基于区块链的无线网络通信数据加密传输方法探究

陈于枫,兰泽勇
(中通服中睿科技有限公司,广东 广州 510630)

摘 要:为提高无线网络通信的安全性,深入探讨基于区块链的无线网络通信数据加密传输方法,并分析其优势和应用场景。通过对这一新兴技术的研究和理解可以更好地抵御日益增长的网络威胁,保护个人隐私和敏感信息,推动无线通信领域的进一步发展,以此为相关人员提供实践参考。

关键词:区块链;网络通信;加密传输
中图分类号:TN918 **文献标识码**:A **文章编号**:1004-7344(2023)38-0136-03

0 引言

在当今数字化时代的无线网络通信已经成为我们生活中不可或缺的一部分。随着无线通信技术的迅速发展和广泛应用，数据安全性和隐私保护面临着日益严峻的挑战。为了解决这些问题,基于区块链的无线网络通信数据加密传输方法应运而生。区块链作为一种去中心化、公开透明的分布式账本技术具有高度的安全性和防篡改能力。它可以提供一个安全的环境确保通信数据的机密性、完整性和可靠性。

1 区块链加密传输优势

1.1 实现去中心化

区块链是一种去中心化的分布式数据库，其主要特点是去中心化、信息不可篡改。在传统无线网络通信数据加密技术中，如果节点受到攻击或者计算机程序被篡改则会导致信息泄露。基于区块链的无线网络通信数据加密传输具有去中心化的特点，这意味着没有单一的控制机构或服务器来管理和保护数据。数据存储在分布式网络中的多个节点上，并通过密码学算法进行加密和验证。这种去中心化的结构使得攻击者很难入侵系统，因为他们需要同时攻破多个节点才能篡改数据[1]。

1.2 实现信息共享

区块链技术可以实现无线网络通信数据的加密传输、保障数据的安全性、保证数据传输的及时性。传统的加密方法在加密时需要通过密钥进行对称加密,当密钥泄露时很难保证通信数据的安全性。使用非对称加密算法对通信数据进行处理时，通信双方需要通过公钥和私钥对通信数据进行加密以保障数据的安全性。当无线网络通信双方需要交换信息时可以通过公钥和私钥对信息进行加密。在区块链技术中还可以实现信息共享。区块链技术具有去中心化和集体维护等特点,其能够有效保证信息共享的安全性。区块链技术提供了对数据操作的透明度和可追溯性。每笔数据交易都会被记录在区块链上,并且不可更改。这意味着任何人都可以查看和验证数据的完整性和真实性，从而确保通信数据的安全性。如果发生数据泄露或攻击事件可以通过区块链上的交易记录进行追溯并找到并解决问题的根源[2]。

1.3 增加安全性

目前的无线网络通信数据加密技术只能保证通信数据的完整性,却无法保证通信数据的真实性。在区块链技术的支持下可以有效地解决这一问题。

首先，区块链技术可以将所有的节点都连接到一起,每个节点都有一个公钥和私钥,任何人都可以通过这两个密钥解密通信数据，从而保证了通信数据的真实性,常用加密结构如图 1 所示。其次,区块链技术可以通过时间戳对通信数据进行加密，这种加密方式可以避免时间戳信息被篡改。区块链技术使用哈希函数和非对称加密算法来保证数据的完整性和真实性。每个数据块都包含一个唯一的哈希值，该哈希值基于前一个数据块的哈希值计算而成。这种链接结构使得任何尝试篡改数据的行为变得容易被检测到，因为它会破坏整个区块链的连续性。通过使用非对称加密算法,只有拥有正确私钥的用户才能解密和访问数据，其有效地防止了数据的伪造和未经授权的访问。

1.4 智能合约的自动执行

基于区块链的无线网络通信数据加密传输可以通过智能合约实现自动执行,过程如图 2 所示,这是一种具有预设规则和条件的计算机程序。以下是智能合约自动执行的优势。

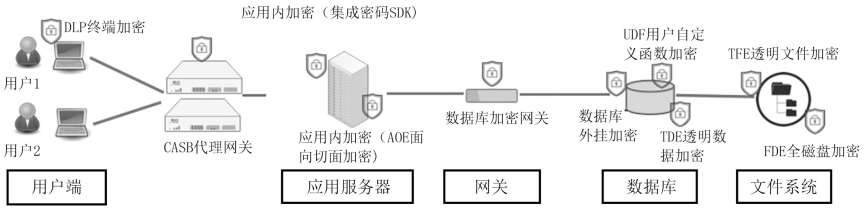

图 1 常用加密结构

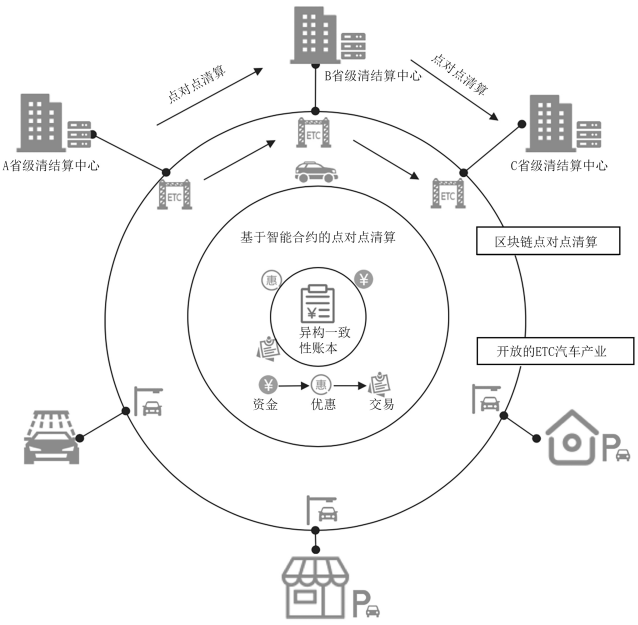

图 2 智能合约执行过程

(1)自动化操作。智能合约可以根据预先设定的规则和条件自动执行加密传输操作。例如，在数据发送时，智能合约可以验证接收方身份并确保仅授权用户才能解密和访问数据。这消除了人为错误和潜在的安全漏洞，提高了数据传输的可靠性和安全性。

(2)实施权限管理。智能合约可以定义不同级别的访问权限，并根据参与者的身份进行自动验证和控制。只有经过身份验证的用户才能执行特定操作，如数据解密、签署或修改。这样可以防止未经授权的访问和篡改确保数据的完整性和安全性。

(3)时间触发功能。智能合约可以根据时间触发来执行特定的操作。例如，可以设置定期更换加密密钥的规则以增强数据的安全性。当指定的时间到达时，智能合约会自动触发更新密钥的操作，确保系统始终使用最新的加密算法和密钥来保护数据[3]。

(4)不可篡改性。智能合约中的代码被存储在区块链上，并且不可更改。这意味着无法对已部署的智能合约进行擅自修改，从而确保了操作的一致性和可信度。这种不可篡改性可以防止恶意攻击者利用漏洞或后门来破坏数据传输的安全性。

2 区块链加密传输方法

2.1 通信数据加密传输需求分析

无线网络通信数据加密传输技术是保证无线网络通信数据安全的一种技术手段，其中采用加密算法对信息进行加密处理，使其在传输过程中不被非法篡改，以防止信息泄露。在实际的应用过程中，无线网络通信数据传输会受到多种因素的影响，从而导致信息泄露现象严重。首先，无线网络通信数据传输过程中的硬件条件不完善，无线网络通信数据传输时通常需要借助有线网络进行通信数据的传输，如果无线网络通信数据传输所采用的硬件设备性能不佳，在数据传输时就容易受到其他因素的干扰而造成信息泄露。其次，无线网络通信数据在传输过程中存在人为因素的干扰，由于人们的操作不规范或者是用户素质等方面原因，其中使用户在使用过程中容易出现失误，从而导致信息泄露。最后，无线网络通信数据在传输过程中受到信道的影响，不同信道所传输的信息质量不相同，信道质量不好也会导致信息泄露。根据无线网络通信数据加密传输需求分析可知，在进行无线网络通信数据加密传输时必须保证通信数据在传递过程中不被非法篡改和窃取。因此，对无线网络通信数据进行加密处理是十分必要的。采用区块链技术进行无线网络通信数据加密处理具有诸多优点，其能够有效提高无线网络通信数据在传递过程中的安全性。

2.2 系统结构设计

节点层负责对无线网络通信数据的加密处理，从物理层(加密原理如图 3 所示)、网络层、框架层、应用层进行信息传递，网络和框架层之间存在接口，网络间的数据交互通过链路层实现，系统整体结构如图 4 所示。在无线网络通信数据传输过程中，通过对数据进行加密处理，对节点间的信息交互进行控制，使节点能够及时地完成信息交互。

网络层负责无线网络通信数据加密处理。在无线网络通信数据加密过程中需对通信数据进行加密处理，将加密后的通信数据通过区块链技术对其进行存储管理，从而确保在网络中传输的通信数据安全性。在

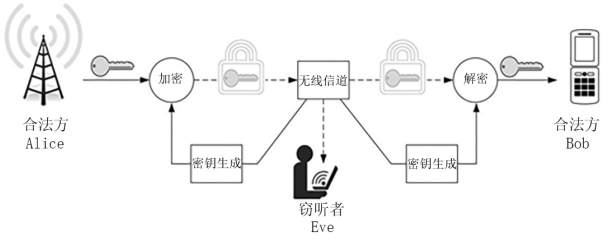

图 3 物理层的加密原理

图 4 系统整体结构

无线网络通信过程中需要对传输路径进行规划，从物理层、链路层和传输层 3 个方面进行控制和管理，将信息按照一定的路径发送给接收端。

框架层负责将传输的信息进行处理，将处理后的信息通过链路传递给应用层。应用层指为用户提供服务的软件程序，对用户开放访问权限，将信息以明文或密文形式在应用层中进行传递。

应用层负责对明文或密文信息进行解密处理。明文和密文信息均可以被解密得到相应的密码体制的数字信息和明文信息，通过对明文和密文信息的处理可以实现无线网络通信数据加密传输。

2.3 数据加密传输系统实现过程

基于区块链的无线网络通信数据加密传输过程，主要由 4 个部分组成：节点层、链路层、传输层和应用层。节点层是整个系统的核心，在网络中承担数据加解密的主要任务，可以采用多节点组合方式进行组网；链路层是系统的基础，负责整个系统的传输功能，需要保证数据传输过程中的安全性；传输层是系统中数据传输的核心部分，主要负责数据传输过程中的安全保障功能；应用层则是系统最上层，实现数据加解密及应用服务。

在对无线网络通信数据进行加密处理时，首先需要对通信数据进行编码，利用密码学算法对编码后的通信数据进行加密处理，同时采用数字签名技术确保通信数据的完整性。其次需要将加密后的通信数据以明文形式通过网络进行传输。最后完成对密文信息的解密处理。采用区块链技术完成对无线网络通信数据的存储管理，利用私钥和公钥实现对无线网络通信数据的加密传输。

2.4 数据加密传输流程与密钥管理设计

在数据加密传输系统中，通信数据加密传输流程主要包括以下步骤：首先，进行通信数据的生成；其次，采用私钥进行密钥管理，获取通信数据的密钥，通过加密算法将通信数据进行加密；最后，完成加密传输后的通信数据在区块链上的存储管理[4]。

在基于区块链技术的无线网络通信数据加密传输系统中，区块链是一种分布式数据库，它由多个节点组成，每个节点都存储有一份完整的交易信息，而其他节点只负责存储和同步区块链上的信息。由于无线网络通信数据加密传输系统具有强依赖性和开放性，区块链可以作为无线网络通信数据加密传输系统中的信任基础，通过对区块链技术在无线网络通信数据加密传输系统中应用进行研究，分析其可行性。在基于区块链的无线网络通信数据加密传输系统中，数据存储管理包括私钥和公钥两种类型。其中私钥是由节点通过特定方式生成，公钥是由节点根据自身情况生成。公钥使用时可以由用户进行选择[5]。

3 结语

基于区块链的无线网络通信数据加密传输方法为通信传输提供了一种创新而强大的解决方案，其可以有效应对日益增长的数据安全和隐私保护挑战。通过利用区块链技术的去中心化、公开透明和防篡改特性，其能够建立一个安全可靠的通信环境确保用户的数据得到充分保护。

参考文献

[1] 彭鹏.基于区块链的无线网络通信数据加密传输方法[J].无线互联科技，2023，19(2)：20-23，31.

[2] 王玉.网络通信中的数据信息安全保障技术策略探讨[J].中国新技术新产品，2022(22)：131-133.

[3] 郭建方，曹丽娜，朱方娥.短距离无线网络通信安全中的数据加密技术[J].信息与电脑(理论版)，2021，33(4)：171-173.

[4] 白翔，许从方，柳兴，等.区块链物联网安全技术综述及关键技术分析[J].信息技术，2022(10)：24-30，40.

[5] 董志鹏.支持区块链的无线接入网络中安全资源分配[D].南京：南京邮电大学，2022.

作者简介：陈于枫(1995—)，男，汉族，广东湛江人，本科，工程师，主要从事电子通信广电行业设计工作。

通信作者：兰泽勇(1978—)，男，汉族，湖北黄冈人，硕士研究生，高级工程师，主要从事通信网络与 IT 系统规划设计工作。