文章编号：2096-1472(2020)-12-50-04
DOI:10.19644/j.cnki.issn2096-1472.2020.12.015

基于区块链的物联网信息安全平台设计与实现

周立广[1]，韦智勇[2]

(1.南宁市第二人民医院五象医院，广西 南宁 530219；
2.南宁职业技术学院财经学院，广西 南宁 530008)
✉1960480023@qq.com; 122570724@qq.com

摘 要：由于在区块链系统中，随着各种设备的不断接入，会产生信息安全隐患，本文根据物联网存在的安全漏洞问题，结合区块链技术，设计了一种分布式的物联网信息安全管理系统，该系统可通过身份认证策略进行设备接入，对各种设备进行权限控制，同时在智能合约中融入安全仲裁机制，在信息管理方面，以数据进行分类存储，从而确保了数据的安全性。最后对系统各功能的测试，检测系统的安全性和有效性，通过对系统输入各类相关的信息数据，检验系统的输入结果，均达到了预期的目的。

关键词：物联网；区块链技术；认证策略；仲裁机制；入侵检测
中图分类号：TP311.5 **文献标识码**：A

Design and Implementation of a Blockchain-based IoT Information Security Platform

ZHOU Liguang[1], WEI Zhiyong[2]

(1.*Wuxiang Hospital of Nanning Second Peoples Hospital, Nanning* 530219, *China*;
2.*School of Finance and Economics*, *Nanning College for Vocational Technology*, *Nanning* 530008, *China*)
✉1960480023@qq.com; 122570724@qq.com

Abstract: Security problems occur when multiple different devices are continuously connected with blockchain system. Aiming at these security problems in Internet of Things (IoT), this paper proposes to design a distributed IoT information security management system based on blockchain technology. This system can access devices through identity authentication and it will control the permissions of various devices. At the same time, security arbitration mechanism is integrated into a smart contract. In terms of information management, data is classified and stored in order to ensure data security. Finally, function test is conducted to test the safety and effectiveness. Various related data is used as system input and the system output results reach the expected goals.

Keywords: IoT; blockchain technology; authentication strategy; arbitration mechanism; intrusion detection

1 引言(Introduction)

物联网作为信息化的一项重要技术，在各行各业中都得到了广泛运用，例如在电力系统、供水企业、交通部门、智慧生活等，都存在物联网技术的运用。然而，随着大量的设备接入网络，这样可能会造成外界的入侵或病毒的攻击，信息安全问题也显得越来越突出，物联网的安全问题比互联网要更严重，而且处理起来比较棘手。根据国外市场的调查，平均每年有将近百亿台终端设备接入物联网中，这些设备不仅是电脑终端，还包括手机、平板等无线接入设备，将来还会有更多的设备接入，这样，物联网信息安全问题也将成为信息界研究的热点问题[1]。

近年来，由于区块链技术的高速发展，已融入了各个行业当中，也为解决物联网信息安全问题提供了极大的帮助，由于在物联网中，接入网络的设备及终端与日俱增，而且各类繁多，维护压力较大，而传统的集成式网络模式由于存在单点信任的问题，已不适合当前的发展，逐步被分布式网络模式取代，而区块链技术也正是采用分布式存储模式，这就给物联网提供了的安全保障。另外，区块链的另一个特点就是去中心化，区块链是由一连串的数据结点按照时间戳的顺序连接而成

的一个分布式账本，区块之间通过共享机制确保数据不可篡改、不可复制，同时每个账本均备份，这样可确保数据的安全性。

关于区块链技术的研究，在国内外都得到了广泛的重视，最初区块链技术主要应用于比特币，现在主要应用于政策部门、各金融机构、证券期货、企业生产、医疗卫生、信息产业等，都有各自的研究项目，这些项目全球学术界的关注，并且都在不断地技术更新与发展，区块链技术在今后的应用范围还会更加广泛。

2 相关技术(Correlation technique)

2.1 区块链相关技术

区块链是一个基于分布式网络的数据存储系统，链上的每个点称这区块，账本是区块链的核心机制，主要包括数据块和链接。区块链技术具有去中心化的特点，整个网络可看成是一个分布式的账本，而区块链网络中每个节点的账本均通过信息备份；区块链具有严格的认证机制，在交易过程中，所有的交易产生的数据必须要半数以上的节点确认后才能生效，这个是各个节点共同遵守的认证机制；区块链数据具有不可篡改的特性，在区块链网络中的节点都保存有数据信息，如果要修改数据信息，必须能前一节点进行hash校验，而且至少要校验一半以上的结点，这些节点要一致通过后才可以修改，这样可确保数据的安全性；区块链具有智能合约的功能，合约程序存在于区块链当中，在双方进行交易时，双方交易平台的设备会通过合约程序，自动实现智能交互，这样可保证交易的真实性、有效性和安全性[2]。

2.2 认证机制

当物联网的设备接入网络前，必须要按照认证机制对该设备的身份进行认证，这样可确保系统用户合法有效，此外可对接入网络的用户进行认证备案，以此作为今后的系统使用凭证。区块链的认证机制主要包括识别和认证两个过程，是进入物联网系统的重要环节，对于非法用户，认证机制会禁止该用户进入网络内，而对于合法用户则系统会进行认证准许后连接进入系统，这样可防止网络受到外界入侵，同时，对于连入网络的设备终端，在进行相互通讯时，也要先进行身份认证，即用户的认证证书随时备查，同时系统也对认证过程进行数据备份，这样可保证了网络的安全性。区块链的认证的方式主要两种，即用户间认证和系统间认证，而目前使用较多的是用户间认证，形式有密码、钥匙卡、人脸识别、指纹、面部表情等。

2.3 权限控制策略

对于物联网的每个用户，都有自己的使用权限，而且根据权限访问相应的网络资源，对于权限以外的，用户将无法访问，权限控制是物联网安全的一项重要技术，通过权限控制策略，对所有用户进行实时监控，杜绝非法用户访问非授权的网络资源，这样可确保网络资源的安全性。权限控制一般使用角色控制，在该模式中，用户与访问的权限还是一一对应的关系，而是在两者中用角色替换，即用户可能以其他角色出现，而这个角色又被授予了相应的使用权限，而权限的范围主要根据工作的具体内容而定，对于权限移除时，角色也将一并取消，这样可确保授权的快捷性[3]。

智能合约是用区块链的技术进行的一种数字化合约方式，一般通过程序代码写入区块链中，主要通过特定的运行机制来保障交易的进行，该合约的操作不受外界的干扰，智能合约的方式首先通过双方的合约内容进行协商，如果双方达成一致认可，系统将通过程序代码按照合约逻辑把合约内容发布在系统中。合约一旦确立，写入系统后，合约将自动生效，外界将无法进行修改[4]。因此，订立合约时双方必须要严谨，另外合约双方无须到场进行面签，只要双方在网上通过智能合约系统便可完成，这就保证了智能合约的安全性和高效性。

2.4 入侵检测机制

在物联网中，外来入侵对网络安全构成了严重的威胁，系统必须要有相应的机制应对这个安全威胁，入侵检测机制是系统应对外来入侵的一种保护机制[5]。该机制主要根据操作者的行为、操作日志、系统审计结果等数据信息进行有效监控，根据这些数据信息，系统会通过大数据分析，判断该用户的操作行为是否属于入侵行为，系统会立即采取预警措施，采用强行机制使禁止用户的行为，防止入侵的一步发生，同时系统会启用修复功能，把遭到破坏的系统文件和相关数据恢复，确保系统的安全与稳定性。

3 系统设计分析(System design analysis)

3.1 系统需求分析

本系统需求分析，主要分为设备接入管理、设备操作管理、设备数据传输、数据及资源获取等功能进行分析和认证。对于设备接入管理，主要是终端设备在接入物联网之前，必须先进行注册认证，认证通过后即注册成功，就可以接入物联网，使用该平台进行各种操作，认证过程主要是针对该设备的身份证合法性，主要运用区块链的合约功能实现，尽可能使区块链上的每个节点都通过认证，这样可确保认证过程真实有效，同时认证通过后系统会对认证的信息自动备份，防止被篡改；设备操作管理，主要是当用户接入物联网后，要求对所有设备进行统一的管理，一般而言，物联网设备的运行状态主要分为在线和离线两种，如果由离线转到在线状态，主要通过系统登录的方式进行，系统会自动从账本中读取已经登记的设备列表，与登录的设备进行比对，进行身份认证，认证通过后才能根据各自的权限进行各项操作；设备数据传输，主要是对物联网设备之间进行通讯和数据交换的管理，对于设备在数据传输之前，系统先查看一下该设备是否具有数据传输的权限，同样，这个过程也需要由合约程序来实现，也同样经过各节点的一致认证，认证过程也和设备操作管理过程相类似，以确保各设备传输数据的安全性；数据及资源获取，主要是物联网设备在接收别的设备发过来的数据信息或在网上搜索别的设备的相关信息时，同样也需要进行认证，认证过程同前面所述。此外，系统会对所有传输的数据信息进行统一的管理，这样不仅可以对设备传输过程进行全程监控，也可为今后数据的查找与溯源提供方便，同时也提升了整个网络的安全性和有效性[6]。

3.2 系统用例图

根据系统功能需要分析，本文绘制出了系统的用例图，具体如图1所示。

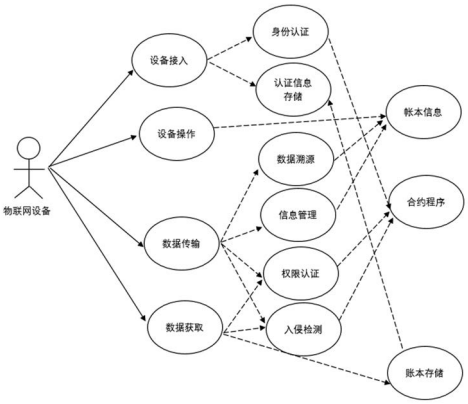

图1 系统用例图

Fig.1 Diagram system use case

图1中，系统所涉及的所有设备为接入物联网的设备，进入系统前先经过身份认证，认证过程由合约程序自动完成，认证过程中数据信息会存储在账本中，登录进入系统后的设备操作，系统会自动读取账本的已注册的设备登记表，进行比对认证，当设备对过认证后，在网络内进行数据传输和信息获取时，也是通过设备权限认证，通过后才能进行数据传输，对于数据资源的获取[7]。系统同样也要权限认证后方可进行。整个系统的所有信息都必须进行统一的管理。此外，系统还有入侵检测功能，所有的判断都由合约程序完成，都要经过各个节点的一致通过。

3.3 系统架构设计

本系统主要处理物联网内设备之间的数据交换，交换信息需要通过认证机制及权限的有效管理，以及入侵检测机制，系统中的各个节点主要用于信息处理及加工、封装服务、系统管理等，而区块链的各个节点主要用于数据的存储与认证管理，具体系统框架如图2所示。

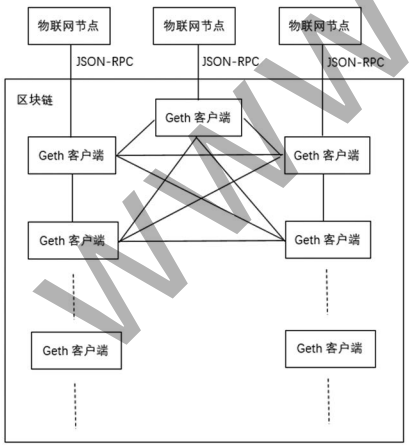

图2 系统架构图

Fig.2 System architecture

系统的底层主要是由区块链的各个节点形成的网络，各节点即Geth客户端，主要功能是在双方交易过程的信息验证、交易信息的备份及合约数据的返回等。另外，各节点对上层的请求进行通过前的认证，必须要一致通过后方可通过，认证信息保存在区块链的账本中[8]。

系统的上层是物联网的网络层，由各个分节点组成，每个分节点与底层的节点一一对应。上层节点主要功能是对接入物联网的设置进行通讯和数据传输，对交互的信息进行统一管理，对物联网的所有设备进行接入前的认证，并分配相应的权限与实时监管，同时对外来入侵进行实时防控，另外，还对系统的对外业务提供服务接口[9]。

系统的分节点与底层的客户商进行通讯，主要通过JSOM-RPC方式来完成，整个系统的安全策略主要由物联网系统与区块链系统合作分工完成的，其中包括身份证认证、各个设备的权限控制、节点的仲裁判定、交易过程的智能合约等，均由两者共同完成[10]。

3.4 系统功能模块设计

根据整个物联网系统的需求分析与总体架构的设想，本文将系统的功能模块主要分成认证管理模块、操作管理模块、安全检测模块、信息管理模块四大功能。

(1)认证管理模块。对于物联网的各个设备终端在接入网络前必须进行身份认证，系统认证请求发给接入管理模块，该模块把请求进行格式转换，并把转换后的请求信息发送给区块链的节点中，区块链系统会自用调用合约程序进行身份认证，把认证的结果返回给该模块，同时把认证的信息进行存储，对于认证结果的返回，如果认证通过，则返回认证成功的相关消息，否则返回认证失败的消息，所有信息都会保存在区块链的账本中。另外，系统对接入的所有设备进行统一管理，把设备接入表保管在账本中[11]。

(2)操作管理模块。本功能主要是对物联网的各个设备进行操作业务的管理及权限的控制。网上的设备进行操作主要包括信息发送和信息获取，并且各项操作都必须在各自的权限范围内进行，设备进行信息发送前，首先要先确认自己是否具有信息发送的权限，这就要求通过权限认证过程，认证过程主要是通过区块链合约程序来完成，认证过程的所有信息都保存在区块链的账本中，便于今后的数据溯源，认证结果会发送给操作管理模块，如果通过，该设备可以进行信息发送，否则将禁止发送，对于信息获取，其流程也同信息发送相同；另外对于物联网的所有设备，统一进行权限的分配与管理，所有的权限均保存在权限分配表中，与设备接入表一同存储在区块链的账本中[11]。

(3)安全检测模块。本模块功能主要是确保整个网络的安全性。安全检测主要包括对内检测和对外检测，对于接入物联网的设备，如果该设备发送一些恶意信息，对网络进行破坏，系统必须对该设备进行权限的禁止，必要时还会使其脱离网络，对于设备发出的信息，都由系统的事件分析器进行检测，则把处理结果通知安全检测模块，如果该设备发出的信息属于恶性攻击，该模块立即对设备进行警告或限制其使用权限，如果仍进一步发恶性信息，则会强行该设备退出网络[12]。

(4)信息管理模块。本模块主要包括数据处理、消息管理和数据展示三大功能。数据处理主要是对物联网的设备发出的请求进行简单封装，然后再进行数据传输；消息管理主要对整个系统的信息进行监控、统计和存储，便于信息今后的查找与溯源；数据展示主要将系统的一些数据进行表格化或图形化处理，为与外部的接口提供数据转换，便于对外部设备的数据传输。

4 系统的实现(Implementation of the system)

4.1 区块链网络构建

由于区块链在分布式环境下运行，主要将客户端分别安装到多台电脑中，分别以每台电脑作为区块链的节点。在电脑中分别部署节点，主要工作就是设置每台电脑的创世纪块，先创建第一个，然后按照顺序把其他电脑都添加新的区块，这样就可以各个节点连接在一个模拟的区块链网络中，其中各台电脑终端所设置的相同的创世纪块，以便共同维护账本。各节点部署后运行Geth客户端，使其相互链接，同时，把各个节点添加到一个列表中，以便各节点进行数据传输，这样就构成了一个简易的区块链网络。

4.2 系统的功能实现

4.2.1 认证管理模块的实现

在目前的物联网系统中，设备的身份认证主要有三种模式，即静态密码认证、动态密码认证和生物特征识别认证[13]。静态密码认证主要是通过用户预先设置的密码进行认证，该密码是静态的，如果用户不修改，则密码将一直有效；动态密码主要根据内置的密码芯片进行运算推出动态口令，密码认证必须其动态口令和内置密码芯片共同完成；生物特征识别认证主要是根据人体的某一特征进行识别，例如人脸识别、指纹识别、表情识别等[14]。本文根据系统的特点设计了一个综合识别方式，主要是把设备的制造商、设备类型和设备出厂编码等信息记录下来，写入设备接入表，并保存在区块链账本中，作为身份认证的唯一识别代码，认证表的结构主要包括设备名称、识别代码、设备特性和备注信息等。当设备接入网络时，先获取这三项信息，然后与设备接入表的数据进行比对，如果比对成功则认证通过。

4.2.2 操作管理模块的实现

当物联网的设备之间进行信息发送和信息获取时，系统的交互模块接收设备的信息，并把发送请求传给数据传送模块，数据传送模块向区块链系统发送权限验证请求，区块链的合约程序会自动验证该设备的权限，并把验证结果返回给数据传送模块，如果验证通过，则数据传送模块把信息传送给交互模块，进行信息发送，否则，将不通知交互模块。同样对于信息接收也是同一原理来完成设备的操作管理。

4.2.3 安全检测模块的实现

安全检测功能，主要通过CIDF程序来实现，CIDF程序主要包括三个子程序，即事件产生程序、事件分析程序和数据写入程序，系统首先对所发送的信息进行运行状态监测，然后把测试的结果发送给事件分析程序，事件分析程序对该消息行为与恶性事件数据库进行比对，如果比对成功，则说明该信息属于恶意消息，则把消息返回给系统，对该设备进行权限进行限制。

4.2.4 信息管理模块的实现

数据处理功能主要通过调用JSON−PRC接口程序来实现，该程序通过调用形式，根据请求的类型，把信息打包封装起来，然后必须到对应的地址中；消息管理主要也是通过数据处理功能实现，JSON−PRC接口程序会调用系统的消息管理器，对信息进行分类保存；对于数据展示功能，主要是调用对外服务接口程序来实现，对数据进行图形和表格化处理[15]。

4.3 系统测试

4.3.1 测试环境

本系统是基于几台电脑进行模拟构建的，用于测试区块链的网络部署和系统的功能测试。在测试环境中，电脑的硬件要求是I5四核以上的处理器，内存容量为4G以上，操作系统是windows 10专业版(64位)，开发工具为eclipse，数据库选择MySQL。

4.3.2 功能测试

本系统的测试主要模拟物联网设备，对系统输入相关的数据信息，看一下实际测试结果与预期效果进行对比，检测系统的各功能模块是否存在系统错误。功能测试主要包括认证管理模块、数据管理模块、安全检测模块和信息管理模块的测试。

认证管理模块测试主要对设备的接入进行身份认证，通过向系统分别输入真实的设备信息和虚假的设备信息，对于正确设备信息系统会提示“认证通过”，对于虚假的设备信息，则提示“认证失败”；数据管理模块测试主要是对设备发送与接收信息的管理，对两个不同权限的设备进行信息发送操作，其中一个设备具有发送的权限，另一个没有发送的权限，经过测试，对于具有权限的设备，系统提示“消息发送成功”，对于没有权限的设备，系统提示“您无权发送消息”，同时通过后台的数据库，可查看到整个过程已备份到数据库当中；安全检测模块测试主要检测系统是否存在恶意信息，在同一设备中分别发送两条信息，一条是正常的信息，另一条是恶意攻击的信息，对于正常的信息，系统提示“消息发送成功”，而对于恶意攻击的信息，系统提示“恶意信息，拒绝发送”，对于连续发送恶意信息再进行测试，系统会本设备隔离出来，无法连入网络中；信息管理模块测试主要检测系统消息的存储管理，通过上述的几个操作，在后台数据库中都能找到消息的存储记录和存储时间。

4.3.3 测试结果分析

通过上述对认证管理模块、数据管理模块、安全检测模块和信息管理模块进行了具体、有效的测试，实际测试结果与预期的结果完全一致，此外，整个系统操作简单，流程非常清晰，而且系统运行稳定、效率高，没有明显的错误，达到了预期的目的。

5 结论(Conclusion)

由于物联网在各行业中得到了广泛的运用，大量的终端设备都接入到物联网中，对工作和生活带来了极大的推动作用，然而物联网的信息安全问题也日显突出，尤其在网络管理上显得十分棘手，为此，本文提出了基于区块链技术的信息安全平台系统的设计方案，用来解决这一技术难题，取得一定的科研成果，但是系统仍然存在一些不足之处，对于物联网系统的设备，发送的消息缺乏统一的格式，每个行业都各自为政，消息格式无法统一。对于安全检测，恶意消息的检测范围有待拓宽，检测的策略有待改进，使检测范围更加全面，检测机制更

(下转第46页)