软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于区块链和 IPFS 技术实现粮食供应链隐私信息保护*

范贤丽[1], 范春晓[1], 吴岳辛[1]

[1](北京邮电大学 电子工程学院,北京 100876)

通讯作者: 范贤丽, E-mail: fanxianli@bupt.edu.cn

摘 要: 针对粮食供应链中信息共享时各主体面临的隐私问题,设计与实现了一个基于区块链和IPFS(InterPlanetary File System)技术的隐私保护系统.该系统利用区块链来保存加密隐私信息的哈希值和用户设置的权限访问控制策略,而真正的隐私信息则在加密后存储于 IPFS,在实现隐私信息安全存储的同时保障了用户对自身信息的有效掌控。为了实现灵活的权限管理,系统将隐私信息进行了分类;为了提升访问透明度以及鼓励用户共享隐私信息,系统还设计了一种积分方案.

关键词: 粮食供应链;区块链;隐私保护;IPFS

中图法分类号: TP311

Realization of privacy protection of food supply chain based on blockchain and IPFS

FAN Xian-Li[1], FAN Chun-Xiao[1], WU Yue-Xin[1]

[1](School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Aiming at the privacy issues faced by individuals in the sharing of information in the food supply chain, we designed and implemented a privacy protection system based on blockchain and IPFS (InterPlanetary File System). The system uses the blockchain to store the hash value of the encrypted private information and the permission access control policy set by the user, while the real private information is stored in the IPFS after being encrypted, which ensures the effective control of users to their own information while realizing the storage of privacy information security. In order to achieve flexible privilege management, the system classifies the privacy information; and in order to improve access transparency and encourage users to share their privacy information, the system also designs an integral scheme

Key words: food supply chain; blockchain; privacy protection; IPFS

粮食供应链是由粮食及其产品生产和流通中涉及的农户、粮食收储中心、粮食加工企业、粮食配送中心、零售商及最终消费者连成一体的功能网络结构模式[1].在粮食供应链各主体间进行信息共享能有效解决目前存在的“牛鞭效应”[2]、“双重边际效应”[3]、食品安全问题频发、举证追责困难等多个难题.虽然信息共享有诸多好处,但实际却难以推广,这是因为企业在共享信息时面临着隐私泄露的风险,比如合作伙伴在了解到自己的库存、需求等信息后可能会采取压价、抬价行为使得企业在竞价过程中身处劣势[4].为了解决信息共享时的隐私保护问题,需要技术与制度的双重努力,而当前比较热门的区块链技术,作为一个分布式的共享总账,其具有的去中心化、永久记录、数据透明、方便审计等特点与隐私保护中追求的访问过程透明可控、责任主体明确可查等目标具有良好的契合度[8],通过区块链技术,可以将数据所有权真正地从第三方信用中介转移到用户手中,区块链技术的出现为信息共享过程中的隐私保护提供了解决问题的新思路.

本文针对粮食供应链中信息共享时面临的隐私问题,基于相关领域已有的一些研究成果,结合区块链、智能合约和 IPFS 等关键技术,设计与实现一个隐私保护系统,在解决粮食供应链场景中的隐私保护问题的同时为区块链技术在隐私保护方面的运用提供参考.

本文第 1 节总结分析国内外相关研究成果,提出存在的一些不足,并概述本文做出的改进.第 2 节简要介绍

系统中用到的一些关键技术.第 3 节详细介绍了系统的设计与实现.第 4 节总结全文,并展望未来的研究工作.

1 国内外研究现状

区块链技术特有的属性使其在隐私保护方面具有诸多优势,因而成为各界研究的热点,现阶段,基于区块链技术的隐私保护研究已初见成效. 在通用平台研究方面,Zyskind 等提出了一个去中心化的个人数据管理系统,通过对比特币系统交易的重新定义,使其可以传递存储、查询和数据共享等指令,从而确保用户能够拥有和控制自己的敏感信息[5].在医疗保健领域,Azaria 等实现了一种基于区块链的患者医疗数据的访问和权限管理系统 MedRec,该系统通过将患者分散的医疗记录的哈希和存储位置统一保存在区块链上的方式,有效地解决了系统间互操作性问题和患者对数据所有权的控制问题,并以数据作为挖矿奖励的方式来鼓励医疗相关人员参与网络维护[6];梅颖提出了一个基于区块链和云存储技术的医疗记录安全存储方案,从而实现患者对个人医疗记录所有权的控制和对隐私数据的安全存储[7].针对互联网租车场景中暴露的隐私问题,章宁等通过使用基于区块链的第三方数据库和数据交互审计平台来完成乘客隐私信息的保护[8].对于区块链本身的数据透明性而引发的数据安全隐患问题,零钞 Zcash 中使用了零知识证明技术,这种技术可以实现证明者在不提供原始信息的情况下使验证者能够证明某个论断是正确的[9];Kosba 等提出了一个名为 Hawk 的去中心化智能合约系统,用于实现隐藏智能合约输入的功能[10].

综合分析现有的基于区块链的隐私保护的研究成果与方案,大多采用了区块链与第三方数据库结合的链上链下存储方式来达成隐私保护的目标,这种方式具有以下几个优点:

(1) 真正的隐私数据加密保存在链下数据库中,而区块链上保存数据的哈希值和链下存储位置,可以有效解决区块链的容量扩展问题,从而减少带宽和存储资源的浪费;

(2) 将用户的授权、除权等操作记录在区块链上并在全网达成共识能够提升监管的透明度并在发生纠纷时提供可靠的证据;

(3) 数据加密保存在第三方数据库,解密密钥掌握在有权限的用户手中,这样即使第三方数据库被恶意攻击,也能将用户隐私泄露的风险降到最低;

(4) 链上存哈希值,链下保存的原始数据即使修改 1 比特也会导致其哈希值与链上不一致,从而有效防止篡改,而且链上不保存原始数据也能有效地规避区块链本身数据透明引发的安全隐患.

鉴于链上链下结合的隐私保护方案存在诸多优点，本文也将以这种方式作为总体设计方针，但结合本文研究的粮食供应链场景，现有研究成果中还存在以下几点不足:

(1) 权限控制缺乏灵活性.在粮食供应链中,涉及大量信息的交互,在不同时期,对于不同的共享方,企业往往有不同的共享策略,这就需要提供一种细粒度的权限访问控制方式;

(2) 选择的链下数据库不能与区块链很好地配合.现有的链下数据库一般采用中心化数据库,这就又会导致一些中心化的弊端,比如单点失效,从而削弱区块链发挥的作用,而且为了能顺利找到链下原始数据,链上还需要额外存储链下数据的存储位置;

(3) 用户缺乏信息共享的直接动因.在粮食供应链中,共享隐私信息带来的利益在数据的所有方和共享方之间的分布是不均衡的,通常共享方获得的利益远大于所有方,为了让用户积极主动地共享出真实可靠的信息以保证系统的可持续运行,需要采取合理的激励措施;

(4) 数据访问过程不够透明.数据读取过程不会在区块链上留下任何足迹,为了让用户能够实时掌握自己信息的被访问情况以及为日后举证追责留存更多的信息,记录数据读取行为也是有必要的.在现有的研究成果中,对于这一问题还都缺乏明确的解决方案.

基于上述问题，本文提出以下改进:

(1) 本文将粮食供应链中的隐私信息划分为库存信息、成本信息、需求信息和质量信息 4 类,用户在进行权限控制时可以将四类信息进行自由组合从而实现灵活的访问控制;

(2) 链下存储系统采用 IPFS,IPFS 作为一个点对点分布式超媒体分发协议,与区块链具有很好的兼容性,

同时,IPFS 基于哈希寻址,区块链上只需保存数据的哈希就能从 IPFS 中成功检索出对应信息[14];

(3) 设计一种积分方案,在获取数据之后,从共享方账户自动转移一定数量积分给数据所有者,这样不但可以解决共享激励问题,还将数据读取行为与积分转移过程绑定,巧妙实现了数据访问透明性.

2 系统背景技术

2.1 区块链

区块链源自 2008 年化名为“中本聪”的学者提出的比特币应用的底层技术[11],是一个由多方共同维护的、去中心化的分布式数据库。核心在于通过 P2P 网络协议、共识算法、非对称加密、哈希散列等关键技术解决数据传递与交换过程中的信任问题.

区块链按照时间顺序以区块为单位组织为链状数据结构,区块链中的每个数据区块包含区块头和区块体两部分。区块头包含前一区块哈希值、Merkle 根、时间戳、难度目标、随机数等,区块体则封装了自上一区块创建以来的多笔交易记录,这些记录通过 Merkle 树的哈希过程生成对应的 Merkle 根并写入区块头,从而使区块体的变动能在区块头中反映出来[12-13].区块链的结构如图 1 所示.

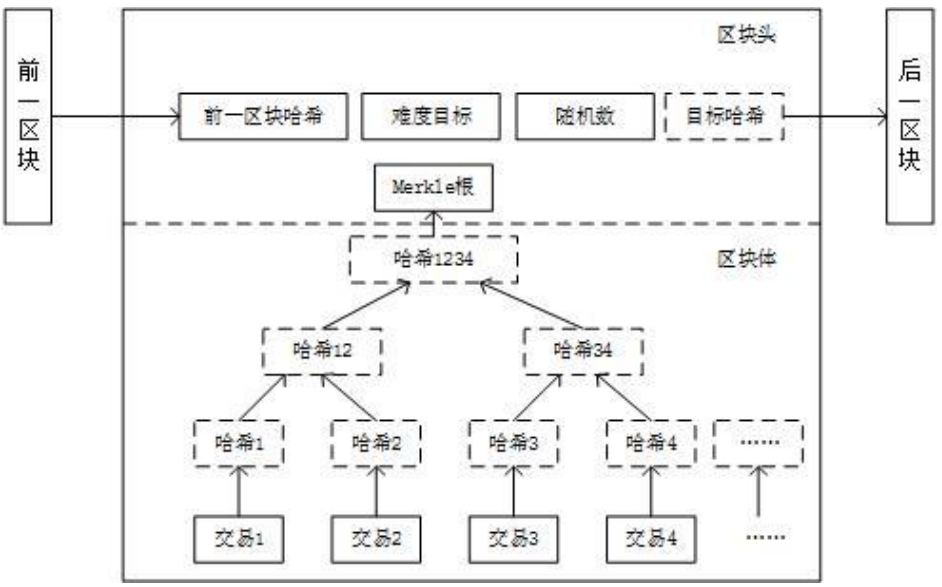

Fig.1 structure of blockchain

图 1 区块链结构图

2.2 智能合约

智能合约是运行在区块链上的一段可自动触发的计算机程序,其赋予了区块链可编程特性,从而为区块链的推广运用奠定了基础.依照业务逻辑编写完成智能合约之后,将其部署到区块链网络节点上,该智能合约就可以继承区块链的分布式记录、不可篡改和伪造、强制执行等特性.

智能合约根据实际应用场景定义交易规则,外部应用通过调用智能合约,并按照合约定义的方式执行链上交易和访问区块链上保存的数据.智能合约与外部应用之间的关系可类比传统数据库与存储过程之间的关系,存储过程用于访问关系数据库中的数据,智能合约则为外部应用访问区块和状态数据搭建了桥梁[12-13].

2.3 IPFS

IPFS 是一个点对点分布式超媒体分发协议,IPFS 的设计中集成了 DHT、BitTorrent、自认证文件系统 SFS

和 Git 的优点,能够实现文件的永久和去中心化保存.同时也被认为是最有可能取代 HTTP 的新一代互联网协议.不同于 HTTP 的基于位置寻址方式,IPFS 基于内容寻址,将信息保存到 IPFS 节点中,IPFS 系统将会返回基于该信息计算得出的唯一哈希值.哈希值与信息内容一一对应,即使只对信息做轻微修改,也会得到完全不同的哈希值.当 IPFS 被请求一个文件哈希时,它会使用一个分布式哈希表找到文件所在的节点,取回文件并验证文件数据.

IPFS 是通用目的的基础架构,基本没有存储限制.大文件会被切分成小分块,下载时可从多个服务器同时获取.IPFS 的网络是不固定的、细粒度的、分布式的网络.可以很好的适应内容分发网络的要求[14].

3 系统设计

本文设计的基于区块链和 IPFS 的隐私保护系统,主要实现粮食供应链中隐私信息的安全存储和授权访问.粮食供应链中的隐私信息是指除去满足消费者知情权的基本信息后可能会暴露企业商业机密的、对企业利益有较大影响的信息,比如:企业的生产成本、生产进度安排、库存水平、销售数据等.对于不同的隐私信息,企业通常有不同的共享策略,即允许哪个企业在何时共享何种信息,为满足这一需求,本系统将隐私信息分为库存、成本、需求和质量信息 4 类,以便企业可以灵活地进行组合.本系统的核心功能包括:用户注册、密钥生成、隐私信息上传、权限管控、隐私信息访问,同时为了鼓励隐私信息共享以及达成数据访问透明的目标,本系统还设计了积分管理功能,在企业提供的信息被有权限的他方成功访问后,企业会收到相应的积分奖励.

为防止区块链账本增长过快,本系统仅将隐私信息的哈希值记录到区块链中,而原始信息则在加密后保存到链外数据库,为了与区块链特性兼容,采用 IPFS 作为链外数据库,此外,区块链还记录权限信息和积分信息.

3.1 系统整体架构

本系统分为 WebApp、IPFS 和区块链 3 个部分.WebApp 支持 B/S 架构模式,用户通过浏览器使用系统功能,WebApp 会根据用户操作进行相应的处理,选择要调用的智能合约,以及协调 IPFS 和区块链的工作.IPFS 负责存储加密后的隐私信息,并返回哈希路由.区块链负责存储智能合约代码和执行智能合约,并将执行结果打包成区块,经过共识后写入区块链账本.系统整体架构如图 2 所示.

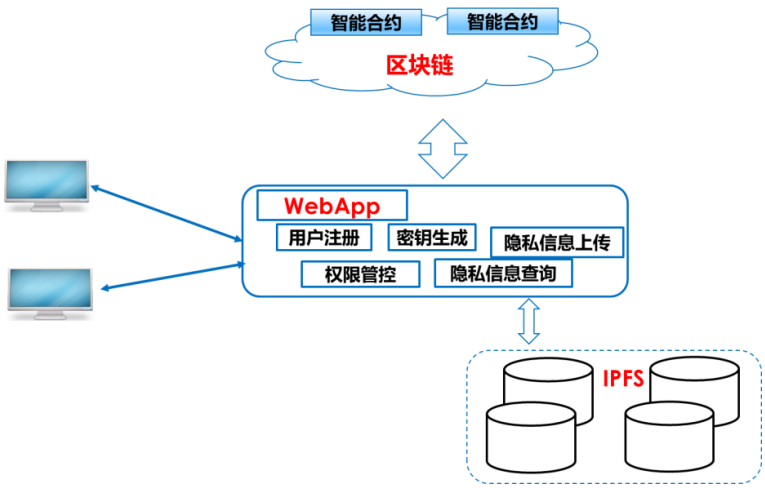

Fig.2 structure of system

图 2 系统架构

3.2 智能合约设计

本系统中的智能合约本质上是根据用户注册、隐私信息的上传和访问、权限的授予和撤销、积分的分配

和转移这几个过程的业务规则进行编码,部署在区块链网络中,并由所有节点达成共识和运行的程序,WebApp 通过调用相应的智能合约将数据保存到区块链上或从区块链中检索出所需数据.针对不同功能,本系统设计了对应的智能合约,智能合约接口见表 1.

Table 1 interface of smart contract

表 1 智能合约接口

合约名称	接口定义	接口描述
注册合约 RegisterC	userRegister	用户注册
数据上传合约 StoreDataC	saveInfo	将隐私信息哈希值写入区块链
	getInfo	受控查询隐私信息哈希值
权限控制合约 ConfigPermissionC	setPermission	授予访问权限
	getPermission	查询访问权限
	cancelPermission	撤销访问权限
积分合约 IntegrationC	initIntegration	积分的初始化分配
	transferIntegration	积分转移

4 系统实现

4.1 用户注册

用户通过 WebApp 输入 ID、密码和其他基本信息(如企业名称、企业地址)后发起注册请求;WebApp 验证提交的信息后根据输入的密码生成用户的公私钥对和区块链地址,并向区块链节点请求调用 RegisterC.userRegister 完成用户注册请求,注册成功后会调用 IntegrationC.initIntegration 给用户的区块链地址存入 1000 积分作为其初始的积分数.

4.2 密钥生成

对应于 4 类隐私信息,每个用户需要 4 个对称加密密钥来加密相应的隐私信息以防未授权用户的非法访问,为达到较高的安全级别并兼顾加解密效率,本系统采用 AES-128 对称加密算法.在生成加密密钥时,用户需要输入密码以作为日后使用密钥的凭据,WebApp 会根据用户输入密码以及系统当前时间生成相应的密钥,密钥保存在用户本地计算机中.

4.3 隐私信息上传

隐私信息上传的步骤为:(1) 用户通过 WebApp 提供的功能界面录入信息后发起保存请求并用自己私钥对请求进行签名;. (2)WebApp 判断提交的信息类型提示用户输入密码来获取对应密钥以加密信息;(3)WebApp 向 IPFS 节点请求将加密信息存入 IPFS 中并获取 IPFS 返回的哈希;(4)WebApp 向区块链节点请求调用 StoreDataC.saveInfo,并将哈希值和信息类型作为参数传入,区块链节点收到请求先验证用户的签名,验证通过后执行智能合约将哈希值、信息类型与用户 ID 绑定并广播该请求给其他节点执行相同的操作,在节点间达成共识后将智能合约执行结果写入区块链账本,然后提示用户信息保存成功.隐私信息上传流程如图 3 所示.

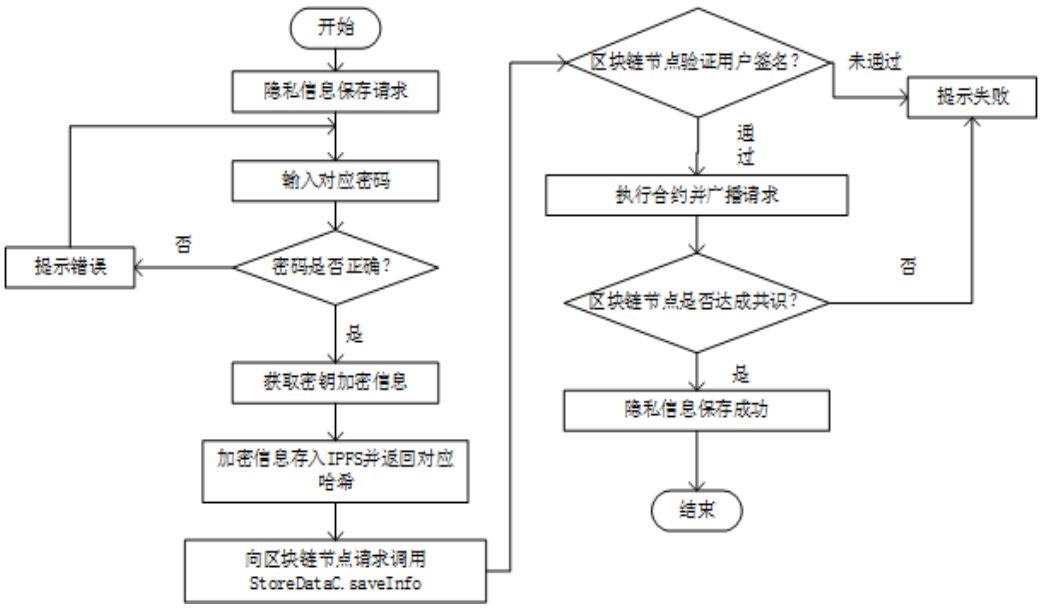

Fig.3 flow chart of uploading private information

图 3 隐私信息上传流程图

4.4 权限管控

(1) 授权.

用户通过授权操作来允许其他用户访问自己的隐私信息,由于本系统将隐私信息分为 4 类,所以在授权时可以通过对 4 种类别的自由组合来限定信息共享范围.授权的步骤为:(1)用户 A 通过 WebApp 选择共享用户 B 和授权信息类别后 (如库存信息,需求信息)发起授权请求并对请求进行签名;(2)WebApp 向区块链节点请求调用 ConfigPermissionC.setPermission 并将用户 B 的 ID 和信息类别作为参数传入;(3)区块链节点先验证用户 A 的签名,再执行智能合约并广播该请求给其他区块链节点,达成共识后将授权信息记入区块链账本;(4)WebApp 使用用户 B 的公钥将对应的密钥加密后发送给用户 B,用户 B 通过自己的私钥解密出密钥.

(2) 除权.

用户通过除权操作来撤销曾授予其他用户的访问权限.除权的步骤为:(1)用户 A 通过 WebApp 选择要除权的用户 B 和除权信息类别后发起除权请求并对请求进行签名;(2)WebApp 向区块链节点请求调用 ConfigPermissionC.cancelPermission 并将用户 B 的 ID 和信息类别作为参数传入;(3)区块链节点先验证用户 A 的签名,再执行智能合约并广播该请求给其他区块链节点,达成共识后将除权信息记入区块链账本;(4)WebApp 提示用户输入新密码重新生成对应的密钥,并将新密钥发送给仍具有权限的各方.

4.5 隐私信息访问

当用户需要访问其他用户的隐私信息时,可通过 WebApp 提供的功能界面发起查询请求,查询成功后会触发积分转移功能以对信息所有者进行补偿.查询的步骤为:(1)用户 A 在 WebApp 页面选择隐私信息的所有者用户 B 后输入组合查询条件发起查询请求,如查询 B 当前的小麦库存;(2)WebApp 分析查询请求,提取信息类别,然后向区块链节点请求调用 StoreDataC.getInfo 并将 A 和 B 的 ID、查询条件及查询类别作为参数传入;(3)区块链节点执行智能合约 StoreDataC,StoreDataC 将调用 ConfigPermissionC.getPermission 并传入 A 和 B 的 ID 参数,ConfigPermissionC 执行后向 StoreDataC 返回 A 和 B 之间的授权信息,StoreDataC 对比授权信息和查询类别判断用户是否具备权限,对于有权限的用户从区块链账本中检索出查询信息对应的所有哈希记录;(4)WebApp

根据哈希记录向 IPFS 节点发起请求查询出对应的加密隐私信息;(5)WebApp 提示用户输入密钥解密信息,信息解密成功 WebApp 对信息进行处理后展示给用户 A;(6)WebApp 根据访问的信息量折算成积分数量后向区块链节点请求调用 IntegrationC.transferIntegration 并将 A、B 的 ID 和积分数作为参数传入,区块链节点对 IntegrationC 的执行结果达成共识后自动将积分从 A 的区块链地址转移给 B 的区块链地址并给用户发送通知.隐私信息访问流程如图 4 所示.

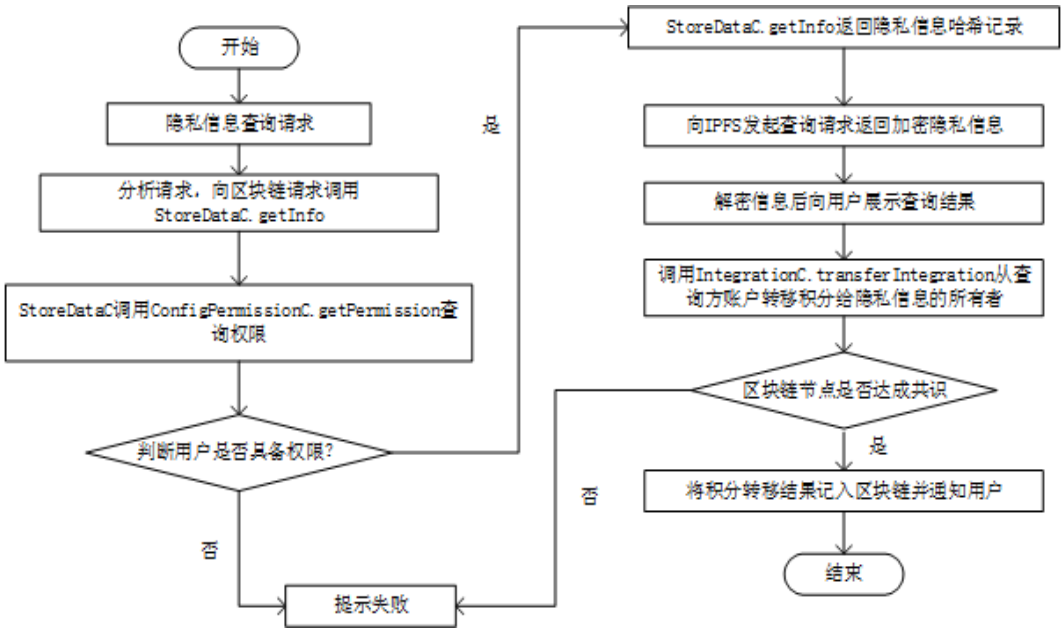

Fig.4 flow chart of accessing private information

图 4 隐私信息访问流程图

5 结语

隐私保护问题是粮食供应链主体在进行信息共享时很关注的一个问题,如果一个信息共享系统存在隐私披露的风险,那么会很难得到用户的青睐.区块链技术的特性使其在隐私保护方面具有传统解决方案不可比拟的优势,所以本文针对粮食供应链场景,设计与实现了一个基于区块链的隐私保护系统,该系统将用户隐私信息分为 4 类以便提供灵活的权限控制和细粒度访问控制.在系统中,粮食供应链各主体对自己的数据具有绝对的所有权,能够决定自己的数据如何共享;同时本系统能够提供较高的数据访问透明度,用户能够看到自己的数据何时被谁访问;此外系统还实现了细粒度的访问控制,使用户对权限的控制更加灵活和个性化.

本文结合粮食供应链场景,创新性地将区块链技术和 IPFS 技术运用于解决供应链主体的隐私保护问题,从初始权限配置、隐私信息上传、隐私信息的授权访问和撤销权限几个方面全面描述了系统的实现细节.但该系统的应用目前还处在实验阶段,是否能进行推广应用还需要进一步的测试与验证,而且未来可尝试将该系统推广到其他应用场景

References:

[1] Yang CH. Research of Grain Supply Chain's Optimization and Management Based on the Perspective of Grain Security. Reformation & Strategy, 2013,29(12):47–51 (in Chinese with English abstract)

[2] Da QL, Zhang Q, Shen HC. Research on the Bullwhip Effect in Supply Chain. Journal of Management Sciences in China, 2003(03):86–93

[3] Ma LS, Ma Y. Research on Coordination Strategy of "Double Marginal Effect" in Decentralized Supply Chain. Modern Business Trade Industry, 2016,37(11):34−35

[4] Chen QH. Preserving Cost and Demand Information in Two—Echelon Supply Chain Decisions. Southeast University, 2009. DOI:10.7666/d.y1579067 (in Chinese with English abstract)

[5] Zyskind G, Nathan O, Alex. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]// IEEE Security and Privacy Workshops. IEEE Computer Society, 2015:180-184

[6] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using Blockchain for Medical Data Access and Permission Management[C]// International Conference on Open and Big Data. IEEE, 2016:25-30

[7] Mei Y. The Utilizing Blockchain-Based Method of the Secure Storage of Medical Records. Journal of Jiangxi Normal University(Natural Science), 2017,41(5):481−487 (in Chinese with English abstract)

[8] Zhang N, Zhong S. Mechanism of personal privacy protection based on blockchain. Journal of Computer Applications, 2017,37(10):2787−2793 (in Chinese with English abstract)

[9] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// Security and Privacy. IEEE, 2014:459-474

[10] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]// Security and Privacy. IEEE, 2016:839-858

[11] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008)

[12] Yuan Y, Wang FY. Blockchain: The State of the Art and Future Trends. Acta Automatica Sinica, 2016,42(04):481−494 (in Chinese with English abstract)

[13] Shao QF, Jin CQ, Zhang Z, Qian WN, Zhou AY. Blockchain: Architecture and Research Progress. Chinese Journal of Computers, 2018,41(05):969−988 (in Chinese with English abstract)

[14] Yin L, Wang HW. Research on Distributed Data Sharing System Based on IPFS. Internet of Things Technologies, 2016,6(6):60−62