doi:10.6041/j.issn.1000-1298.2023.07.039

基于智能合约和数字签名的马铃薯种薯防窜溯源研究

孙传恒[1,2]　魏玉冉[1,2]　邢　斌[2,3]　徐大明[2,3]　李登奎[2,3]　张　航[1]

(1. 天津农学院计算机与信息工程学院，天津 300384；2. 国家农业信息化工程技术研究中心，北京 100097；
3. 农产品质量安全追溯技术及应用国家工程实验室，北京 100097)

摘要：随着区块链技术在农产品溯源领域研究的不断发展，农产品的质量安全得到有效保障。由于我国马铃薯种薯生产过程复杂、实物形态差异化明显、每个环节的生产周期长、品种繁多等原因，所有生产环节的溯源数据共享难度大，容易发生种薯品种、等级等窜货问题，种薯生产溯源无法得到切实保障，生产基地及相关监管部门无法得到全部有效溯源数据，当发生窜货问题以及最终消费者进行种薯生产溯源时，责任环节定位不明确，难以准确找到责任生产环节及相关责任人等问题源头。基于上述问题，提出了基于智能合约和数字签名的马铃薯种薯防窜溯源模型，利用区块链技术不可篡改、数据透明、数据共享等特点，通过智能合约进行种薯生产全环节溯源数据的上链存储，实现种薯生产全环节溯源数据的高度共享，并将智能合约与数字签名相结合，利用公私钥对验证和智能合约高度自治的区块链网络生态环境，解决生产过程中易发生的生产窜货问题。基于 Hyperledger Fabric 设计面向种薯生产基地的防窜溯源模型，相关测试结果表明，该模型可以实现种薯生产溯源、防窜、窜货报警信息上链与查询等功能。种薯生产溯源数据的平均上链时间为 2 566 ms，平均查询时间为 95 ms，报警触发与报警信息上链的平均时间为 2 562 ms，查询具体报警信息的平均时间为 77 ms。模型综合性能较高，能够实现种薯生产全环节溯源数据的安全存储，并有效解决种薯的生产窜货问题，满足种薯生产溯源数据的上链与查询需求，完善种薯生产质量溯源保障，为防止种薯生产窜货以提高整体效率和安全溯源方面提供了借鉴和参考。

关键词：种薯生产；溯源；防窜；智能合约；数字签名；数据共享

中图分类号：TP309.2；TS201.6　　**文献标识码**：A　　**文章编号**：1000-1298(2023)07-0392-12　　**OSID**：

Anti-channeling Traceability of Seed Potatoes Based on Smart Contracts and Digital Signatures

SUN Chuanheng[1,2]　WEI Yuran[1,2]　XING Bin[2,3]　XU Daming[2,3]　LI Dengkui[2,3]　ZHANG Hang[1]

(1. *College of Computer and Information Engineering*, *Tianjin Agricultural University*, *Tianjin* 300384, *China*
2. *National Engineering Research Center for Information Technology in Agriculture*, *Beijing* 100097, *China*
3. *National Engineering Laboratory for Agri-product Quality Traceability*, *Beijing* 100097, *China*)

Abstract: With the continuous development of blockchain technology in the field of traceability of agricultural products, the quality and safety of agricultural products have been effectively guaranteed. Due to the complex production process of Chinese seed potatoes, obvious physical form differentiation, long production cycle of each link, and many varieties, it is difficult to share the traceability data of all production links, which is prone to the problem of seed potato varieties, grades and other goods transmission. Seed potato production traceability cannot be effectively guaranteed, and the production base and relevant supervision departments cannot obtain all effective traceability data. When the problem of transshipment occurs and the final consumer traces the source of seed potato production, the positioning of the responsibility link is not clear, and it is difficult to find the exact responsible production link and the responsible person and other problems. Based on the above problems, a channe-proof traceability model of seed potato was proposed based on smart contract and digital signature. By using the characteristics of block chain technology, such as tamper-proof, data transparency and data sharing,

收稿日期：2022-12-02　修回日期：2022-12-22

基金项目：国家自然科学基金面上项目(31871525)

作者简介：孙传恒(1978—)，男，研究员，博士，主要从事农产品追溯技术研究，E-mail：sunch@nercita.org.cn

通信作者：张航(1981—)，男，讲师，博士，主要从事农业智能化信息技术研究，E-mail：zhanghrz@126.com

intelligent contract was used to store the traceability data of the whole link of seed potato production and realize the highly sharing of the traceability data of the whole link of seed potato production. In addition, the smart contract and digital signatures were combined to solve the problem of cross-production easily occurring in the production process by using the public-private key pair verification and the highly autonomous blockchain network ecological environment of smart contract. Based on Hyperledger Fabric, an anti-channeling traceability model for seed potato production base was designed. The related test results showed that the model could realize the functions of seed potato production traceability, anti-channeling, channeling alarm information chain and query. The average link time of seed potato production traceability data was 2 566 ms, the average query time was 95 ms, the average alarm trigger and alarm information link time was 2 562 ms, and the average query time of specific alarm information was 77 ms. The model had high comprehensive performance, which can realize the safe storage of seed potato production traceability data, effectively solve the problem of seed potato production channeling, meet the link and query requirements of seed potato production traceability data, improve the seed potato production quality traceability guarantee, and provide reference for preventing seed potato production channeling to improve the overall efficiency and safety traceability.

Key words: seed potato production; traceability; anti-channeling; smart contract; digital signature; data sharing

0　引言

马铃薯在全球重要粮食作物中排名第 4 位，也是我国主要粮经作物[1]。近年来，我国产业结构调整，使得马铃薯产业在国民经济增长中的占比越来越重，马铃薯主粮化战略已经启动[2]。但我国马铃薯整体生产水平仍然较低，这主要是因为我国种薯质量不高，直接影响了马铃薯的最终产量和质量[3]。因此，研究马铃薯种薯的生产溯源，通过信息技术提高种薯的产量及质量，对加快我国马铃薯产业化、主粮化进程有着重大意义[4]。

我国马铃薯种薯生产全环节流程复杂、周期较长、品种繁多，对种薯生产溯源数据进行信息化记录的技术储备不健全，导致种薯溯源困难[5]。对此，相关研究人员提出了一些传统溯源解决方案。文献[6]采用数据库、二维码等技术创建溯源平台，实现对马铃薯种薯全供应链的溯源。文献[7]通过对马铃薯进行连续 3 年的跟踪监测，建立了基于稳定同位素和矿质元素的马铃薯产地溯源模型，并开发了马铃薯质量信息识别与产地溯源专家系统。文献[8]使用射频识别技术和二维码技术达到防伪防窜货目的，对整个供应链进行全过程监控。然而，传统质量溯源通过中心化平台来进行，生产溯源数据的存储方式为集中式存储，溯源数据易被篡改[9]。区块链技术是分布式的网络架构[10]，网络中的所有节点遵守统一的共识机制，共同维护一个区块链账本，所有交易操作均会被记录，篡改某数据非常困难[11]。近年来，随着区块链技术在农业领域的迅速发展，文献[12]采用“区块链 + 数据库”的双存储模式，实现红茶从茶园到茶桌的全程可信溯源。文献[13]提出一种高效且低成本运行的方法，利用公有链和私有链两套区块链确保溯源数据的真实可靠。文献[14]设计出基于区块链智能合约的框架，用于记录农作物生长、流通等数据，旨在消除供应链企业间的信息孤岛。文献[15]使用嵌入式控制等物联网技术与区块链相结合实现防篡改、透明化、可溯源的农产品溯源系统。文献[16]结合以太坊智能合约和星际文件系统(InterPlanetary file system, IPFS)管理和控制供应链生态系统中所有参与者之间的交互和交易，并在大豆供应链方面实现了溯源应用。文献[17]设计出一种基于边缘计算和区块链的防伪溯源模型，并采用离散波长转换和遗传算法来提高系统的安全性，优化系统的性能。文献[18]提出了“On-Chain + Off-Chain”的农产品质量安全溯源策略，降低链上存储空间压力的同时实现了农产品供应链之间溯源信息的真实可靠。文献[19]通过智能合约实现果蔬农产品溯源模型，并提出了对称加密与椭圆曲线混合加密的隐私数据授权访问方法，实现供应链各企业间隐私数据的隔离存储。根据文献表明，众多区块链技术研究人员研究农产品和食品安全溯源相关领域[20-22]，实现全食品业和农业生产信息透明化和共享数据精准化[23]，从源头解决食品和农产品质量安全问题是未来的发展趋势[24]。然而，将区块链技术应用于马铃薯种薯的生产溯源方面的研究较少。此外，种薯生产期间的实物形态差异化明显[25]，在生产过程中易出现品种、等级等窜货问题，将区块链技术应用于马铃薯种薯生产溯源时，还应考虑其生产窜货问题。

针对上述问题，结合分析马铃薯种薯生产过程中的关键环节及溯源数据，本文提出一种基于智能

合约[26-27]和数字签名[28-29]的马铃薯种薯防窜与溯源方法,为种薯整个生产环节设计一条溯源区块链。以智能合约和数字签名为实现方式,解决种薯的生产窜货问题,并保障种薯各项生产溯源数据的安全可靠,最终提高种薯生产基地的整体生产效率。采用 Raft 共识机制[30]实现区块链间的节点共识,每个环节作为种薯区块链中的联盟组织,每个联盟组织中都包含多个节点共同维护一个分布式账本,实现种薯生产溯源数据的真实可信;利用数字签名机制与种薯生产过程中的接收环节对应培育节点进行公私钥对绑定,用于防止种薯生产窜货的第 1 层保障;通过智能合约实现种薯培育目的地的防窜货报警设计,使种薯区块链网络中的所有节点背书完成后共同遵守统一的逻辑规则,用于防止种薯品种、等级等生产窜货的第 2 层保障;同时将报警信息进行上链存储,更高效地解决种薯生产窜货数据的溯源问题;最后对本文所提出的马铃薯种薯生产溯源模型通过应用案例进行验证分析。

1 马铃薯种薯生产全环节分析及区块链网络模型

1.1 种薯生产全环节及溯源数据分析

马铃薯种薯生产过程中涉及的关键环节包括种苗资源保存、脱毒苗扩繁、原原种培育、原种培育和仓储环节。种薯生产环节众多,实物形态在不同的环节有所不同,生产基地同时培育的品种繁多,极其容易发生窜货问题。因此,本文在深入分析种薯生产全环节及关键溯源数据的基础上,在区块链网络中设计种薯生产窜货报警环节,一旦发生窜货,将进入该环节进行窜货报警处理,同时将对应窜货报警数据进行上链存储。各环节的关键溯源数据如表 1 所示。

表 1 种薯生产全环节关键溯源数据

Tab. 1 Key traceability data of seed potato production

生产环节	关键上链数据	关键防窜数据
种苗资源保存	批次编号、资源编号、种苗名称、资源库编号、入资源库时间、出资源库时间、种苗来源、品种名称、工人编号、工人姓名、抽检员编号、抽检员姓名、抽检编号、抽检结果	批次编号、资源编号、种苗名称、品种名称
脱毒苗扩繁	批次编号、扩繁编号、种苗名称、品种名称、培养室编号、入培养室时间、出培养室时间、工人编号、工人姓名、抽检员编号、抽检员姓名、抽检编号、抽检结果	批次编号、扩繁编号、种苗名称、品种名称
原原种培育	批次编号、原原种编号、种薯名称、品种名称、温室大棚编号、移栽时间、收获时间、工人编号、工人姓名、抽检员编号、抽检员姓名、抽检编号、抽检结果	批次编号、原原种编号、种薯名称、品种名称
原种培育	批次编号、原种编号、种薯名称、品种名称、地块编号、播种时间、收获时间、原原种来源、原种级别、工人编号、工人姓名、抽检员编号、抽检员姓名、抽检编号、抽检结果	批次编号、原种编号、种薯名称、品种名称、原种级别
仓储	批次编号、仓储编号、种薯名称、品种名称、仓库编号、入库时间、出库时间、种薯来源、种薯级别、工人编号、工人姓名、抽检员编号、抽检员姓名、抽检编号、抽检结果	批次编号、仓储编号、种薯名称、品种名称、种薯级别
窜货报警	批次编号、种薯溯源编号、报警编号、报警时间、报警环节、报警触发点、工人编号、工人姓名	

1.2 种薯区块链网络模型

马铃薯种薯生产全环节的溯源数据参差不齐,目前尚且没有种薯生产业务集成技术和手段,也没有统一的生产溯源信息接口和标准规范,造成了种薯生产全环节的信息孤岛,不仅影响种薯生产基地的总体生产效率,还使消费者和相关监管部门可信溯源困难。区块链技术具有去中心化、篡改存储数据困难、多节点共同维护、数据透明等特点,通过分布式网络中的各节点数据备份实现溯源数据的安全存储。本文通过开源许可区块链框架 Hyperledger Fabric 使种薯生产全环节共同维护一个区块链账本,每个相关环节安装不同的智能合约,利用智能合约完成溯源数据的更新上链,不相关的环节无法相互之间进行种薯转送交易操作和溯源数据更新上链,以此来规范化种薯生产流程,最终提高可信溯源。种薯生产溯源区块链网络模型如图 1 所示。

种薯生产全过程的溯源数据通过一条综合区块链进行存储,将种薯生产溯源中的全部环节映射为区块链中的相关组织,即种苗资源保存组织、脱毒苗扩繁组织、原原种培育组织、原种培育组织和仓储组织,将防窜报警环节映射为窜货报警处理组织,并将各个环节的关键溯源数据均通过智能合约进行上链存储,非关键溯源数据使用传统数据库存储,可以从源头减轻区块链的存储压力。同时,将消费者、相关监管部门等溯源用户映射为外部组织,作为查询相关溯源数据的组织节点。

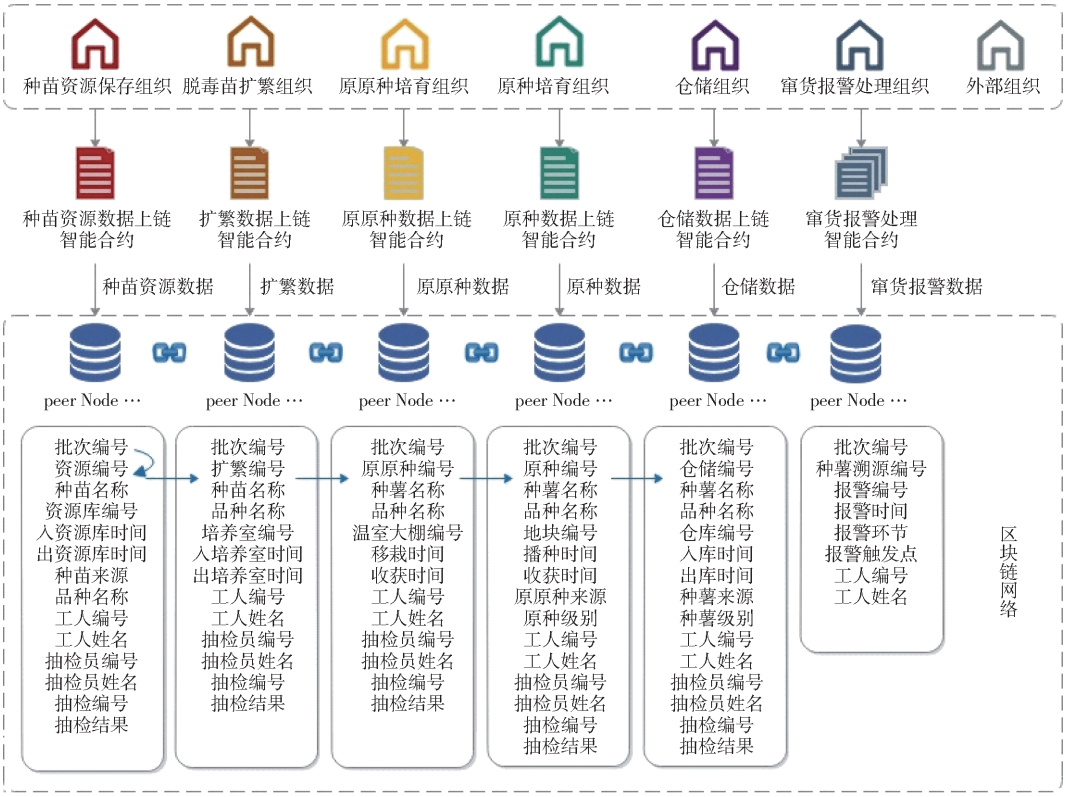


图 1　种薯生产溯源区块链网络模型

Fig. 1　Blockchain network model for seed potato production traceability

区块链中的每个组织都有自己的 peer 节点来分布式存储对应溯源数据，每批种薯都有一个唯一的批次编号，种薯在全部生产环节流通时都需关联此唯一批次编号上传所有关键溯源数据。此外，本文还利用区块链种薯全生产链全连接溯源编码设计为每个生产环节对应产生一个与批次编号相关联的二级编号，如资源编号对应种苗资源保存环节、扩繁编号对应脱毒苗扩繁环节等。

2　种薯防窜报警方法设计

2.1　区块链种薯全生产链全连接溯源编码设计

在种薯区块链溯源模型中，需通过种薯溯源编码在区块链网络中获取该编码所对应的全部生产溯源数据。为了使区块链种薯溯源编码具有唯一溯源性，设计区块链种薯全生产链全连接编码，并利用该编码与对应种薯生产全环节溯源数据相关联。种薯溯源编码在马铃薯种苗资源保存环节进行批次编码初始化处理，包含种苗资源保存环节在内的种薯生产全环节开始培育时，顺序连接对应环节的溯源编码，在仓储环节实现种薯溯源编码的全环节连接，最终聚焦到以箱为单位的种薯溯源编码，实现一箱一码，保证种薯溯源编码的唯一性，为利用区块链技术实现种薯防窜生产溯源打下源头基础。

具体编码设计如表 2 所示，例如，在种苗资源保存环节进行批次编码初始化处理，此时的种薯批次编码为 B001。在种苗资源保存环节开始对该批次编码所对应的种苗进行培育时，顺序连接种苗资源保存环节的溯源编码 R001，此时对应种薯溯源编码为 B001R001，直至对应种薯顺利进入仓储环节，形成最终种薯溯源编码为 B001R001D001YY001Y001WH001。当对应种薯在其生产过程中发生窜货报警时，将不继续连接当前发生窜货环节的对应环节编码，种薯溯源编码的连接停留在上一环节，同时生成对应窜货报警编码。例如，对应种薯在脱毒苗扩繁环节发生窜货报警，则此时的种薯溯源编码为 B001R001，对应窜货报警编码为 W001。此外，所有环节的溯源编码数字项顺序生成。例如，批次编码为 B001 的下一批次编码为 B002。

表 2　区块链种薯全生产链全连接溯源编码设计

Tab. 2　Fully connected traceability coding design for whole production chain of seed potato in blockchain

批次	种苗资源保存	脱毒苗扩繁	原原种培育	原种培育	仓储	报警
B001	B001R001	B001R001D001	B001R001D001YY001	B001R001D001YY001Y001	B001R001D001YY001Y001WH001	W001

2.2 数字签名机制

种薯生产各环节的培育节点众多,生产基地繁育品种数量庞大,由于对应种薯被送往错误接收环节培育节点而引发的生产窜货问题频繁出现,严重降低整体生产效率。椭圆曲线数字签名算法(Elliptic curve digital signature algorithm,ECDSA)是一种非对称加密算法,使用私钥签名、公钥验证确保数据的真实性并防止交易数据被篡改,使用公钥加密、私钥解密确保可验证节点的唯一性。同时,ECDSA 具有在已知公钥的情况下,无法推导出该公钥对应私钥的特点,本文利用该特点对种苗/薯转送交易进行公钥数字签名加密,相关接收环节对应培育节点使用本节点私钥进行解密验证,确保该种苗/薯转送接收环节对应培育节点的唯一正确性。该方法是种苗/薯接收环节对应培育节点的归属证明,实现防止种薯生产窜货的第 1 层保障。椭圆曲线公式为

$$y^2 = x^3 + ax + b(\mathrm{mod}p) \quad (4a^3 + 27b^2 \neq 0(\mathrm{mod}p)) \tag{1}$$

式中 a、b——椭圆曲线参数

p——质数 mod——取模运算符

以资源保存环节培育完毕,需要将种苗送往脱毒苗扩繁环节对应培育节点进行培育为例,椭圆曲线数字签名加密、解密过程如下:

(1)脱毒苗扩繁环节对应培育节点选定一条椭圆曲线 $F_p(a,b)$,同时选取椭圆曲线上一点作为基点 G,其中 n 为椭圆曲线的阶,即 $nG = \infty$。

(2)脱毒苗扩繁环节对应培育节点选择一个随机数作为私有密钥 k,并根据离散点计算原则生成公有密钥 $K = kG$。

(3)脱毒苗扩繁环节对应培育节点将椭圆 $F_p(a,b)$ 和点 G、K 传送给种苗资源保存环节对应节点。

(4)种苗资源保存环节对应节点接到信息后,将待传输的明文编码到 $F_p(a,b)$ 上的一点 A,并产生一个随机整数 $r(r < n)$。

(5)种苗资源保存环节对应节点通过椭圆曲线公钥 K 加密:$C_1 = A + rK$,$C_2 = rG$,加密后的数字签名密文 C 是一个点对。

(6)脱毒苗扩繁环节对应培育节点接收到数字签名密文 C 后,可通过私钥 k 解密 $C_1 - kC_2$,计算 $A + rK - k(rG) = A$,对点 A 解码就可以得到明文。以种苗资源保存环节和脱毒苗扩繁环节为例,数字签名机制如图 2 所示。

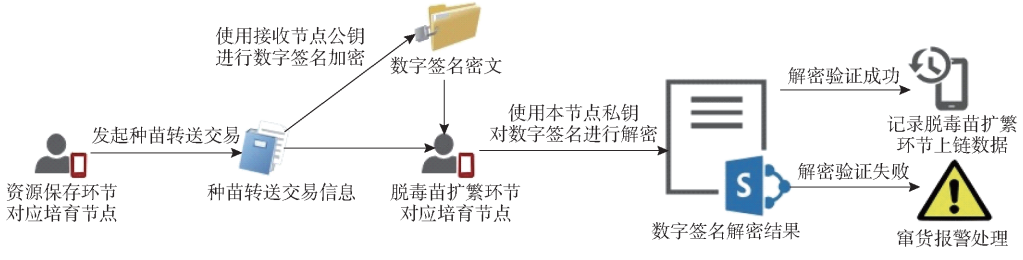


图 2 数字签名机制

Fig. 2 Digital signature mechanism

在种薯生产溯源区块链网络中,每个节点都拥有所有节点的公钥以及本节点的私钥,通过公私钥对严格匹配的策略确保种苗/薯转送接收环节对应培育节点的唯一正确性。例如,种苗在资源保存环节培育完毕,需要将其送往脱毒苗扩繁环节进行下一步培育,资源保存环节对应培育节点会在区块链网络中产生一个种苗转送交易,并使用脱毒苗扩繁环节对应接收节点的公钥对该交易进行数字签名加密。脱毒苗扩繁环节对应培育节点接收到需要进行下一步培育的种苗后,需使用本节点的私钥对该种苗转送交易进行数字签名解密验证。解密验证成功,则说明接收节点正确,可以记录脱毒苗扩繁环节相关上链数据;解密验证失败,则说明接收节点错误,可能发生窜货,此时会触发窜货报警处理,给予相关窜货报警提示,并将对应报警信息进行上链存储。

2.3 种薯防窜报警溯源模型

种薯生产基地培育品种繁多,除接收环节对应培育节点易发生窜货问题外,培育节点因错误识别种薯品种、等级等信息,致使种薯的培育方式发生改变、种薯成品混杂的情况也频繁发生,最终导致种薯整体生产效率和质量水平低下。解决种薯生产窜货问题是本文的研究重点,通过智能合约与数字签名相结合的方式实现防止种薯生产窜货的双层保障。在种薯生产溯源区块链中,每个相关环节间都需安装部署对应的区块链智能合约,在数字签名验证接收环节对应培育节点正确后,通过智能合约将当前种苗/薯与对应链上存储信息进行对比,符合窜货条件时触发窜货报警处理,实现防止种薯生产窜货的第 2 层保障。实物数据采集通过种薯生产全环节安装部署各种物联网设备获取,通过二维码等标识技术结合区块链种薯全生产链全连接溯源编码将实物

数据对应转化为数字数据并存入区块链中，所有生产环节都进行上述实物与链上数据的锚定。

智能合约是运行在区块链网络中的一种计算机协议，以代码的形式体现出该协议去中心化、自动执行、高确定性、高自治性等特点，区块链中的相关节点均安装部署对应智能合约则可以达到网络环境高度自治的效果。在本文所提出的种薯防窜报警溯源模型中，智能合约可以实现种薯全生产环节溯源数据的安全上链、按合约条件触发防窜报警机制、查询具体溯源数据等功能，实现对种薯生产全环节溯源数据的全方位正向记录、逆向溯源，为种薯生产基地提供强大的数据记录与查询、防止种薯生产窜货的技术支撑。利用智能合约完成种薯开始培育前的品种、等级等自动化确认，与前生产环节的上链信息进行对比验证，有效防止种薯生产窜货的问题，也为生产基地、消费者和相关监管部门等追溯用户提供安全可信的溯源信息。种薯防窜报警溯源模型如图 3 所示。

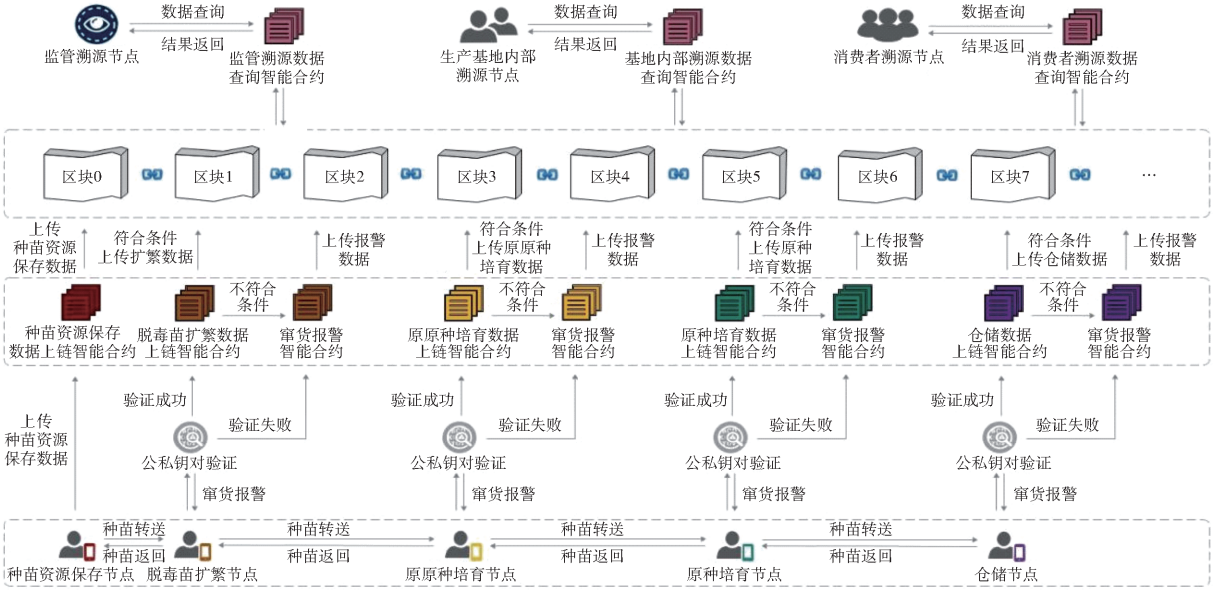


图 3　种薯防窜报警溯源模型

Fig. 3　Seed potato anti-channeling alarm traceability model

在该模型中，由于种苗资源保存环节是种薯生产全环节的初始环节，不存在生产窜货的发生，因此不在该环节中设计窜货报警智能合约，仅利用智能合约将相关生产溯源数据进行上链存储。脱毒苗扩繁及其后环节将对接收种苗/薯的实际情况与前环节上传的溯源数据进行对比分析，作为判断当前环节是否发生窜货的数据依据，同时将该溯源数据作为全部种薯生产溯源数据的一部分。种薯生产全环节将本环节培育完毕的种苗/薯送往至下一生产环节进行培育时，需要使用接收环节对应培育节点的公钥对种苗/薯转送交易进行数字签名加密，接收环节对应培育节点收到该种苗/薯时，需要使用本节点私钥对已加密的前环节种苗/薯转送交易进行数字签名解密验证。解密验证失败，则说明接收环节对应培育节点错误，此时通过智能合约触发相关窜货报警处理；解密验证成功，则说明接收环节对应培育节点正确，此时会自动调用智能合约要求该节点通过各种物联网设备获取并录入对应培育节点当前接收种苗/薯的品种、等级等信息，并与前环节相关节点存入区块链网络中的信息进行对比，全部符合则说明种苗/薯送至正确培育节点目的地，同时正确识别该种薯的品种、等级等信息，并正确安排其对应培育方式；有一项及以上不符合则说明种薯送至正确培育节点目的地，但错误识别该种苗/薯的品种、等级等信息，无法正确安排其对应培育方式，此时进行窜货报警处理，将种薯溯源编号、报警编号、报警时间、报警环节等相关窜货报警信息存储至区块链网络中，并给予相关窜货报警提示。此外，利用区块链存储数据的不可篡改等特性，使得种薯生产溯源数据在区块链溯源网络中得以可信存储，并利用不同数据查询智能合约实现不同追溯用户的溯源查询，种薯生产基地、消费者和相关监管部门可通过溯源节点调用对应数据查询智能合约获取区块链中对应种薯的相关溯源信息。

2.4　智能合约设计

本文使用 Hyperledger Fabric 平台，结合种薯种植领域专家意见、种薯生产基地的实际情况等制定相关的智能合约规则和一系列合约触发条件。智能合约业务逻辑设计如表 3 所示。

表 3 智能合约设计

Tab. 3 Smart contract design

合约功能	合约方法	描述	输入	输出
数据上链	createSeedPotatoes( )	将种薯基本信息写入区块链	种薯基本信息	True/False
	recordResourceGrow( )	将种苗资源保存环节溯源信息写入区块链,当发生窜货时触发防窜报警合约	种苗资源保存信息	True/False
	recordDetoGrow( )	将脱毒苗扩繁环节溯源信息写入区块链,当发生窜货时触发防窜报警合约	脱毒苗扩繁信息	True/False
	recordYuanssGrow( )	将原原种培育环节溯源信息写入区块链,当发生窜货时触发防窜报警合约	原原种培育信息	True/False
	recordYuansGrow( )	将原种培育环节溯源信息写入区块链,当发生窜货时触发防窜报警合约	原种培育信息	True/False
	recordWarehouseGrow( )	将仓储环节溯源信息写入区块链,当发生窜货时触发防窜报警合约	仓储信息	True/False
数据查询	querySeedPotatoesByBatchId( )	查询种薯基本信息	批次 ID	种薯基本信息
	queryResourceGrowByResourceId( )	查询种苗资源保存环节溯源信息	批次 ID/资源 ID	种苗资源保存信息
	queryDetoGrowByDetoxificateId( )	查询脱毒苗扩繁环节溯源信息	批次 ID/扩繁 ID	脱毒苗扩繁信息
	queryYuanssGrowByYuanssId( )	查询原原种培育环节溯源信息	批次 ID/原原种 ID	原原种培育信息
	queryYuansGrowByYuansId( )	查询原种培育环节溯源信息	批次 ID/原种 ID	原种培育信息
	queryWarehouseByWarehouseId( )	查询仓储环节溯源信息	批次 ID/仓储 ID	仓储信息
防窜报警	recordWarn( )	将窜货报警信息写入区块链	窜货报警信息	True/False
	queryWarnInfoByWarnId( )	查询窜货报警信息	报警 ID	窜货报警信息

将种薯各生产环节的溯源信息写入区块链均由智能合约实现。在各环节上传对应生产溯源信息时,如果发生窜货则会触发防窜报警智能合约,接续进行防窜报警处理。具体算法如下:

算法 1:发送方数据上链智能合约

输入:以种苗资源保存环节为例,批次编号 BatchId,资源编号 ResourceId,种苗名称 SeedName,品种名称 BreedName 等

输出:上链成功返回交易 ID,区块高度 numBlock,数据哈希 dataHash,前一个区块哈希 previousHash,上链失败返回错误原因

区块链中的种苗资源保存环节对应 peer 节点发起 invoke 上链请求

if len(args) //判断请求中的数组长度是否符合规定长度标准

return shim. Error; //数组长度不符合标准,上链失败,返回具体错误原因

else //符合上链要求,请求上链

ECDSA_Encode( ); //使用接收节点公钥加密

APIstub. PutState (args [2], resourceGrowInfoAsBytes);

return success; //返回交易基本信息

算法 2:接收方数据上链智能合约

输入:以脱毒苗扩繁环节为例,批次编号 BatchId,种苗名称 SeedName,扩繁编号 DetoxificateId,品种名称 BreedName 等

输出:上链成功返回交易 ID,区块高度 numBlock,数据哈希 dataHash,前一个区块哈希 previousHash,上链失败返回错误原因

区块链中的脱毒苗扩繁环节对应 peer 节点发起 invoke 上链请求

if len(args) //判断请求中的数组长度是否符合长度标准

err : = ECDSA _ Decode; // 使用本节点私钥解密

if err ! = nil //判断私钥是否解密成功

recordWarn( ); //解密失败,触发防窜报警合约

return shim. Error; //返回具体错误原因

else //解密成功

if args[1] ! = resourceBatchIdGrow //判断请求中的批次 ID 是否与前生产环节对应上链数据相符

recordWarn( ); //如果批次 ID 不符则触发防窜报警合约

return shim. Error; // 上链失败,返回具体错误原因

elseif args[2] ! = resourceResourceIdGrow //判断请求中的资源 ID 是否与前生产环节对应上链数据相符

recordWarn( ); //如果资源 ID 不符则触发防窜报警合约

return shim. Error; // 上链失败,返回具体错误原因

elseif args[3] ! = resourceSeedNameGrow //判断请求中的种苗名称是否与前生产环节对应上链数据相符

recordWarn( ); //如果种苗名称不符则触发防窜报警合约

return shim. Error; //上链失败,返回具体错误原因

elseif args[4] ! = resourceBreedNameGrow //判断请求中的品种名称是否与前生产环节对应上链数据相符

recordWarn( ); //如果品种名称不符则触发防窜报警合约

return shim. Error; //上链失败,返回具体错误原因

else //符合上链要求,请求上链

APIstub. PutState (args [5], detoxificateGrowInfoAsBytes);

return success; //返回交易基本信息

窜货报警智能合约将触发窜货报警时的相关报警信息进行上链存储。具体算法如下:

算法 3:窜货报警智能合约

输入:种薯当前编号 NowSeedPotatoId,报警时间 WarnTime,报警环节 WarnLink 等

输出:上链成功返回交易 ID,区块高度 numBlock,数据哈希 dataHash,前一个区块哈希 previousHash,上链失败返回错误原因

触发防窜报警时发起报警数据上链请求

if len(args) //判断请求中的数组长度是否符合规定长度标准

return shim. Error; //数组长度不符合标准,上链失败,返回具体错误原因

var warnInfo = WarnInfo{BatchId: args[1], NowSeedPotatoId: args [2], WarnId: args [3], WarnTime: args [4], WarnLink: args [5], WarnPoint: args [6], WorkerId: args [7], WorkerName: args[8]}; //将报警信息存入待上链数组

APIstub. PutState (args[2], warnInfoAsBytes); //请求上链

return success; //返回交易基本信息

数据查询智能合约在区块链中通过用户输入的查询编号进行对应的数据查询。具体算法如下:

算法 4:数据查询智能合约

输入:以查询窜货报警信息为例,报警编号 WarnId

输出:报警编号对应的具体信息

if len(args) //判断请求中的数组长度是否符合规定长度标准

return shim. Error; //查询失败,返回具体错误原因

warnInfoAsBytes, _ : = APIstub. GetState (args [0]); //通过当前 Key 值获取对应 Value 值

retrun success; //查询成功,返回数据

3　系统设计与实现

3.1　系统架构设计

本研究基于 Hyperledger Fabric 构建面向种薯生产全环节溯源的模型架构,通过区块链技术对溯源数据进行管理和维护,实现种薯生产全环节溯源数据的高度共享;种薯各生产环节分布式上传本环节内的溯源数据,并利用数字签名结合智能合约的方式高效防止生产窜货的发生,保证各生产环节种薯溯源数据的真实性、实时性以及安全性。种薯生产溯源模型架构如图 4 所示,共分为 4 层,由下至上分别为存储层、服务层、接口层和应用层。

存储层利用区块链技术不可篡改等特点,实现所有相关节点共同维护同一个数据账本,且所有交易操作均记录对应时间戳,确保生产溯源数据的真实可靠。同时,为减少种薯溯源的查询时间,溯源数据通过面向文档的数据库管理系统(Cluster of unreliable commodity hardware database,CouchDB)存储,并通过 Key - Value 键值索引进行数据查询;服务层采用 Raft 共识机制,以智能合约为具体实现方式,结合 ECDSA 椭圆曲线数字签名算法,保证种薯生产全环节溯源数据的成功上链,实现防止生产窜货的自动处理;接口层面向种薯生产过程中的 5 个关键溯源环节和 1 个窜货报警环节,封装相关溯源数据公钥加密接口、私钥解密接口以及对于种薯生产溯源数据和窜货报警数据上链接口和查询接口,满足种薯生产全环节的溯源数据共享、查询以及防止生产窜货的发生等需求;应用层通过系统为种薯生产全环节的相关方提供不同的便捷服务。

3.2　系统实现

本文所提出的马铃薯种薯防窜溯源模型应用于云南省马铃薯种薯质量溯源系统,种薯生产全环节节点通过对应区块链接口在该系统中实现种薯生产溯源数据的上传及查询功能,系统网络中的所有节点共享一个区块链分布式帐本,共同参与全网的共识记账。如图 5a 所示,种薯生产过程中的 5 个关键环节均可以上传相关溯源信息。上传成功,则会在系统中生成相应的环节编号,并在状态栏显示成功,同时会显示该上传操作交易在区块链网络中生成的

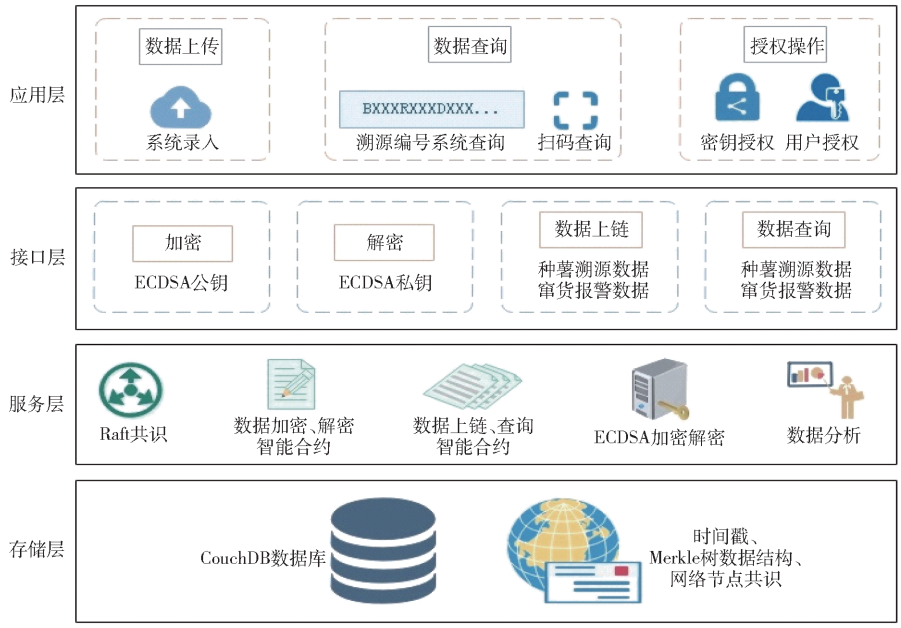
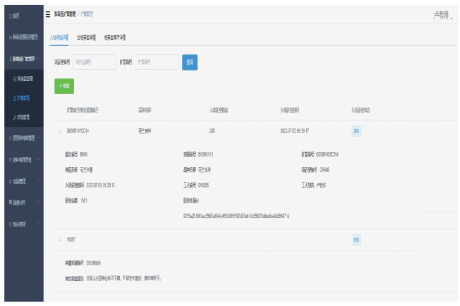
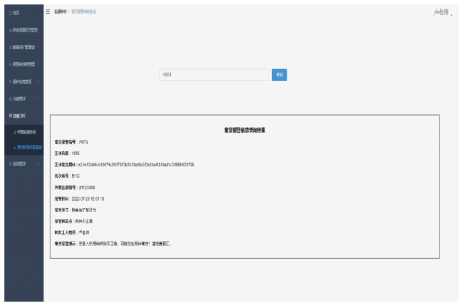


图 4 种薯生产溯源模型架构

Fig. 4 Model architecture of seed potato production traceability



(a) 溯源信息上传



(b) 窜货报警信息查询

图 5 云南省马铃薯种薯质量溯源系统界面

Fig. 5 Yunnan seed potato quality tracing system interface

区块高度以及区块交易 ID;上传失败,则会在系统中生成相应的窜货报警编号,在状态栏中显示失败,并给出窜货报警提示。如图 5b 所示,可根据窜货报警编号查询对应窜货报警的详细信息。在该系统中设有用户节点权限机制,用户节点只能进行本环节内的相关种薯生产溯源信息上传等操作,不能进行其他环节的相关操作。同时,所有生产环节生成的交易操作信息、种薯溯源信息和窜货报警信息的详情全部用户节点均可查看,可用来监督种薯生产全环节间共享原始数据。

同时,为满足相关用户溯源需求,种薯质量溯源系统提供扫码溯源功能,可通过扫描种薯外包装上的二维码获取相关生产溯源数据。如图 6 所示,经过查询后,可获取产品介绍信息、企业信息、溯源信息和防伪信息。其中溯源信息展示种薯生产全环节的关键数据,防伪信息展示区块链地址、追溯 Hash 值、区块高度等信息。

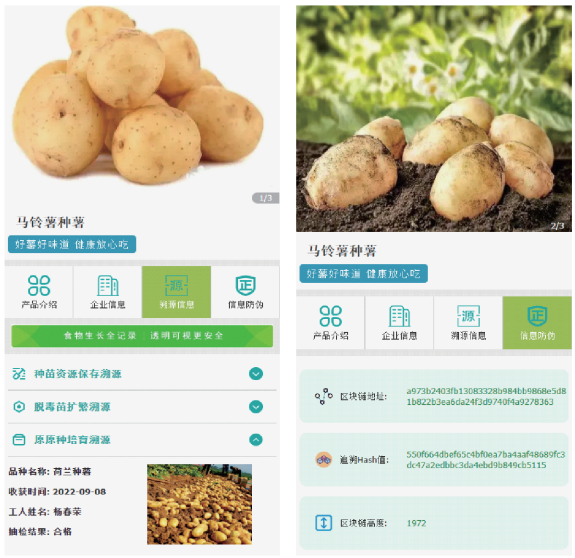


图 6 扫码溯源界面

Fig. 6 Scanning code tracing interface

4 系统测试

4.1 测试环境

本研究的测试环境基于 Hyperledger Fabric 1.4.4、Hyperledger Explorer 1.1.8 搭建,使用虚拟机系统版本为 Ubuntu 16.04 LTS。性能测试将智能合约通过 balance-transfer 接口进行封装,使用外

部接口测试工具 Postman 9.31.0 进行 30 轮次的测试。硬件配置为：4 GB 内存、8 核处理器、50 GB 硬盘。区块链通过 16 个节点存储种薯生产溯源数据，其中包含种苗资源保存节点、脱毒苗扩繁节点、原原种培育节点、原种培育节点、窜货报警节点、外部溯源节点各 2 个，另外包含仓储节点 4 个。种薯区块链中的所有节点均采用状态数据库 CouchDB 存储上链数据，通过 Key－Value 键值对检索状态数据库查询相应数据。具体测试环境配置如表 4 所示。

表 4　区块链配置信息

Tab. 4　Configuration information of blockchain

区块链配置	数值	描述
链数	1	种薯生产基地的 5 个生产环节、1 个防窜报警环节和相关溯源节点共同维护一个区块链分布式账本
组织数量	7	种苗资源保存组织、脱毒苗扩繁组织、原原种培育组织、原种培育组织、仓储组织、窜货报警处理组织、外部组织
节点数量	16	种苗资源保存组织、脱毒苗扩繁组织、原原种培育组织、原种培育组织、窜货报警处理组织、外部组织各包含 2 个节点，仓储组织包含 4 个节点
数据库	CouchDB	整个区块链采用 CouchDB 状态数据库存储上链数据
共识机制	Raft	采用 Raft 共识机制使区块链中的所有节点共同维护账本一致性
出块时间/s	2	发布交易并打包生成区块的时间
区块最大交易数量	100	每个区块中所包含的最大交易数量
区块最大容量/MB	100	每个区块中存储数据的最大容量
每条交易最大占据存储空间/KB	512	每条交易的存储大小，最大为 512 KB

4.2　窜货报警功能分析

测试以脱毒苗扩繁环节接收种苗进行下一阶段培育，将该接收种苗的相关信息进行上链为例。如图 7a 所示，如果脱毒苗扩繁环节对应培育节点私钥解密失败，或申请入培养室时上传的种苗相关信息与区块链账本中存储的该种苗对应品种、等级等信息不符时，则将该上链申请给予窜货报警处理，并给出窜货报警原因提示。如图 7b 所示，通过 Hyperledger explorer 显示该窜货报警交易所在区块信息，其中区块高度（区块号）为 2701，区块哈希为 6939b143ab66e4db59e89ee9c6c9612461fbf1daba85236ac0e1b2908341fa8b，前一区块哈希为 99bc65133e24ad81bf3cbdcc7a87e97084aee88d0081ad4e67cbdc1911018371。窜货报警交易详情如图 7c 所示，其中交易 ID 为 b3a2c205f71c2fd17c58e3c9cae0e4262fd946f3be6019e86f87b0838948c12d，调用链码为 alarmcc，写入账本的 Key 为“W230”（窜货报编号）、Value 为“batch_id：B288，trace_seed_potato_id：B288R016，warn_id：W230，warn_time：2022－11－25 11：50：18，warn_link：脱毒苗扩繁环节，warn_point：私钥解密失败，worker_id：DW018，worker_name：袁艺”（种薯溯源编号、窜货报警时间、环节、触发点）等信息。

(a) 窜货报警触发

(b) 窜货报警交易所在区块信息

(c) 窜货报警交易信息

图 7　防窜报警功能测试

Fig. 7　Function test of anti-channeling alarm

4.3　数据上链与查询性能分析

4.3.1　种薯生产溯源数据上链与查询

数据上链性能测试结果如图 8a 所示，种薯生产溯源数据的平均上链时间为 2 566 ms，能够满足种薯生产基地全环节实时更新种薯溯源数据的需求；数据查询性能测试结果如图 8b 所示，种薯生产溯源数据的平均查询时间为 95 ms，能够满足相关溯源用户快速查询种薯各项生产信息的需求；由测试结果可以得出，该种薯防窜溯源区块链的数据上链和数据查询效率较高，可以满足各相关用户的日常需求。

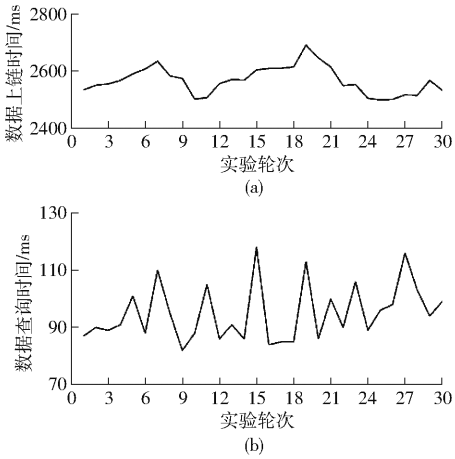


图 8 数据上链与查询性能测试

Fig. 8 Performance testing of data link and query

4.3.2 窜货报警触发上链与查询

种薯生产溯源防窜设计是基于智能合约和数字签名实现的,在某种程度上,这两种方式的结合可以在种薯生产过程中高度防止窜货的发生。因此,本研究在防窜货的报警触发与报警信息上链和查询的平均时间方面进行性能分析。测试结果如图 9 所示,报警触发与报警信息上链的平均时间为2 562 ms,查询具体报警信息的平均时间为77 ms。由测试结果可以得出,该种薯防窜溯源区块链的防窜报警性能较好,可以满足种薯生产基地的相关需求。

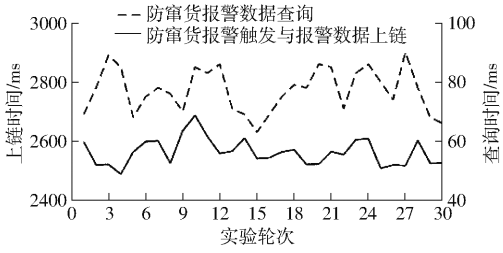


图 9 防窜货性能测试

Fig. 9 Performance testing of anti-channeling cargo

5 结论

(1)提出了基于智能合约和数字签名的马铃薯种薯防窜溯源模型,对种薯的整个生产环节建立溯源区块链,使种薯生产全环节共同维护一个区块链分布式帐本,保证种薯生产溯源数据的统一共享;通过数字签名公私钥对验证和智能合约联合解决种薯生产过程中的窜货问题,防止生产窜货,提高生产溯源效率和准确率,满足种薯生产基地的标准化生产需求。

(2)提出的防窜溯源模型能够实现种薯溯源数据的安全存储,并高度防止生产窜货的发生。相关测试结果表明,种薯生产溯源数据的平均上链时间为 2 566 ms,平均查询时间为 95 ms,报警触发与报警信息上链的平均时间为 2 562 ms,查询具体报警信息的平均时间为 77 ms,模型性能较高,可以满足种薯生产溯源数据的上链与查询需求,在防止种薯生产窜货方面具有一定的参考价值。

参 考 文 献

[1] 尚晋伊,史小峰. 中国马铃薯主食产业化发展现状与前景展望[J]. 科技资讯,2018,16(21):109 - 111,115.
SHANG Jinyi, SHI Xiaofeng. Present situation and prospect of potato staple industrialization in China[J]. Science & Technology Information, 2018,16(21):109 - 111,115. (in Chinese)

[2] 罗其友,伦闰琪,高明杰,等. 2021—2025 年我国马铃薯产业高质量发展战略路径[J]. 中国农业资源与区划,2022,43(3):37 - 45.
LUO Qiyou, LUN Runqi, GAO Mingjie, et al. Strategy path of high-quality development of potato industry in China from 2021 to 2025[J]. Chinese Journal of Agricultural Resources and Regional Planning, 2022,43(3):37 - 45. (in Chinese)

[3] 罗其友,高明杰,张烁,等. 中国马铃薯产业国际比较分析[J]. 中国农业资源与区划,2021,42(7):1 - 8.
LUO Qiyou, GAO Mingjie, ZHANG Shuo, et al. Comparative analysis on potato industry between China and other countries[J]. Chinese Journal of Agricultural Resources and Regional Planning, 2021,42(7):1 - 8. (in Chinese)

[4] 姚妮娜,刘石祥. 对马铃薯种薯质量控制体系建设的思考[J]. 种子科技,2019,37(14):116 - 117.
YAO Ni'na, LIU Shixiang. Consideration on the construction of quality control system of seed potato[J]. Seed of Science and Technology, 2019,37(14):116 - 117. (in Chinese)

[5] 胡柏耿,梁希森,孙莎莎,等. 马铃薯种质资源现状及可溯源系统建设[J]. 农业工程技术,2020,40(6):43 - 44.
HU Baigeng, LIANG Xisen, SUN Shasha, et al. Present situation of potato germplasm resources and construction of traceability system[J]. Agricultural Engineering Technology, 2020,40(6):43 - 44. (in Chinese)

[6] 申宇. 马铃薯种薯质量溯源平台的设想与实现[J]. 信息技术,2016(9):202 - 204.
SHEN Yu. Conceive and application of traceability platform of seed potatoes quality[J]. Information Technology, 2016(9):202 - 204. (in Chinese)

[7] 张福金. 内蒙古马铃薯质量优势与溯源鉴别关键技术研究[D]. 呼和浩特:内蒙古自治区农牧业科学院,2020:12 - 18.
ZHANG Fujin. Research on key technologies of quality superiority and traceability identification of Inner Mongolia potato[D]. Huhhot:Inner Mongolia Academy of Agricultural & Animal Husbandry Sciences, 2020:12 - 18. (in Chinese)

[8] 李小平,闫富海,马世军. 种子防伪防窜货管理系统研究[J]. 安徽农业科学,2018,46(26):188 - 190.
LI Xiaoping, YAN Fuhai, MA Shijun. Research on the management system for anti-counterfeiting and anti-fleeing goods[J]. Journal of Anhui Agricultural Sciences, 2018,46(26):188 - 190. (in Chinese)

[9] 孙传恒,于华竟,徐大明,等. 农产品供应链区块链追溯技术研究进展与展望[J]. 农业机械学报,2021,52(1):1 - 13.
SUN Chuanheng, YU Huajing, XU Daming, et al. Review and prospect of agri-products supply chain traceability based on

blockchain technology[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021,52(1):1 - 13. (in Chinese)
[10] 李旭东,杨千河,姚竟发,等. 基于区块链的农产品溯源技术研究综述[J]. 江苏农业科学,2022,50(6):16 - 24.
LI Xudong, YANG Qianhe, YAO Jingfa, et al. Study on traceability technology of agricultural products based on blockchain: a review[J]. Jiangsu Agricultural Sciences, 2022,50(6):16 - 24. (in Chinese)
[11] 张哲,杨信廷,于合龙,等. 基于区块链技术的生鲜农产品溯源系统研究进展[J]. 农业大数据学报,2022,4(1):25 - 34.
ZHANG Zhe, YANG Xinting, YU Helong, et al. Progress of research to develop a traceability system for fresh agricultural products using blockchain technology[J]. Journal of Agricultural Big Data, 2022,4(1):25 - 34. (in Chinese)
[12] 邢斌,于华竟,徐大明,等. 基于区块链的红茶质量安全追溯系统开发及应用[J]. 中国农机化学报,2022,43(11):133 - 138.
XING Bin, YU Huajing, XU Daming, et al. Development and application of traceability system for black tea based on blockchain[J]. Journal of Chinese Agricultural Mechanization, 2022,43(11):133 - 138. (in Chinese)
[13] 刘家稷,杨挺,汪文勇. 使用双区块链的防伪溯源系统[J]. 信息安全学报,2018,3(3):17 - 29.
LIU Jiaji, YANG Ting, WANG Wenyong. Traceability system using public and private blockchain[J]. Journal of Cyber Security, 2018,3(3):17 - 29. (in Chinese)
[14] WANG L, XU L, ZHENG Z, et al. Smart contract-based agricultural food supply chain traceability[J]. IEEE Access, 2021, 9: 9296 - 9307.
[15] FERRANDEZ-PASTOR F J, MORA-PASCUAL J, DIAZ-LAJARA D. Agricultural traceability model based on IoT and blockchain: application in industrial hemp production[J]. Journal of Industrial Information Integration, 2022, 29: 100381.
[16] SALAH K, NIZAMUDDIN N, JAYARAMAN R, et al. Blockchain-based soybean traceability in agricultural supply chain[J]. IEEE Access, 2019, 7: 73295 - 73305.
[17] QIU Z, ZHU Y F. Traceability anti-counterfeiting system based on the ownership of edge computing on the blockchain[J]. Journal of Ambient Intelligence and Humanized Computing, 2023,14(1): 257 - 270.
[18] 刘双印,雷墨鸳兮,徐龙琴,等. 基于区块链的农产品质量安全可信溯源系统研究[J]. 农业机械学报,2022,53(6):327 - 337.
LIU Shuangyin, LEI Moyixi, XU Longqin, et al. Development of reliable traceability system for agricultural products quality and safety based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022,53(6):327 - 337. (in Chinese)
[19] 孙传恒,于华竟,罗娜,等. 基于智能合约的果蔬区块链溯源数据存储方法研究[J]. 农业机械学报,2022,53(8):361 - 370.
SUN Chuanheng, YU Huajing, LUO Na, et al. Blockchain traceability data storage method of fruit and vegetable foods supply chain based on smart contract[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(8): 361 - 370. (in Chinese)
[20] LIN W, HUANG X, FANG H, et al. Blockchain technology in current agricultural systems: from techniques to applications [J]. IEEE Access, 2020, 8: 143920 - 143937.
[21] DEMESTICHAS K, PEPPES N, ALEXAKIS T, et al. Blockchain in agriculture traceability systems: a review[J]. Applied Sciences, 2020, 10(12): 4113.
[22] 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 - 315,345.
YI Weiguo, HE Jianguo, LIU Guishan, et al. Development and implementation of blockchain to enhance traceability and reliability of fruit and vegetable quality[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022,53(2): 309 - 315,345. (in Chinese)
[23] 赵巧润,曹宇璇,曹怡凡,等. 互联网 + 区块链技术在食品安全溯源体系中的应用及研究进展[J]. 食品工业科技,2023, 44(6):24 - 32.
ZHAO Qiaorun, CAO Yuxuan, CAO Yifan, et al. Application and research progress of Internet + blockchain technology in food safety traceability system[J]. Science and Technology of Food Industry, 2023,44(6):24 - 32. (in Chinese)
[24] KATSIKOULI P, WILDE A S, DRAGONI N, et al. On the benefits and challenges of blockchains for managing food supply chains[J]. Journal of the Science of Food and Agriculture, 2021, 101(6): 2175 - 2181.
[25] 邱彩玲,申宇,高艳玲,等. 中国马铃薯种薯生产及质量控制[J]. 中国马铃薯,2019,33(4):249 - 254.
QIU Cailing, SHEN Yu, GAO Yanling, et al. Seed potato production and quality control in China[J]. Chinese Potato Journal, 2019,33(4):249 - 254. (in Chinese)
[26] HEWA T, YLIANTTILA M, LIYANAGE M. Survey on blockchain based smart contracts: applications, opportunities and challenges[J]. Journal of Network and Computer Applications, 2021, 177: 102857.
[27] 吴烨. 智能合约:通过合同的自治框架[J]. 河南财经政法大学学报,2022,37(5):42 - 53.
WU Ye. Smart contracts: self-governance framework through contracts[J]. Journal of Henan University of Economics and Law, 2022,37(5):42 - 53. (in Chinese)
[28] 王方鑫. 基于椭圆曲线的签名方案[J]. 电脑知识与技术,2019,15(1):53,60.
WANG Fangxin. Signature scheme based on elliptic curve[J]. Computer Knowledge and Technology, 2019,15(1):53,60. (in Chinese)
[29] 汪潇潇,程鸿芳. 浅析椭圆曲线数字签名的研究与发展[J]. 科技风,2020(34):90 - 91.
WANG Xiaoxiao, CHENG Hongfang. The analysis of the research and development of elliptic curve digital signature[J]. The Wind of Science and Technology, 2020(34):90 - 91. (in Chinese)
[30] 吴奕,仲盛. 区块链共识算法 Raft 研究[J]. 信息网络安全,2021,21(6):36 - 44.
WU Yi, ZHONG Sheng. Research on Raft consensus algorithm for blockchain[J]. Netinfo Security, 2021,21(6):36 - 44. (in Chinese)