Kafka 节点认证的电力用户信息联盟链管理技术研究

许俊晓 崔昊杨
(上海电力大学电子与信息工程学院 上海 200090)

摘 要 为了保障电力用户信息的安全和隐私,提出一种基于联盟区块链技术的电力用户信息管理系统,利用联盟链去中心化、不可篡改等特点保证信息安全。同时,为了提高系统运行效率,采用 Kafka 作为共识机制,并且使用改进 2FA 双因子认证技术来保证登入节点的合法性,进一步增强对电力用户信息的保护。系统通过链码和前端的设计,可以实现对用户信息的查询和修改。从不可篡改性、隐私性和抗攻击性三方面论证了系统的安全性,通过测试证明了系统的可用性和高效性。

关键词 联盟链 电力用户信息 Kafka 改进双因子节点认证 链码

中图分类号 TP302 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.11.004

MANAGEMENT TECHNOLOGY OF POWER USER INFORMATION ALLIANCE CHAIN BASED ON KAFKA NODE AUTHENTICATION

Xu Junxiao Cui Haoyang
(*School of Electronics and Information Engineering*, *Shanghai Electric Power University*, *Shanghai 200090*, *China*)

Abstract In order to ensure the security and privacy of power user information, this paper proposes a power user information management system based on alliance blockchain technology, which uses the characteristics of alliance chain decentralization and non-tampering to ensure information security. At the same time, in order to improve the operating efficiency of the system, Kafka was used as a consensus mechanism, and the improved 2FA two-factor authentication technology was used to ensure the legitimacy of the login node, and to further enhance the protection of power user information. The system could query and modify user information through the chain code and front-end design. This paper demonstrated the security of the system from three aspects: immutability, privacy and anti-attack ability, and the usability, and the efficiency of this system was proved through tests.

Keywords Alliance chain Information of power user Kafka Improved two-factor node authentication Chain code

0 引 言

目前,区块链技术已经成为当今保证信息安全的重要手段[1-2]。在电力行业,保障用户信息安全也急需重视。目前我国正在逐步推进电力市场化[3],电力用户信息的价值和重要性也在逐步攀升,一旦信息安全出现漏洞,会给改革中的电力市场带来不小的影响。

为了保护用户数据隐私和安全,许多专家学者提出了不同的解决方案,例如基于对角数据聚合方法的数据隐私保护解决方案[4]、基于云的可撤销的代理重加密方案[5],以及可扩展的隐私支持架构和上下文感知的隐私保护方案[6]等。但是这些方案大部分都非常依赖于第三方,如果数据存储过于中心化,一旦单点遭受攻击,那么所有数据的安全都会受到威胁。

区块链技术可以解决数据存储过度中心化的问题。区块链作为一种不可篡改的[7]、去中心化的[8]分布式账本,能够通过公私钥加密,Hash 加密等技术保障用户信息的正确性、完整性和隐私性[9]。近年来,有许多学者对区块链技术应用于保障用户信息安全进行了研究。文献[10-11]将区块链技术用于保障数据的安全,研究了区块链的结构,探讨选择了适用于保障

收稿日期:2021-05-21。国家自然科学基金项目(61107081)。**许俊晓**,硕士,主研领域:区块链技术,电力信息安全。**崔昊杨**,教授。

用户数据的区块链共识机制。但更多的是在理论探讨,没有说明具体的实现细节。文献[12]提出了使用以太坊公有链保存个人数据信息的方法,并且给出了详细的系统设计和实现方法,但会使得数据信息过于透明。文献[13]将区块链技术用于存储医疗信息,从而保证信息的安全性,并且设计了系统模型,但是由于潜在作恶节点的存在,需要制定共识机制,以牺牲吞吐量来保证节点的安全性,所以交易效率会有所下降。综上所述,公有链[7]过于透明,不适合存储隐私要求高,数据量大的电力用户信息。并且传统的共识机制算法以及其衍生算法具有自身的局限性,例如工作量证明(PoW)算法[14]和权益证明(PoS)算法[15]需要算力的支撑,而拜占庭容错(PBFT)算法[16]需要全节点投票,十分浪费时间。

为了保证电力用户信息的安全和隐私,同时保证对信息管理的高效,本文提出了基于联盟链[17]技术的电力用户信息管理系统。采用联盟链构建系统,以加强信息的私密性和安全性。使用 Apache Kafka 代替传统的共识机制,提高系统的交易吞吐量,并且使用改进 2FA 双因子认证技术来保证链上节点的合法性,防止黑客冒充节点入侵系统。本文在最后论证了系统的安全性,通过测试证明了系统的可用性和高效性。

1 电力用户信息联盟链管理系统设计

为了保证对用户信息的安全存储和隐私保护,采用联盟链技术构建电力用户信息联盟链管理系统。本文使用 Hash 加密算法[18],共识机制,联盟链准入机制等技术保证信息的安全和隐私,以区块为存储电力用户信息数据的载体将信息上链保存。电力用户信息联盟链管理系统的参与主体主要有三个,分别为用户,电力单位和电力用户信息存储链,三者关系如图 1 所示。

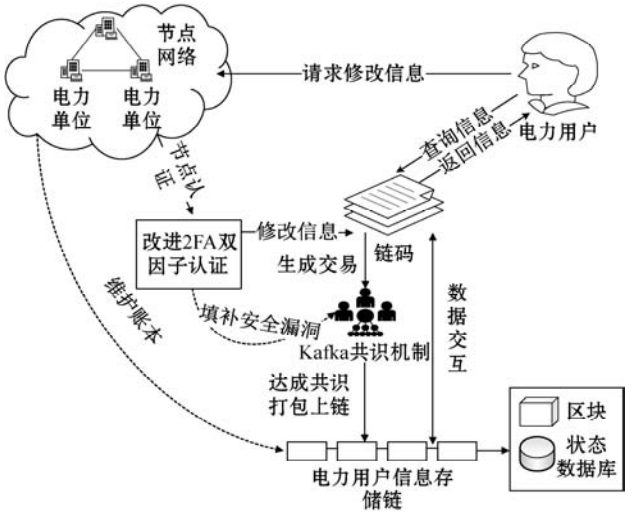

图 1 电力用户信息管理系统结构

电力用户信息管理系统完成的工作如图 1 所示,电力用户信息(包括身份证号码、联系方式、住址、用电量等)由节点存储上链,节点主要由电网信息管理部门构成,节点需要通过 2FA 双因子认证才能参与联盟链账本的维护。电力用户对自己的信息有绝对的所有权和查阅权,用户可以提供身份信息查询个人信息。但是用户无权修改信息,因为修改用户信息需要由节点发起交易来完成。修改信息的交易发起后,全节点接收,打包成新的区块上链,从而修改电力用户信息存储链的世界状态。

本系统利用联盟链不可篡改性、加密功能和准入功能抵御篡改、窥视等非法攻击,并且使用改进 2FA 双因子认证保障节点的合法性,避免攻击者登入节点,主动作恶。下面从各方面阐述电力用户信息管理系统的构成。

1.1 电力用户信息存储链

图 1 中的电力用户信息存储链是管理系统中保存用户信息的数据库,它主要由区块和账本的状态数据库构成。区块是存储电力用户信息的主要载体,它由区块头和区块头两部分组成,如图 2 所示。区块头是区块的核心部分,区块头中包含版本号、时间戳、上一区块 Hash 值和 Merkle 树根。

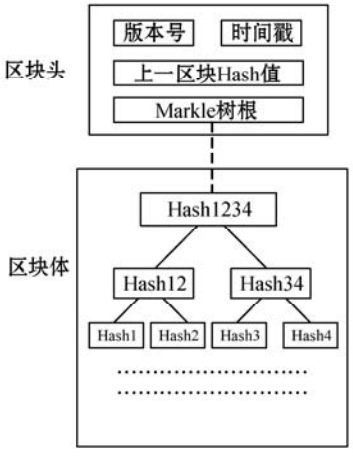

图 2 区块结构

1.1.1 版本号及时间戳

版本号代表区块链目前最新的版本。时间戳记录着区块创建的时间。它以秒为单位,可以保证用户的信息每一次存储和修改都会记录在链上,使得每一次存储和修改都是可追溯的,保证用户信息的安全。

1.1.2 Merkle 树根

Merkle 树根是交易 Hash 值的汇总,区块中的交易信息都是以 Merkle 树的形式存储的。如图 2 所示,每一笔交易信息都通过 Hash 加密算法形成 Hash 值,不同的两笔交易的 Hash 值结合做新的 Hash 计算,不停迭代,最终形成 Merkle 树根。使用 Merkle 树根存储用

户信息可以尽量减少信息所需的存储空间,以节省资源。若要进行特定交易的快速查询,不需要下载所有信息,只需垂直查询 Merkle 树的特定分叉,使得查询操作便捷快速。

1.1.3　上一区块 Hash 值

上一区块 Hash 值(PreHash)使得从创世区块开始所有的区块都能够联系起来,让区块之间彼此依赖,从而使对于区块的单点篡改攻击失效。如果攻击者对一个区块进行篡改,那么此区块的 Hash 值将会变动。一旦区块的 Hash 值与下一区块的 PreHash 不同,篡改攻击会被察觉并阻止,有效保障用户信息的安全。

1.1.4　账本状态数据库

账本的状态数据库主要用作记录全链的世界状态,具有存储键值,支持电力用户的查询操作等功能。账本状态数据库包括 LevelDB 和 CouchDB。由于 CouchDB 不仅可以依据制定的 key 值进行信息查询,还可以在各种应用场景下实现复杂查询,所以本方案选择 CouchDB 作为账本状态数据库。

1.2　节点网络

电力用户信息存储链是由各个节点共同维护的,所有的节点组成了一个点对点网络,保证了通信的一致性。在每个节点网络中,都会有一个 leader 节点,它是通过领导人选举机制选择出来的,负责将获得的新区块分发给网络中其他的 peer 节点。节点网络中所有的节点都由不同级别的电网信息管理部门单位构成。由于 leader 节点负责区块的分发,是整个网络的枢纽,所以本文的 leader 节点通过静态选举,制定由省级及以上的信息管理部门构成。而普通 peer 节点,包括背书节点、排序节点等就由市、县级信息管理部门构成。完全可信各级电力单位承担了电力用户信息存储链的维护工作,保证了信息的安全性。

1.3　Kafka 共识机制及节点认证

在分布式场景下,节点维护账本需要保持对于交易或者数据的一致性,共识机制[19]可以实现这一点。共识机制不仅能够实现所有节点异步通信的一致性,也能够处理故意篡改交易或者恶意发送交易的节点,是区块链的核心模块。

1.3.1　Kafka 共识流程

为了避免类似传统共识机制对于算力资源和时间的浪费,同时提高完成交易的效率,本文采用 Kafka[20]作为本系统的共识机制。由于系统中所有的节点均由不同的电力相关单位构成,所以可认为节点并不存在主动作恶的可能,因此共识机制只需要能够最大限度地满足本系统高并发,低延迟的需求即可,而 Kafka 可以满足这一需求。

Kafka 是一种基于发布与订阅的消息系统,具有高并发,低延迟的特点。本文将 Kafka 用于交易的排序,保证交易顺序的一致性和交易发送的高效性。Kafka 共识实现如图 3 所示,应用端收到需要添加或修改电力用户信息的交易请求后,将交易请求发送给相应的多个背书节点,由背书节点来提前调用链码进行模拟执行。执行完成后,如果没有问题,背书节点就会对这笔交易进行背书签名,如果有超过两个节点签名,那么此交易就会被认可。被认可的交易会被发送给排序节点,排序节点根据本文设定的共识机制——Kafka 来确定交易的顺序,然后将交易打包成区块,最后将打包完成的区块进行广播。

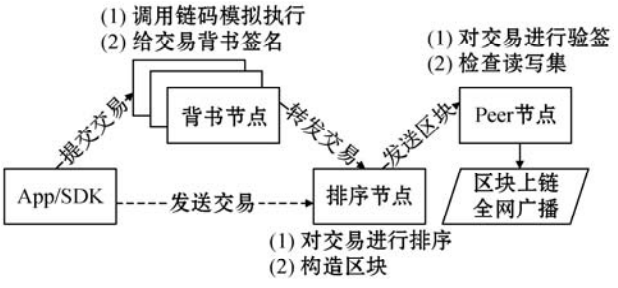

图 3　Kafka 共识实现流程

大多数时候,由于电力用户的用电信息需要经常修改,系统会在短时间内接收到大量的交易,所以不会出现一个交易一个区块的情况,而是根据排序将多个交易打包成一个区块,能够极大地提高效率,这也是 Kafka 在本系统中最重要的功能。Kafka 能够在短时间内接收大量的交易消息,并且可以保存相当一段时间,在此期间,交易将会被快速排序并且保存在新区块中输出。peer 节点接收到新区块后,进行最后一次验证,包括检查读写集,确认是否重复提交,防止出现恶意的,类似于分布式拒绝服务(DDoS)攻击的重复提交攻击,确认交易的正确性和有效性,将无效的区块剔除。最后由 leader 节点将通过验证的区块全网广播,成功添加或修改电力用户信息。

由于系统中存储的数据过于重要,而且 Kafka 与其他的传统共识机制不同,并不存在对于作恶节点的惩罚机制或者验证交易合法性的投票机制,所以本文使用经区块链技术改进的 2FA 双因子认证对节点进行身份认证,弥补 Kafka 的安全漏洞,以免有攻击者登入节点,进一步提高电力用户信息的安全性和隐私性。

1.3.2　改进 2FA 双因子认证

2FA 双因子认证在单因子认证的基础上加了另一层认证,需要用户提供两个认证因素来完成身份认证,从而提高访问数据的安全性。但是 2FA 双因子认证的认证因素是 2FA 中央数据库提供的,所以它仍然具

有集中式的缺点,容易受到单点攻击。

为了解决 2FA 中央数据库易受单点攻击的问题,本文提出了区块链解决方案。通过利用区块链去中心化的特点,我们可以使认证信息不会永远停留在集中的 2FA 数据库中。由于区块链具有不可篡改性,所以不能随意删改数据,保证了数据的安全性。由于节点认证的重点在于保证其安全性,对于吞吐量的要求不那么高,所以改进 2FA 双因子认证并不使用上文的 Kafka 共识机制,而是使用 PBFT 共识机制,通过投票的方式来保持所有节点的一致性。与电力用户信息管理系统相似,维护认证信息链的所有节点均由电力相关单位组成。

改进 2FA 双因子认证包含注册和验证两个部分,首先节点需要进行注册,将认证信息上链保存,注册的步骤如图 4 所示,首先为每个节点设置不同的身份特征值 N,将 N 和相关身份信息上传给接收请求节点,由接受请求的节点发起交易。N 和身份信息将以 Hash 的形式通过 Markle 树算法,最终形成根值 H。然后接收请求节点需要让全网节点达成共识,由于认证系统使用的共识机制是 PBFT,该机制需要全网进行投票,所以接收请求节点将 N 值向全网广播,请求投票。网络中的其他节点对于 N 值进行哈希计算,将计算结果与请求节点的计算结果进行对比,如果相同,则投票同意该交易合法,如果有 2/3 的节点投出了同意票,则代表达成共识。达成共识后,接收请求节点使用 RSA 加密算法将 H 值进行签名和加密操作处理,得到处理后的 H_{sign} 值,然后将其与 N 值写入区块,认证信息成功上链。RSA 加密算法是一种不对称加密算法,使用不同的加密密钥和解密密钥,即私钥(PrivateKey)和公钥(PublicKey)。而 H_{sign} = PrivateKey(H),所以请求节点会返回 PublicKey 用于之后登录节点的身份认证。

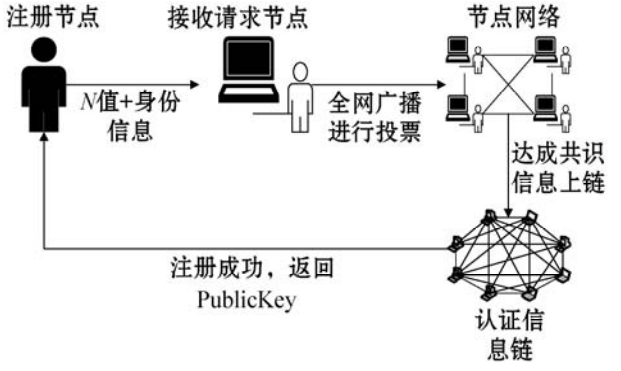

图 4 节点注册流程

当节点登入系统时需要使用 N 值,身份信息和返回的 PublicKey 来完成验证操作,验证的流程如图 5 所示,首先需要认证的请求节点将 PublicKey,N 值和身份信息上传给接收请求节点,接受请求节点根据 Markle 树算法对身份信息进行处理,得到 H 值。接着接受请求节点使用 PublicKey 对认证信息链中各个区块中包含的 H_{sign} 进行解密和验签操作,得到不同的 H_1 值。最后遍历全链各个区块,将所有 H_1 值与请求认证节点的 H 值一一对比,查看是否存在两者相同的情况,如若存在,则 H 值验证成功,如若不存在,则验证失败。接下来对比请求节点上传的 N 值与该区块中的 N 值是否相同,如若相同,则 N 值验证成功,如若不同,则验证失败。只有 H 值和 N 值同时验证成功,认证才能通过。

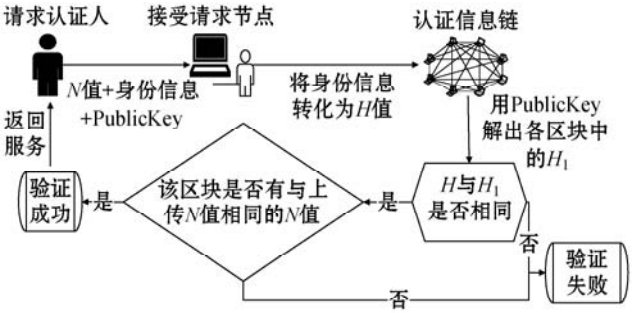

图 5 节点认证流程

节点想要通过认证,首先需要上传 N 值和身份信息这 2 个认证所需因子以及 PublicKey,系统通过比对上传信息与链中的注册保存信息是否相同,只有比对全部通过,认证才算完成。即使攻击者得到了节点的身份信息,没有正确的 N 值,也无法进入电力用户管理系统进行操作。因此本文的改进 2FA 认证技术不仅能保证登入节点的合法性,同时还能避免了攻击者对认证信息数据库的单点攻击,这也进一步加强了对于电力用户信息管理系统中用户数据的保护。

1.4 链 码

由于电力用户信息管理系统是运行在对等计算机网络上的,所以本系统是一种去中心化应用(dApp)。传统的 Web 应用和去中心化的 dApp 都是通过 HTML,CSS 等传统的 Web 前端技术来构建前端界面,而两者不同的地方就在于获取数据的方式。传统 Web 应用通过 API 调用来得到相关数据库的数据,而 dApp 是使用联盟链上部署的链码[21]来获取数据。

链码,也称智能合约,是由图灵完备的编程语言编写的,它使得系统能在没有第三方的监督管理下,自动执行制定的合约。本系统通过链码,将数据与键值一一对应,上链存储。用户如要查询信息,需要提供键值相应的数据,节点如要修改信息,则需要上传符合键值要求的数据对象。

本文将身份证号码设置为查询键值,用户可以使用身份证号码查询个人信息,实现流程如下:首先业务层接收用户发送的身份证号码字符串,接着调用链码

中的键值溯源函数。调用成功后,先验证上传的参数个数是否符合要求,然后遍历区块链数据库,根据查询键值查询相应用户信息对象的状态,查询成功后,将查询到的数据反序列化后返回。

对信息的修改操作只能由节点通过认证后完成,实现流程如下:首先业务层接收一个用户信息数据的对象,将对象进行序列化操作,将其转化为字节数组,接着调用链码上传。上传成功后,先检查上传的参数是否符合要求,然后检查是否有完全相同的数据存在,若存在则返回错误,若不存在则将数据存入账本,即节点发出交易,用户信息成功上链。

2　分析与测试

2.1　安全性分析

本文使用了联盟链技术和改进 2FA 认证技术保障了电力用户信息的安全性,下面从防篡改性、隐私性和抗攻击性三方面分析本系统的安全性。

2.1.1　防篡改性

链中区块的核心信息包括上一区块哈希值(PreHash)、本区块的 Markle 树根、时间戳、随机数等等。其中 PreHash 和时间戳将各个区块链接起来,一旦攻击者对于区块中的数据有任何修改,区块的 Hash 值就会变化,全链会立即察觉并且修复。通过时间戳、PreHash、Hash 加密算法和 Merkle 树的共同作用,增强了用户信息存储链的安全性。即使合法节点需要修改信息,也只能再次发起交易上传信息,不能直接修改,保障了电力用户信息的不可篡改性。

2.1.2　隐私性

本系统采用联盟链技术,与公有链不同,联盟链使用准入机制限制节点的加入,因此链上的电力用户信息并不透明,只有准入的节点才能知晓链上的全部信息,而用户需要提供相关身份信息,通过富查询得到相关信息。如果节点需要查看链上的任何信息,也需成功通过改进 2FA 双因子认证,否则无法获得查询的资格。

2.1.3　抗攻击性

本系统采用改进 2FA 认证方法保证登入节点的合法性,防止攻击者非法入侵系统。即使攻击者获取了节点的认证信息,获得了存储系统的节点入口,由于 Hash 加密算法的单一性和不可逆性,攻击者也无法在没有公钥的情况下通过 Markle 树根倒推出区块内的所有信息。

2.2　功能测试

2.2.1　测试环境

本系统采用 Hyperledger Fabric 搭建联盟链系统框架,整个测试的组成包括 1 个 Leader 节点、1 个 CA 节点、1 个 org 通道、2 个 peer 节点、2 个 order 排序节点。系统的测试是在虚拟机上完成的,虚拟机的配置如表 1 所示。

表 1　测试环境虚拟机配置

配置	版本或参数
操作系统	Ubuntu 16.04LTS
CPU	2.10 GHz 4V
内存	3 GB
硬盘	30 GB
Hyperledger Fabric	1.2.0
Fabric CA	1.2.0
Kafka	1.0.0
Docker	18.09.7
Golang	1.8.3

2.2.2　测试流程

系统首先在链码中声明一个结构体,用作存储电力用户的个人信息和用电信息。为了之后的测试,测试程序设置了两个测试对象,两个数据对象的数据在实体化链码时被保存在联盟链账本中。本系统的链码可以实现用户对本人信息的查询操作。用户需要提供键值,即本人的身份证号码才能查询到相关信息,查询操作界面如图 6 所示。

图 6　电力用户信息查询界面

输入在实例化链码时被存储上链的测试对象的身份证号码,系统会根据身份证这一键值在状态数据库中查询相应的状态,反序列化操作后,系统将完整的个人信息和用电信息返回,数据界面如图 7 所示。

图 7　电力用户信息查询结果界面

而数据的修改只能由链中的节点,即相关电力单位才能完成。节点通过 2FA 双因子认证,合法登录后可以进行数据的添加及修改操作,如图 8 所示,节点尝试修改测试对象的用电不良记录。

图 8 修改电力用户信息界面

因为区块链具有不可篡改性,所以对于链上数据信息的修改并不是将原有信息进行覆盖抹除,而是再次产生一个交易,如果在修改后进行查询,系统将根据键值自动返回最近一次添加的数据,这保证了用户任何时期的数据都是被完整保存的。因此节点修改测试对象的用电不良信息时会发出交易,如图 9 所示,节点发出了交易,数据上链后,系统再次使用键值进行查询操作,返回了进行修改操作后上传的数据,信息更新成功。

图 9 修改后发出交易以及更新数据

2.3 吞吐量测试

吞吐量是指区块链在单位时间内完成的交易个数。为证明本系统采用的 Kafka 共识机制的高效性,本文使用联盟链测试工具 Hyperledger Caliper 对系统进行测试,一共进行了 15 次测试。由于网络存在波动,所以 15 次测试的吞吐量数据存在差异,测试数据如图 10 所示,15 次测试的平均吞吐量为 214 TPS,即每秒平均可以完成 214 笔交易,与当前主流的比特币区块链(吞吐量约为 7 TPS)和以太坊(吞吐量约为 100 TPS)相比,本文方案的效率更高。

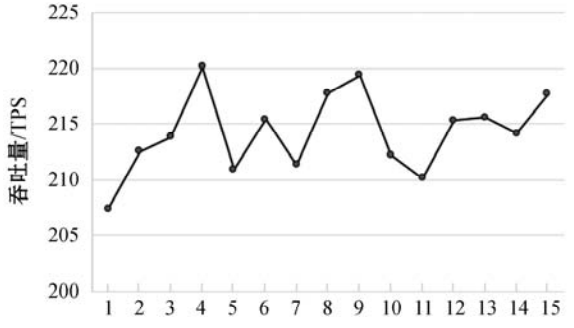

图 10 测试吞吐量

3 结 语

就解决电力用户信息的安全隐私问题,本文提出了一种基于联盟链技术的电力用户信息管理系统。为了保证用户信息的隐私,利用联盟链技术来严格控制维护账本的节点。为了提高系统的交易吞吐量,使用 Kafka 作为联盟链的共识机制,同时为了弥补 Kafka 可能出现的安全问题,本文使用能够抵抗单点攻击的改进 2FA 双因子认证技术来验证登入节点的合法性,进一步提高电力用户信息的安全性。通过分析证明,电力用户信息管理系统能够保证电力用户信息的安全和隐私。通过测试证明,电力用户信息管理系统能够实现用户查询和节点维护的功能,系统的交易吞吐量性能表现也较优。在实际的电网环境下,节点数量必然会更多,所以我们下一步将研究区块链扩容技术,考虑在大量节点产生大量交易的情况下,系统应当如何保证并且提高交易的吞吐量。

参 考 文 献

[1] 张奥,白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报,2020,31(5):1406 - 1434.

[2] 王胜寒,郭创新,冯斌,等. 区块链技术在电力系统中的应用:前景与思路[J]. 电力系统自动化,2020,44(11):10 - 24.

[3] 张显,史连军. 中国电力市场未来研究方向及关键技术[J]. 电力系统自动化,2020,44(16):1 - 11.

[4] Singh K, Batten L. Aggregating privatized medical data for secure querying applications[J]. Future Generation Computer Systems,2017,72(9):250 - 263.

[5] Liang K, Liu J K, Wong D S, et al. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing[C]//19th European Symposium on Research in Computer Security,2014:257 - 272.

[6] Jabben F, Hamid Z, Wadood A, et al. Enhanced architecture for privacy preserving data integration in a medical research environment[J]. IEEE Access, 2017, 5: 13308 - 13326.

[7] Zheng Z B, Xie S A, Dai H N, et al. An overview of blockchain technology: Architecture, consensus, and future trends[C]//6th IEEE International Congress on Big Data, 2017:25 - 30.

[8] Yuan R, Xia Y B, Chen H B, et al. ShadowEth: Private smart contract on public blockchain[J]. Journal of Computer Science and Technology,2018,33(3):542 - 556.

[9] 刘明达,陈左宁,拾以娟,等. 区块链在数据安全领域的研究进展[J]. 计算机学报,2021,44(1):1 - 27.

(下转第 52 页)

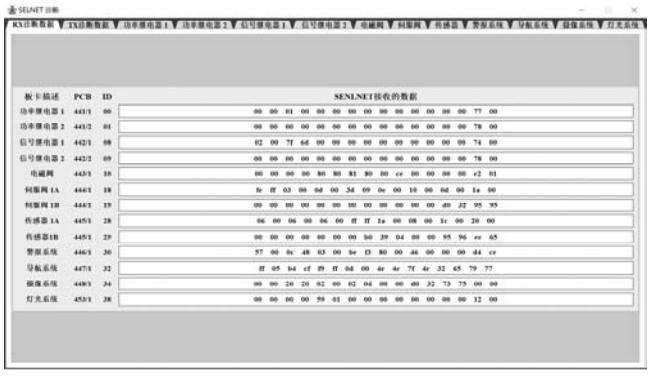

图 13 数据诊断界面

4 结 语

本文基于海龙系列 ROV 平台,利用 Qt 开发框架,设计实现一套水面监控软件。针对软件的实时性要求,详细研究了基于上行数据帧格式定义和数据帧同步算法的软件实时性策略。同时针对传统水面监控软件可视化程度低、人机交互性能差的问题,利用 Qt 自定义控件开发技术设计实现虚拟罗盘、姿态仪表、位置仪表和推进器仪表等 ROV 虚拟仪表。

经测试,该 ROV 水面监控软件可在 Windows 操作系统下稳定运行,各项功能测试正常,具备实时通信、数据处理、状态监视、设备控制、警报显示等功能,能够有效地对水下 ROV 进行在线监控,具备良好的实时性和友好的人机交互性能。值得注意的是,软件的设计开发过程不仅仅局限于潜水器的水面监控软件,对于其他领域相似的上位机,比如无人机地面监控站软件,也具备一定的参考价值。

参 考 文 献

[1] 黄明泉,徐景平,施林炜. ROV 在海洋油气田开发中的应用及展望[J]. 海洋地质前沿,2021,37(2):77 - 84.

[2] 赵羿羽,曾晓光,金伟晨. 海洋科考装备体系构建及发展方向研究[J]. 舰船科学技术,2019,41(19):1 - 6.

[3] 连琏,魏照宇,陶军,等. 无人遥控潜水器发展现状与展望[J]. 海洋工程装备与技术,2018,5(4):223 - 231.

[4] 曹俊,胡震,刘涛,等. 深海潜水器装备体系现状及发展分析[J]. 中国造船,2020,61(1):204 - 218.

[5] 钟宏伟. 国外无人水下航行器装备与技术现状及展望[J]. 水下无人系统学报,2017,25(4):215 - 225.

[6] 杜志元,杨磊,陈云赛,等. 我国与美国潜水器的发展和对比[J]. 海洋开发与管理,2019,36(10):55 - 60.

[7] 沈克,严允,晏红文. 我国深海作业级 ROV 技术现状及发展展望[J]. 控制与信息技术,2020,4(3):1 - 7.

[8] 刘畅. 腹部作业型 ROV 定深控制及水面监控系统设计[D]. 武汉:华中科技大学,2017.

[9] 任峰,张莹,张丽婷,等. "海龙Ⅲ"号 ROV 系统深海试验与应用研究[J]. 海洋技术学报,2019,38(2):30 - 35.

[10] 温贝托·塞万提斯,里克·卡斯曼. 软件架构设计:实用方法及实践[M]. 刘旭斌,陈瑶,邵元英,等译. 北京:机械工业出版社,2017.

[11] 王中华,葛彤,朱继懋. ROV 动力定位系统控制时序与逻辑设计[J]. 海洋工程,2006,4(2):61 - 66.

[12] 陈孟春,冯建文. 基于有限状态机的高速串口通信收发器的 FPGA 设计[J]. 计算机应用与软件,2017,34(12):178 - 183.

[13] 崔彦坤,马萌. CRC 校验算法的设计与实现[J]. 计算机与网络,2019,45(1):62 - 64.

[14] 周奋,王婷. 嵌入式系统中串口通信帧的同步方法[J]. 单片机与嵌入式系统应用,2006(10):73 - 75.

[15] 李帅,范项媛. 基于 Qt 的无人机地面站软件系统的设计[J]. 雷达科学与技术,2017,15(4):410 - 414,420.

(上接第 38 页)

[10] Zhang Y B, Cui M, Zheng L J, et al. Research on electronic medical record access control based on blockchain[J]. International Journal of Distributed Sensor Networks, 2019, 15(11):450 - 456.

[11] 田国华,胡云瀚,陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报,2021,32(5):1495 - 1525.

[12] 张乐君,刘智栋,谢国,等. 基于集成信用度评估智能合约的安全数据共享模型[J]. 自动化学报,2021,47(3):594 - 608.

[13] Daraghmi E Y, Daraghmi Y A, Yuan S M. MedChain: A design of blockchain-based system for medical records access and permissions management[J]. IEEE Access, 2019, 7: 164595 - 164613.

[14] Jakobsson M, Juels A. Proofs of work and bread pudding protocols[J]. Secure Information Networks, 2008, 10(5): 258 - 272.

[15] Kiayias A, Russell A, David B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol[J]. Advances in Crytology, 2017, 45(12):357 - 388.

[16] 王同贺,华昊辰,曹军威. 共识边缘计算及其在能源互联网中的应用[J]. 电力建设,2021,42(2):116 - 125.

[17] Baig M I, Shuib L, Yadegaridehkordi E. State of the art and research challenges[J]. Information Processing & Management, 2019, 56(6):76 - 81.

[18] 芦效峰,付淞兵. 属性基加密和区块链结合的可信数据访问控制方案[J]. 信息网络安全,2021,21(3):7 - 14.

[19] Ren W, Hu J, Zhu T Q, et al. A flexible method to defend against computationally resourceful miners in blockchain proof of work[J]. Information Sciences, 2020, 507:161 - 171.

[20] Kato K, Takefusa A, Nakada H, et al. A study of a scalable distributed stream processing infrastructure using ray and Apache Kafka[C]//IEEE International Conference on Big Data, 2018:5351 - 5353.

[21] 张志威,王国仁,徐建良,等. 区块链的数据管理技术综述[J]. 软件学报,2020,31(9):2903 - 2925.