区块链技术与计算机通信安全相结合,可以在一定程度上解决通信过程中的安全问题,提高通信质量。因此,此次研究主要探究区块链技术在计算机通信安全中的应用与挑战。
[关键词] 区块链技术；计算机通信安全；应用；挑战
中图分类号：G623.58　文献标识码：A

Application and challenge of blockchain technology in computer communication security

Jun Li
Civil Aviation Air Traffic Control Technology Equipment Development Co., LTD

[Abstract] With the rapid development of network communication technology, communication security issues have become increasingly prominent. In order to ensure communication security, it is of great practical significance to apply blockchain technology to network communication. Blockchain technology has the characteristics of information decentralization and credit decentralization, and its application to computer communication security helps to improve communication security and prevent information data from being stolen, tampered with or damaged. The core advantage of blockchain technology is its decentralized nature, which eliminates the need for data transmission and storage to go through third-party institutions, thus reducing the risk of data tampering. In addition, blockchain technology uses encryption algorithms to encrypt and check data, ensuring the security and integrity of data transmission. By combining blockchain technology with computer communication security, security problems in the communication process can be solved to a certain extent and the quality of communication can be improved. Therefore, this study mainly explores the application and challenges of blockchain technology in computer communication security.
[Key words] blockchain technology; Computer communication security; Apply; Challenge

引言

通信安全问题会对国家安全、社会稳定和个人隐私构成严重威胁。区块链技术诞生于2008年,是一种具有创新性的分布式数据库技术,其在信息安全和信用体系建设方面具有独特的优势。将区块链技术应用于计算机通信安全领域,有望解决传统通信安全手段难以解决的问题以及提高通信质量。基于此,本文将探讨区块链技术在计算机通信安全中的应用及其所面临的挑战。

1 区块链技术及其特征分析

区块链技术是一种创新的分布式数据库技术,最初以虚拟货币的形式出现,后来在金融机构的数据保护中得到了良好的应用与发展。目前,区块链技术已经成为网络通信领域中的一项重要的数据信息保护技术,在网络信息的储存和传输中发挥关键性的保护作用[1]。其特征主要包括四个方面,第一,多方写入。区块链技术采用分布式数据存储方式,数据由多个节点共同维护,而非由单一的中心节点控制。这意味着区块链系统中的数据可以由多个参与者进行写入,提高了数据的安全性和可信度。第二,公开账本。区块链技术采用公开的账本记录所有交易和数据变更,账本中的数据对所有参与者都是可见的。这种公开性有助于提高数据透明度,降低信任成本,并防止中心化控制者对数据

进行篡改。第三,去中心化。区块链技术采用去中心化的网络架构,数据不依赖于中心节点进行存储和传输,而是通过分布式节点共同维护。这种去中心化的特点有助于提高数据的安全性,降低单点故障的风险,并防止中心化控制者对数据进行篡改。第四,不可篡改。区块链技术通过加密算法对数据进行加密和验签,确保数据传输的安全性和完整性。同时,区块链采用分布式账本,任何一方想要篡改数据都需要同时篡改整个账本中的所有数据,这在实际操作中几乎是不可能的。因此,区块链技术具有很高的防篡改能力,确保了数据的可靠性。

2 区块链技术在计算机通信安全中的应用

2.1总体结构设计

基于区块链技术的移动智能终端安全通信方案总体结构包括几大方面,例如,采用去中心化的网络架构,通过区块链技术将移动智能终端设备连接起来,形成一个安全、可靠的通信网络[2]。借助区块链技术的分布式账本,实现对移动智能终端设备的节点身份进行验证。每个设备在加入网络时,需要通过区块链上的共识算法进行身份认证,确保其身份的真实性和可信度。基于区块链技术的移动智能终端安全通信方案采用加密算法对通信信息进行加密传输与储存,在通信过程中,每个节点都需要使用私钥对数据进行加密,公钥用于解密。这样,即使数据在传输过程中被截获,由于没有对应的私钥,数据也无法被解密,从而保证了通信的安全性。区块链技术的分布式账本可以用于存储通信过程中的数据。每个节点都可以将通信数据存储在区块链上,形成一个完整的数据链。这种数据存储方式不仅安全可靠,还可以防止数据被篡改。

2.2通信方案架构设计

2.2.1数据层

数据层在区块链技术在计算机通信安全中的应用通信方案架构设计中起着重要的作用。区块链技术可以通过加密算法对通信信息进行处理,生成摘要或哈希值[3]。数据层的一个主要作用是储存这些经过加密处理的通信信息摘要,确保通信信息的完整性和安全性,因为通过对比通信信息的摘要,可以验证通信信息是否被篡改过。数据层可以使用分布式存储技术,将这些摘要以分布式的方式储存在区块链网络的各个节点中,提高数据的可靠性和容错性。边缘计算是一种将计算和数据存储推向网络边缘的方法,可以使得数据更加接近终端用户,提高通信的效率和响应速度。数据层可以记录和储存通信信息在边缘计算装置中的具体位置。通过记录通信信息在边缘计量装置中的位置,可以在需要时快速定位并获取通信信息,提高通信的实时性和可用性。

2.2.2网络层

网络层采用对等网络结构,也称为点对点网络结构,所有参与通信的节点都是对等的,没有中心化的控制节点。这种结构使得通信更加去中心化、公开透明,并且不容易受到单点故障的影响。网络层可以将区块链中的信息进行广播,也就是将信息发送给整个网络中的所有节点[4]。通过广播信息,所有节点可以及时获取最新的区块链数据,保持整个网络的一致性和安全性。同时,广播信息也可以用于通知其他节点有关特定事件或交易的发生,促进节点间的交互和合作。不仅如此,网络层可以对区块链中的信息进行验证,验证信息的过程包括验证信息的完整性和真实性,以及验证信息是否符合预设的规则和条件。网络层可以通过对区块链中的信息进行哈希运算、数字签名验证等方式,确保信息的完整性和真实性,并能够对新的信息进行验证,以防止不合法的信息被添加到区块链中,保护区块链的安全性和稳定性。

2.2.3共识层

共识层的主要功能是提供共识机制,即一种协商规则来确保网络中的各个节点就区块链数据的产生和验证达成共识。共识机制是区块链的核心特性之一,通过共识机制,网络中的节点可以达成一致,保证区块链的一致性和安全性。共识机制可以确保数据的可靠性、防止双重支付等问题,同时也可以防止恶意节点对网络进行攻击或篡改。共识层通过共识机制,让区块链网络中的节点以竞争的形式来产生记账节点,进而实现一种分布式的共识效果。在区块链中,记账节点负责验证和打包交易,并将其添加到区块链中。通过竞争的方式选择记账节点,可以确保网络中的节点是具有一定信任和能力的节点,有效地防止恶意行为和欺诈行为的发生。竞争机制可以基于各种算法和规则,如工作量证明(PoW)、权益证明(PoS)、权威证明(PoA)等。共识层通过共识机制实现一种分布式的共识效果。分布式共识指的是网络中的多个节点通过一致的规则和算法达成共识,无需依赖中心化的控制机构。这种分布式的共识机制可以实现区块链的去中心化特点,提高系统的可靠性和安全性。每个节点都可以参与共识过程,验证交易的合法性,并在达成共识后将交易添加到区块链中,确保数据的一致性和完整性。

2.2.4激励层

激励层的主要功能是通过激励机制中的各个激励节点来共同验证网络安全维护效果。在区块链中,网络安全的维护是至关重要的,激励层通过引入激励机制来激励节点参与到安全维护中。激励节点通过验证和确认交易的合法性以及区块的有效性,保证网络的安全性和一致性[5]。激励层通过激励节点的参与和验证,确保网络中的数据不受篡改和攻击,增强通信的安全性。在激励层中,信用积分被用作代币来进行终端设备的信用评分。节点的信用分数反映了其在网络中的信任程度和行为的可靠性。具体而言,如果节点能够将有效的交易计入区块中,其信用分数将会增加。而如果节点无法将交易计入区块中,或是将交易计入无效区块中,其信用分数将会扣除。通过信用积分的应用,激励层在网络中建立了一种信任机制,鼓励节点遵守规则,提高网络的安全性和可靠性。

2.2.5应用层

应用层能够向移动智能终端设备发布相应的应用,包括区块链钱包、身份验证应用、加密通信应用等。通过发布应用,用户可以使用移动智能终端设备进行区块链的验证、接入和通

信。应用层需要提供友好的用户界面和功能，方便用户操作和管理区块链通信。应用层通过相应的应用，实现移动终端设备的验证和接入。在区块链通信中，移动终端设备需要进行身份验证，以确保其合法性和安全性。通过应用层提供的验证机制，用户可以通过移动终端设备进行身份验证，获得相应的权限和访问权。应用层也需要提供接入功能，让移动终端设备可以接入到区块链网络中，参与通信和交易。应用层需要提供通信功能，让移动终端设备可以进行加密通信和数据传输。

3 区块链技术在计算机通信安全中存在的挑战

3.1性能瓶颈

目前，区块链技术的处理速度相对较慢，这限制了其在通信安全领域的应用范围。尽管有一些优化算法，如分片技术、闪电网络等，可以在一定程度上提高区块链的性能，但这些技术仍然需要进一步研究和改进，以满足通信安全领域的高性能需求。

3.2法律法规和监管缺失

由于区块链技术的去中心化特点，使得通信过程中的数据不再受单一的中心节点控制。这给监管带来了难度。目前，关于区块链技术的法律法规尚不完善，导致一些不法分子利用区块链技术进行非法活动。因此，有必要完善相关法律法规和监管体系，为区块链技术在通信安全领域的应用提供有力保障。

3.3隐私保护问题

尽管区块链技术具有数据加密和防篡改等特点，但在一定程度上仍然难以满足通信过程中的隐私保护需求。由于区块链上的数据对所有参与者都是可见的，这使得一些敏感信息在区块链上存储和传输时容易受到泄露。因此，有必要研究更为有效的隐私保护措施，以提高区块链技术在通信安全领域的隐私保护能力。

3.4安全漏洞和攻击

尽管区块链技术具有一定的安全防护能力，但仍然可能存在一些安全漏洞，如智能合约漏洞、私钥泄露等。这些安全漏洞可能被黑客利用，对通信安全造成威胁。因此，有必要加强对区块链技术的安全研究和防范措施，以降低安全风险。

4 总结

综上所述，区块链技术在计算机通信安全领域具有巨大的应用潜力，它所带来的去中心化、安全可靠的特点为解决通信安全问题提供了新的思路。然而，区块链技术在通信安全领域的应用仍面临诸多挑战，在未来的研究中，随着区块链技术不断的发展与完善，相信它将在计算机通信安全领域发挥更大的作用。为了充分发挥区块链技术的优势，还应该不断地提高区块链技术在通信安全领域的性能、优化算法、降低能耗以及提高处理速度。并且要关注区块链技术在隐私保护方面的挑战，研究更为有效的隐私保护措施。通过持续研究、创新和发展，能够将区块链技术更好地应用于通信安全领域，为构建安全、可靠的通信环境贡献力量。

[参考文献]

[1]吴小迪.基于区块链的计算机通信网络安全加密控制系统设计[J].信息记录材料,2022,23(11):163-165.

[2]林璐.基于区块链及Signal的物联网安全通信技术研究[D].北方工业大学,2022.

[3]张桂鹏.基于区块链的云数据安全存储技术研究[D].广东工业大学,2022.

[4]孙闯.基于区块链技术的电网数据安全研究[D].南京邮电大学,2021.

[5]陈思源.基于密钥派生算法的区块链安全通信技术的设计与实现[D].北京邮电大学,2021.

作者简介：

李军(1976--),男,汉族,河北省青县人,中级工程师,一级建造师(民航空管技术及工程民航空管技术装备发展有限公司。