doi:10.6041/j.issn.1000-1298.2022.06.035

基于区块链的农产品质量安全可信溯源系统研究

刘双印[1]　雷墨鬻兮[1]　徐龙琴[2]　李景彬[3]　孙传恒[4]　杨信廷[4]

(1. 仲恺农业工程学院智慧农业创新研究院, 广州 510225; 2. 广东省高校智慧农业工程技术研究中心, 广州 510225;
3. 石河子大学机械电气工程学院, 石河子 832003; 4. 国家农业信息化工程技术研究中心, 北京 100097)

摘要: 为解决现有农产品质量溯源系统存在的数据中心化存储、数据易篡改和数据信任等问题,以及保障农产品质量安全、维护消费者权益和提高生产企业品牌竞争力,在分析农产品产业链业务流程和区块链关键技术的基础上,设计了农产品可信溯源区块结构,确保农产品溯源数据不可伪造和安全可信;提出了"On-Chain + Off-Chain"农产品质量安全溯源信息协同管理存储策略,解决农产品溯源区块链网络中各节点数据存储压力大、查询效率低和数据爆炸等问题;采用 Kafka 共识机制实现多主体参与的共识操作,提供实时数据高吞吐量和低延时的处理能力;制定了农产品溯源智能合约规则集和合约触发条件,确保农产品数据的可靠性和溯源平台的公信力;基于 Hyperledger Fabric 区块链平台研制了农产品质量安全可信溯源系统,并对红茶产品质量安全溯源进行验证分析。结果表明,本文研制的农产品质量安全可信溯源系统,解决了农产品产业链生产、加工和流通多节点之间数据安全和溯源信息真实可信等问题,取得了较好的应用效果。

关键词: 农产品; 可信溯源系统; 区块链; 共识机制; 智能合约

中图分类号: TP391　　**文献标识码**: A　　**文章编号**: 1000-1298(2022)06-0327-11　　**OSID**:

Development of Reliable Traceability System for Agricultural Products Quality and Safety Based on Blockchain

LIU Shuangyin[1]　LEI Moyixi[1]　XU Longqin[2]　LI Jingbin[3]　SUN Chuanheng[4]　YANG Xinting[4]

(1. *Academy of Intelligent Agricultural Innovations, Zhongkai University of Agriculture and Engineering, Guangzhou* 510225, *China*
2. *Intelligent Agriculture Engineering Technology Research Center of Guangdong Higher Education Institutes, Guangzhou* 510225, *China*
3. *College of Mechanical and Electric Engineerings, Shihezi University, Shihezi* 832003, *China*
4. *National Engineering Research Center for Information Technology in Agriculture, Beijing* 100097, *China*)

Abstract: Aiming to solve the problems of centralized data storage, easy data tampering, and data trust in the existing agricultural product quality traceability system, as well as to ensure the quality and safety of agricultural products, protect the rights and interests of consumers and improve the brand competitiveness of production enterprises. Based on the analysis of the agricultural product industry chain business process and the key technologies of the blockchain, the trusted traceability block structure of agricultural products was designed to ensure that the traceability data of agricultural products were unforgeable, safe and reliable; the "On-Chain + Off-Chain" agricultural product was proposed. The collaborative management and storage strategy of quality and safe traceability information solved the problems of high data storage pressure, low query efficiency and data explosion of each node in the agricultural product traceability blockchain network. Kafka consensus mechanism was used to achieve consensus operations with multi-agent participation and provide real time data with high throughput, high-volume and low-latency processing capabilities; and agricultural product traceability smart contract rule sets and contract trigger conditions were developed to ensure the reliability of agricultural product data

收稿日期: 2021-06-25　修回日期: 2021-08-16

基金项目: 国家自然科学基金项目(61871475、61471133)、广州市创新平台建设计划项目(201905010006)、广东省科技计划项目(2019B020215003、2017B010126001、2017A070712019、2016A020210122)、广东省普通高校省级重大科研项目(2016KZDXM001)和广东省教育厅特色创新项目(2017KTSCX094、2017KQNCX098)

作者简介: 刘双印(1977—),男,教授,博士,主要从事区块链、智能信息系统和农业信息化技术研究,E-mail: shuangyinliu@126.com

通信作者: 孙传恒(1978—),男,研究员,博士,主要从事区块链和农产品质量安全溯源研究,E-mail: sunch@nercita.org.cn

and the credibility of the traceability platform. A trusted traceability system was developed for agricultural product quality and safety based on the Hyperledger Fabric blockchain platform, and the verification and analysis were conducted on the traceability of the quality and safety of black tea products. The results showed that the developed agricultural product quality and safety credible traceability system can solve the problems of data security and authenticity of traceability information among multiple nodes in the production, processing and circulation of the agricultural product industry chain, which achieved good application results.

Key words: agricultural products; reliable traceability system; blockchain; consensus mechanism; smart contract

0 引言

近年来,农产品质量安全问题频发,各国政府高度关注,并出台系列法律法规以保障农产品质量安全[1-3]。各国政府、高校科研院所和企业采用条形码、射频识别、二维码、产品电子代码、物联网、云计算等技术等构建系列的农产品质量安全溯源系统[4-8],并在水产品、蔬菜、畜禽肉蛋类、粮油、水果等领域得到广泛应用,取得一些成效[9-10]。但因农产品全产业链具有产业链长、参与主体多、涉及面广、环节复杂、周期长、信息多源异构等特性,再加上传统的溯源系统多采用数据中心化存储,各自管理,尤其是农产品质量高附加值信息被选择性公开,使现有溯源系统存在共享性差、数据易篡改、信息不透明和不对称、数据可信任性差等问题,导致农产品质量安全事件仍多发[11]。因此,为解决上述问题,研究先进的溯源技术及其系统对保障农产品质量安全具有重要的研究价值。

区块链是一种分布式账本技术,具有去中心化、不可篡改、成本低、可追溯、安全可靠等特征[12-15]。一些国内外学者研究将区块链技术应用在农产品质量安全溯源领域,文献[16]提出了一种统一的食品本体论,该理论可提高全球食品可追溯性、质量控制和数据整合,它是一个由联盟驱动的项目,为建立一个全面的、容易获得的全球农场,它准确且一致地描述了常见的食物。文献[17]采用区块链技术构建了粮油食品供应链信息安全管理模型,并通过双模数据存储机制和基于智能合约的供应链信息管理,实现了信息存储与传输安全可信。文献[18]提出了“数据库 + 区块链”的链上链下追溯信息双存储模型,通过 Hyperledger Fabric 设计了区块链农产品追溯信息存储模型和查询方法,实现了农产品追溯信息高效存储和快速查询。文献[19]采用基于危害因子的食品风险评估和区块链溯源技术构建了食品质量安全管理系统,实现了大米质量安全管控。文献[20]设计了一个旨在为养鱼户提供安全的存储空间,以保存大量不能被篡改的农业数据平台,实现了使用智能契约来自动完成养鱼的不同过程,减少了错误操作。文献[21]提出了一种利用区块链和智能合约有效地执行商业交易,以实现整个农业的大豆跟踪和可追溯所有信息供应链,该方案以高完整性提高效率和安全性,实现了为用户提供高透明度和可追溯性的供应链生态系统。上述研究采用区块链技术实现质量安全溯源,一定程度上解决了传统溯源系统的问题,但存在数据存储压力大和查询效率低等问题,尤其是随着农产品产业链节点拓展和数据剧增,溯源系统负荷压力将增大。

本文首先对农产品溯源信息双链存储模式和智能合约进行设计,然后采用联盟区块链技术构建从田间到餐桌的农产品全产业链质量安全可信溯源系统,以期为农产品质量安全管控提供技术支撑。

1 农产品可信溯源系统与关键技术

1.1 农产品全产业链

农产品产前、产中和产后等全产业链涉及的活动主体主要有:育种企业、生产资料企业(生产化肥、农药等)、种养殖企业、加工企业、仓储企业、物流企业、分销商、零售商和消费者,其关键控制节点主要有种苗、种植、收获、加工、仓储、冷链物流、质检、销售、消费等环节。各节点的信息主要包括种苗信息(种子编号、种子名称、所属品种、来源)、环境信息(土壤、水质、气象等多参数)、投入品信息(投入品编号、名称、成分含量、投入量和库存量、来源、购买人、使用人)、检验检疫信息(重金属类别及含量、农药类别及残留含量、微生物类别及含量、检测检验方式、农产品品质量等级、检验人、检验单位)、控制信息(温度、光照强度、湿度、投入品配比等技术指标)、资质管理(企业资质、管理制度、执行标准)、人员信息(人员 ID、姓名、工种类别、联系方式、所学专业等)、地块等其他信息(地块编号、时间、生产批次、土壤关键指标等)等[22]。由上可知,农产品产业链参与的主体众多,涉及节点多且各节点信息

化水平参差不齐，缺乏统一的数据接口、标准规范和业务集成，形成诸多各自管理的“数据孤岛”，严重制约农产品全产业链质量安全有效监管和可信溯源[23-24]。

1.2　农产品可信溯源系统关键技术

1.2.1　农产品可信溯源区块模型结构

区块是区块链存储交易信息的链式数据结构，由区块头和区块体两部分组成，通过区块头中父区块头 Hash 值按时序排列将相邻区块首尾连接组成区块链[25-26]，其区块结构如图 1 所示。采用哈希算法对区块体存储的农产品产业链各参与主体的交易关键数据加密成不可逆转的 Hash 值[27]，并作为 Merkle 树叶子节点，将两两叶子逐层递归哈希计算，生成区块头的 Merkle 树根节点[28]。区块通过 Merkle 树特性、时间戳、版本号、区块复杂度、数字签名等措施[29-30]，确保农产品溯源信息难以篡改[31]，若某节点篡改溯源关键数据，通过区块 Hash 值比对，可快速追踪该节点，从而保障了农产品溯源系统数据不可伪造、安全可信[32-34]。

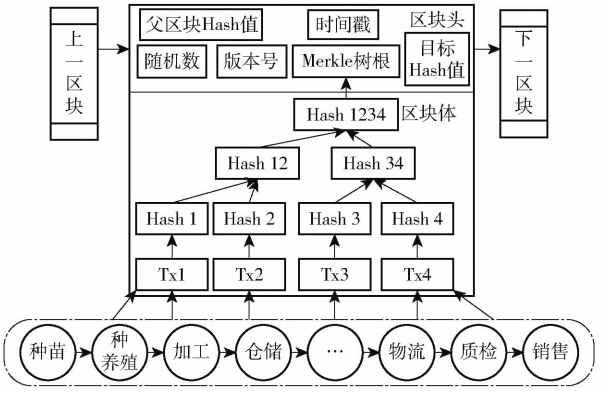

图 1　区块链式结构图

Fig. 1　Structure diagram of blockchain

1.2.2　“On-Chain + Off-Chain”双模式存储策略

农产品全产业链具有参与主体节点多、产业链长、涉及范围广、数据量大且多源异构等特征[35]，在农产品溯源过程中，随着节点增加和数据量增大，若每次都把各节点所有数据全部上传到区块链网络中，不仅上传速度慢还易造成网络阻塞，导致区块链网络中各节点数据存储压力大，查询效率低，数据安全隐患大，还对数据存储系统的设备性能和投入成本都提出较高要求，影响了基于区块链的溯源系统的实施[36-37]。链上存储的主要压力如表 1 所示。

为此，本文提出了“On-Chain + Off-Chain”农产品质量安全溯源信息协同管理存储策略，其基本思想为：首先对农产品产业链各节点产出的数据进行标准化和规范化；其次采用智能合约对各节点规范化后的详细数据进行验证，把通过验证的大部分农

表 1　链上存储数据开销与效率

Tab. 1　Analysis of cost and efficiency within storing data on chain

	开销	效率
共识	PoW 消耗大量电力；PoS 靠抵押资产获得记账权；Kafka 对消息重复执行；PBFT 多次往返投票，流程步骤繁杂；dBFT 容易产生分叉，增加系统不必要的花销	分布式系统共识过程复杂，节点难以达成高度一致，共识效率不高
计算	除了加解密、协议解析等计算之外，为了验证区块链上智能合约的执行结果，所有节点都会无差别地执行合约代码	区块链系统对智能合约的执行，对数据的加解密以及对协议和路径的解析计算速率不高，计算效率较低
网络	网络的开销与节点数呈指数关系，节点越多，网络的路径越复杂，带宽和流量开销就越大，若数据包的有效载荷增加，网络负载过重	数据包扩容节点增加带宽增大，大量数据涌入网络容易造成网络拥塞甚至出现丢包现象，网络效率较低
存储	存储开销与节点数成正比，所有上链的数据，都会一致地写入所有节点的硬盘，节点越多数据冗余越大，对缓冲区的要求也越高	海量数据到达节点进行排队存储，高冗余的数据除了增加了硬盘的工作量，缩短了硬盘寿命，还降低了存储工作效率
访问	每一次的读取都需要从节点账本中进行索引，海量的数据造成的索引开销巨大	高频的访问对存有大量数据的系统而言伤害大，读取效率较低

产品产业链数据和区块链位置信息存储在本地或云服务器上的关系型和非关系型数据库中；然后将农产品溯源关键信息使用 MD5 对局部数据（图像、视频等）和持有人签名一起计算上链，并在链下建立索引，在链上仅进行 Key-Value 的精准读写。同时为了保证智能合约的隐私性，在必要的情况下智能合约也可以采用链下存储，使用计算节点进行合约的计算记录，共识节点记录合约的状态记录；最后，对于链下的溯源数据的存储要尽可能地详尽，链上经哈希算法计算过的数据要尽可能地精简，上链的数据一定是需要经过共识的，因此该“On-Chain + Off-Chain”协同管理存储策略能很灵活地应对网络拥塞、传输时延等的影响。对于链上数据的快速查询达到了效率、成本以及隐私安全的平衡。设计的农产品质量安全溯源信息协同管理存储模型如图 2 所示。

链下存储的数据为当前区块高度、当前 Hash 值、溯源码，溯源码则包含了农产品从出产到销售整个流程的信息，也称为二维码溯源，如产品介绍、溯源信息、食品安全、企业信息以及信息防伪等各项数据的 Hash 值。当前 Hash 值是集当前的版本号

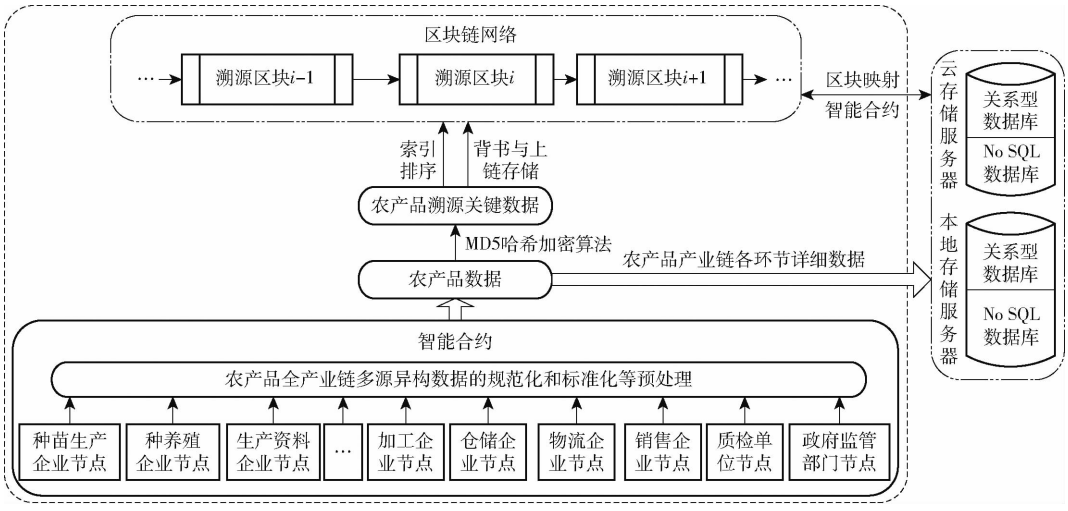

图 2 农产品质量安全区块溯源信息协同管理存储模型

Fig. 2 Cooperative management and storage model of block traceability information for agricultural product quality and safety

(Version)、前区块 Hash 值(Previews Hash)、时间戳(Timestamp)、随机数(Nonce)以及默克尔树(Merkle Tree)所包含所有事务的 Hash 值(Merkle Hash)等各项信息经 MD5 哈希算法处理之后得到的结果。链下存储着由链上数据共同参与哈希计算产生的 Hash 值,链上分布式账本记录着所有的原始数据,块与块相连接,每一块的当前 Hash 值都有前一区块的 Hash 值参与计算完成,默克尔树的根 Hash 值无法篡改,得到的链下数据的上链情况如表 2 所示。

表 2 上链数据

Tab. 2 On-chain data

区块	当前 Hash 值	前驱 Hash 值	当前高度
1	LvFySXoU4jsslgWLE/19DBcVOhDF9cjwSUaGNviispU =	If/kJ9fK3PQMk/NeU6H7Yq82lLVHbkyLYoErq8nHe08 =	15 295
2	EhrCgZx884ne8U7PpEkcVXzaNe21hTMGPwpYEjYsoac =	LvFySXoU4jsslgWLE19DBcVOhDF9cjwSUaGNviispU =	15 296
3	CYSRHW4mUxTQoBZJ2NGmJnwFN0aTr + IL + Voqo/d6KDU =	EhrCgZx884ne8U7PpEkcVXzaNe21hTMGPwpYEjYsoac =	15 297
4	Tn76PG6h1ggbhV0mI9RzmQyc1H0DleLJqKhcl6oPcd8 =	CYSRHW4mUxTQoBZJ2NGmJnwFN0aTr + IL + Voqo/d6KDU =	15 298

1.2.3 农产品产业链共识机制

共识算法是区块链去中心化的核心要素,影响区块链系统的执行效率[38-39]。公有链共识算法主要依靠计算机算力完成共识机制,存在计算资源浪费问题[40]。私有链共识机制主要应用于企业内部,常采用传统分布式一致性算法完成共识操作,不适于多主体参与的农产品质量安全溯源领域[41-42]。而联盟链网络由通过授权的联盟成员共同维护,常采用 Kafka 共识模式[43]或者实用拜占庭容错算法[44](Practical Byzantine fault tolerance,PBFT)。

Fabric 区块链的共识过程包括 3 个阶段:背书、排序和校验,背书(Endorsement)阶段是背书节点对客户端发来的事务进行合法性校验,背书节点模拟并签署提案书,对结果作出批准或拒绝响应,根据设定的背书逻辑判断是否支持该交易,如果背书逻辑决定支持交易,会把交易签名后发回给客户端。背书节点和提交节点之间有重叠,背书节点作为一种特殊的提交节点,它们必须持有智能合约,每个背书节点通过在其模拟环境中调用智能合同,用来接收并执行交易建议,这样的模拟交易结果不会更新到分类账中,而是由背书节点将模拟结果捕获到一组特定的读写数据集(Read\Write set,RW set)中。读取数据以捕获当前状态的最新读写集(RW set),保存模拟事务写入数据时将写入世界状态,背书节点在这些 RW 集上提供签名,然后将其返回给客户端应用程序。排序(Ordering)阶段是排序节点接受背书节点返回的所有交易并对这些交易进行排序的过程,排序服务是共识机制中重要的一环,所有交易通过 Kafka 机制排序服务进行排序才可以达成全网共识,客户端应用程序将对已签名的模拟事务结果进行打包,然后将该事务连同 RW 集一起提交给排序节点。当网络对提交的事务达成共识时,此事务将被打包成一个块,并将其交付给所有提交节点进行验证。验证(Validation)阶段是由排序节点与提交节点共同完成的,每个提交节点都会验证交易程序通过检查这些 RW 集是否与当前世界状态相匹配,交易的 RW 集是否符合多版本并发控制[45](Multiversion concurrency control,MVCC)的校验等。

一旦交易验证，即可将其写入分类账中，并根据 RW 集设置更新世界状态写入数据。最后，这些提交节点生成异步消息以通知客户端所提交的事务是否已成功执行。整个事务的合约过程都由共识机制强制参与执行，每当事件发生时，客户端应用程序就可以订阅每个提交节点的事件通知。Fabric 利用 Kafka 对交易信息进行排序处理，为实时数据提供统一的、高吞吐量、低延时的处理能力，并且在集群内部支持节点故障容错；PBFT 解决拜占庭将军问题，但需要 $O(N^2)$ 时间复杂度（N 表示同一消息共识次数）的网络通信才能完成 n 个网络节点共识，导致网络带宽压力大，影响算法共识效率。图 3 为基于联盟链共识机制设计的农产品溯源共识机制原理。

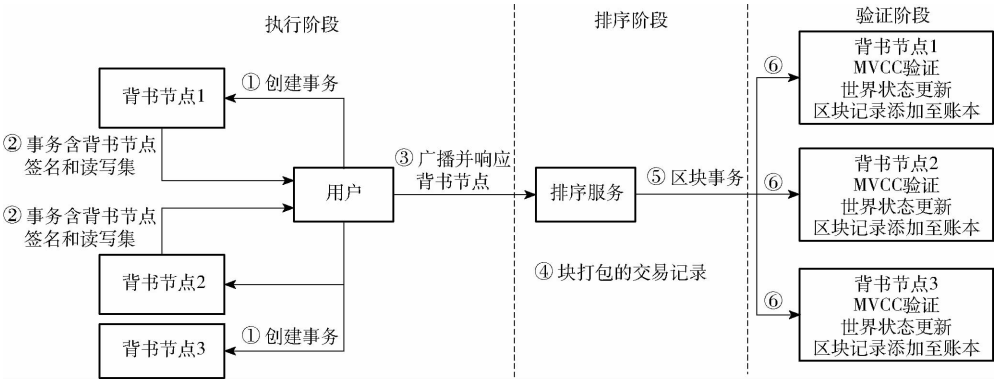

图 3　农产品溯源共识机制

Fig. 3　Consensus mechanism of agricultural product traceability

1.2.4　农产品产业链智能合约机制

智能合约是一种具有确定性、自校验、自治化、去中心化、自动执行、不可篡改等特点，能执行合同条款的可计算的计算机协议[46-48]。智能合约根据事先预置好和可自动执行的合约条款及业务逻辑机制，就可以为区块链网络中各节点活动主体提供数据交互、防篡改的交易记录、价值转移、关键数据上链存储等功能，也是在区块链网络上实施更加灵活、更细粒度的访问控制机制[49-51]。本系统以 Hyperledger Fabric[52] 为区块链开发平台，结合国家食品安全法规、行业标准，领域专家经验等，制定农产品质量安全溯源智能合约规则集和合约触发条件，通过编写的智能合约，实时验证拟上链的合约数据、监控区块链网络上的交易信息，实现对农产品全产业链各环节产品精准管控，为农产品生产企业优化生产工艺、保障产品质量和提高企业品牌提供技术支撑；同时也为广大消费者和农产品质量安全检测部门提供可信溯源信息。系统智能合约使用标准编程语言编写，但不能直接访问分类帐状态，而且它们在容器环境中运行以进行隔离。系统中智能合约主要体现在 3 方面：①对上链数据的验证及维护，智能合约以编程方式访问分类帐的两个不同的部分，一个不可更改地记录所有交易历史的区块链，以及一个持有当前这些状态值的世界状态。所以上链的数据经过验证之后不能更改，账本状态会记录所有的写入操作。智能合约打包并部署到区块链网络中，可以在同一包内定义多个智能合约，一旦合约部署完成，包内的所有智能合约都可提供给应用程序。因为智能合约是允许多步骤流程自动化的脚本，其操控的分散应用程序可完全按照代码条件触发，所以不会有任何审查、欺骗或宕机的风险。②对销售商品的赔付方面，在农产品从生产到销售的过程中需要经历各个阶段的合作加工处理过程，一旦其中某个环节出现问题，智能合约会根据事先约定的情况对出现的损失进行赔付，而不需要人为地计算损失与惩罚，这样既节省了成本也提高了效率。③对该“On-Chain + Off-Chain”协同管理存储策略的保护措施，外部应用程序会与智能合约在区块链网络上进行交互执行操作，由于区块链包含不可变记录，以反映这些操作产生的更改，所以“On-Chain + Off-Chain”协同管理存储策略可以支持最新的缓存信息，且对于数据的检索更加快速便捷，因此对于没有授权的应用程序开发人员则无法选择或修改验证阶段进行评估认可策略，在最终系统审计过程中，背书策略作为系统中事务验证的静态库执行操作，只能通过链码实行参数化，之后将分类帐更新结果作为响应返回到外部应用程序，因此可以保证用户和数据的安全。其农产品溯源智能合约如图 4 所示。

列出系统两个合约执行的算法逻辑（Query 与 Compare），即用户扫描溯源码得到溯源码内的信息，这些数据信息都来自以上链的信息。其中块与块相连接，每一块上存有大量事务，每个事务都有唯一标示 ID，以及有上链的时间戳共同参与哈希计算，当链上返回的原始数据经过哈希计算后得到的

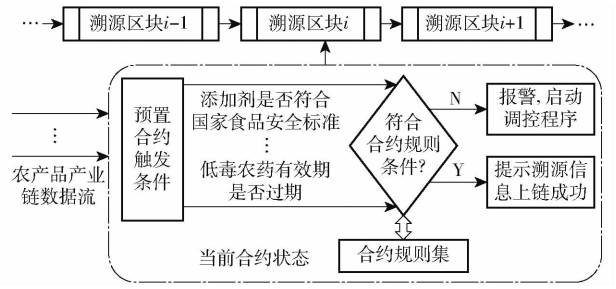

图 4 农产品溯源智能合约

Fig. 4 Smart contract of agricultural product traceability

字符串与本地数据库存储的字符串相匹配,合约自动执行对比逻辑进行数据调取,当 tx. ID1 = = tx. ID2 成立时,查询成功,否则合约调用失败,云端数据库返回源数据不成功,查询失败。两个合约如下:

合约 1:Query

```
1. Contract Simplequery(off_infm)
2. var buffer bytes. Buffer
3. while(PreviousHash! = NULL){
4.  hash : = sha256. Sum256(buffer. Bytes(off_infm))
5.  if(hash in PreviousHash. select) :
6.  tx. ID1 = hash[:] //从链下数据计算得到的 Hash 值中取 ID
7. PreviousHash = PreviousHash. next}
8. returntx. ID1
```

合约 2:Compare

```
1. Contract Simplecompare(tx. ID,on_infm)
2. while(PreviousHash! = NULL){
3.  if(on_infm = = hash) :
4.  tx. ID2 = on_infm[:]
5.  if(tx. ID1 = = tx. ID2)
6.  fmt. Println(off_infm)
7. return true} //查询成功!
```

2 农产品质量安全可信溯源系统设计与实现

2.1 可信溯源系统功能模块设计

以农产品全产业链分析和企业溯源需求为基础,对农产品溯源各环节数据进行梳理分析、归纳合并,并以“高内聚、低耦合”的现代软件工程思想进行系统功能划分。该系统由我的农场、基地管理、生产操作、作物追溯、系统设置、大数据分析共 6 大功能模块组成,每个功能模块又由多个子功能构成,实现农产品从农田到餐桌可信溯源。其系统功能模块如图 5 所示。

2.2 可信溯源系统架构设计

结合农产品全产业链产前、产中和产后企业的

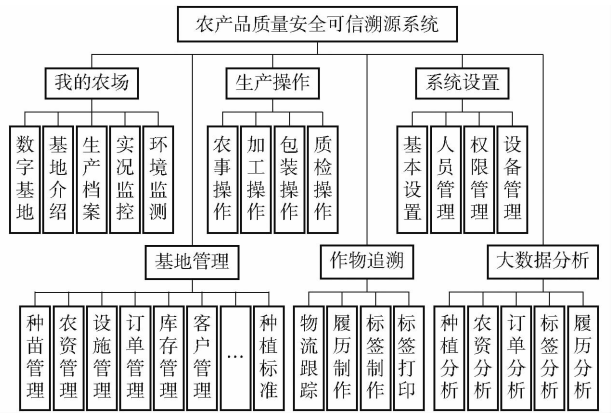

图 5 系统功能模块

Fig. 5 Diagram of system function module

实际生产过程和农产品可信溯源的需求,设计的系统整体架构如图 6 所示。该系统架构主要由数据采集层、数据存储层、服务管理层、接口层、业务逻辑层、用户层等 6 层组成。

数据采集层主要采用物联网系统、多参数智能传感器、分析仪等设备在线或离线采集农产品产业链各节点的数据,并通过无线传感器网络、4G/5G、LoRa、WIFI 等网络把数据传输到数据存储层。

数据存储层采用链上和链下双存储模式存放所有数据,首先对数据进行清洗、转化、融合等预处理,然后把通过智能合约和共识机制验证的溯源关键数据、分布式账本、时间戳、数字签名、区块头 Hash 值等信息上链存储到联盟区块链网络中,该链上数据可通过不同身份验证和访问权限查看不同数据;将通过智能合约的各节点大量的数据和区块链网络映射关系都存储到链下关系型和非关系型数据库中,这种链上和链下双存储模式可有效提高存储效率及保障数据安全可靠。

服务管理层主要包括安全服务体系、分布式账本、资源管理服务 3 部分,其中安全服务体系负责管理整个系统的账号、密钥、认证、权限、签名、共识算法、合约等信息;分布式账本负责管理所有交易记录、数据共识、智能合约,登记和交换实体或虚拟的资产等;资源管理服务负责系统算法库、农产品质量安全法律法规库、农产品行业标准库、规则库、专家知识库、编码规则与管理、边缘计算设备、虚拟机和容器等通过 API 应用接口,支持业务逻辑层的功能应用。

业务逻辑层主要负责整个溯源系统的数据采集、溯源信息查询、大数据统计分析、区块链管理、溯源编码等业务功能,为企业、质检部门、监管部门和消费者提供真实可靠的溯源信息和决策支持。

2.3 农产品可信溯源信息查询执行过程

在实现了上述溯源系统设计的基础上,需要将

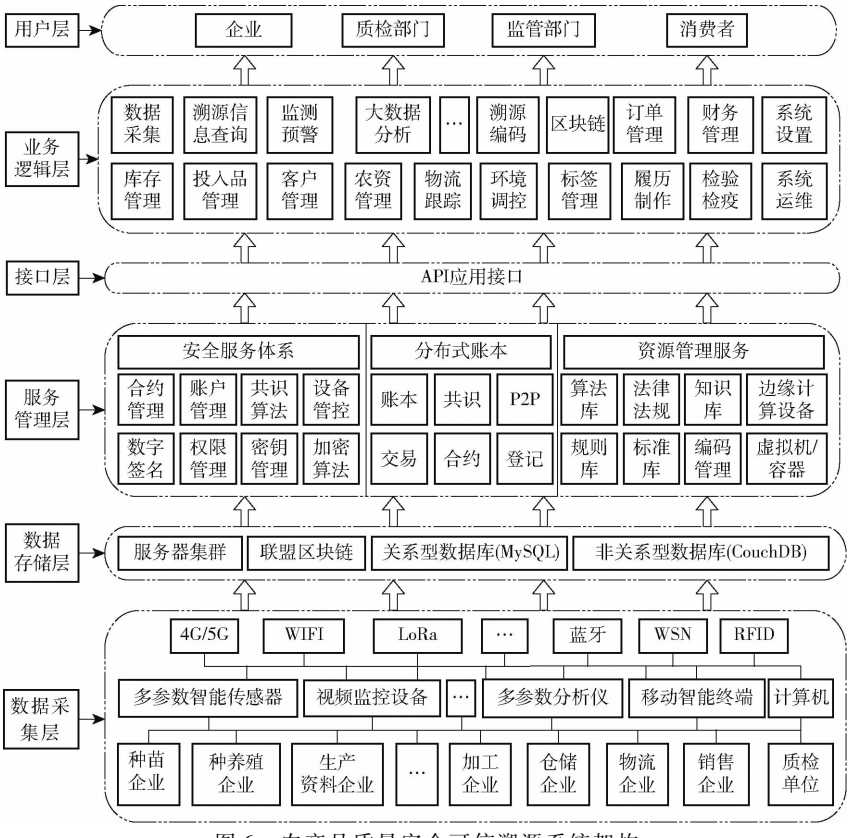

图 6　农产品质量安全可信溯源系统架构

Fig. 6　Architecture diagram of reliable traceability system for agricultural product quality safety

溯源信息清晰地呈现给企业、质检部门、监管部门以及消费者，因此该系统还需能够快速检索到链上所存储的溯源信息。

存储溯源信息时，客户端 SDK 将农产品生产、加工、运输、包装和销售等信息通过 invoke 函数发送到背书节点(Endorser Peer)，背书节点将与链码(Chain Code)实例通信，并为其提供模拟的世界状态(World State)读写集，即链码会执行完溯源信息查询的逻辑任务，但并不会在执行参数时将模拟得到的读写集写入数据库，然后由排序节点对溯源信息进行排序打包入块，最终由提交节点进行验证并提交至账本更新状态数据集；查询溯源信息时，以 ID 标示码为 key 值查询账本记录，通过检索 key 值来依次遍历区块，索引的 value 值为溯源信息的 Hash 值，有时会多次检索 key 值，键-值引入键值的版本号加以标识，版本由块序列号和事务(存储条目)的序列号组成，因此该版本独特且单调递增，每次对同一个 key 值进行写入操作时其版本号(version)都会递增，遍历过程中以 version 的最大值为标准查询。同时，溯源信息与对应的区块号存储在本地数据库，即在查询时将链上、链下两次得到的 Hash 值进行对比以验证溯源数据是否被篡改。对应的合约执行解析区块信息如下

合约 3：Parsing

```
1. contract parsing( )
2. var (
3.    block_height int
4.    recorded_block_height int
5.    block_seq int
6.    )// 定义变量
7. Set max_block_height := retrieve block_height from the ledger
8. Set current_block_height := recorded_block_height
9. If current_block_height < max_block_height:
10. For block_seq in (current_block_height, max_block_height):
11.    Set recorded_block_height := block_seq// 解析区块序号得到 key-value
12. parsing blocks
```

2.4　系统实现

基于区块链的农产品质量安全可信溯源系统采用多层的浏览器/服务器结构，由客户端、服务器和数据库构成。其软件开发环境为区块链平台 Hyperledger Fabric，操作系统 Ubuntu 16.04，应用容器引擎 Docker 18.09、开发语言 Go、Java、JavaScript、HTML 和 CSS，开发框架 Node.js 和 Bootstrap，数据库服务器 CouchDB、LevelDB、MySQL，其中 CouchDB

和 LevelDB 为链上分布式存储的数据库，MySQL 为链下存储数据库等。硬件环境：内存 8 GB、硬盘容量 500 GB、带宽 10 Mb/s。Fabric 联盟区块链使用 Kubernetes 集群服务，由 1 个命令行接口（CLI）节点、3 个控制器节点、1 个负载平衡器、1 个网络文件系统（NFS）节点和多个工作节点组成，每个节点都在 Ubuntu 16.04 虚拟机上运行，Kubernetes 集群的控制器节点负责调度，对等节点和排序节点由 Kubernetes 调度程序以循环的方式部署在工作节点上，以实现分布式存储、防篡改和农产品质量安全可信溯源的目的。

在基于 Hyperledger Fabric 开发平台中，账本（Ledger）作为系统文件记录着数据的更新，由状态数据库（StateDB）维护着真实世界状态（World State），其中 StateDB 就包括 LevelDB 和 CouchDB。其中区块链网络主要由许多对等点组成，其中还包含了向分类帐写入链上的多个智能合约。区块链是一个不断增长的记录列表，称为块。实际上，块包含先前块的 Hash 值、时间戳、事务数据和一些其他信息。除非打破散列 Hash 值，否则不可能篡改分类帐数据，因为分类帐上的所有事务都是按顺序并加密链接在一起的。区块链网络中的数据存储可以是本地数据库或云存储数据库，例如关于茶场的信息（茶场情况、用户简介、设备概况、来自传感器的环境数据以及执行器的控制参数等）。最终用户可以通过各种终端设备读取区块链网络或将数据写入区块链网络。

该系统从用户使用的角度分为管理端、客户端和移动端 3 个子系统，其中管理端是对系统进行管理和运维，管理端控制了客户端和移动端的数据连接，移动端是消费者查询农产品溯源信息子系统，提供了以应用程序接口控制用户界面的形式来显示数据，使用手机扫码的形式来反馈区块信息供用户访问。客户端是农产品产业链多个企业节点进行生产管理、农事作业、加工、运输、包装、销售等使用的子系统，包含产生结果的所有业务逻辑，其中产生的数据使用类似于 JSON 的形式编码，模块之间以 JSON 数据形式进行数据交互，它是一种简易、存取便捷、可读性强的编码形式，更重要的是它的树形结构天然具有可扩展性，对后期各个阶段需要添加更多的数据信息到链中可以扩展，对现有的数据结构仍具有兼容性。客户端使用面向服务的架构提供的接口，以实现与系统服务器的连接，消费者可以从系统获取溯源信息，例如生产数据或成品数据，各个阶段的参与者，如茶庄、加工厂、经销商等都能通过链上的信息对农产品数据进行确认核实。将开发的农产品质量安全可信溯源系统应用于广东清远英德红茶溯源中，其红茶追溯系统客户端、管理端和移动端界面如图 7 ~9 所示。

(a) 产业园区地图展示界面

(b) 数据入库界面

图 7 红茶追溯系统客户端界面

Fig. 7 Client interface of black tea traceability system

图 8 红茶追溯系统管理端界面

Fig. 8 Management interface of black tea traceability system

农产品产业链可信溯源流程如图 10 所示，虚线框内代表红茶溯源安全供应链的材料流程，茶叶从茶园生产出来，经过工厂加工成茶叶或茶叶制品，然后运输到各个厂商进行处理，包装上会印上各自供应商的商标、茶叶的生产日期以及产地，最后摆放在货架上等待售出。这是一个复杂的溯源网络，在每个阶段都有多个合作伙伴，各阶段都有各自的供应商负责进行数据的上链和交互，每个合作伙伴都从多渠道采购原材料提供给上游的供应商，并且上下游的数据信息都是相通的，上链的数据存储进账本就不可以再更改。最终消费者扫描得到的溯源信息是上传到区块内的数据最终选择性的输出结果，其中包括茶叶的溯源码、当前区块的高度以及区块的哈希地址，消费者对买到的农产品通过扫描溯源码进行查询其来源，确保农产品质量溯源数据真实可靠。

图 9　红茶追溯系统移动端界面

Fig. 9　Mobile terminal interface of black tea

3　结论

(1)设计的农产品溯源区块结构,确保农产品溯源数据不可篡改或伪造;“On-Chain + Off-Chain”区块链溯源信息链上链下双链协同管理存储策略,有效减少区块链网络中各节点数据存储压力大、查询效率低等问题;采用 Kafka 共识机制对多参与主体上链的事务进行有效排序,提供数据高吞吐量和低延时的处理能力;同时结合国家食品安全法规编写智能合约,使农产品产业链的数据得以标准和规范,以实时验证拟上链的合约数据、监控区块链网络上的交易信息,触发验证机制对合法信息进行存储,确保农产品数据的可靠性和溯源平台的公信力。

(2)基于 Hyperledger Fabric 区块链平台,对农产品质量安全可信溯源系统进行整体的设计,系统分为数据采集层、数据存储层、服务管理层、接口层、业务逻辑层、用户层 6 层,体现了由物理空间到网络空间、链下数据到链上数据、分散到统一、信息壁垒到透明可靠的全方位设计,解决了传统溯源系统中心化服务效率低、信息不透明、安全风险大等问题。

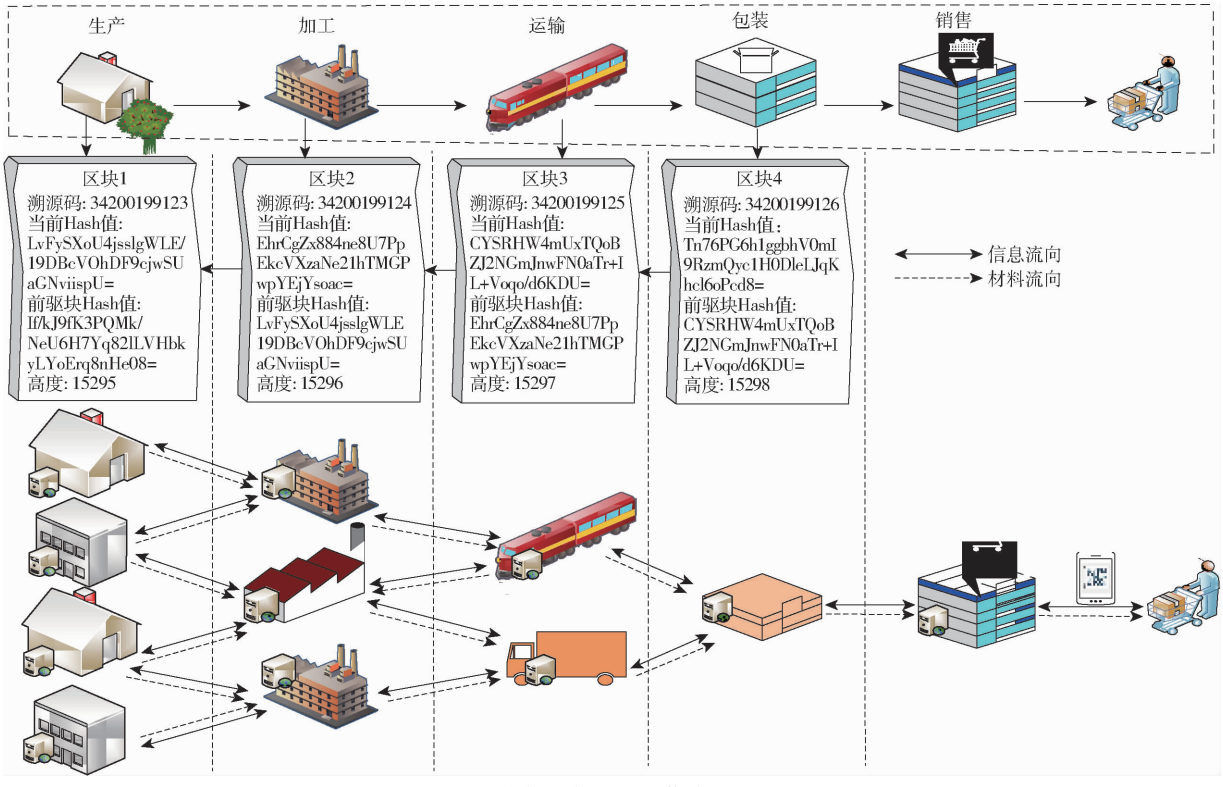

图 10　农产品产业链可信溯源流程图

Fig. 10　Reliable traceability process of agricultural products industry chain

(3)不仅实现了系统数据分散存储、安全规范上链、真实透明存储,消费者还能快捷地查询到所购买农产品的溯源信息,实现了从农田到餐桌全过程生产链、农资供给链、销售链、监督链等多链有机融合,建立了农产品溯源信息不可篡改、全程留痕、公开透明、集体维护的农产品质量安全可信溯源体系,实现了“农企-监管部门-消费者”之间良好的信任氛围,可为其他产品溯源提供借鉴和参考。

参 考 文 献

[1] TILMAN D, CASSMAN K G, MATSON P A, et al. Agricultural sustainability and intensive production practices[J]. Nature, 2002, 418(6898): 671 - 677.

[2] WALES C, HARVEY M, WARDE A. Recuperating from BSE: the shifting UK institutional basis for trust in food[J]. Appetite, 2006, 47(2): 187 - 195.

[3] KUMVENJI D C E, CHAMBA M V M, LUNGU K. Effectiveness of food traceability system of local beef and beef sausages in Malawi: a food safety perspective[J]. Food Control, 2022,137: 108839.

[4] FAN B,QIAN J,WU X,et al. Improving continuous traceability of food stuff by using barcode-RFID bidirectional transformation equipment: two field experiments[J]. Food Control,2019,98: 449 - 456.

[5] CHEN T,DING K,HAO S,et al. Batch-based traceability for pork: a mobile solution with 2D barcode technology[J]. Food Control,2020,107: 106770.

[6] ALFIAN G,SYAFRUDIN M,FAROOQ U,et al. Improving efficiency of RFID-based traceability system for perishable food by utilizing IoT sensors and machine learning model[J]. Food Control,2020,110: 107016.

[7] XIAO X,LI Z,MATETIC M,et al. Energy-efficient sensing method for table grapes cold chain management[J]. Journal of Cleaner Production,2017,152: 77 - 87.

[8] 傅泽田,邢少华,张小栓. 食品质量安全可追溯关键技术发展研究[J]. 农业机械学报,2013,44(7): 144 - 153.
FU Zetian,XING Shaohua,ZHANG Xiaoshuan. Development trend of food quality safety traceability technology[J]. Transactions of the Chinese Society for Agricultural Machinery,2013,44(7):144 - 153. (in Chinese)

[9] 李道亮, 李震. 无人农场系统分析与发展展望[J]. 农业机械学报, 2020, 51(7): 1 - 12.
LI Daoliang,LI Zhen. System analysis and development prospect of unmanned farming[J]. Transactions of the Chinese Society for Agricultural Machinery,2020, 51(7): 1 - 12. (in Chinese)

[10] BOSONA T, GERBRESENBET G. Food traceability as an integral part of logistics management in food and agricultural supply chain[J]. Food Control, 2013, 33(1): 32 - 48.

[11] 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报,2018,29(7):2092 - 2115.
LIU Aodi, DU Xuehui, WANG Na, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7):2092 - 2115 (in Chinese)

[12] 张奥,白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报,2020,31(5):1406 - 1434.
ZHANG Ao, BAI Xiaoying. Survey of research and practices on blockchain privacy protection[J]. Journal of Software, 2020, 31(5):1406 - 1434. (in Chinese)

[13] YANG Xinting, LI Mengqi, YU Huajing, et al. A trusted blockchain-based traceability system for fruit and vegetable agricultural products[J]. IEEE,2021, 9: 36282 - 36293.

[14] 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)

[15] WONG D R, BHATTACHARYA S,BUTTE A J. Prototype of running clinical trials in an untrustworthy environment using blockchain[J]. Nature Communications, 2019, 10(1):1 - 8.

[16] DOOLEY D M,GRIFFITHS E J,GOSAL G S,et al. FoodOn: a harmonized food ontology to increase global food traceability, quality control and data integration[J]. NPJ Science of Food,2018,23(2):1 - 10.

[17] 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)

[18] 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.
YANG Xinting, WANG Mingting, XU Daming, et al. Data storage and query method of agricultural products traceability information based on blockchain[J]. Transactions of the CSAE, 2019, 35(22): 323 - 330. (in Chinese)

[19] 陶启,崔晓晖,赵思明,等. 基于区块链技术的食品质量安全管理系统及在大米溯源中的应用研究[J]. 中国粮油学报, 2018,33(12):102 - 110.
TAO Qi,CUI Xiaohui,ZHAO Siming,et al. The food quality safety management system based on block chain technology and application in rice traceability[J]. Journal of the Chinese Cereals and Oils Association, 2018, 33(12): 102 - 110. (in Chinese)

[20] LEI H, ULLAH I, KIM D H. A secure fish farm platform based on blockchain for agriculture data integrity[J]. Computers and Electronics in Agriculture, 2020, 170:105251.

[21] SALAH K, NIZAMUDDIN N, JAYARAMAN R, et al. Blockchain-based soybean traceability in agricultural supply chain[J]. IEEE Access, 2019, 7:73295 - 73305.

[22] 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)

[23] COCCO L,MANNARO K, TONELLI R, et al. A blockchain-based traceability system in agri-food SME: case study of a traditional bakery[J]. IEEE,2021, 9:62899 - 62915.

[24] WU Y, JIN X, YANG H, et al. Blockchain-based Internet of Things: machine learning tea sensing trusted traceability system [J]. Journal of Sensors, 2022(Special Issue):8618230.

[25] SHAKHBULATOV D, ARORA A, DONG Z, et al. Blockchain implementation for analysis of carbon footprint across food

supply chain[C]//2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019: 546 - 551.
[26] 郭上铜,王瑞锦,张凤荔. 区块链技术原理与应用综述[J]. 计算机科学,2021,48(2):271 - 281.
GUO Shangtong, WANG Ruijin, ZHANG Fengli. Summary of principle and application of blockchain[J]. Computer Science, 2021,48(2):271 - 281. (in Chinese)
[27] HABIB M, MEHMOOD T, ULLAH F, et al. Performance of WiMAX security algorithm (the comparative study of RSA encryption algorithm with ECC encryption algorithm)[C]//2009 International Conference on Computer Technology and Development. IEEE, 2009:108 - 112.
[28] 黄根,邹一波,徐云. 区块链中 Merkle 树性能研究[J]. 计算机系统应用,2020,29(9):237 - 243.
HUANG Gen, ZOU Yibo, XU Yun. Performance analysis and research of Merkle trees with blockchain[J]. Computer Systems & Applications,2020,29(9):237 - 243. (in Chinese)
[29] 袁勇, 倪晓春, 曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11):2011 - 2022.
YUAN Yong, NI Xiaochun, ZENG Shuai, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011 - 2022. (in Chinese)
[30] RAY P P, KUMAR N, DASH D. BLWN: blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare[J]. IEEE Systems Journal, 2020, 99:1 - 12.
[31] JAN M A, CAI J, GAO X C, et al. Security and blockchain convergence with Internet of Multimedia Things: current trends, research challenges and future directions[J]. Journal of Network and Computer Applications, 2021, 175: 102918.
[32] 何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1 - 7,15.
HE Pu, YU Ge, ZHANG Yanfeng, et al. Survey on blockchain technology and its application prospect[J]. Computer Science, 2017, 44(4): 1 - 7, 15. (in Chinese)
[33] UDDIN M. Blockchain medledger: a hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry[J]. International Journal of Pharmaceutics, 2021, 597:120235.
[34] 焦通,申德荣,聂铁铮,等. 区块链数据库:一种可查询且防篡改的数据库[J]. 软件学报,2019,30(9):2671 - 2685.
JIAO Tong, SHEN Derong, NIE Tiezheng, et al. Blockchain DB: a querable and immutable database[J]. Journal of Software, 2019, 30(9): 2671 - 2685. (in Chinese)
[35] TARUN K A, VK A, RP A, et al. Blockchain-based framework for supply chain traceability: a case example of textile and clothing industry[J]. Computers & Industrial Engineering, 2021, 154: 107130.
[36] WAN Z, LO D, XIA X, et al. Bug characteristics in blockchain systems: a large-scale empirical study[C]//IEEE/ACM International Conference on Mining Software Repositories. ACM, 2017.
[37] 王千阁,何蒲,聂铁铮,等. 区块链系统的数据存储与查询技术综述[J]. 计算机科学,2018,45(12):12 - 18.
WANG Qiange, HE Pu, NIE Tiezheng, et al. Survey of data storage and query techniques in blockchain systems[J]. Computer Science, 2018, 45(12): 12 - 18. (in Chinese)
[38] GUPTA S, RAHNAMA S, HELLINGS J, et al. ResilientDB: global scale resilient blockchain fabric[J]. Proceedings of the VLDB Endowment, 2020, 13(6):868 - 883.
[39] SURJANDARI I, YUSUF H, LAOH E, et al. Designing a permissioned blockchain network for the halal industry using hyperledger fabric with multiple channels and the raft consensus mechanism[J]. Journal of Big Data, 2021, 8(1):1 - 16.
[40] YE C, LI G, CAI H, et al. Analysis of security in blockchain: case study in 51%-attack detecting[C]//2018 5th International Conference on Dependable Systems and Their Applications (DSA). Dalian, 2018:15 - 24.
[41] TEAM D. Blockchains tutorials [EB/OL]. https://data-flflair.training/blogs/types-of-blockchain/.
[42] FENG H, WANG X, DUAN Y, et al. Applying blockchain technology to improve agri-food traceability: a review of development methods, benefits and challenges[J]. Journal of Cleaner Production, 2020, 260: 121031.
[43] 孟吴同,张大伟. Hyperledger Fabric 共识机制优化方案[J]. 自动化学报,2021, 47(8): 1885 - 1898.
MENG Wutong, ZHANG Dawei. Optimization scheme for Hyperledger Fabric consensus mechanism[J]. Acta Automatica Sinica, 2021, 47(8): 1885 - 1898. (in Chinese)
[44] WANG Y, CAI S, LIN C, et al. Study of blockchains's consensus mechanism based on credit[J]. IEEE, 2019,7:10224 - 10231.
[45] JEETA A C, RUBEN M, HANS A J. Why do my blockchain transactions fail? A study of hyperledger fabric (extended version)[C]//Computer Science,2021:1 - 18.
[46] LUU L, CHU D H, OLICKEL H, et al. Making smart contracts smarter[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16). New York: Association for Computing Machinery, 2016: 254 - 269.
[47] WANG S, HUANG C, LI J, et al. Decentralized construction of knowledge graphs for deep recommender systems based on blockchain-powered smart contracts[J]. IEEE,2019,7:136951 - 136961.
[48] VACCA A, DI S A, VISAGGIO C A, et al. A systematic literature review of blockchain and smart contract development: techniques, tools, and open challenges[J]. Journal of Systems and Software, 2021, 174: 110891.
[49] MS A,MRJ B,NSS C,et al. Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues[J]. Journal of Network and Computer Applications,2021,178(1):10 - 29.
[50] OKTIAN Y E,LEE S G. BorderChain: blockchain-based access control framework for the Internet of Things endpoint[J]. IEEE Access, 2020, 9: 3592 - 3615.
[51] 王璞巍, 杨航天, 孟佶,等. 面向合同的智能合约的形式化定义及参考实现[J]. 软件学报, 2019, 30(9):2608 - 2619.
WANG Puwei, YANG Hangtian, MENG Jie, et al. Formal definition for classical smart contracts and a reference implementation[J]. Journal of Software, 2019,30(9):2608 - 2619. (in Chinese)
[52] ANDROULAKI E, MANEVICH Y, MURALIDHARAN S, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//The Thirteenth EuroSys Conference, 2018:1 - 15.