doi:10.6041/j.issn.1000-1298.2022.05.029

面向猕猴桃质量溯源的联盟链跨组织链上合同交易机制

景　旭　秦源泽

（西北农林科技大学信息工程学院，陕西杨凌 712100）

摘要：针对区块链猕猴桃溯源未考虑产业链由不同组织构成而导致溯源数据不连续的问题，结合生产实践中合同交易的过程，提出了一种面向猕猴桃质量溯源的联盟链跨组织链上合同交易机制。通过两次链上的关联确认，将现实交易中双方签字确认合同条款的过程转移到联盟链上，实现跨组织的不可否认交易。选择联盟链搭建猕猴桃全产业链溯源系统的区块链网络，借助智能合约技术将猕猴桃生产过程信息价值化；采用散列值上链减轻链上压力；通过组织间交易合同的合同编号关联溯源数据、责任人和责任企业。基于 Hyperledger Fabric 猕猴桃全产业链溯源系统的测试分析表明，用户每上链一条数据平均用时约 102 ms，在增加链上合同交易机制的条件下系统进行一次完整溯源的时间延长了约 7.11 ms。研究保证了多组织溯源的数据连续性与可追溯性，对提升农产品质量安全具有重要意义。

关键词：联盟链；Hyperledger Fabric；质量溯源；链上合同交易；猕猴桃

中图分类号：TP391　　**文献标识码**：A　　**文章编号**：1000-1298(2022)05-0282-09　　**OSID**：

Consortium Blockchain Inter-organizational Contract Transaction Mechanism for Kiwi Fruit Quality Traceability

JING Xu　QIN Yuanze

(*College of Information Engineering*, *Northwest A&F University*, *Yangling*, *Shaanxi* 712100, *China*)

Abstract: To solve the problem caused by the ignorance of organization-compositional diversity in blockchain-based kiw fruit traceability system, a consortium blockchain inter-organizational contract transaction mechanism for kiwi fruit quality traceability was proposed. Through two link confirmations on the blockchain, the process of signing and confirming the terms of the contract in the actual transaction was transferred to the consortium blockchain, so as to realize the cross-organization incontestable transaction. The consortium blockchain was chosen to construct the blockchain network for kiwi fruit industry chain traceability system, the smart contract technology was used to make the information of the kiwi fruit production process valuable, and the Hash value was used to light the on-blockchain stress. The transaction contract number was used to realize the association of the trace data, responsible person and responsible enterprise. Result of test analysis showed that each piece of data on the blockchain was about 102 ms. The time of one complete traceability was extended by about 7.11 ms. When on-blockchain contract transaction was increased. The research ensured the data continuity and traceability of multi-organization tracing, which was of great significance to improve the quality and safety of agricultural products.

Key words: consortium blockchain; Hyperledger Fabric; quality traceability; on-blockchain contract transactions; kiwi fruit

0　引言

基于区块链技术实现农产品溯源，可以有效提升信息的完整性、可追溯性及可信性，能实现多个主体协作信任，有利于供应链管理的技术创新与模式升级[1-2]，对于提升农产品的质量保障，进而从食源

收稿日期：2021-06-24　修回日期：2021-08-29

基金项目：陕西省重点研发计划项目(2019ZDLNY07-02-01)和国家重点研发计划项目(2020YFD1100601)

作者简介：景旭(1971—)，男，副教授，主要从事农业信息化、信息系统安全和区块链技术研究，E-mail：jingxu@nwsuaf.edu.cn

上保证人民生命健康具有重要意义。

基于区块链技术的特点，国内外学者在农产品溯源方面开展了广泛的研究。YANG 等[3]针对农产品追溯系统提出了基于 q - ROF 集（q - Rung orthopair fuzzy）的设计模型选择决策算法。GEORGE 等[4]提出了基于区块链和产品标识符的餐厅溯源模型，从供应链的不同利益相关者获取数据并分离，应用食品质量指数（Food quality index，FQI）算法生成 FQI 值。许继平等[5]提出了适用于粮油食品供应链的双模型存储机制和管理供应链信息的智能合约，实现了粮油食品供应链信息的采集、查询、监控和追溯。葛艳等[6]提出了基于区块链的危害分析及关键控制点（Hazard analysis and critical control points，HACCP）的质量溯源模型，设计智能合约实现溯源数据的上下链和质量自动判断。任守纲等[7]基于信誉监督机制改进了拜占庭容错算法，构建了基于联盟链的农作物全产业链信息溯源平台。可以看出，在现有基于区块链的农产质量溯源研究中，基本上均假设整个产业链的生产活动在一个组织内完成，并通过一个固定溯源码将各环节的生产信息依次记录在区块链中，按照既定溯源码反向追溯实现溯源。它仅适用于单组织管理的产业链溯源，没有考虑产业链分为多个组织后跨组织溯源的问题，导致不同组织在账本中的数据缺乏逻辑上的连续性与完整性。

在实际农业生产环境中，农资供应、田间生产、场内加工与储藏、电商销售等生产环节在时间和空间上跨度均比较大[8]，所以每个生产环节基本由相互独立的组织承担，在同一个组织内部的不同环节也基本由相互独立的部门承担。不同组织的生产溯源信息通过组织间的合同交易关联，合同交易一般依赖第三方中心机构管理。合同交易时，采购商向供应商发起采购意向书，供应商拟定合同，与采购商签署交易合同。双方均对合同签名，合同生效，交易完成。

针对上述问题，结合生产实践中合同交易的过程，提出一种面向猕猴桃质量溯源的联盟链跨组织链上合同交易机制。将现实供应链中交易双方对合同条款签字确认的过程，转移到联盟链上。通过两次链上的关联确认，实现跨组织的不可否认交易。保证交易双方权益，无需依赖第三方中心机构管理，更好地发挥供应链的不同组织在溯源体系中的作用。本文选择联盟链搭建猕猴桃全产业链溯源系统的区块链网络，借助智能合约技术将猕猴桃生产的过程信息价值化；采用散列值上链减轻链上压力；通过组织间交易合同的合同编号关联产业链的溯源数据、责任人和责任企业，组织与组织间的交易合同可使猕猴桃在全产业链的溯源数据在链上具有逻辑连续性，当单节点伪造数据时，其他环节信息无法追溯，可快速定位到问题组织。

1　基于联盟链的猕猴桃全产业链溯源体系结构

按照开放程度，区块链可以划分为公有链[9]、私有链[10]和联盟链[11]。公有链的访问门槛低、节点数目过多、共识时间较长、交易速度慢，不符合交易频繁的区块链溯源系统对性能和效率的要求。私有链由中心机构管理，交易不需要所有节点确认，违背了去中心化的初衷[12]，链上数据存在被私自修改的可能，不能从根本上解决作弊问题。联盟链是由多个机构共同管理的组织体系，联盟链的 Fabric ca 身份认证服务依赖于 PKI 体系[13]和密码技术[14]以保证网络具有安全可靠的准入制；联盟链有灵活的智能合约[15]定制机制，可以满足供应链不同组织复杂多变的业务需求；联盟链可以支持多种共识机制[16]，交易效率较高，可以满足用户无感知的溯源需求[17]。在猕猴桃全产业链溯源中，产业链的上下游主体在现实中既存在竞争关系，也有一定信任关系，构成天然的联盟组织链条[18-19]，因此本研究选用联盟链搭建猕猴桃全产业链溯源系统的区块链网络。通过分析猕猴桃从农业合作社采购生产资料、田间生产到销售、运输至消费者手中的整个产业链，本研究将猕猴桃全产业链分为农资采购、种植采摘、生产加工、质检、销售物流等 5 个生产环节。每个生产环节由相互独立又相互依赖的组织承担，构成联盟链中的组织单位，包括农资电商、农业合作社、加工厂、质检部门、电商平台。联盟各个组织在实际生产中是相互独立的实体，除了农资电商、电商平台无生产环节外，其余生产组织均有产、购、储、加、销等环节，而各个组织联合在一起构成了猕猴桃完整的产业链。

每个组织详细记录猕猴桃当前生产过程的数据，包括生产基本信息、物联网设备实时监测数据、生产活动记录等。通过跨组织链上合同交易机制，完成以上 5 个组织生产活动溯源数据的链接，构成全产业链的数据链条闭环。以消费者的订单号作为溯源码，消费者通过溯源码在账本中查询该批次猕猴桃在联盟链内不同生产阶段的交易合同编号，完成猕猴桃在各个生产组织有关产地、猕猴桃品质等溯源信息查询。消费者仅能溯源猕猴桃质量相关的数据，监管部门溯源到每个生产环节的责任企业和责任人。基于联盟链的猕猴桃全产业链溯源体系结构如图 1 所示。

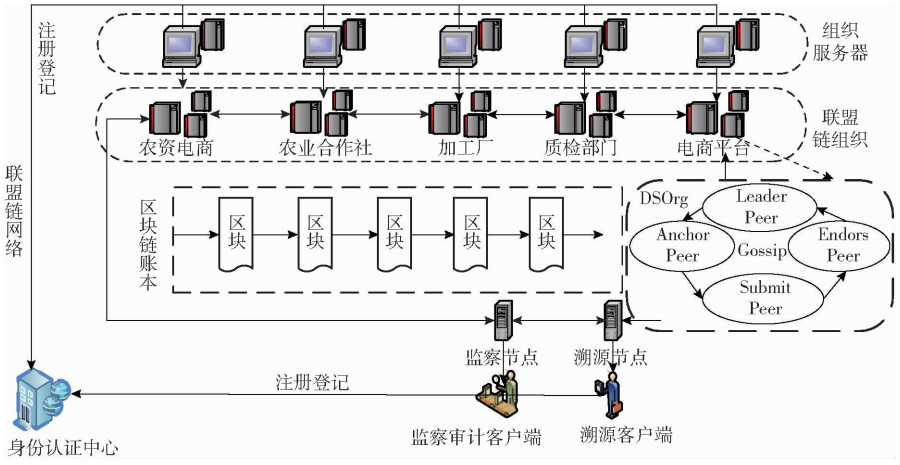


图 1 基于联盟链的猕猴桃全产业链溯源体系结构

Fig. 1 Traceability architecture of kiwi fruit industry chain based on consortium blockchain

在图 1 中,各组织通过分工合作形成产业链。农资电商平台负责猕猴桃生产资料的采购、储藏和销售。农业合作社负责农资采购和猕猴桃的种植、施肥、喷药、采摘和销售等过程。加工厂负责猕猴桃的采购、分拣、脱毛、糖检等,并按照品质为猕猴桃商品装箱、冷库储藏和销售。质检部门负责猕猴桃的质量检测。电商平台负责猕猴桃商品采购、销售和物流。组织平台的 Web 服务器通过建立资源客户端与区块链网络节点连接,使用代表合法身份的数字证书[20]与公钥私钥[21]证明身份,调用已安装的智能合约在联盟中进行交易。

在图 1 中,通过组织间的协同与链上合同交易实现产业链的监督。通过对比跨组织的采购合同与销售合同数量,监管部门可实现跨组织全产业链的监管;通过农资采购量、生产环境数据可预估合作社的产量,比对合作社销售量与预估值,判断合作社是否使用劣质农资;通过比对加工厂采购量与销售量,判断加工厂是否采购劣质猕猴桃;通过电商平台采购量与销售量比对,判断是否存在电商平台采购劣质猕猴桃。监管部门通过比对各个组织在账本中的采购合同与销售信息可监管每个环节交易量,实现猕猴桃全产业链的质量监测,以及发生质量问题时可追责至具体企业与责任人。

2 联盟链内跨组织链上合同交易机制

在联盟链的合同交易过程中,交易合同由联盟链内所有组织成员节点共同管理。不同阶段的合同交易业务对应不同链码,客户端通过 SDK 提供的 API 构建交易提案请求,并使用代表客户端合法身份的证书对交易签名(sign),sign 过程对应实际供应链交易方签署合同的过程。客户端发起交易提案后,将事务提交给背书节点进行背书签名;收集到足够数量的签名后,将交易发送给排序节点打包成区块;区块被发送到主节点,主节点传播给记账节点,完成记账后交易结束。利用灵活的智能合约体系和联盟链的不可篡改[22]、时间戳[23-24]等特性,可以有效地将繁杂耗时的合同签署过程用交易双方两次链上合同交易生成交易的方式保存在区块链账本中。

以加工厂与电商组织的交易流程为例,联盟链内跨组织链上合同交易流程如图 2 所示。

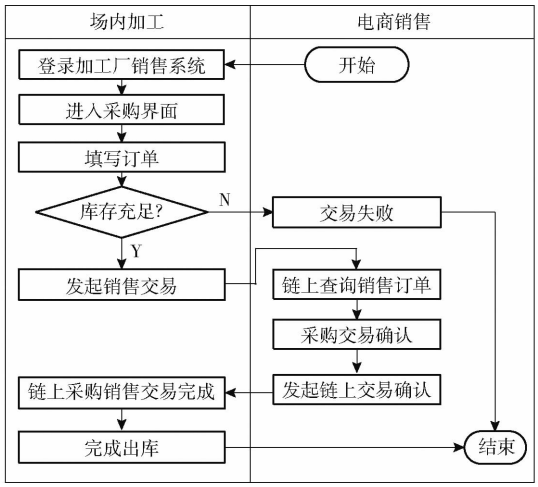


图 2 联盟链内跨组织链上合同交易流程

Fig. 2 Cross-organization contract transaction process within consortium blockchain

详细步骤包括:

(1)电商采购方按照采购计划在加工厂销售平台填写采购单,包括品名、数量、价格、交易平台信息、采购人信息等,系统生成一个采购单号(SaleOrderNum)。为将责任实体信息与采购信息关联,以保证责任实体信息完整性和减轻链上压力,采用 sha256 安全散列算法[25]生成实体信息的散列值,将实体信息标识、实体信息的散列值和采购信息共同上链。采购订单的具体数据项见表 1。

(2)加工厂客户端通过创建资源客户端以连接 peer0. factory. itcast. cn 节点(FactoryNode),电商平

表 1　采购订单数据项

Tab. 1　Purchase order data items

序号	字段名	类型	说明	入库生成方式
1	SaleOrderNum	varchar(16)	电商采购合同单编号	订单信息 sha256 结果取前 20 位
2	CoopSaleInfoNum	varchar(16)	合作社售卖批次编号	加工厂销售平台自动绑定
3	FactoryId	int	加工厂编号	加工厂销售平台自动绑定
4	FactoryHash	varchar(64)	加工厂平台信息散列	Ajax 查库信息拼串,sha256 运算得到
5	SaleId	int	电商平台编号	采购员手动输入
6	SaleHash	varchar(64)	电商平台信息散列	Ajax 查库信息拼串,sha256 运算得到
7	OrderCustomerId	int	采购人编号	手动输入
8	OrderCustomerHash	varchar(64)	采购人信息散列	Ajax 查库信息拼串,sha256 运算得到
9	MonkeyPick	varchar(40)	猕猴桃种类	采购员手动选择
10	Count	int	采购数量	采购员手动输入
11	OrderDate	date	采购日期	系统自动获取
12	Price	double	单位价格	平台自动绑定
13	IsDeleted	int	订单状态	初始化为 2

台客户端以相同方式连接 peer0. dj. itcast. cn 节点(DsNode)。在合同交易前,两个节点需要安装相同的链码,负责两组织合同交易及相关业务。加工厂销售平台自动判断库存是否满足电商采购单的需求;确认信息无误后,将订单信息作为交易合同的内容,通过 FactoryNode 调用智能合约将销售合同信息上链,实现向联盟链发起销售合同交易;将加工厂本地数据库中销售单状态变更为 3,等待电商组织向区块链发起采购合同交易。

(3)电商采购方通过 DsNode 在当前通道账本中查询加工厂销售交易合同信息,调用智能合约发起采购确认,达成合同交易;对应 state 的 key 值是 S + SaleOrderNum,value 是订单信息散列值与采购方信息散列值;当采购意向合同交易完成后,将电商本地数据库的采购单状态变更为 1,采购入库完成。

(4)加工厂销售方以 S + SaleOrderNum 为 state 的 key 值,通过 FactoryNode 在当前通道账本中查询采购交易合同信息;确认无误后,对加工厂数据库的销售单的状态变更为 1,销售出库完成。采购方、销售方的链上交易完成,并且双方组织的本地数据库入库、出库均完成,跨组织链上合同交易完成。

采购合同单编号生成算法 OrderPost 表示采购员提交订单(输入数据 + 责任实体信息散列)获取采购合同编号,其中,QueryByMonkeyPickAndCount 表示按订单品名和数量查找前一生产阶段的销售交易合同编号;QueryBySaleId 表示按照电商平台工商号查询平台信息;QueryByFacotryId 表示按照加工厂工商号查询加工厂信息;QueryByCustomer 表示按照采购员工号查询采购员信息;Hash 表示使用 sha256 算法对参数生成定长的散列值;Left(20,str)表示对字符串取前 20 位操作;CurNum 表示合同编号。采购合同单编号生成如算法 1 所示。

算法 1: OrderPost (FactoryId; SaleId; OrderCustomerId; MonkeyPick; Count; OrderDate; Price);

输入:{ FactoryId; SaleId; OrderCustomerId; MonkeyPick; Count; OrderDate; Price};

输出:{CurNum};

CoopSaleInfoNum = QueryByMonkeyPickAndCount(MonkeyPick, Count)

SaleHash = Hash(QueryBySaleId(SaleId))

FactoryHash = Hash (QueryByFacotryId (FacotyId))

OrderCustomerHash = Hash(QueryByCustomerId (CustomerId))

CurNum = Left (20, Hash (PreOrgNum, OrderCustomerId, OrderCustomerHash, Price))

return CurNum

加工厂发起销售合同交易算法,Trade 表示加工厂客户端将销售交易合同(业务处理过的数据 args[ ])上链。其中,stub. GetState( )_length 表示判断当前通道账本中是否存在 state 的 key 值为“F + args[0]”的交易合同;TradeContent 表示交易合同结构体,all_fileds 表示交易合同结构体的具体数据项,对应表 1 字段 2 ~ 12;Marsh 表示将交易合同结构体的格式转换成可上链的 json 格式。加工厂发起销售合同交易如算法 2 所示。

算法 2: (this * TracePlantCC) Trade (stub shim. ChaincodeStubInterface, args [ ] string) peer. Response;

输入:{args[ ]};

输出:{更新区块链账本 new_chain };

if stub. GetState("F" + args[0])_length ! = 0;

```
        return Exit
    else:
        var tradeInfo TradeContent;
        var i =1;
        for field in all_fileds:
            tradeInfo.filed <- args[i++]
        new_chain = stub.PutState("F" +args[0],
Marsh(tradeInfo));
        return
```

在联盟内跨组织链上合同交易流程中,各组织可采用当前组织的采购交易合同编号作为溯源码。每个组织的交易合同编号与前一个生产组织交易合同编号在链上直接关联,随着生产流程和组织交易动态生成。消费者最终的订单编号生成规则同组织交易合同编号规则类似,消费者订单编号与电商采购猕猴桃的交易合同编号直接关联。这种类似 merkle 树[26]结构的交易合同编号编码方式,使得联盟链的每个组织的交易合同在账本中构成一条完整的合同链条。

3 猕猴桃质量溯源应用

本文以陕西齐峰果业有限公司的猕猴桃全产业链为研究模型,包含产前、产中和产后多阶段,是关联农资采购、种植采摘、生产加工、第三方质检、物流销售等多环节的完整链状结构。本文研究跨组织链上合同交易业务场景下的溯源平台要求参与方之间信息共享、风险共担,最终实现“多赢”。溯源信息来源于物联网设备数据、第三方检测数据、生产活动信息等。每个组织的溯源信息及责任实体散列值通过智能合约记录到联盟链通道账本中,并以当前组织采购交易合同编号作为溯源码对组织内猕猴桃生产溯源信息进行记录和追溯。

根据联盟链跨组织链上合同交易机制,结合猕猴桃全产业链溯源业务的实际需求,针对各个组织设计了一种单个生产环节溯源数据的存储方案。某一环节的链上溯源数据包括溯源信息散列值,责任人身份证号、责任组织工商号与其信息散列值。具体链下溯源数据和责任实体明文信息存储在各自组织的数据库中。实现“链上链下双存储”的数据存储方案,提供了对同一批次的猕猴桃与生产活动、责任人、责任企业等信息进行关联的数据化方案。追溯数据采用 Key - Value 的方式进行存储,将生产环节责任人身份证号(IdNumber)、责任人信息散列值(staffHash)、本地数据库溯源信息记录标识(InfoId)和溯源信息散列值(InfoHash)封装,作为 Value 写入账本,Key 则采用当前生产阶段字母 + 当前组织订单编号的组合,作为账本 Value 中 InfoId 的索引和唯一标识。

在溯源系统内,不同组织平台通过联盟链内跨组织链上合同交易机制,保证各个组织的溯源信息在区块链内逻辑具有完整性与一致性。链上的采购、销售合同交易经过联盟组织的成员节点共识后以交易的方式记录在账本中,交易信息公开透明。通过消费者溯源码与各个组织的交易合同编号对一个批次的猕猴桃进行标识,实际生产活动中,各个组织以生产环节首字母和组织的交易合同编号作为 state 的 key 值,按照追溯数据链上存储结构,对当前组织内所有生产环节的溯源数据依次上链。电商平台与加工厂、加工厂与合作社、合作社与农资平台之间的交易合同编号在联盟内形成一条完整的链,各个交易合同编号又对各个组织溯源信息进行关联,进而将整个联盟内同一批次猕猴桃的溯源信息在账本中关联成一条完整的链。联盟内溯源信息逻辑结构如图 3 所示。

以加工厂工序为例介绍溯源数据上链流程。加工厂从合作社采购一批猕猴桃,需要经过临时储藏、脱毛、糖分检测、质量测量、第三方抽样、装箱包装和冷藏等环节,加工厂组织使用采购合同编号与生产环节首字母作为 key 值,依次对各个生产环节溯源数据散列值同该环节负责人、责任企业的散列值等

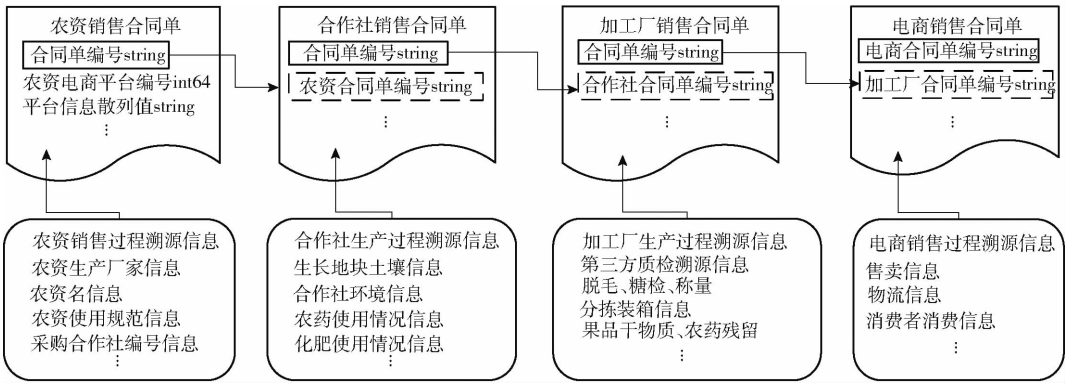


图 3 联盟内溯源信息逻辑结构

Fig. 3 Logical structure of traceability information within consortium blockchain

信息执行上链操作。

猕猴桃溯源流程包括：消费者和监管部门通过溯源码进行溯源，通过最终生成的溯源码在链上获取各个组织的溯源码，分别调用相应的智能合约查询各组织的溯源数据，包括从账本获取某一组织的某一个生产环节的溯源数据标识、责任人身份证号、企业工商号与各自散列值。通过溯源信息标识查询组织本地数据库，获取溯源数据与实体的明文信息，计算得出对应明文的 sha256 散列值，以链上的散列为标准，对链下的溯源数据生成散列值进行校验。根据校验结果，判断链下数据是否被篡改，如果发生篡改，消费者端显示溯源异常，监管部门可进一步追责具体责任人和责任企业。

4　测试

4.1　测试环境

本文研究了一种面向猕猴桃质量溯源的联盟链跨组织链上合同交易机制，基于这种联盟链内跨组织链上合同交易机制设计并实现了猕猴桃质量溯源系统。选择 Hyperledger Farbic 1.4 搭建区块链网络，操作系统是 64 位的 Ubuntu16.04LTS，内存 4 GB，磁盘空间 40 GB。测试环境如下：

（1）基本环境：安装 Hyperledger Fabric 的依赖容器服务 docker19.03.6，使用命令行 sudo apt install docker.io，完成后安装应用程序 docker-compose，使用命令行 sudo apt install docker-compose，使用脚本下载 fabric 镜像。

（2）溯源系统区块链网络：在 crypto-config.yaml 中配置联盟组织与节点信息，在 configtx.yaml 中配置创世区块和通道（Channel）信息；采用 solo 共识算法，将每个区块最大打包时间间隔为 2 s、区块的最大交易数为 10 笔、区块最大字节数为 32 MB；在 docker-compose.yaml 中配置网络的容器信息，使用 cryptogen 工具和 ca 服务器为联盟网络生成组织结构和身份文件；使用 configtxgen 生成创始区块和生成通道文件、锚节点更新文件等；每个组织配置了键值对数据库 leveldb 备份区块链数据，运行 docker-compose up -d 启动区块链网络。测试区块链网络的节点信息如表 2 所示。

表 2　节点设置说明

Tab.2　Node setup instructions

节点域名	端口号	所属组织	参与方机构
peer0.jg.itcast.cn	-7151:7051、-7153:7053	JGMSP	加工厂
peer0.coop.itcast.cn	-7251:7051、-7253:7053	COMSP	农业合作社
peer0.nz.itcast.cn	-7351:7051、-7353:7053	NZMSP	农资平台
peer0.ds.itcast.cn	-7351:7051、-7353:7053	DSMSP	电商平台
peer0.sc.itcast.cn	-7451:7051、-7453:7053	SCMSP	监管部门
ca.trace.itcast.cn	-7056:7056	CA	联盟链证书颁发中心（CA）
orderer.itcast.cn	-7050:7050	Orderer	

（3）服务器与区块链网络交互环境：组织的 Web 服务器通过 Fabric-SDK-Go 与区块链网络交互，智能合约实现组织业务逻辑；使用 beego 框架搭建服务器，前端使用 bootstrap4.0 搭建自适应页面框架；通过 data 组件、JQuery 和 Ajax 等进行前后端数据交互，组织通过权限控制管理存储各组织本地明文信息 mysql 数据库；终端用户使用手机 App 或浏览器连接组织节点。

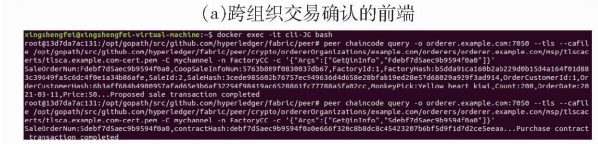
（4）区块链账本查看工具：选择 peer0.jg.itcast.cn 节点（可以选择通道内任意 peer 节点）配置区块链浏览器（Hyperledger Explorer），用于随时查看当前通道内账本的交易和区块信息，包括区块高度、区块哈希、交易发起组织、链码信息、背书节点等。

4.2　测试与分析

（1）跨组织链上交易

采购人员登陆销售组织平台下单，销售管理人员验证订单合法后向区块链发起交易，采购人员在账本中查询销售方的销售意向，最后向区块链发起采购确认，如图 4a 所示。双方链上合同交易完成，跨组织交易结束。账本中对应的合同交易信息如图 4b 所示。

(a)跨组织交易确认的前端



(b)跨组织交易确认的链上信息

图 4　跨组织交易确认

Fig.4　Inter-organizational transaction confirmation

（2）消费者溯源

以消费者对单号 2976e176b0f9726ae4ac 溯源为

例,在账本中仅需查找得到加工厂溯源码 452935032f6296b9086a 和合作社溯源码 Ob25f0fc68959230a96f。按照各组织溯源码查询链上溯源信息 id 与散列值;根据 id 查询组织本地数据库,将得到的明文信息拼成字符串;比对校验拼接字符串的 sha256 散列值与链上对应 id 的散列值;校验成功后显示猕猴桃的产地、生产厂家、销售物流和猕猴桃糖分、农药残留等质量相关的明文信息,如图 5 所示。

图 5 溯源功能结果

Fig. 5 Traceability function results

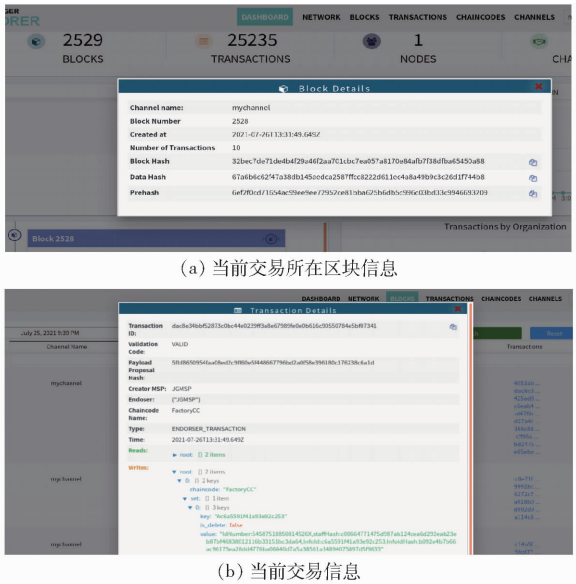
(3)当前上链交易信息

测试以加工厂节点通过调用智能合约,上链批次 c6a5591f41a93e92c253 的分拣生产数据为例。

通过 Hyperledger Explorer 显示该交易所在的区块信息,如图 6a 所示,其中区块号(区块高度)为 2528,区块哈希为 32bec7de71de4b4f29a46f2aa701cb c7ea057a8170e84afb7f38df ba65450a88,前一区块哈希为 6ef2f0cd71654ac99ee9ee72952ce81bba625b6db 5c996c03bd33 c9946693209。上链交易具体信息如图 6b 所示,其中 Txid 为 dac8e34bbf52873c0bc44e 0239 ff3a8e67989feOe0b616c90550784e5bf07341,调用链码为 FactoryCC,写入账本 state 的 key 为"Ac6a5591f41a93e92c253"(环节字母 + 交易合同编号)、value 为" ldNumber:545875188508145 26X, staffHash: c00664771475d987abl24cea6d292eab23eb 87bf468380121l6b33151bc3da64, Infold:c6a5591f41 a93e92c253, InfoldHash:b092e4b7b66ac96175ea28dd 4776ba06640d7a5a38561a14894075897d5f9633"(操作人员身份证号、信息散列值、溯源数据号、溯源信息散列值)等信息。

(4)用户数据上链时间

分别测试 1×10^4、3×10^4、5×10^4、7×10^4、9×10^4、1.1×10^5 条记录的上链时间,取相同记录运行 10 次的时间作为上链时间,测试结果如图 7 所示。



(a) 当前交易所在区块信息

(b) 当前交易信息

图 6 交易信息上链

Fig. 6 Uploading transactional information to blockchain

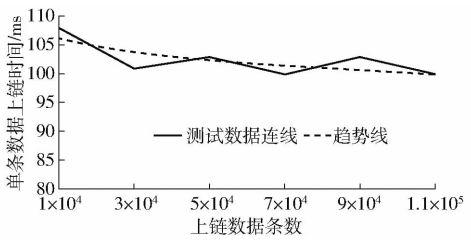


图 7 上链交易时间

Fig. 7 Time of uploading transactional data to blockchain

由图 7 可以看出,用户在不同上链数据条数下,执行一次上链操作平均用时约 102 ms,不受账本中记录总量影响。这是由于如果网络中上链交易量不能达到生成区块的交易条数时,上链一条数据与配置文件设置的最大出块时间 2 s 一致,上链交易时间由设置的出块条件和共识算法决定。

(5)链上溯源效率

与其他非合同交易机制的区块链溯源系统(简称非合同机制)相比,本文溯源模型采用合同交易机制(简称合同机制)增加了订单查询和校验过程。通过测试 state 的 key 键遍历查询方法,在账本数据总量分别为 1×10^4、3×10^4、5×10^4、7×10^4、9×10^4、1.1×10^5 条记录的条件下,设置 1、200、400、600、800、1 000、1 200 批次 6 组溯源实验在非合同机制与合同机制的查询时间。为了避免偶然性误差每个数据项都取 10 次实验的平均值作为结果。

非合同机制与合同机制的溯源查询时间效率 η 计算公式为

$$\eta(A,B)=\frac{t_A-t_B}{t_A}\times100\% \tag{1}$$

式中 t_A——联盟链两组织交易合同模式下消费者进行批次溯源的时间

t_B——不使用订单交易只通过唯一标识在各组织内部进行批次溯源的时间

$N = |\eta(A,B)|$，r 表示相关系数，其计算公式为

$$r = \frac{\mathrm{Cov}(X,Y)}{\sqrt{D(X)D(Y)}} \tag{2}$$

式中　$\mathrm{Cov}(X,Y)$——X、Y 的协方差

$D(X)$、$D(Y)$——X、Y 的方差

当账本数据量相差两万条数据时，查询时间变化很小，对比账本中存在 10^4 条记录和 1.1×10^5 条记录查询时间如图 8 所示，6 组溯源实验在不同存储条数下的 N 如表 3 所示。

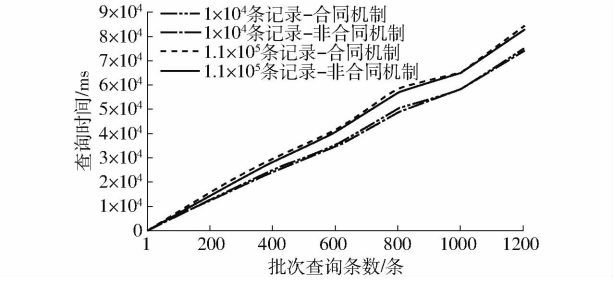


图 8　查询效率对比

Fig. 8　Comparison of query efficiency

表 3　不同存储条件下不同批次的溯源效率

Tab. 3　N of different batches under different storage conditions　%

查询条数/条	账本中记录总量/条						平均值
	1×10^4	3×10^4	5×10^4	7×10^4	9×10^4	1.1×10^5	
1	9.434	5.160	0.998	3.306	3.752	4.531	4.530
200	2.830	1.670	3.620	2.637	8.989	4.758	4.800
400	3.400	2.614	3.572	0.302	1.061	7.020	2.995
600	1.217	4.767	2.427	2.078	4.387	2.220	2.849
800	3.374	5.949	4.554	3.669	3.878	3.204	4.105
1 000	0.153	1.652	2.009	2.761	0.198	0.667	1.240
1 200	1.617	2.214	1.819	0.493	1.437	1.857	1.573
平均值	3.143	3.432	2.714	2.718	3.386	3.465	

由图 8 可以看出，在 1×10^4 和 1.1×10^5 的存储条数下，批次查询 1 000 条完整溯源数据，查询时间由 5.843×10^4 ms 变为 6.554×10^4 ms，平均每条完整溯源时间延长 7.11 ms。

由表 3 可以得出，在存储 1×10^4、3×10^4、5×10^4、7×10^4、9×10^4、1.1×10^5 条记录的条件下，$r=0.0976$，表明查询时间效率变化率与区块链网络中的存储条数变化关系不大。在批次查询 1、200、400、600、800、1 000、1 200 条记录条件下，$r=-0.819$，N 与批次查询条数呈负线性相关，且查询条数超过 1 200 条后，N 趋近 0。跨组织链上合同交易机制在实际溯源系统的应用中，随着溯源批次量增加，对效率的影响变小。

本文所设计联盟内跨组织链上交易合同机制，相对于大多数区块链溯源系统，溯源效率影响很小，在用户可接受范围内。

5　结论

（1）以猕猴桃全产业链生产为研究对象，提出了联盟链跨组织链上合同交易机制。该机制通过交易双方在链上发起采购合同交易和销售合同交易，将现实中双方签字确认合同的过程以交易的形式保存在区块链账本中。联盟链的各个组织使用当前组织交易合同编号作为溯源码，使得每个组织的溯源码与前一生产组织的溯源码在链上直接关联，产业链各个组织的溯源数据通过链上环环相扣的溯源码实现逻辑串联。生产环节数据上链时将溯源数据散列值与现实中代表责任实体的标识同散列值一同上链，不仅减轻了链上数据压力，同时解决了数据库主键易篡改、追责效率低等问题。通过跨组织数据协调校准，实现监管部门监管全产业链。本研究有效解决了实际生产中同一个批次猕猴桃溯源信息在多组织的联盟链账本的逻辑的连续性与完整性问题，有利于提升猕猴桃质量溯源可信度，保障猕猴桃生产质量。

（2）基于 Hyperledger Fabric 搭建了一个猕猴桃全产业链溯源平台，实现了跨组织的链上合同交易、消费者质量溯源和监管追责；当区块链网络中上链交易量较大时，用户上链一条数据的平均时间约为 102 ms；当区块链网络中上链交易量较小时，上链数据与最大出块的平均时间约为 2 s；通过对比合同机制与非合同机制溯源的查询效率，可以看出本系统平均每条完整溯源平均时间延长约 7.11 ms，在用户可接受范围内。

参　考　文　献

[1] LIM M K, LI Y, WANG C, et al. A literature review of blockchain technology applications in supply chains: a comprehensive analysis of themes, methodologies and industries[J]. Computers & Industrial Engineering, 2021, 154(4): 1-14.

[2] 于丽娜, 张国锋, 贾敬敦, 等. 基于区块链技术的现代农产品供应链[J]. 农业机械学报, 2017, 48(增刊): 387-393. YU Li'na, ZHANG Guofeng, JIA Jingdun, et al. Modern agricultural product supply chain based on block chain technology [J]. Transactions of the Chinese Society for Agricultural Machinery, 2017, 48(Supp.):387-393. (in Chinese)

[3] YANG Z L, LI X, HE P. A decision algorithm for selecting the design scheme for blockchain-based agricultural product traceability system in q-rung orthopair fuzzy environment[J]. Journal of Cleaner Production, 2020, 290(1): 125191-125208.

[4] GEORGE R V, HARSH H O, RAY P, et al. Food quality traceability prototype for restaurants using blockchain and food

quality data index[J]. Journal of Cleaner Production, 2019, 240: 118021 - 118028.
[5] 许继平, 孙鹏程, 张新, 等. 基于区块链的粮油食品全供应链信息安全管理原型系统[J]. 农业机械学报, 2020, 51(2): 341 - 349.
XU Jiping, SUN Pengcheng, ZHANG Xin, et al. Prototype system of information security management of cereal and oil food whole supply chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(2): 341 - 349. (in Chinese)
[6] 葛艳, 黄朝良, 陈明, 等. 基于区块链的 HACCP 质量溯源模型及系统实现[J]. 农业机械学报, 2021, 52(6): 369 - 375.
GE Yan, HUANG Chaoliang, CHEN Ming, et al. HACCP quality traceability model and system implementation based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(6): 369 - 375. (in Chinese)
[7] 任守纲, 何自明, 周正己, 等. 基于 CSBFT 区块链的农作物全产业链信息溯源平台设计[J]. 农业工程学报, 2020, 36(3): 279 - 286.
REN Shougang, HE Ziming, ZHOU Zhengji, et al. Design and implementation of information tracing platform for crop whole industry chain based on CSBFT - blockchain[J]. Transactions of the CSAE, 2020, 36(3): 279 - 286. (in Chinese)
[8] 吴晓彤, 柳平增, 王志铧. 基于区块链的农产品溯源系统研究[J]. 计算机应用与软件, 2021, 38(5): 42 - 48.
WU Xiaotong, LIU Pingzeng, WANG Zhihua. Traceability system of agricultural products based on blockchain[J]. Computer Applications and Software, 2021, 38(5): 42 - 48. (in Chinese)
[9] TANG H, SHI Y, DONG P. Public blockchain evaluation using entropy and TOPSIS[J]. Expert Systems With Applications, 2019, 117(3): 204 - 210.
[10] DINH T T A, WANG J, CHEN G, et al. Blockbench: a framework for analyzing private blockchains[C]// Proceedings of the 2017 ACM International Conference on Management of Data, 2017: 1085 - 1100.
[11] LI Z, KANG J, YU R, et al. Consortium blockchain for secure energy trading in industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2017, 14(8): 3690 - 3700.
[12] 董云峰, 张新, 许继平, 等. 基于区块链的粮油食品全供应链可信追溯模型[J]. 食品科学, 2020, 41(9): 30 - 36.
DONG Yunfeng, ZHANG Xin, XU Jiping, et al. Blockchain-based traceability model for grains and oils whole supply chain [J]. Food Science, 2020, 41(9): 30 - 36. (in Chainese)
[13] 叶岳洋, 张兴兰. Fabric 中的匿名身份认证技术研究[J]. 网络与信息安全学报, 2021, 7(3): 1 - 7.
YE Yueyang, ZHANG Xinglan. Research on anonymous identity authentication technology in Fabric[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 1 - 7. (in Chainese)
[14] 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理:问题与方法[J]. 软件学报, 2018, 29(1): 150 - 159.
QIAN Weining, SHAO Qifeng, ZHU Yanchao, et al. Research problems and methods in blockchain and trusted data management[J]. Journal of Software, 2018, 29(1): 150 - 159. (in Chinese)
[15] 赵辉, 李星, 谭嘉诚, 等. 智能合约安全问题与研究现状[J]. 信息技术与网络安全, 2021, 40(5): 1 - 6,19.
ZHAO Hui, LI Xing, TAN Jiacheng, et al. Research status of smart contract security[J]. Information Technology and Network Secutity, 2021, 40(5): 1 - 6,19. (in Chinese)
[16] 靳世雄, 张潇丹, 葛敬国, 等. 区块链共识算法研究综述[J]. 信息安全学报, 2021, 6(2): 85 - 100.
JIN Shixiong, ZHANG Xiaodan, GE Jingguo, et al. Overview of blockchain consensus algorithm[J]. Journal of Cyber Security, 2021, 6(2): 85 - 100. (in Chinese)
[17] 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)
[18] 于洋, 谭峰. 基于区块链技术的农产品质量溯源系统结构设计[J]. 农业工程, 2021, 11(1): 33 - 39.
YU Yang, TAN Feng. Structure design of agricultural product quality traceability system based on blockchain technology[J]. Agricultural Engineering, 2021, 11(1): 33 - 39. (in Chinese)
[19] BAI C, ZHU Q, SARKIS J. Joint blockchain service vendor-platform selection using social network relationships: a multi-provider multi-user decision perspective[J]. International Journal of Production Economics, 2021, 238: 108165 - 108180.
[20] ZHU Wentao, LIN Jingqiang. Generating correlated digital certificates: framework and applications[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(6):1117 - 1127.
[21] 夏云浩. 数据信息安全中公钥密码体制若干关键技术研究[D]. 南京:南京邮电大学, 2020.
XIA Yunhao. Research onseveral key techiques of public key cryptography for data information security[D]. Nanjing:Nanjing University of Posts and Telecommunications, 2020. (in Chinese)
[22] 黄俊飞, 刘杰. 区块链技术研究综述[J]. 北京邮电大学学报, 2018, 41(2): 1 - 8.
HUANG Junfei, LIU Jie. Survey on blockchain research[J]. Journal of Beijing University of Posts and Telecommunications, 2018, 41(2): 1 - 8. (in Chinese)
[23] 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 future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481 - 494. (in Chinese)
[24] 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.
SHAO Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969 - 988. (in Chinese)
[25] RAO P V, THAMMI R K, SURESH V P. ASH - 160: a novel algorithm for secure hashing using geometric concepts[J]. Journal of Information Security and Applications, 2015, 21: 52 - 63.
[26] WEI Pengcheng, WANG Dahu, ZHAO Yu, et al. Blockchain data-based cloud data integrity protection mechanism[J]. Future Generation Computer Systems, 2020, 102(1): 902 - 911.