基于区块链、智能合约和物联网的供应链原型系统

叶小榕[1],邵晴[2],肖蓉[3]

1. 中国科学技术信息研究所,北京 100038
2. 北龙中网(北京)科技有限责任公司,北京 100190
3. 科学技术部信息中心,北京 100862

摘要 为利用区块链、智能合约和物联网等新技术的优势,提高供应链信息化水平,设计开发了基于区块链、智能合约和物联网的供应链原型系统。借助物联网中的二维码、RFID和NFC实现供应链各主体数据的自动化上传;利用区块链和智能合约,完整保存了整个供应链各主体的数据,保证了数据公开透明、可追溯且不可篡改,同时兼顾了隐私数据的加密保护;并针对不同用户提供了不同程度的数据查询功能。通过这些优化和改进,使供应链系统更加自动化、更加安全可信,便于监管溯源。

关键词 区块链;智能合约;物联网

近年来,商贸物流中"互联网+"的应用越来越多,利用互联网技术不断提升着经济创新力和生产力。2017年2月,中国商务部等5部门联合发布《商贸物流发展"十三五"规划》,明确提出"加强商贸物流信息化建设,深入实施'互联网+'高效物流行动,……推广应用物联网、云计算、大数据、人工智能、机器人、无线射频识别等先进技术,促进从上游供应商到下游销售商的全流程信息共享,提高供应链精益化管理水平。"供应链[1-2]是将供应商、制造商、运输商、零售商以及消费者连成一个整体的网链结构。当前越来越多的企业建设供应链系统,实现供应链信息化,以满足供应链中各实体的业务需求,使操作流程和信息系统紧密配合,实现参与主体信息共享;实现各环节流程的无缝链接,促使各实体通过供应链组成一个利益共同体,有了加强责任追究和监管的动力;提高整体的自动化生产效率、提升利润、降低成本。但是当前供应链系统存在如下不足:1)缺乏信任:供应链各个参与主体的各环节的信息分散保存在各主体自身内部,各个主体之间信息不够透明、信息传递速度较慢、易被人为修改,造成各个主体彼此之间缺乏信任;2)监管追溯困难:由于各个主体间未建立信任体系,一旦出现纠纷或质量问题,查找问题原因时效率较低、时间较长,追溯易被中断,举证追责困难,难以监管溯源;3)数据透明和隐私保护难以平衡:一方面,根据法律规定,企业的部分数据需要提供给主管部门,并且向公众和其他主体证明已经提交;另一方面,因为涉及到商业机密,企业又担心数据对外泄露,使得企业在数据透明和隐私保护两者之间难以平衡;4)自动化程度低:供应链的部分环节需要人工录入数据,没有实现完全自动化,成本较高、效率较低且易出错。

针对上述问题,本研究组设计开发了基于区块链、智能合约和物联网的供应链原型系统。系统应用区块链技术以及智能合约技术,将供应商、制造商、运输商、零售商等供应链各主体从原材料供应、产品制造加工、物流运输及最终销售的所有数据,均完整的记录保存,记录的数据公开透明、可追溯且不可更改,并加密了其中的隐私数据,解决了供应链主体之间的信任问题、监管溯源问题和数据隐私保护问题。同时系统采用的二维码[3-4]、无线射频识别RFID[5-6]和近距离无线通信技术NFC等物联网技术[7-11]实现了信息录入的自动化,减少了人工失误,解决了自动化问题。

1 系统架构

本系统包括物联网模块、智能合约模块、区块链模块、证书中心模块和供应链模块。1)物联网模块负责读取产品的二维码、RFID或NFC,获取产品信息,之后将产品信息、供应链系统各主体的相关数据,包括公开数据和使用证书中心提供的公钥加密后的隐私数据,一起通过智能合约模块将数据上传到区块链模块,作为整个供应链系统的数据来源;2)智能合约[12-15]模块负责提供交互接口,包括合约生成和合约执

收稿日期:2017-10-16;修回日期:2017-11-07

作者简介:叶小榕,高级工程师,研究方向为计算机软件、数字图书馆,电子信箱:yeelfine@sina.com

引用格式:叶小榕,邵晴,肖蓉. 基于区块链、智能合约和物联网的供应链原型系统[J]. 科技导报, 2017, 35(23): 62-69; doi: 10.3981/j.issn.1000-7857.2017.23.010

行两个子模块:合约生成子模块负责将各主体共同制定的智能合约代码提交存储到区块链模块中;当有上传、查询等操作时,合约执行子模块负责运行智能合约代码;3)区块链[16-20]模块是整个系统的核心技术部分,实现两部分功能,一是将智能合约模块生成的智能合约代码存储到区块链中,作为智能合约模块调用的基础;二是根据智能合约模块的调用程序,存储和查询区块链模块中的数据[21];4)证书中心[22-23]模块负责生成公钥、私钥和版本号,提供给物联网模块和供应链模块使用;5)供应链模块分为面向主管部门的监管子模块和面向各主体和消费者的公共查询子模块,模块通过调用智能合约模块的合约程序,从区块链模块中查询数据,返回查询结果,其中隐私数据使用证书中心提供的私钥进行解密后查看。架构如图1所示。

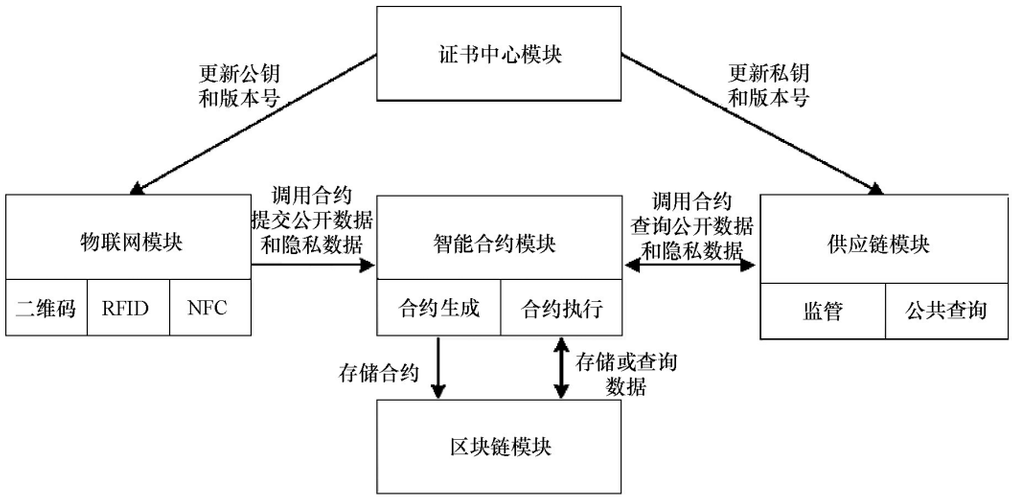

图1 系统整体架构

Fig. 1 Overall system architecture

2 物联网模块

物联网模块实现的功能是:供应商、制造商、运输商、零售商等供应链系统的各主体,根据自己的特性,选择二维码、RFID、NFC中的一种扫描设备扫描产品后,系统将自动获取产品的信息,获取的产品信息包括产品名称、产品型号等;之后将产品信息与供应链各主体提交的相关数据,包括各主体的公司名称、公司地址、原材料来源、制造加工时间、制造加工地点、运输起始时间、到达时间、销售地点、上架时间等公开数据,及通过证书中心模块的公钥加密后的各主体公司法人、产品内部型号、内部生产数据、完税证明等隐私数据,通过智能合约模块提供的接口,上传保存到区块链模块中,作为整个供应链系统的数据源。

物联网模块支持二维码、RFID、NFC等多种信息传感设备,二维码成本低廉,适用于低价产品;RFID成本适中,适用范围广,适用于中间价位的产品;NFC更加安全可靠,适用于核心和高价的产品。系统可以根据产品类型的不同,采用不同的信息读取方式。

2.1 二维码

二维码是使用特定的黑白相间的图形记录数据信息的一种编码方式。当扫描二维码后,系统将扫描得到的图像流,利用Zxing开源库来进行解析,从而得到产品的信息。Zxing库专门用来解析二维码,识别率高,识别速度快。伪代码为:

```
PlanarYUVLuminanceSource source = new PlanarYUVLuminanceSource(
        data, width, height, dstLeft, dstTop, dstWidth, dstHeight); //封装图像data
BinaryBitmap bB=new BinaryBitmap(new HybridBinarizer(source)); //转换为bitmap格式
MultiFormatReader reader = new MultiFormatReader();
String productInfo = reader.decode(bB).getText(); //解析图像得到产品信息
```

2.2 RFID

无线射频识别(RFID:Radio Frequency Identification)是一种非接触式的自动识别技术,扫描设备通过射频信号识别嵌入产品中的RFID芯片,从而获取信息。针对不同的扫描设备,读取RFID的方法有所差异,本系统主要是针对使用Phidgets公司的RFID扫描设备,利用RFIDTagListener()和onTag()等函数读取产品信息。

2.3 NFC

近距离无线通信技术(NFC:Near Field Communication)是一种短距高频的无线电技术,能在短距离内进行非接触式的识别和数据交换。NFC有多种数据格式,本系统主要是针对常见的NDEF格式[24],伪代码为:

```
Parcelable[] par=
    getIntent().getParcelableArrayExtra(NfcAdapter.EXTRA
_NDEF_MESSAGES);
NdefMessage ndefM=(NdefMessage)par[0]; //转换为NDEF
格式
NdefRecord ndefR=ndefM.getRecords()[0];
String productInfo=new String(ndefR.getPayload(),"UTF-
8"); //读取产品信息
```

同时,NFC支持数据的双向交互,扫描者、扫描时间、地点等扫描信息均会被记录到NFC芯片中,确保每次扫描都有据可查。

3 区块链模块

区块链(Blockchain)是一个由多方参与共同维护的持续增长的分布式数据库,核心在于通过分布式网络、时序不可篡改的密码学及分布式共识机制等技术建立起了彼此之间的信任关系,实现了在不可信网络中进行信息传递交换的可信机制[25-26]。在事务处理方面,与传统数据库采用ACID原则不同,区块链采用的是最终一致性原则,从而确保所有的节点数据在经过一段时间的同步后,最终能够达到一致的状态。区块链具有的去中心化、共同维护、数据透明、不可篡改等特性,使其更适用于供应链这种有多个参与主体,且需要建立公开、透明、彼此信任机制的环境。

本系统中的区块链模块是整个系统的核心部分,模块应用区块链技术,实现存储智能合约代码、根据智能合约程序存储数据和查询数据的功能。

3.1 区块链模块的数据结构

区块链是以区块为单位的链状数据块结构,每隔固定的时间就会生成新的区块,区块链中的每一个区块记录了在创建时间内产生的所有数据。应用这一特性,本模块将供应链系统的智能代码和各个主体的数据,永久的存储在区块链中。区块链模块单个区块数据结构如图2所示。

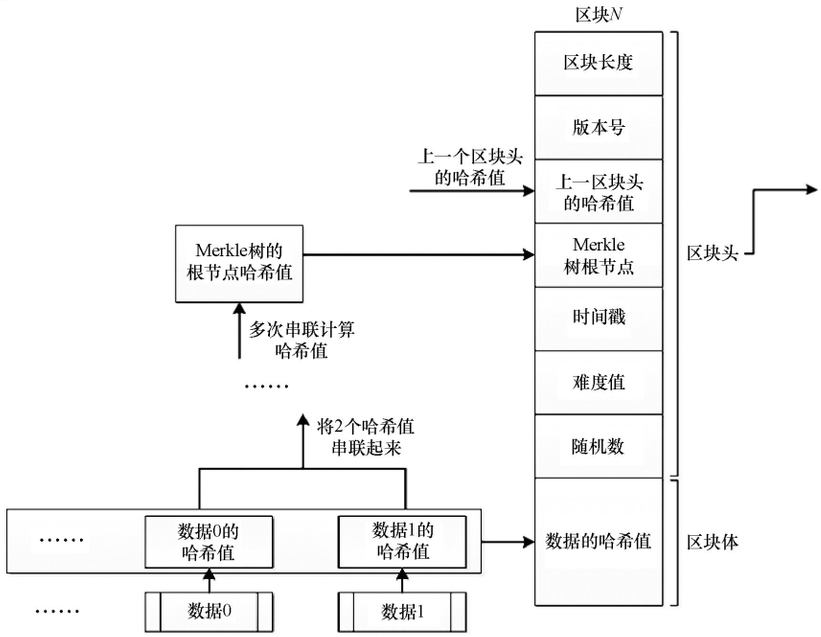

图2 区块链模块单个区块数据结构

Fig. 2 Single block data structure of blockchain module

从图2可见,区块链包括区块头和区块体。区块链使用区块头的哈希值作为区块的唯一标识,存储在下一个区块的区块头"上一区块头的哈希值"字段中,通过记录区块头的哈希值,形成了一条从最新区块追溯到第一个区块的数据链条,保证了供应链系统可以追溯查找各个主体在每一个时间阶段的数据;此外,区块体的"数据的哈希值"字段记录了在此区块的时间阶段内各主体的每条数据的哈希值,保证了供应链系统中各主体的每条数据都可以追溯;通过区块链的这两个部分,使供应链系统的数据可追溯,便于追责和监管;

区块头中的"Merkle树的根节点哈希值"字段,是将区块体中的数据反复迭代计算哈希值,并将最终的哈希值记录到区块头中。区块头的"上一区块头的哈希值"和"Merkle树的根节点哈希值"字段,均利用了哈希算法的单向性和抗冲突性,确保了每一条数据都不可篡改,一旦有篡改还可以迅速定位,提高了供应链系统数据的可靠性和可信度。

3.2 区块链模块的存储业务流程

区块链模块的存储业务过程是将各主体新产生的数据存入新生成的区块中,并保证各主体作为节点的自有服务器上的数据一致。具体流程是:1)供应链系统利用共识机制在区块链的各节点中选出授权节点;2)各主体的节点产生的新

数据,通过点对点传输到授权节点上;3) 授权节点利用共识机制定时生成新区块;4) 授权节点将新数据利用签名算法、哈希算法等进行处理,并加上“上一区块哈希值”、“时间戳”、“难度值”等字段内容,一起填充到新区块中;5) 授权节点利用点对点传输机制将新区块向全网传输;6) 各节点接收到新区块后,利用签名算法、哈希算法等进行验证,验证通过后,将新区块加入到已有区块链的链尾。

区块链模块的存储业务流程利用了共识机制、点对点传输、签名算法、哈希算法等技术,保证了数据的一致性、防篡改性、安全性,保证了各节点的数据对其他节点均是公开透明的,增强了供应链系统各主体之间的信任。区块链模块的存储业务流程如图3所示。

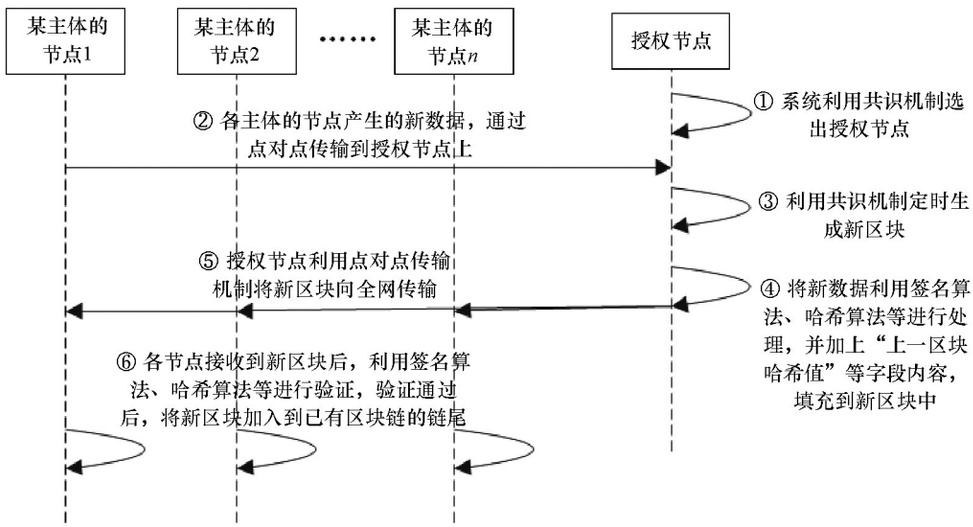

图3 区块链模块存储业务流程

Fig. 3 Blockchain module storage business process

区块链模块的查询业务流程比较简单,各主体发送查询请求,即可利用区块链中记录的数据的哈希值查询得到结果。

4 智能合约模块

智能合约模块负责提供交互接口,分为合约生成和合约执行两个子模块,合约生成子模块负责将智能合约代码提交到区块链模块中进行存储;合约执行子模块负责运行智能合约代码,实现从区块链模块中存储或查询数据的功能。

4.1 技术原理

智能合约是一种用计算机语言取代法律语言去记录条款的合约,可视作一段部署在区块链上可自动运行的程序,其涵盖的范围包括编程语言、编译器、虚拟机、事件、状态机、容错机制等。

本系统中的智能合约模块,应用基于区块链技术的智能合约,合约代码、执行过程、执行结果对供应链各主体均公开透明,且结果不可篡改,提升了系统的可信度,有利于监管和溯源管理。

当前主流的智能合约平台是以太坊(Ethereum)[27]和超记账本(hyperledger fabric),两者对比,以太坊更加的便于部署和二次开发,因此本系统采用了以太坊。以太坊是当前被广泛采用的基于区块链的开源智能合约应用平台;系统采用了专门用于以太坊的Solidity语言,Solidity语言可以实现供应链、记账、购物等各种类型的智能合约;以太坊提供了Json-RPC、JavaScript、geth等多种接口供外部程序调用,本系统采用了Json-RPC接口。

以太坊对上述区块链模块的数据结构做了优化修改,增加了1个Merkle Patricia类型的状态树(state root),在此状态树中最重要的是增加了“合约代码的哈希值”(CODEHASH)字段,用以存储合约代码地址,本系统的物联网模块和供应链模块根据此地址来调用合约程序。

4.2 合约生成子模块

合约生成子模块负责将智能合约代码存储到区块链模块中。智能合约代码由供应链系统的各主体共同制定,格式分为结构体和函数两部分,结构体记录了产品信息和供应链系统各主体的相关数据,包括公开数据和隐私数据;函数提供了对外操作的接口代码,比如存储、查询接口。本系统智能合约的Solidity伪代码为:

```
contract SupplyChain {
    //结构体部分
    struct Product {      //定义数据结构,保存产品信息和供应链系统各主体的相关数据
        uint versionId;   //版本号
        uint productId;   //产品id
```

```
        string supplier;//定义供应商
        string supplierSource;//原材料来源
        ….    //供应商需要提交的相关数据
        string supplierEncrypted;//供应商的加密信息
        string logistics1;//定义将原材料从供应商运送到制造商的运输商
        ….    //运输商需要提交的相关数据
        string logistics1Encrypted;//运输商的加密信息
        string producer;//定义制造商
        ….    //制造商需要提交的相关数据
        string producerEncrypted;//制造商的加密信息
        string logistics2;//定义将产品从制造商运送到零售商的运输商
        ….    //运输商需要提交的相关数据
        string logistics2Encrypted;//运输商的加密信息
        string dealer;//定义零售商
        ….    //零售商需要提交的相关数据
        string dealerEncrypted;//零售商的加密信息
    }
    Product[] products;//通过数组存储以上数据

    //函数部分
    //存储数据,同时进行初始化
    function setSupplier(uint versionId,uint productId,
            string supplier,…,string supplierEncrypted) {
        products[productId].versionId = versionId;
        products[productId].productId = productId;
        ……
        products[productId].supplierEncrypted = supplierEncrypted;
}
    function setLogistics1(){…}  //存储将原材料从供应商运送到制造商的运输商数据
    function setProducer(){…}  //存储制造商数据
    function setLogistics2(){…}  //存储将产品从制造商运送到零售商的运输商数据
    function setDealer(){…}    //存储零售商的数据
  //查询供应链系统中的公开数据
function queryPublicSupplyChain(uint productId) returns (string) {
return assemblePublicInfo(products[productId]);
}
  //查询供应链系统中的所有数据,既有公开数据,也有隐私数据
function queryAllSupplyChain(uint productId) returns (string){
    return assembleAllInfo(products[productId]);
    } }
```

合约代码制定后,本模块负责通过系统的授权节点将智能合约代码部署到区块链模块上,存储在“合约代码哈希值”(CODEHASH)字段上。

4.3 合约执行子模块

合约执行子模块的业务流程是:某个节点的供应链模块或物联网模块通过以太坊的Json-RPC接口来执行合约生成子模块中生成的智能合约;同时,其他各个节点也会执行此智能合约,各节点执行智能合约是相互独立的;当各节点执行完毕后,将彼此验证结果是否一致;验证通过后,系统会将执行的结果返回给供应链模块或者物联网模块,也会将此结果存入到各节点的区块链中(图4)。

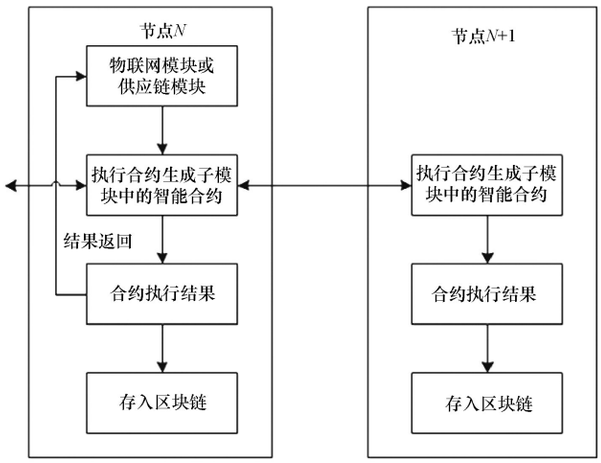

图4 合约执行子模块业务流程

Fig. 4 Contract execution sub module business process

5 证书中心模块

证书中心模块负责生成公钥和私钥,分别提供给物联网模块和供应链模块。为提高系统的安全性,公钥和私钥将定时更新,每次更新时会生成新的密钥版本号,密钥版本号也将同时提供给物联网模块和供应链模块。生成公钥和私钥的伪代码为:

```
KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("RSA"); //初始化RSA库
keyPairGen.initialize(2048);  //密钥长度为2048位
KeyPair keyPair = keyPairGen.generateKeyPair();  //生成公私钥对
RSAPublicKey publicKey = (RSAPublicKey) keyPair.getPublic();  //取得公钥
RSAPrivateKey privateKey = (RSAPrivateKey) keyPair.getPrivate(); //取得私钥
```

隐私数据的加解密流程是:证书中心生成公钥、私钥和密钥版本号后,将公钥和密钥版本号推送到物联网模块,同时将私钥和密钥版本号以离线方式发送给供应链模块中的

监管子模块;物联网模块使用公钥将隐私数据加密,加密后将隐私数据和密钥版本号通过智能合约模块上传;主管部门可以通过供应链模块的监管子模块,使用密钥版本号对应的私钥进行解密,查看隐私数据。流程如图5所示。

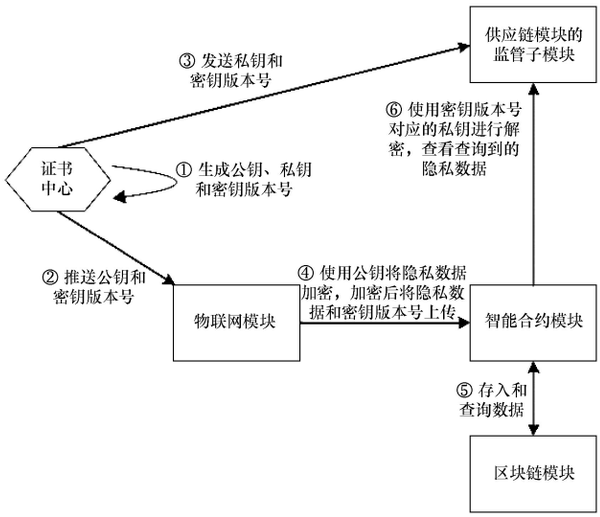

图5 隐私数据加解密流程

Fig. 5 Privacy data encryption and decryption process

6 供应链模块

供应链模块分为面向主管部门的监管子模块、面向各主体和消费者的公共查询子模块等两个子模块。模块通过调用智能合约模块,从区块链模块中查询数据,提供给主管部门、供应商、制造商、运输商、零售商及消费者。

6.1 面向主管部门的监管子模块

面向主管部门的监管子模块通过调用智能合约模块中的queryAllSupplyChain()接口得到公开数据和加密的隐私数据,使用私钥对隐私数据进行解密,使主管部门既能得到供应链系统的公开数据,也能得到各主体的隐私数据,提升了监管力度,实现了数据透明和隐私保护之间的平衡。伪代码为:

```
byte[] key = getPrivKey(versionId); //根据密钥版本号获取私钥字符串
String all = SmartContactUtil.queryAllSupplyChain(productId);//通过智能合约模块的接口查询所有数据
String pub = DataUtil.getPubData(all);//得到公开数据
String privEncrypted = DataUtil.getPrivData(all); //得到加密的隐私数据
KeyFactory factory = KeyFactory.getInstance("RSA"); //初始化RSA类库
PrivateKey privateKey = factory.generatePrivate(
        new PKCS8EncodedKeySpec(key.getByte())); //将私钥字符串转换为私钥类
Cipher cipher = Cipher.getInstance(factory.getAlgorithm()); //初始化加解密类
cipher.init(Cipher.DECRYPT_MODE, privateKey); //设定为解密方式,并传入私钥类
String priv=cipher.doFinal(privEncrypted.getBytes()); //执行解密,得到了隐私数据
```

6.2 面向各主体和消费者的公共查询子模块

供应链系统的各主体和消费者使用公共查询子模块,通过调用智能合约模块中的queryPublicSupplyChain()接口查询公开的数据,比如供应商数据、运输商数据、制造商数据等。由于本系统利用了区块链的特性,各节点的数据完全相同且无法篡改,因此查询结果可信可靠,可用于溯源和举证追责;系统利用了区块链的多节点部署机制,因此不存在单节点故障问题,能满足大量用户的查询请求。此外,即使有用户想要查看其他主体的隐私数据,由于缺少私钥也无法解密,保证了隐私数据的安全性。

7 结论

设计开发了基于区块链、智能合约和物联网的供应链原型系统。此系统已经在测试平台运行,由9台服务器组成,其中3台搭建了物联网模块,分别对应二维码子模块、RFID子模块和NFC子模块;3台搭建了以太坊模块和区块链模块;1台搭建了证书中心模块;2台搭建了供应链模块,分别用于监管子模块和公共查询子模块;服务器的cpu分别为16核到32核的志强处理器,内存为16 G到32 G,操作系统为CentOS7;软件包括go-ethereum1.6.7、Solidity0.4.15。测试运行期间,系统通过扫描二维码、RFID和NFC得到产品信息,系统各主体提交相关数据,包括公司名称、公司地址等公开数据和随机生成的隐私数据;在对隐私数据利用公钥进行加密后,将公开数据和隐私数据一起通过智能合约模块存入区块链模块中;供应链模块的公共查询子模块调用智能合约模块,可以快速查询到公开数据,查询得到的数据与扫描后得到数据完全一致;供应链模块的监管子模块利用私钥可以解密隐私数据,查询得到的隐私数据与提交给系统的完全一致。通过此原型系统,实现了整个供应链数据的上传、存储、查询、加解密等功能,数据公开透明、可追溯且不可更改,解决了各主体之间的信任问题、监管溯源问题、数据隐私保护问题和自动化问题。本系统下一步将结合具体的生产环境,继续完善,比如公共查询时提供多种查询方式,如微信查询和APP查询。

参考文献(References)

[1] 孙旭. 基于NFC技术的生鲜农产品供应链可追溯系统设计及应用研究[D]. 吉林: 吉林大学生物与农业工程学院, 2016.
Sun Xu. Study on the design and application of fresh agricultural products supply chain traceability system based on near field communication(NFC) technology[D]. Jilin: College of Biological and Agricultural Engineering, Jilin University, 2016.

[2] 王雪. 面向整车供应链的发动机追溯系统的设计与实现[D]. 吉林: 吉林大学交通学院, 2013.
Wang Xue. The design and implementation of automobile-supply-chain-oriented engine traceability System[D]. Jilin: School of Transportation, Jilin University, 2013.
[3] 陈扬扬, 宓永迪. 二维码与RFID和NFC技术在图书馆中的应用[J]. 科技情报开发与经济, 2013, 23(5): 46-48.
Chen Yangyang, Mi Yongdi. The application of QR code, RFID and NFC in library[J]. Sci-Tech Information Development & Ec onomy, 2013, 23(5): 46-48.
[4] 文斌, 梁鹏, 罗自强. 基于QR二维码和数据聚合的农业产品追溯服务系统设计[J]. 小型微型计算机系统, 2014, 35(2): 261-265.
Wen Bin, Liang Peng, Luo Ziqiang. Agricultural product traceability based on QR 2-dimension code and data aggregation[J]. Journal of Chinese Computer Systems, 2014, 35(2): 261-265.
[5] 王卉. 基于RFID的蔬菜质量追溯系统的设计与实现[D]. 南京: 南京农业大学信息科学技术学院, 2013.
Wang Hui. System design and implementation for vegetables´ quality trace based on RFID[D]. Nanjing: College of Information Science & Technology, Nanjing Agricultural University, 2016.
[6] 颜波, 石平, 黄广文. 基于RFID和EPC物联网的水产品供应链可追溯平台开发[J]. 农业工程学报, 2013, 29(15): 172-183.
Yan Bo, Shi Ping, Huang Guangwen. Development of traceability system of aquatic foods supply chain based on RFID and EPC Internet of Things[J]. Transactions of the Chinese Society of Agricultural Engineering, 2013, 29(15): 172-183.
[7] 中国信息通信研究院. 物联网白皮书[EB/OL]. (2016-12-28) [2016-12-29]. http://www.caict.ac.cn/kxyj/qwfb/bps/201612/P020161228288013550597.pdf.
China Academy of Information and Communications Technology. Internet of Things White Paper[EB/OL]. (2016-12-28) [2016-12-29]. http://www.caict.ac.cn/kxyj/qwfb/bps/201612/P020161228288013550597.pdf.
[8] 林宇洪, 林敏敏, 林承操, 等. 基于物联网的肉产品质量安全信息的追溯[J]. 华北科技学院学报, 2015, 12(5): 98-102.
Lin Hongyu, Lin Minmin, Lin Chengcao, et al. The quality and safety information traceability about meat food based on IOT[J]. Journal of North China Institute of Science and Technology, 2015, 12(5): 98-102.
[9] 刘凯, 吕璐. 基于物联网技术的产品可追溯系统研究[J]. 湖北理工学院学报, 2015, 31(2): 27-30.
Liu Kai, Lv Lu. Research on product traceability system based on Internet of Things[J]. Journal of Hubei Polytechnic University, 2015, 31(2): 27-30.
[10] 赵震, 张龙昌, 韩汝军. 基于物联网的食品安全追溯研究[J]. 计算机技术与发展, 2015, 25(12): 152-155.
Zhao Zhen, Zhang Longchang, Han Rujun. Research on food safety traceability based on IoT[J]. Computer Technology and Development, 2015, 25(12): 152-155.
[11] 张丽, 杨怀卿, 刘晓亮. 基于物联网技术的化肥质量安全追溯系统[J]. 物流技术, 2015, 34(15): 244-246.
Zhang Li, Yang Huaiqing, Liu Xiaoliang. Study on IOT-based fertilizer quality and safety tracing system[J]. Logistics Technology, 2015, 25(12): 152-155.
[12] 胡凯, 白晓敏, 高灵超, 等. 智能合约的形式化验证方法[J]. 信息安全研究, 2016, 2(12): 1080-1089.
Hu Kai, Bai Xiaomin, Gao Lingchao, et al. Formal verification method of smart contract[J]. Journal of Information Security Research, 2016, 2(12): 1080-1089.
[13] 黄涵禧. 应用智能合约的简易承兑汇票实践[J]. 金融科技时代, 2017(2): 38-44.
Huang Hanxi. Practice of simple acceptance bill with smart contract [J]. Financial Technology Time, 2017(2): 38-44.
[14] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things[J]. IEEE Access, 2016(4): 2292-2303.
[15] 陈志东, 董爱强, 孙赫, 等. 基于众筹业务的私有区块链研究[J]. 信息安全研究, 2017, 3(3): 227-236.
Chen Zhidong, Dong Aiqiang, Sun He,et al. Research on private Blockchain based on crowdfunding[J]. Journal of Information Security Research, 2017, 3(3): 227-236.
[16] 张宁, 王毅, 康重庆, 等. 能源互联网中的区块链技术:研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15): 4011-4022.
Zhang Ning, Wang Yi, Kang Chongqing, et al. Blockchain technique in the energy internet: Preliminary research framework and typical applications[J]. Proceedings of the CSEE, 2016, 36(15): 4011-4022.
[17] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
Yuan Yong, Wang Feiyue. Blockchain: The state of the art and the future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
[18] Watanabe H, Fujimura S, Nakadaira A, et al. Blockchain contract: A complete consensus using blockchain[C]//2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Osaka, Japan: IEEE, 2016: 577-578.
[19] Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform [C]//2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, South Korea: IEEE, 2017: 464-467.
[20] 周立群, 李智华. 区块链在供应链金融的应用[J]. 信息系统工程, 2016(7): 49-51.
Zhou Liqun, Li Zhihua. Application of block chain in supply chain finance[J]. China CIO News, 2016(7): 49-51.
[21]黄洁华, 高灵超, 许玉壮,等. 众筹区块链上的智能合约设计[J]. 信息安全研究, 2017, 3(3): 211-219.
Huang Jiehua, Gao Lingchao, Xu Yuzhuang, et al. The design of smart contracts on crowd funding private Blockchain[J]. Journal of Information Security Research, 2017, 3(3): 211-219.
[22] 朱建明, 付永贵. 基于区块链的供应链动态多中心协同认证模型[J]. 网络与信息安全学报, 2016, 2(1): 27-33.
Zhu Jianming, Fu Yonggui. Supply chain dynamic multi-center coordination authentication model based on block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(1): 27-33.
[23] 朱岩, 甘国华, 邓迪, 等. 区块链关键技术中的安全性研究[J]. 信息安全研究, 2016, 2(12): 1090-1097.
Zhu Yan, Gan Guohua, Deng Di, et al. Security architecture and key technologies of blockchain[J]. Journal of Information Security Research, 2016, 2(12): 1090-1097.
[24] 叶小榕, 邵晴. 结合物联网和室内定位的手机图书馆推荐系统[J]. 科技导报, 2016, 34(23): 127-136.
Ye Xiaorong, Shao Qing. A mobile library recommendation system based on Internet of Things and indoor location[J]. Science & Technology Review, 2016, 34(23): 127-136.
[25] 工业和信息化部信息化和软件服务业司, 中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书(2016)[EB/OL]. (2016-10-18) [2017-03-10]. http://www.cbdforum.cn/index/dd/7.do.

Information and Software Services Department, Ministry of Industry and Information Technology of the People's Republic of China. China blockchain technology and industry development forum. China blockchain technology and application development white paper (2016) [EB/OL]. (2016-10-18) [2017-03-10]. http://www.cbdforum.cn/index/dd/7.do.

[26] 中国信息通信研究院. 全球区块链应用发展十大趋势[EB/OL]. (2017-05-26) [2017-06-29]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/201705/P020170526650562843788.pdf.

China Academy of Information and Communications Technology. Ten trends of application and development of global block chain[EB/OL]. (2017-05-26) [2017-06-29]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/201705/P020170526650562843788.pdf.

[27] Ethereum Foundation. White Paper [EB/OL]. (2015-09-30) [2016-10-29]. https://github.com/ethereum/wiki/wiki/White-Paper.

A supply chain prototype system based on blockchain, smart contract and Internet of Things

YE Xiaorong[1], SHAO Qing[2], XIAO Rong[3]

1. Institute of Scientific and Technical Information of China, Beijing 100038, China
2. KNET Co., Ltd., Beijing 100190, China
3. Information Center, Ministry of Science and Technology of PRC, Beijing 100862, China

Abstract In order to take the advantages of new technologies such as blockchain, smart contract and Internet of Things, and improve the informatization level of supply chain, a supply chain prototype system, which is based on blockchain, smart contract and Internet of Things, is developed. With the help of two-dimensional code, RFID and NFC in the Internet of Things, automatic uploading of the supply chain data is implemented. The system uses blockchain and smart contract to completely save the data of the whole supply chain, thus it ensures the data is transparent, traceable and cannot be tampered with. Meanwhile it takes protection of privacy data into account and provides data query functions at different levels for users. Through these improvements, the supply chain system is more automated, safer and more reliable, and makes traceability easy.

Keywords blockchain; smart contract; internet of things

（责任编辑　陈广仁）