江苏农业学报(*Jiangsu J.of Agr.Sci.*),2023,39(2):434-443
http://jsnyxb.jaas.ac.cn

伍德伦,饶　元. 基于身份验证的果蔬区块链信息存储溯源模型设计[J].江苏农业学报,2023,39(2):434-443.
doi:10.3969/j.issn.1000-4440.2023.02.016

基于身份验证的果蔬区块链信息存储溯源模型设计

伍德伦[1,2]，　饶　元[1,2]
(1.安徽农业大学信息与计算机学院,安徽 合肥 230036；2.智慧农业技术与装备安徽省重点实验室,安徽 合肥 230036)

摘要： 现有的果蔬溯源系统中,物联网数据采集设备身份验证机制不完善,果蔬数据传输效率不高,且无法保证数据在存储于区块链前未被篡改。构建了基于身份验证的果蔬区块链信息存储溯源模型,对模型进行分析后,首先提出果蔬供应链数据流动模型,通过物联网设备将采集的数据存储于星际文件系统(Interplanetary file system,IPFS),环节数据存储完成后,系统将IPFS返回的哈希值存入区块链网络,提高了数据的安全性;其次设计了果蔬供应链数据传输流程,提高了果蔬数据传输效率;最后利用Blake2改进型Ed25519算法实现了物联网设备的身份验证机制,提高了系统的安全性。在此基础上设计了基于身份验证的果蔬区块链信息存储溯源系统,并在某果蔬企业进行了实际应用,进行相关测试后发现,本系统的全供应链数据存储平均耗时4.738 s,数据查询平均耗时0.452 s。测试结果表明,此系统可在保障数据安全的前提下,提高用户的溯源速度,可为果蔬溯源系统的设计与研发提供参考。

关键词： 区块链；果蔬；溯源；存储优化；身份验证
中图分类号： TP309.2;TS207.7　　**文献标识码：** A　　**文章编号：** 1000-4440(2023)02-0434-10

Design of storage and traceability model of fruits and vegetables blockchain information based on authentication

WU De-lun[1,2]，　RAO Yuan[1,2]
(1.*School of Information and Computer*, *Anhui Agricultural University*, *Hefei* 230036, *China*; 2.*Anhui Key Laboratory of Smart Agricultural Technology and Equipment*, *Hefei* 230036, *China*)

Abstract: In the existing traceability system for fruits and vegetables, the authentication mechanism of data collection equipment of the internet of things (IoT) is not perfect, the transmission efficiency of fruits and vegetables data is not high, and there is no guarantee that the data are not tampered before being stored in the blockchain. A storage and traceability model of blockchain information of fruits and vegetables based on authentication was constructed. Firstly, a data flow model of fruits and vegetables supply chain was proposed after the model was analyzed. The collected data were stored in interplanetary file system (IPFS) through the IoT devices in each link. After the link data were stored, the system stored the Hash value returned from IPFS into the blockchain network, which improved the security of the data. Secondly, the data transmission process of fruits and vegetables supply chain was designed, and the efficiency of data transmission was improved. Finally, the authentication mechanism of IoT devices was implemented by using Blake2 improved Ed25519 algorithm, which improved the security of the system. On the above basis, a blockchain information storage and traceability system for fruits and vegetables based on authentication was designed and applied in a fruits and vegetables enterprise. After relevant tests, it was found that the system took an average of 4.738 s for the whole supply chain data storage and 0.452 s for the data query. The test results revealed that, the system designed in the study can improve the traceability speed of users on the premise of ensuring data

收稿日期:2022-04-14
基金项目:安徽省重点研究和开发计划项目(201904a06020056);安徽省自然科学基金项目(2008085MF203)
作者简介:伍德伦(2000-),男,安徽池州人,本科,主要从事农业物联网、区块链技术研究。(E-mail)3195949821@qq.com
通讯作者:饶　元,(E-mail)raoyuan@ahau.edu.cn

security, and can provide reference for the design and development of fruits and vegetables traceability system.

Key words: blockchain; fruits and vegetables; traceability; storage optimization; authentication

果蔬含有维生素等多种人体所需成分,具有较高的营养价值,消费者对果蔬的质量、安全等需求也在不断提升[1]。但近几年果蔬质量安全问题频发,化学药品滥用、微生物污染等严重影响消费者对果蔬质量的信任[2],迫切需要建立果蔬追溯体系,使消费者能够快速追溯果蔬的来源,搭建消费者与果蔬之间的信任桥梁[3]。现有的溯源系统大多采用本地数据库存储溯源信息,无法保证信息的安全性和可靠性。区块链的去中心化存储、数据不可篡改等特性可以很好地适用于溯源系统设计。近些年,学者们从不同角度探索区块链技术在溯源系统中的应用。杨信廷等[4]、弋伟国等[5]采用"数据库+区块链"的链上链下双模存储机制保证了数据的真实性,提高了用户的溯源速度。张新等[6]、于华竟等[7]利用智能合约实现了数据的链前监管与节点的链上管控。许继平等[8]、于合龙等[9]采用数据加密算法保证了链上数据的安全性。然而,目前果蔬区块链可信溯源系统还存在诸多不足[10-11]。在果蔬产品生产过程中,监控设备、移动端设备、温湿度传感器等设备采集到果蔬关键数据的时间点不同,考虑到数据区块链存储成本等因素,现有的追溯模型往往采用全部设备采集数据整体存储于区块链的方式,如何保证数据全部上链前已采集数据真实性的问题需要解决;同时,果蔬供应链数据具有多源、异构、海量的特点,负责数据采集的物联网设备较多,如何提高系统安全性也需要进一步探讨。

针对以上果蔬供应链溯源系统面临的问题,本研究提出果蔬供应链数据流动模型,采用星际文件系统(Interplanetary file system,IPFS)存储各物联网设备提供的关键数据,区块链网络存储 IPFS 根据关键数据生成哈希值的设计,保证了数据的真实性。本研究通过设计果蔬供应链数据传输流程,以期提高数据处理与传输效率,利用 Blake2 改进型 Ed25519 算法以期实现物联网设备的身份验证。

1 材料与方法

1.1 技术介绍

1.1.1 区块链 区块链作为一种链式数据结构,由不断增长的区块利用哈希指针前后链接而成,区块链中的数据只能追加,不可删除或篡改[12]。区块链通过分布式节点验证和共识机制,解决了拜占庭将军问题[13],无需信任单个节点就可以构建去中心化可信任系统[14]。本研究以区块链为基础,构建基于身份验证的果蔬区块链信息存储溯源模型,并基于 Hyperledger Fabric 设计了基于身份验证的果蔬区块链信息存储溯源系统。

1.1.2 IPFS 星际文件系统 IPFS 为上传到系统的每个文件提供唯一的哈希地址,使其能够被内容寻址。在区块链架构中部署 IPFS 系统进行存储,可以消除对全节点的依赖,同时保留网络中的可追溯性[15]。任何类型的文件都可以上传到 IPFS 存储,使系统可部署用途广泛的应用程序[16]。基于区块链的追溯模型效率往往受到区块链存储容量难以扩展的限制,此问题可通过区块链集成 IPFS 并采用 IPFS 链下辅助存储的方式进行解决[17]。IPFS 采用默克尔有向无环图(Merkle directed acyclic graph,Merkle DAG)进行数据存储。它是一种使用散列在 DAG 中定位数据的数据结构。使用这种结构,系统中的所有内容都变得防篡改,将使用根据存入数据生成的哈希值进行唯一标记。

1.1.3 Blake2 算法与 Ed25519 算法 Blake2 算法可以产生任意长度的消息摘要[18],它的处理速度要优于 MD5、SHA-1、SHA-2 和 SHA-3 等算法,并且更加安全[19]。Ed25519 是基于 Edwards 曲线的数字签名算法(Edward curve digital signature algorithm,EdDSA),结合 SHA-512/256 哈希算法,采用扭曲爱德华曲线,如公式(1)所示,它比现有的数字签名方案快,且不损失安全性。EdDSA 算法包括公钥生成、签名、验签 3 个功能[20],此算法需要随机数发生器产生私钥,但随机数的产生可能存在安全隐患。针对这个问题,笔者采用 Blake2 改进型 Ed25519 算法,具体实现过程见 1.2.4 节。

$$-x^2+y^2=1-\frac{121\ 665}{121\ 666}x^2y^2 \tag{1}$$

1.2 基于身份验证的果蔬区块链信息存储溯源模型设计

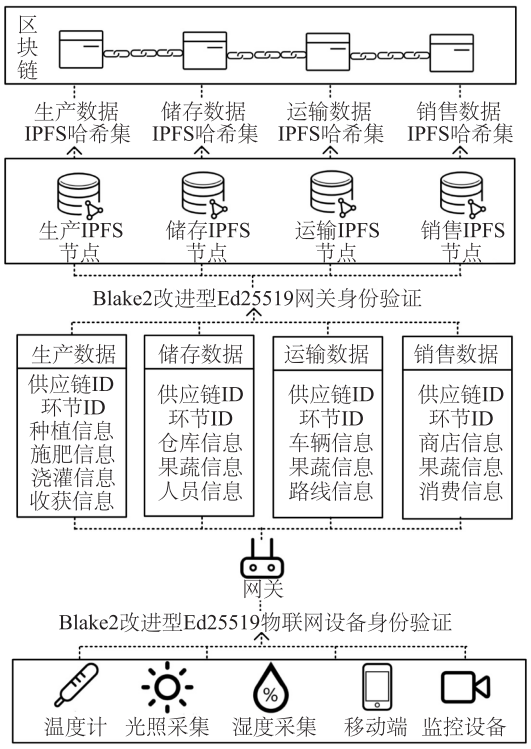
1.2.1 总体框架设计 如图 1 所示,本研究采用区块链技术、IPFS 技术,结合密码学原理,设计了基于

身份验证的果蔬区块链信息存储溯源模型，其原理是通过物联网设备实时采集生产、储存、运输、销售等环节数据，将数据通过区块链、IPFS 等技术进行数据整合与展示。

具体而言，供应链上生产企业、储存企业、运输企业、销售企业决定组建区块链网络后，在企业服务器上设置 IPFS 网络节点，与其他企业 IPFS 节点组建 IPFS 集群，以实现物联网采集数据及时存储并与企业间数据共享；在服务器上设置区块链网络节点与其他企业的区块链网络节点组成区块链网络，利用节点向消费者提供数据查询接口，满足消费者溯源需求。在果蔬产品生产过程中，企业通过在其生产基地或仓库等设置的温湿度采集器、监控等物联网设备采集关键溯源数据，数据采集完成后，将数据转发给网关设备，网关利用 Blake2 改进型 Ed25519 算法对物联网设备进行身份验证，验证通过后，网关对数据进行组织与处理，向 IPFS 服务器发起数据存储请求。同样的，IPFS 服务器利用算法对该网关进行身份验证，验证通过后，网关调用系统提供的 IPFS 数据存储接口将数据存储于 IPFS 中。在该企业溯源数据采集完成后，企业收集网关存入的 IPFS 数据后，IPFS 根据存入数据返回的哈希值，将哈希值整合后存入区块链网络，保证数据的真实性。

基于身份验证的果蔬区块链信息存储溯源模型通过物联网设备采集数据，将采集数据存入 IPFS 系统后，IPFS 根据数据生成的哈希值存入区块链，提高了区块链的存储空间利用率与溯源数据真实性；各企业既可直接在 IPFS 集群中进行企业间数据共享，又可利用区块链网络进行供应链数据查询，提高了企业间数据共享效率。利用 Blake2 改进型 Ed25519 加密算法实现了物联网设备的身份验证，提高了系统的安全性。

1.2.2 *果蔬供应链数据流动模型设计* 在基于身份验证的果蔬区块链信息存储溯源模型基础上，设计了果蔬供应链数据流动模型（图 2），将前者的数据储存、数据查询等操作进行了进一步的实践。当系统初始化时，系统利用 Blake2 改进型 Ed25519 算法为具有数据上传权限的物联网设备生成并发放公钥，同时将公钥进行 MD5 加密后保存于区块链。当供应链上游和下游企业物联网设备采集到数据时，利用其公钥进行身份验证，验证成功后，由网关将物联网设备采集的数据存入 IPFS，在该企业数据存储



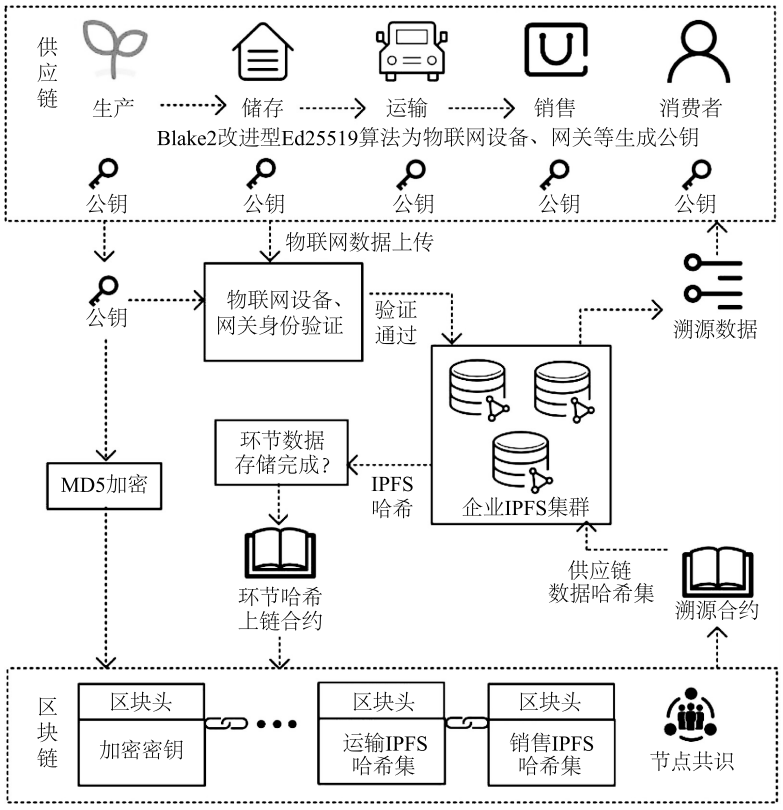
IPFS：星际文件系统；ID：身份识别号。

图 1 基于身份验证的果蔬区块链信息存储溯源模型

Fig.1 Storage and traceability model of fruits and vegetables blockchain information based on authentication

完成后，系统收集各网关上传的溯源数据的 IPFS 哈希值，利用其区块链网络节点调用环节哈希上链合约进行哈希存储。其中环节哈希上链合约内部保存了各环节 IPFS 哈希格式，例如哈希值数量、环节身份识别号（ID）等。当节点上传数据的格式错误时将无法完成哈希值上链。在果蔬供应链数据存储完成后，区块链网络中各节点达成共识完成账本同步。并利用溯源合约提供消费者溯源哈希查询接口。消费者利用移动设备扫码调用接口后，获得供应链数据的哈希集合，利用哈希集合在 IPFS 中获取溯源数据。

在果蔬供应链数据流动模型中，利用环节哈希上链合约检查各环节存储的 IPFS 哈希特征，实现了系统数据哈希存储的智能化。通过溯源合约及区块链节点为消费者提供了溯源信息查询接口，满足了用户溯源的需求。采用公钥加密后链上存储的设计，保证了密钥的安全性，避免了密钥的二次生成、发放带来的系统负担，提升了系统运行效率。



IPFS:星际文件系统。

图 2 果蔬供应链数据流动模型

Fig.2 Data flow model of fruits and vegetables supply chain

1.2.3 *果蔬供应链数据传输流程设计* 采集果蔬生产环节数据的物联网设备往往被安装于野外环境,网络状况差,自身数据处理能力差,无法调用IPFS 数据存储接口进行数据的直接存储,本研究设计了由设备身份验证、数据接收与处理、IPFS 数据存储模块组成的果蔬供应链数据传输流程,三者配合以达到采集数据存储于IPFS 的目的。其中设备身份验证模块由网关利用 Blake2 改进型 Ed25519 算法对物联网设备进行身份验证。数据接收与处理模块用于接收物联网节点上传的数据并对其进行处理,IPFS 数据存储模块用于 IPFS 服务器对网关进行身份验证,以实现物联网采集数据存储于 IPFS。

具体流程如图 3 所示,具体步骤如下:

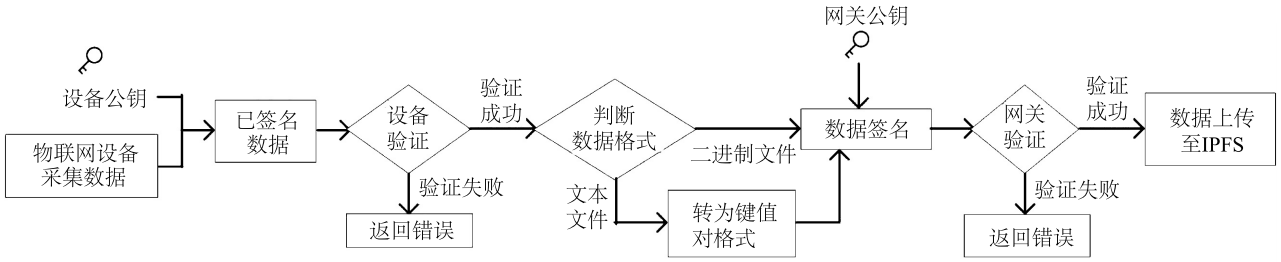
(1)当物联网设备采集到溯源数据时,首先利用改进型 Ed25519 算法结合自身公钥对数据进行签名,将已签名的数据传输给网关,网关利用算法验证签名合法性,若签名不合法,说明物联网设备身份错误,网关拒绝接受该设备上传的数据,并向上级发送提示错误的信息。

(2)由于物联网设备采集的数据格式包括文本文件(字符串、数字等)、二进制文件(图片、视频等),对于文本文件而言,网关内部保存了该环节文本文件各个数据项的名称。当网关获取到物联网设备上传的文本数据时,根据物联网设备的身份,选择文本文件各数据项名称与设备上传的数据对应组合;对于二进制文件而言,则不作处理。同时,网关会检查采集数据的合法性,如数据值不在正常数据范围之内,则说明数据错误或产品不达标,拒绝数据存储并报告错误。

(3)网关利用改进型 Ed25519 算法进行身份验证后,对数据进行签名,经过 IPFS 服务器验证成功后,调用 IPFS 数据存储接口将获得的数据上传至IPFS。

1.2.4 *Blake2 改进型 Ed25519 算法设备的身份验证* 现有的区块链溯源系统中往往不需要进行物联网设备身份验证,降低了系统的安全性。采用 Blake2 改进型 Ed25519 加密算法实现了设备的身

份验证操作,可提高系统安全性。在物联网设备将数据传输给网关、网关将数据传输给 IPFS 服务器时,都需要经过算法的身份验证。系统初始化时,首先利用 Blake2 算法(Blake2 算法涉及的常量、变量及表达式含义见表 1)生成私钥,随后根据私钥生成公钥[21]。



IPFS:星际文件系统。

图 3 果蔬供应链数据传输流程设计

Fig.3 Data transmission flow chart of fruits and vegetables supply chain

表 1 Blake2 相关常量/变量/表达式的解释

Table 1 Related explanations of Blake2 constants/variables/expressions

常量/变量	解释	表达式	解释
w	位数,取 64	$floor(x)$	最大整数≤x
r	轮数,取 12	$ceil(x)$	最小整数≥x
bb	块字节 128	$frac(x)$	x 的正小数部分,$frac(x)=x-floor(x)$
nn	哈希字节,$1\leqslant nn\leqslant 64$,指定散列	2^n	2 的 n 次幂
kk	关键字节,$1\leqslant kk\leqslant 64$,指定密钥	$a\wedge b$	a 和 b 之间的按位异或运算
ll	输入字节,$1\leqslant ll\leqslant 2^{128}$	$a \bmod b$	余数 a 模 b,始终在[0−b−1]范围内
($R1$,$R2$,$R3$,$R4$)	旋转常数取(32,24,16,63)	$x\gg n$	$floor(x/2^n)$。将 x 逻辑右移 n 位
$SIGMA$[0−9]	消息字排列	$x\ll n$	$(x\times 2^w) \bmod (2n)$。将 x 逻辑左移 n
p[0−7]	参数块,定义散列以及密钥大小	$x>>>n$	$(x\gg n)\wedge[x\ll(w-n)]$。将 x 向右旋转 n
M[0−15]	单消息块内的 16 个字	$sqrt(x)$	x 的平方根
h[0−7]	哈希内部状态		
d[0−dd−1]	填充的输入块,每个都有 bb 字节		
t	当前块末尾的消息字节偏移量		
f	最后一个块的标志		
v[0−n−1]	矢量索引是从零开始的;n 元素向量 v 的第一个元素是 v[0],最后一个是 v[n−1]。所有元素都用 v[0−n−1]表示		
$prime(i)$	第 i 个素数(2,3,5,7,11,13,17,19)		

Blake2 算法中调用了混合函数(G)与压缩函数(F),下面对这 2 个函数进行介绍。混合函数(G)的作用是对输入的 x,y 2 个随机字符串使用旋转常数 $R1$、$R2$、$R3$、$R4$ 在向量 v 上返回 4 个字符串 a、b、c、d,结果表示为 v[0−15]。G 函数流程如函数 1 所示:

函数 1 Blake2 中混合函数的操作流程:

输入:a,b,c,d,x,y;

输出:修改向量 v[0−15];

$$v[a]=(v[a]+v[b]+x) \bmod 2^w$$
$$v[d]=(v[d]\wedge v[a])>>>R1$$
$$v[c]=(v[c]+v[d]) \bmod 2^w$$
$$v[b]=(v[b]\wedge v[c])>>>R2$$
$$v[a]=(v[a]+v[b]+y) \bmod 2^w$$
$$v[d]=(v[d]\wedge v[a])>>>R3$$
$$v[c]=(v[c]+v[d]) \bmod 2^w$$
$$v[b]=(v[b]\wedge v[c])>>>R4$$

返回 $v[0-15]$。

压缩函数(F)是将状态向量(h)、消息块向量(m)、$2w$ 位偏移计数器(t)和标志(f)(判断当前是否处于最终块,若为最终块则为 true)、局部向量(v)[0-15]用于混合与压缩操作,可返回 1 个新的状态向量 $h[0-7]$,回合编号从 0 到 $r-1$。其中 $IV[0-7]$ 为初始化向量,如公式(2)所示,根据表 1 中相关系数进行运算后的结果如公式(3)所示。压缩函数(F)操作流程如下,其中函数涉及的 SIGMAS 讯息时间如表 2 所示:

$$IV[i]=floor\{2^w * frac\{sqrt[prime(i+1)]\}\} \quad (2)$$

$$IV[0-7]=\{0x6A09E667F3BCC908, 0xBB67AE8584CAA73B, 0x3C6EF372FE94F82B, 0xA54FF53A5F1D36F1, 0x510E527FADE682D1, 0x9B05688C2B3E6C1F, 0x1F83D9ABFB41BD6B, 0x5BE0CD19137E2179\} \quad (3)$$

表 2 SIGMAS 讯息时间

Table 2 SIGMAS message schedule

环节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$SIGMA[0]$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$SIGMA[1]$	14	10	4	8	9	15	13	6	1	12	0	2	11	7	5	3
$SIGMA[2]$	11	8	12	0	5	2	15	13	10	14	3	6	7	1	9	4
$SIGMA[3]$	7	9	3	1	13	12	11	14	2	6	5	10	4	0	15	8
$SIGMA[4]$	9	0	5	7	2	4	10	15	14	1	11	12	6	8	3	13
$SIGMA[5]$	2	12	6	10	0	11	8	3	4	13	7	5	15	14	1	9
$SIGMA[6]$	12	5	1	15	14	13	4	10	0	7	6	3	9	2	8	11
$SIGMA[7]$	13	11	7	14	12	1	3	9	5	0	15	4	8	6	2	10
$SIGMA[8]$	6	15	14	9	11	3	0	8	12	2	13	7	1	4	10	5
$SIGMA[9]$	10	2	8	4	7	6	1	5	15	11	9	14	3	12	13	0
$SIGMA[10]$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$SIGMA[11]$	14	10	4	8	9	15	13	6	1	12	0	2	11	7	5	3

函数 2 Blake2 中压缩函数的操作流程:

输入:$h[0-7]$,$m[0-15]$,t,f;

输出:$h[0-7]$;

$v[0-7]=h[0-7]$//状态的前半部分

$v[8-15]=IV[0-7]$//IV 的后半部分

//初始化局部工作向量 $v[0-15]$

$v[12]=v[12]\wedge(t \bmod 2^w)$//偏移量的低位字

$v[13]=v[13]\wedge(t\gg w)$//高位字

$If(f=true)$//最后一个块标志

$v[14]=v[14]\wedge 0xFFFFFFFF$//反转所有位.

//密码混合

$for(i=0;i\leqslant r-1;i++)$

//本轮的消息词选择排列。

$s[0-15]=SIGMA[i \bmod 10][0-15]$

$v=G(0,4,8,12,m\{s[0]\},m\{s[1]\})$

$v=G(1,5,9,13,m\{s[2]\},m\{s[3]\})$

$v=G(2,6,10,14,m\{s[4]\},m\{s[5]\})$

$v=G(3,7,11,15,m\{s[6]\},m\{s[7]\})$

$v=G(0,5,10,15,m\{s[8]\},m\{s[9]\})$

$v=G(1,6,11,12,m\{s[10]\},m\{s[11]\})$

$v=G(2,7,8,13,m\{s[12]\},m\{s[13]\})$

$v=G(3,4,9,14,m\{s[14]\},m\{s[15]\})$

$for(i=0;i\leqslant 7;i++)$//两半异或

$h[i]=h[i]\wedge v[i]\wedge v[i+8]$

返回 h[0-7]//新状态。

下面介绍 Blake2 算法。摘要密钥和数据输入被拆分并填充到 dd 消息块 $d[0-dd-1]$ 中,每个 dd 消息块由 bb 字节组成。用“0”进行填充,并设置为 $d[0]$,数据块 $d[dd-1]$ 也用“0”填充到 bb 字节。块数 $dd=ceil(kk/bb)+ceil(ll/bb)$。随后将填充的数据块处理为 nn 字节的最终散列值,具体步骤如算法 1 所示。指定参数块字 $p[0-7]$ 如下:

$p[0]=0x0101kknn$;

$p[1-7]=0$。

Blake2 算法流程如下:

算法 1:Blake2 函数流程。

输入:$dd[0-dd-1]$,ll,kk,nn;

输出:数组 $h[\ ]$的第一个 nn 字节;

$h[0-7]=IV[0-7]$//初始化向量

$h[0]=h[0]\wedge 0x01010000\wedge(kk\ll 8)\wedge nn$

//处理填充键和数据块

if($dd>1$)

For(i=0;i≤$dd-2$,i++)

$h=F(h,d[i],(i+1)*bb,false)$

//最后一个块

if($kk=0$)

$h=F(h,d[dd-1],ll,true)$

Else

$h=F(h,d[dd-1],ll+bb,true)$

返回数组 $h[\ ]$的第一个 nn 字节。

在利用 Blake2 生成私钥后,利用 Ed25519 算法生成公钥,发放给物联网设备。公钥生成的具体流程[22]如下:

(1)选择 256 bit 的 blake2 算法生成的私钥,记为 $sk=(sk_{255},sk_{254},\cdots,sk_1,sk_0)_2$;

(2)对 sk 做 SHA-512 运算,即 $H(sk)=(h_{511},h_{510},\cdots,h_1,h_0)_2$;

(3)取 $H(sk)$的末尾 256 bit 大小数据,并进行修剪,整理为 $s=(0,1,h_{253},h_{252},\cdots,h_3,0,0,0)$;

(4)将 s 解释为小端整数,形成秘密标量,执行标量乘法 sB,$sB=(x,y)=A$,其中,$x=(x_{254},x_{253},\cdots,x_1,x_0)_2$,$y=(y_{254},y_{253},\cdots,y_1,y_0)_2$;

(5)压缩 sB 结果,压缩过程为 $pk=Ay+(Ax\ \&\ 1)$,得公钥 $pk=(x_0,y_{254},y_{253},\cdots,y_1,y_0)_2$。

当物联网设备、网关得到公钥后,需要进行溯源数据片 M 传输时,首先对溯源数据 M 进行签名,签名算法如下。G 为曲线 Edwards25519 的基点,R'和 A 为曲线上的动点,L 为 253 位的素数(2^{252}+27 742 317 777 372 353 535 851 937 790 883 648 493),R 和 pk 分别为点 R'和点 A 的 256 位压缩结果,压缩过程为 $R=R'_y+(R'_x\&1)$。其中 $H(x)$表示为 x 进行 SHA-512 算法运算后的运算结果。

算法 2:Ed25519 数字签名算法的签名流程。

输入:256 位的公钥 pk,任意长度的消息 M,256 位的私钥 sk;

输出:512 位的签名结果 R,S。

1)对 sk 做 SHA-512 运算,$H(sk)=(h_{511},h_{510},\cdots,h_1,h_0)_2$;

2)取 $H(sk)$的高 256 位,$h=(h_{511},h_{510},\cdots,h_{257},h_{256})_2$;

3)$a=2^{254}+\sum_{i=3}^{253}2^i h_i$;

4)$r=H(h,M)\ \mathrm{mod}\ L$;

5)$R'=rG=(R'_x,R'_y)$,压缩点 R'得到 $R=R'_y+(R'_x\ \&\ 1)$;

6)$k=H(R,pk,M)\ \mathrm{mod}\ L$;

7)$S=(r+ka)\ \mathrm{mod}\ L$;

8)返回签名(R,S)。

当网关、IPFS 服务器获得溯源数据片 M 及上传数据的签名结果(R,S)后,将利用之前发放给各物联网设备、网关的公钥 pk 进行验签操作,具体算法如下所示。验签过程的解压操作是密钥生成和签名操作中压缩操作的逆运算。

算法 3:Ed25519 数字签名算法的验签流程。

输入:256 位的公钥 pk,任意长度的消息 M,512 位的签名结果(R,S);

输出:验签的结果;

1)若$(R,S)\notin[1,L-1]$,则验证失败,结束验证流程;

2)解压得到点 R';

3)解压 pk 得到点 A;

4)$k=H(R,pk,M)\ \mathrm{mod}\ L$;

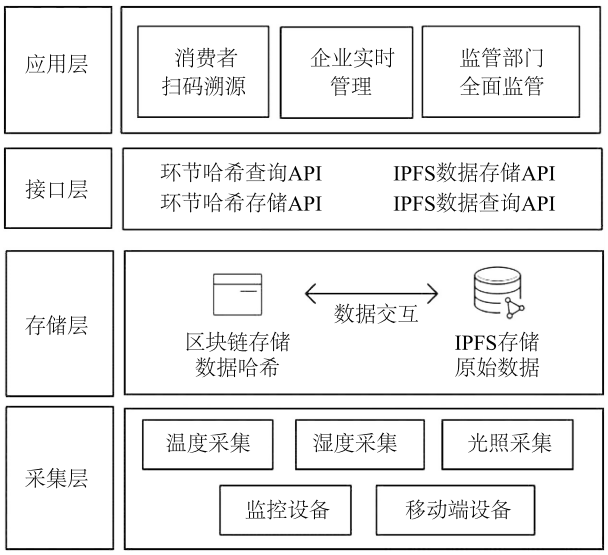
5)验证 $SG=R'+kA$,若等号成立,则验证成功。

在 Ed25519 中的点加与倍点运算需要在拓展四元齐次坐标下完成,具体操作见文献[22]。验签过程中,通过对比 SG 和 $R'+kA$ 的运算结果来判断签名的真实性。当签名验证成功时,表示该设备身份可信。当该设备需要进行二次身份验证时,从区块链中获取公钥 MD5 哈希值,并与本地公钥 MD5 哈希值进行比对,比对成功后表明公钥未被篡改,可使用公钥对数据进行签名完成身份验证。

2 结果与分析

2.1 系统架构与实现

基于身份验证的果蔬区块链信息存储溯源系统的目的是实时监控与保存果蔬产品从生产到销售各环节产生的关键数据,并将数据进行安全储存与展示。对本系统各个功能模块进行了细化,系统分为采集层、存储层、接口层、应用层,系统架构如图 4 所示。



API:应用程序接口;IPFS:星际文件系统。

图 4 系统的架构

Fig.4 System architecture diagram

采集层主要通过各企业设置的温湿度采集设备、移动端设备、监控设备等进行数据采集与录入,保证关键数据采集的全面化与多样化。存储层分为IPFS 链下存储与区块链链上存储两部分,链下存储可以减轻区块链网络存储负担,保证了物联网设备采集数据的及时存储与安全;区块链链上存储保证了溯源数据 IPFS 哈希安全性,并通过区块链节点为用户提供溯源数据查询接口。接口层主要为数据存储、查询提供相应接口,针对模型的特点,提供了IPFS 数据交互接口,满足了网关设备的溯源数据存储的需求和通过数据哈希在 IPFS 中查询溯源数据的需求;提供了区块链数据交互接口,满足了 IPFS 数据哈希上链与消费者扫码调用接口查询 IPFS 哈希的需求。应用层通过微信小程序和 Web 端向消费者、监管部门、企业等提供数据查询、管理页面。

安徽省合肥市某果蔬企业涉及草莓供应链所有环节,需要较多的物联网数据采集设备进行数据采集,为保证各物联网设备采集数据的安全传输与高效存储,保证数据在存储于区块链前未发生篡改,采用本系统进行了优化。图 5 为本系统采集层相关设备,图 5A、5B 分别为土壤温湿度传感器及空气传感器,图 5C 为网关设备。物联网设备运作逻辑为:传感器采集草莓生产过程中的关键数据,通过传输线连接到网关的接线端子,利用网关的树莓派等装置实现将传感器采集数据的组织、传输、存储于 IPFS 等。本系统应用层相关页面如图 6 所示,图 6A 为消费者扫描商品二维码后显示的移动端主页,展示了草莓的品种、产地等信息,用户可选择环节,查看该环节详细信息,例如点击生产信息后,生产信息页面如图 6B 所示,展示了种植商、地址等一系列溯源信息。图 6C 为企业 Web 端页面,展示了区块链管理、基地管理、物联网设备管理等多个功能,当前页面展示了区块链信息,例如智能合约数、交易数、区块数等,可实现企业对供应链的全面管理与信息监测。

A: 土壤温湿度传感器 B: 空气传感器 C: 网关设备

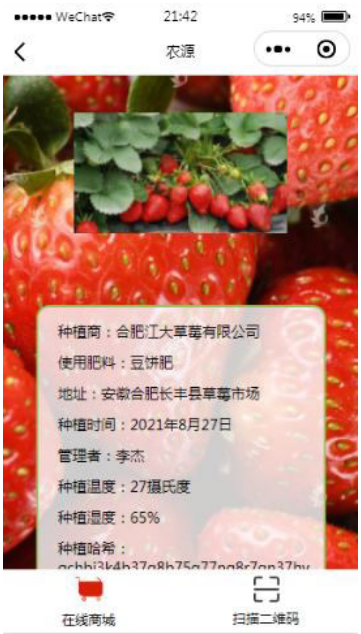
图 5 相关物联网设备

Fig.5 Relevant equipments of the internet of things

2.2 系统效率测试

基于身份验证的果蔬区块链信息存储溯源系统采用 Hyperledger Fabric 构建。其环境基础为 Centos 7.5、Docker 18.09、fabric-sdk-node 2.2。虚拟机配置

A: 移动端扫码主页



B: 生产环节详情页面

C: WEB端企业页面主页

图 6 本系统启用层相关页面

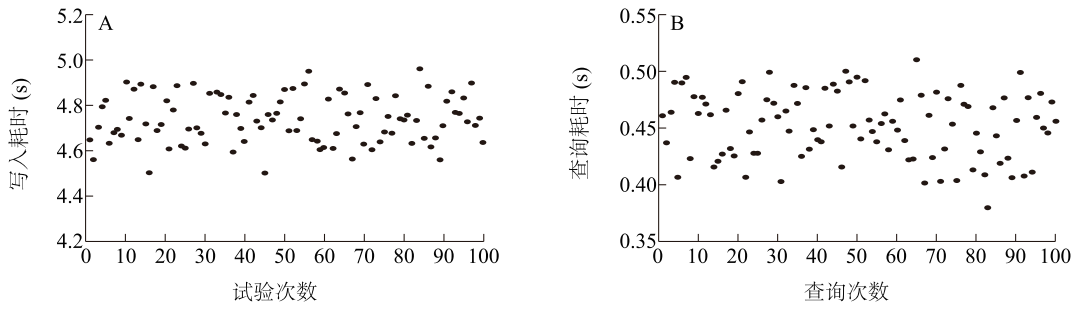
Fig.6 Relevant pages of the enabled layer of the system

为 32 G 内存、16 核处理器、16 G 硬盘，带宽为 20 Mb/s。采用区块链基准测试工具 Hyperledger Caliper 生成测试结果。

为了验证基于身份验证的果蔬区块链信息存储溯源系统的写入与查询效率，测试了全供应链环节数据存储耗时，包括从各物联网设备采集数据存入 IPFS 的平均时间以及 IPFS 哈希存储于区块链的时间，为了保证测试结果的真实可靠，进行了 100 次供应链数据存储效率测试、100 次溯源数据查询效率测试。如图 7A 所示，全供应链数据存入区块链耗时为 4.738 s，单个环节平均耗时 1.190 s；可见数据存储时设备对数据进行签名、验签操作，IPFS 哈希存储等操作对数据存储的负面影响并不明显。如图 7B 所示，用户溯源平均消耗时间为 0.452 s。可见本系统的区块链结合 IPFS 的数据查询机制可以略微提升溯源服务速度，这主要是由于 IPFS 分布式的特点，IPFS 数据查询效率要高于区块链数据查询效率。

3 结 论

本研究应用密码学原理设计了 Blake2 改进型 Ed25519 算法，并以此设计了果蔬供应链数据传输流程，在此基础上结合 IPFS 与区块链技术设计了基于身份验证的果蔬区块链信息存储溯源模型。在进行实际应用及测试后，Blake2 改进型 Ed25519 算法可以实现物联网设备的身份验证，保障了系统的安全性；果蔬供应链数据传输流程可以改善物联网设备数据



A:不同试验次数的写入耗时;B:不同查询次数的查询耗时。

图 7 储存查询效率测试

Fig.7 Test of storage and query efficiency

处理、传输能力不足的问题,提高数据传输的高效性;利用 IPFS 链下存储采集数据,区块链网络链上存储 IPFS 哈希,可以提高区块链存储空间利用率。三者结合可以满足果蔬供应链数据安全性传输、存储的需求。在进行系统测试后,本系统供应链数据存储时间为 4.738 s,数据查询时间为 0.452 s,可以提供高效溯源服务,可为果蔬供应链溯源系统设计提供参考。

参考文献:

[1] 孙海霞,张淑娟,薛建新,等. 基于光谱和成像技术的果蔬质量检测研究进展[J]. 光谱学与光谱分析,2018,38(6):1779-1785.

[2] HAMID S, MAHMOOD Z, IMRAN M , et al. Potentiality of lemon peel as low cost adsorbent for the removal of trypan blue dye from aqueous solution[J]. Journal-Chemical Society of Pakistan, 2011, 33(3):364-369.

[3] 王祖良,郭建新,张 婷,等. 农产品质量溯源 RFID 标签批量识别[J]. 农业工程学报,2020,36(10):150-157.

[4] 杨信廷,王明亭,徐大明,等. 基于区块链的农产品追溯系统信息存储模型与查询方法[J]. 农业工程学报,2019,35(22):323-330.

[5] 弋伟国,何建国,刘贵珊,等. 区块链增强果蔬质量追溯可信度方法研究与系统实现[J]. 农业机械学报,2022,53(2):309-315.

[6] 张 新,彭祥贞,许继平,等. 基于区块链智能合约的稻米供应链动态监管模型[J]. 农业机械学报,2022,53(1):370-382.

[7] 于华竟,徐大明,罗 娜,等. 杂粮供应链区块链多链追溯监管模型设计[J]. 农业工程学报,2021,37(20):323-332.

[8] 许继平,王 健,张 新,等. 区块链驱动的稻米供应链信息监管模型研究[J]. 农业机械学报,2021,52(5):202-211.

[9] 于合龙,陈邦越,徐大明,等. 基于区块链的水稻供应链溯源信息保护模型研究[J]. 农业机械学报,2020,51(8):328-335.

[10] 王志铧,柳平增,宋成宝,等. 基于区块链的农产品柔性可信溯源系统研究[J]. 计算机工程,2020,46(12):313-320.

[11] 于合龙,陈邦越,徐大明等. 基于区块链的水稻供应链溯源信息保护模型研究[J]. 农业机械学报,2020,51(8):328-335.

[12] 邵奇峰,金澈清,张 召,等. 区块链技术:架构及进展[J]. 计算机学报,2018,41(5):969-988.

[13] 夏 清,窦文生,郭凯文等. 区块链共识协议综述[J]. 软件学报,2021,32(2):277-299.

[14] 任艳丽,徐丹婷,张新鹏,等. 可修改的区块链方案[J]. 软件学报,2020,31(12):3909-3922.

[15] 尤 瑶,孔兰菊,肖宗水,等. 一种支持区块链交易溯源的混合索引机制[J]. 计算机集成制造系统,2019,25(4):978-984.

[16] 刘汉卿,阮 娜. 区块链中攻击方式的研究[J]. 计算机学报,2021,44(4):786-805.

[17] ATHANERE S, THAKUR R. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing[J]. Journal of King Saud University Computer and Information Sciences, 2022, 34(4):1523-1534.

[18] 杜飞飞,张德学,王佃涛,等. BLAKE2b 算法优化及 OpenCL 实现[J]. 小型微型计算机系统,2019,40(11):2281-2284.

[19] 刘 勇,陈 宇,陈 钟. 对称密码算法的性能优化[J]. 北京大学学报(自然科学版),2008,44(5):733-738.

[20] 薛一鸣,刘树荣,郭书恒,等. 高速 Ed25519 验签算法硬件架构的设计与实现[J]. 通信学报,2022,43(3):101-112.

[21] 刘宗斌,荆继武,夏鲁宁. BLAKE 算法的硬件实现研究[J]. 计算机学报,2012,35(4):703-711.

[22] 许文龙,王 奕,陈 佐,等. 高性能 BLAKE 算法研究及其 FPGA 实现[J]. 计算机应用研究,2012,29(6):2098-2101.

(责任编辑:陈海霞)