

面向热带作物种质资源管理的区块链共识设计与实现

何云¹, 濮文辉¹, 黄振远², 李琼¹, 洪青梅^{1*}

1. 中国热带农业科学院热带作物品种资源研究所, 海南海口 571101; 2. 北京航空航天大学软件开发环境国家重点实验室, 北京 100191

摘要: 种质资源管理信息化是提升种质资源管理效率的必经之路, 共享是激活现有种质资源利用价值, 实现种业乘数效应的重要手段, 共享活动中的惠益分配是推动种质资源共享的原始激励, 而惠益权属存证是惠益分配的关键依据。目前热带作物种质资源管理面临着资源流动业务链条管理分散、资源及业务链信息数据失真、资源可信惠益分配证据链缺失等问题。针对这些问题, 基于区块链技术, 提出了一种面向热带作物种质资源管理的区块链系统, 利用区块链去中心化、不可篡改、全程留痕、可追溯、集体维护、公开透明等特点, 解决信息不对称问题, 从而实现热带作物种质资源的众多有关机构和环节的协作信任与一致行动, 有效地解决上述问题和挑战。该系统实现了热带种质资源全生命周期中对种质资源所作处理的全程留痕, 以及对种质资源的精准溯源, 为今后农业领域与计算机领域相结合、资源溯源等研究工作奠定基础, 对热带作物种质资源高效管理与潜在价值的挖掘具有重要意义。

关键词: 热带作物种质资源; 区块链系统; 科技基础平台

中图分类号: TP311.1; S326 文献标识码: A

Design and Implementation of Blockchain Consensus for Tropical Crop Germplasm Management

HE Yun¹, PU Wenhui¹, HUANG Zhenyuan², LI Qiong¹, HONG Qingmei^{1*}

1. Tropical Crops Genetic Resources Institute, China Academy of Tropical Agricultural Sciences, Haikou, Hainan 571101, China; 2. State Key Lab of Software Development, Beihang University, Beijing 100191, China

Abstract: Information management of germplasm resources is the only way to improve the efficiency of germplasm resource management, sharing is an important means to activate the utilization value of preserved germplasm resources and realize the multiplier effect of seed industry, benefit distribution in sharing activities is the original incentive to promote germplasm resource sharing, and benefit ownership certificate is the key basis for benefit distribution. At present, the management of tropical crop germplasm resources is faced with the following problems: decentralized management of resource flow business chain; distortion of information data of resources and business chain; lack of evidence chain of credible benefit distribution of resources. To solve these problems, based on block chain technology, we put forward a kind of block chain system for tropical crop germplasm resources management to solve the problem of information asymmetry, by using decentralization, tamper-resistant, marks keeping in whole process, traceability, collective maintenance, and transparency, so as to realize the many relevant institutions of tropical crop germplasm resources and link collaboration trust and consistent action, effectively address the above issues and challenges. The system can keep marks processed and trace back to source, in full life cycle of tropical germplasm resources, laid the foundation for the combination of agriculture and computer agriculture, and resource traceability issues research. It is of great significance to the efficient management of tropical crop germplasm resources and the mining of potential value.

Keywords: tropical crop germplasm resources; blockchain system; basic platform of science and technology

DOI: 10.3969/j.issn.1000-2561.2023.10.010

收稿日期 2022-09-07; 修回日期 2022-09-19

基金项目 海南省重点研发计划项目 (No. ZDYF2020035)。

作者简介 何云 (1980—), 女, 学士, 副研究员, 研究方向: 种质资源管理信息化。*通信作者 (Corresponding author): 洪青梅 (HONG Qingmei), E-mail: 82174074@qq.com。

目前,我国已鉴定的热带植物种类有 1.2 万种,占我国植物种群数量的 30%^[1]。热带植物中存在着许多具有特殊价值的基因资源,是我国多种重要战略物资的原材料,在资源利用和集约化生产方面有着巨大的发展潜力。目前我国热带作物(植)物种质资源保存数量已达 4.7 万份,保存于我国热区 7 省(区)的 23 家科研机构中。基于信息技术的热带作物种质资源管理是提升种质资源利用效率的新范式。借助信息化平台整合种质资源,通过约定资源配置机制来盘活存量资源,提升资源供给效率,促进热带作物科研、种业的跨越式发展。种质资源管理信息化通过信息管理系统把种质资源收集、保存、鉴定评价、创新、利用等各环节集成起来,共享信息和资源,有效支撑管理者决策,达到激活现有种质资源价值,实现种业乘数效应,扩大热带作物影响力,为我国社会经济发展和国家安全贡献热作力量。近 3 年,我国已向国内科研和生产单位以及国外的非洲、东南亚国家提供热带作物种质资源共享 6 万份次,为 189 个国家自然科学基金、国家重点研发计划等各级各类科技计划(项目/课题)以及国内企业提供了资源和技术支撑,支撑产出论文 251 篇、论著 13 部、标准 27 项、软件著作权 10 个、专利(含申请)79 项、审(认)定品种 18 个、植物新品种保护权(含申请)12 件、科技成果及科技奖励 26 项。热带作物种质资源共享极大助力国家“创新驱动”“扶贫攻坚”“乡村振兴”“一带一路”等的推进。

传统的信息化管理和安全认证技术具有明显的中心化特性,这与热带作物种质资源的采集环节多、利用链条长、种源基因信息复杂等现状有着难以调和的矛盾。尽管在管理信息化的加持下,热带作物种质资源不断为科研、育种等活动创造价值,为广大从业者带来利益,但也面临着资源流动业务链管理分散、资源及业务链信息数据失真、资源可信惠益分配证据链缺失等问题,主要表现为^[2-5]:(1)在种质资源从持有者到共享者的流动中,信息提供主体发生改变,业务管理链条却不能保持前后信息承接的流转链条,导致业务链条信息管理前后脱节,各自为阵,出现信息误差,影响信息管理效率。(2)热带作物种质资源从收集到共享,环节多、周期长,是一个动态的过程,在资源流动业务链中各节点出于利益驱动会随意私自篡改所涉及流程的信息数据,导致资

源信息、流程信息失真,给共享各方造成不必要损失。(3)种质资源可信惠益分配证据链不完善。种质资源提供者、共享者的贡献无法通过可信的证据链条得到证明,极易产生利益分配纠纷。目前热带作物种质资源共享者一般以非市场化的方式取得种质资源,种质资源的共享活动没有固定的让渡规则,需要共享双方协商确定,无法通过流程链产生的可信信息形成完整的惠益分配证据链。随着热带作物种质资源共享活动的不断增加,资源的权属、流向、惠益分配等问题对热带作物种质资源共享、利用的制约愈加凸显。与权属相关的数据溯源、安全传输、可信转让等环节亟需可靠、高效的解决方案。而区块链技术具有去中心化、不可篡改、全程留痕、可追溯、公开透明等特点,能够解决信息不对称问题,从而实现热带作物种质资源的众多有关机构和环节的协作信任与一致行动,可以有效地解决上述问题和挑战。

目前,国内将区块链应用在农作物种质资源管理的研究主要集中于数据管理层面。中国农业科学院作物科学研究所刘海洋等^[6-8]针对种质资源管理工作中的数据溯源、安全传输、品种确权等问题,提出了基于区块链的解决方案。将当前农作物种质资源数据管理模式中的数据节点按照区块链中的网络节点进行建模,将数据采集、存储、共享分成三大类型(完备级、次完备级、普通)节点;根据数据标准规范及区块链存储特征对作物种质资源进行存储;节点之间进行数据共识则通过“双中心化”节点;种质资源数据加密主要通过非对称加密技术。高阳平等^[9]将区块链技术应用于品牌农产品溯源,将品牌农产品关键生命周期信息上链,采用多方验证参与的模式,基于区块链分布式存储、点对点传输、共识、可溯源、不可篡改等技术特性,构建整个品牌农产品的全产业链关键信息强信任背书追踪溯源能力。

1 相关技术

自从 2008 年 NAKAMOTO^[10]提出区块链以来,建立了以区块链技术为基础的比特币网络,网络中的节点均存储有记录网络交易信息的账本,采用了 P2P 技术^[11],可以跳过第三方机构直接进行金融交易,其底层的区块链技术逐渐引起了产业界的广泛关注^[12]。随着技术的发展,人们对其进行不断更新演进。其中,智能合约应运而

生,即第三代区块链技术^[13]。目前,区块链作为一种新兴创新技术,已融入不同行业、不同领域、不同产品中^[14-17],促进产业更新升级。

区块链系统层次架构如图 1 所示,包含数据层、网络层、共识层、激励层、合约层和应用层^[18-21]。其中,数据层为区块所含数据,即数据加密、时间戳等基础数据和基本算法;网络层包含分布式网络、数据传播、数据验证方法等;共识层包括区块链节点达成共识所需要的各类共识算法如 PoW、PoS 等;激励层主要包括激励的发行和分配方案等;合约层主要包括链上脚本、算法和智能合约,是热带作物种质资源管理与服务区块链系统的研发重点;应用层主要包括各种场景下的应用程序。



图 1 一般区块链系统的层次架构

Fig. 1 The hierarchical architecture of a general blockchain system

在区块链的层次结构中,位于合约层中的智能合约 (smart contract) 可以通过编程方式在一定条件下自动化完成区块链上一系列操作,是支撑和灵活实现各类型交易流程的基础,也是按需构建各类型应用服务的关键。此外,区块链系统中的智能合约模块还需对区块链网络的链码进行编译、维护等操作,并且为系统的其他基础模块和审计模块提供灵活、关键的中间支持。

区块链主要包括公有链、联盟链和私有链 3

种类型。其中,公有链较为开放,难以管理;私有链的应用场景较窄,缺乏开放性;联盟链能够很好地对链上数据隐私问题进行控制,且具有一定的开放性。因此,联盟区块链技术适用于热带作物种质资源管理服务的应用场景。本研究提出的技术方案选用联盟链类型,构建面向我国热带作物种质资源管理与服务的区块链系统。

2 面向种质资源管理的区块链系统

2.1 系统架构

面向热带作物种质资源管理的区块链系统 (Blockchain System for Tropical Crop Germplasm Resources Management, BTCGRM) 分为 3 层: 底层支撑层、服务管理层和应用层。底层支撑层提供区块链的支撑技术包括数据存储结构、网络通信、共识算法、激励模式以及智能合约执行环境等核心技术,实现弹性存储管理、热插拔数据库管理、容器管理与集群管理等;服务管理层包括智能合约管理、安全管理、运营监控、查询引擎、区块链开发 SDK 等核心服务,并向上层提供区块链数据访问和修改、智能合约管理和访问控制的 API;应用层则构建面向种质资源管理与服务的应用,也是资源管理系统与区块链系统交互的核心。其层次架构见图 2。

在热带作物种质资源管理与服务区块链中,通过执行不同的智能合约所产生的交易来完成对种质资源的各类型操作 (收集、保存、鉴定、上链、浏览和交易等)。BTCGRM 架构为联盟链,由异地多节点组成,节点之间使用 PBFT (practical byzantine fault tolerance) 算法形成共识,该算法形成共识的操作流程如图 3 所示,其中 C 为客户端,0~3 表示服务节点,0 为主节点,3 为故障节点。整个算法的基本过程如下:客户端发送请求 (request),激活主节点 (0) 的服务操作;当主节点接收请求后,启动 3 阶段的协议以向各从节点广播请求。所有节点拥有完整区块链数据并运行相同智能合约,对提交到核心节点的种质资源操作信息进行审核记录。系统中所有对种质资源操作的行为由智能合约进行约束、管理和记录。

在种质资源管理与服务区块链网络中,主要包括集中架设的 CA 节点和 Orderer 节点,统一监管平台、统一服务平台、服务方在线服务系统、所有方在线系统均需架设的 Peer 节点及多类型的终端用户 Client 节点 (图 4)。

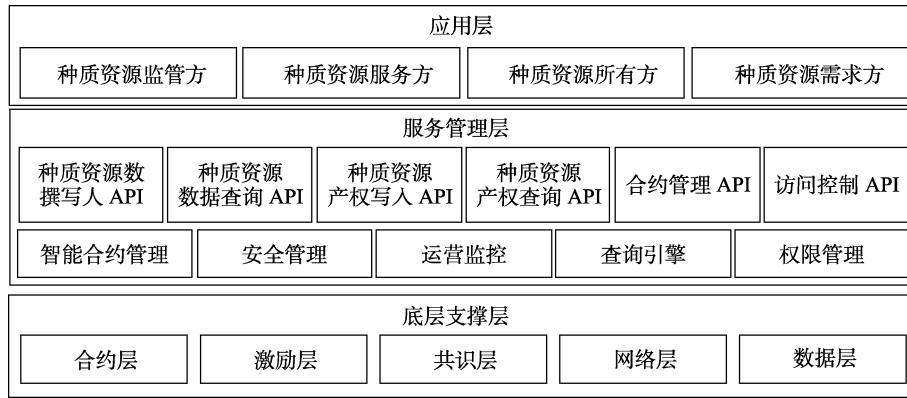


图 2 BTCGRM 的联盟区块链
Fig. 2 Consortium blockchain of BTCGRM

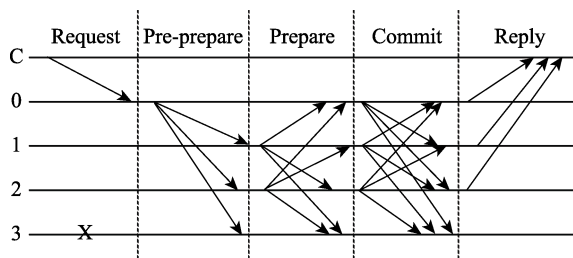


图 3 PBFT 共识算法流程
Fig. 3 PBFT consensus algorithm flow

(1) CA 节点。主要任务是通过加入链内的所有节点（包括上层的终端用户）颁发证书来实现对节点的授权认证，各节点使用证书作为交易流程中的身份识别，其中通过证书认证身份合法性的步骤如下：①客户端收到证书后进行证书

的有效性验证；②客户端使用本地公钥对收到的服务端传来的证书进行解密，得到证书明文和数字签名；③CA 公钥解密数字签名，拿到数字摘要；④hash 证书明文本地生成数字摘要；⑤校验数字摘要是否相同（相同则代表证书明文未做过篡改）；⑥利用服务端的公钥，利用公钥交换对称密钥进行之后的加密通信。

(2) Peer 节点。参与交易的主体代表每个参与到链上的成员，负责储存完整的账本数据即区块链数据，负责共识环节中智能合约的执行。其中维护完整账本数据的 Peer 节点称为记账节点（Committer），并根据具体的业务划分背书策略决定。每个参与到链上的成员都是一个 Peer 节点，

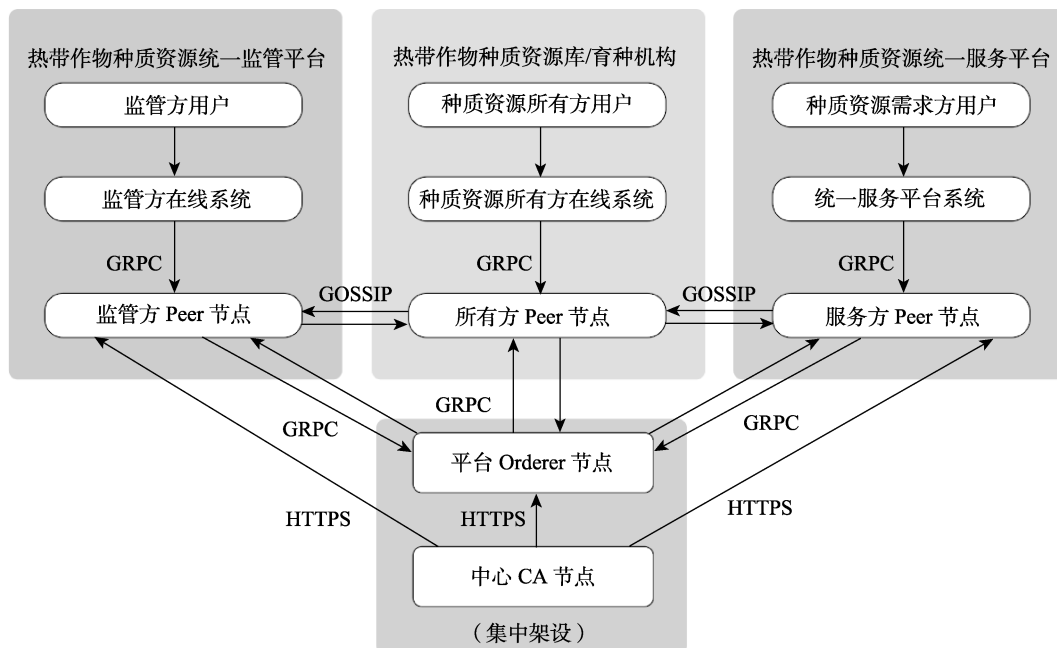


图 4 BTCGRM 技术架构
Fig. 4 Technical architecture of BTCGRM

是参与交易的主体,负责储存完整的账本数据即区块链数据,负责共识环节中智能合约的执行。其中根据节点在交易中的不同角色可以分为背书节点(Endorser)和维护完整账本数据的 Committer。

(3) Orderer 节点。该节点主体功能是收集网络中的交易请求并对交易排序,排序的原则为 First in First Served (FIFS),是由到达 Orderer 的时间来决定,从而保证各 Peer 节点上的数据一致性,然后打包产生新的区块,此外还包含 ACL 访问控制。

(4) Client。Fabric 对各种类型的终端用户提供了 SDK,开发人员可以使用 SDK 发起交易,能够更容易地对接到区块链内的交易环节。

2.2 角色设置

为了兼顾热带作物种质资源易于管控和灵活、可信服务的 2 种需求,在热带作物种质资源管理与服务区块链中,共设置 4 种角色。

(1) 种质资源监管方:依托中国科技资源共享网和中国热带农业科学院热带作物品种资源研究所,联合建设种质资源监管平台,行使管理和考核评价职能,包括种质资源采集监控及统计、种质资源流转监控及统计、种质资源数据质量评测、用户满意度调查、服务性能监测等具体管理任务;

(2) 种质资源服务方:依托中国科技资源共享网和中国热带农业科学院热带作物品种资源研究所,联合建设种质资源服务平台。还包括为种质资源需求使用方提供各类服务的其他机构,包括已经建立的国家热带植物种质资源库,以及其

他社会资金建设的种质资源库、各育种机构等。以上种质资源库和机构均应建立自己的在线服务系统(如网站);

(3) 种质资源所有方:种质资源的产权或其他同类型权益的所有方,既可以独立加入种质资源管理与服务区块链,也可以委托种质资源服务方代理。在有些情况下,种质资源服务方自身也可能持有种质资源的所有权,此时将兼具种质资源服务方、所有方双重角色;

(4) 资源需求使用方:种质资源的终端用户,包括(国内外)科研机构、企业或个人等。

2.3 业务流程

在 BTCGRM 中,一个典型的共享流程如图 5 所示。详细共享流程如下:

(1) 首先由 Client(监管方用户、服务方用户、所有方用户或者种质资源需求方用户)发起共享请求。

(2) 根据事先指定的背书策略,要求监管方 Peer 节点、所有方 Peer 节点和服务平台 Peer 节点中的部分节点参与共享活动,因此 Client 将请求分别发给对应的 Peer 节点。背书策略主要包含主体、门阀阈值。主体定义了期望的签名来源实体,门阀阈值包括阈值和主体,如 T(2, 'A', 'B', 'C') 表示需要 A、B、C 中任意 2 个主体的签名背书。

(3) 每个 Peer 节点接收到 Client 节点的共享请求后,执行各自对应的智能合约产生交易并签名后,分别将输出结果返回给 Client。

(4) Client 在收到所有交易后打包一起发送到 Orderer 节点。

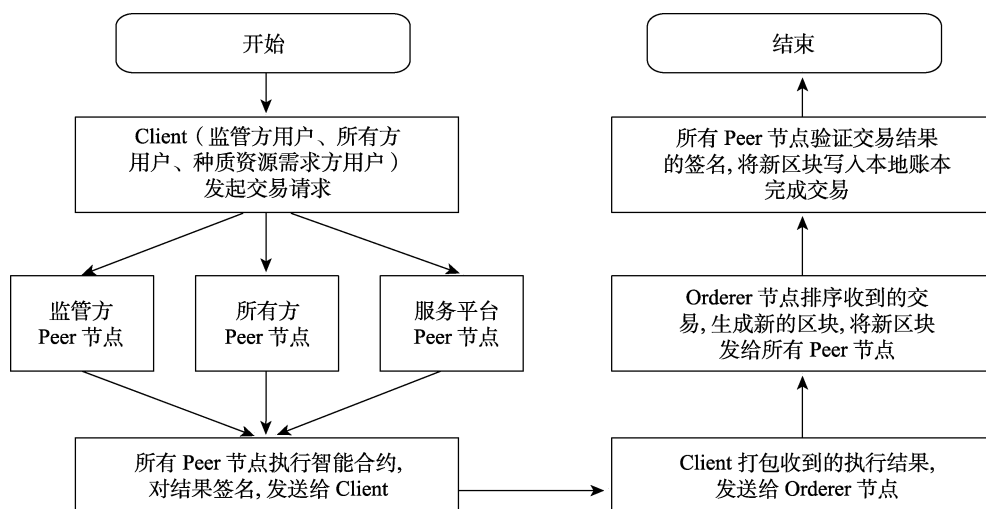


图 5 BTCGRM 典型共享流程

Fig. 5 Typical sharing flowchart of BTCGRM

(5) Orderer 节点将接收到的此次共享在共享池里进行排序并组合打包生成一个新的区块, Orderer 将新的区块发送给所有的 Peer 节点。

(6) 每个 Peer 节点接收到新区块后, 对其中的每一笔共享结果的签名进行验证是否符合背书策略, 并比对读写集合 (Read-Write Set) 与本地的版本是否相同, 如满足所有条件则将新的区

块写入本地账本内完成交易。

3 系统实现

3.1 系统环境

测试环境为 MacOS 系统, 运行在 Mac mini 8G 512G 版本的电脑上, 使用 Java 语言搭建热带作物种质资源管理服务系统, 系统首页如图 6 所示。



图 6 热带作物种质资源管理服务系统首页

Fig. 6 Home page of Tropical Crop Germplasm Resources Management Service System

用户可以登录网站, 对需要了解的种质资源进行搜索, 也可以查看种质资源的统计分类、种质圃 (库)、种质新闻以及特色资源, 并能通过 QQ、电话等方式联系到系统管理员。管理员将时政新闻发布在新闻资讯栏目, 新闻详情页面包含当前所在位置、新闻标题、新闻内容、资讯来源、发布时间、浏览量等信息, 数据从数据库实时获取, 保证了新闻的时效性和发布内容的可控性。

同时, 系统管理员还可以在系统后台实现新闻的发布、种质资源的管理、新增、认定、上链等功能。种质资源信息由管理员或用户提交, 经由执行智能合约、产生交易、打包为区块, 达成共识提交至区块链, 种质资源的上传、下载、传输、授权等过程信息均存储在区块链网络的区块内, 包含种质资源基本信息、收集信息、保存信息、鉴定信息、共享信息等模块, 实现了对种质资源数据的保护确权, 结合区块链技术实现对种质资源的管理和服务。

3.2 系统模块

系统主要包含资源管理模块、文章管理模块、消息管理模块、区块链管理等模块, 各模块主要

负责功能如下: (1) 资源管理模块。对于所有纳入系统管理和服务的种质资源, 种质资源各方应提供种质资源在全生命周期各环节的详细数据, 包括采集、培育、利用等操作记录和相关数据; (2) 文章管理模块。负责系统中的新闻、科技咨询等文章编写与发布; (3) 消息管理模块。负责对种质资源反馈、意见提交处理等; (4) 区块链管理模块。主要负责种质资源溯源、智能合约部署、区块链节点管理、区块信息查询等。

系统的核心流程如图 7 所示。在系统中资源管理角色主要分为: 采集员、鉴定员、保存员、共享人员、区块链管理人员、普通人员。各人员的功能如表 1 所示。

3.3 系统算法

热带作物种质资源管理服务系统中资源上链算法流程如表 2 所示, 其中表 2 算法流程中第 5 步服务器与区块链节点进行上链交易的共识过程可分为 4 步: (1) 各节点独立执行自己的区块; (2) 区块链节点间交换各自执行结果; (3) 统计交换结果; (4) 如超出 2/3 的节点执行结果相同, 则进行交易、出块操作, 否则交易失败。

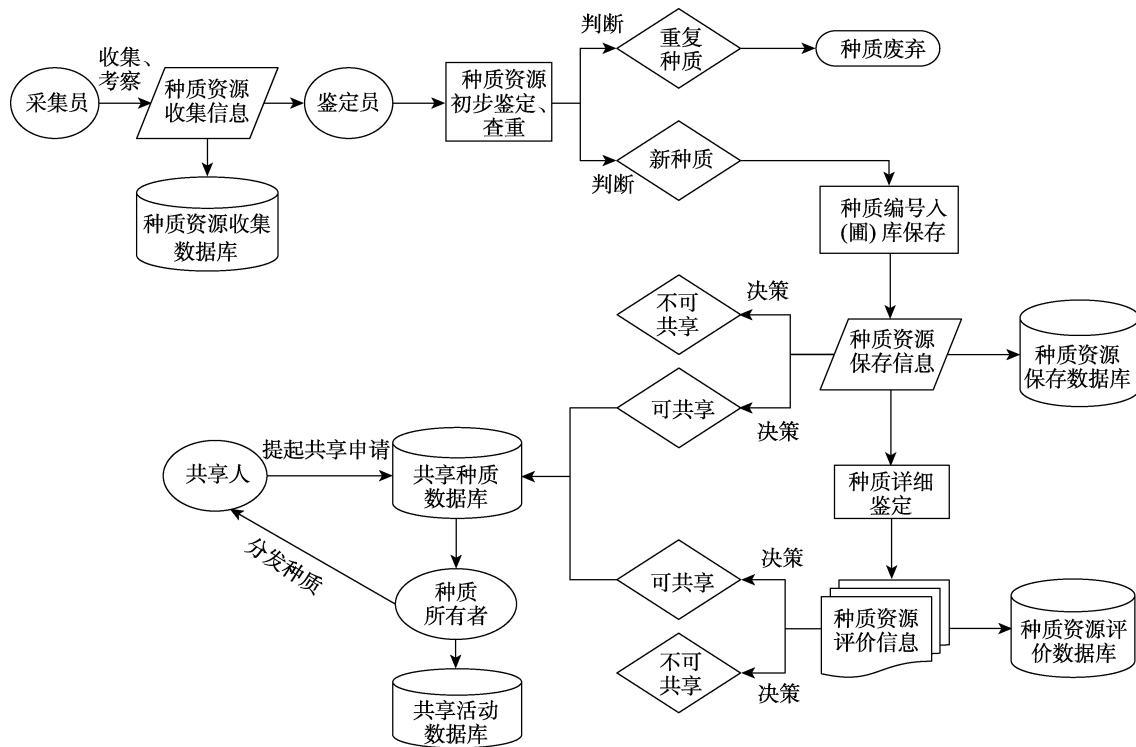


图 7 热带作物种质资源管理系统核心流程图

Fig. 7 Core flow chart of tropical crop germplasm management system

表 1 资源管理角色对应功能

Tab. 1 Resource management roles corresponding function table

管理角色 Management role	功能 Function
采集员	负责户外种质资源的信息采集
鉴定员	对采集人员采集的信息进行鉴定与评价
保存员	对鉴定人员的鉴定信息进行附加消息添加并进行保存入库
共享人员	选择种质资源是否对外共享
区块链管理人员	对最终录入的资源进行上链操作
普通人员	对系统进行普通访问, 如对共享资源的查看等

表 2 系统算法流程

Tab. 2 System algorithm process

序号 No.	区块链系统算法流程 Blockchain system algorithm process
1	输入: 上链资源数据表单
2	输出: 上链结果 (成功或异常情况)
3	step1: 编写资源上链的合约, 进行编译、部署
4	step2: 将部署的合约导出 Java 项目 (将区块链底层与系统项目进行衔接)
5	step3: 将上链的资源数据表单转为 JSON 字符串
6	step4: 通过 http 传输协议传输至服务器 (服务器进行数据的过滤操作, 防止数据被恶意篡改)
7	step5: 服务器与区块链节点进行上链交易 (在交易的过程中, 交易共识采用的是 PBFT 算法)
8	step6: 根据交易回执信息可视化交易结果

4 总结

本文针对当前热带作物种质存在的资源流动业务链管理分散、资源及业务链信息数据失真、资源可信惠益分配证据链缺失等问题, 结合区块链技术提出了热带作物种质资源管理区块链系统方案, 利用区块链的分布式架构、去中心化、不可篡改等特点, 实现了在热带种质资源的全生命周期中, 对种质资源的各种处理做到全程留痕, 以满足在任意环节发起对种质资源的精准溯源。最终加强和促进热带作物种质资源的管理与服务, 由此推动并带动区域产业发展升级, 解决信息不对称问题, 为今后农业领域与计算机领域相结合、资源溯源问题等研究工作奠定基础。但该系统也存在一定的不足之处, 如系统在溯源中会产生较多的区块, 需要进一步对合约优化; 系统对多资源同时上链会有一定的效率低下问题, 需要采取多线程进一步优化。

参考文献

[1] 王文泉, 刘国道. 热带作物种质资源学[M]. 北京: 中国农业出版社, 2008
WANG W Q, LIU G D. Tropical crop germplasm resources[M]. Beijing: China Agricultural Publishing House,

2008. (in Chinese)
- [2] 武晶, 郭刚刚, 张宗文, 王述民. 作物种质资源管理: 现状与展望[J]. 植物遗传资源学报, 2022, 23(3): 627-635.
WU J, GUO G G, ZHANG Z W, WANG S M. Management of crop germplasm resource: advances and perspectives[J]. Journal of Plant Genetic Resources, 2022, 23(3): 627-635. (in Chinese)
- [3] 金黎平, 屈冬玉, 谢开云, 卞春松, 段绍光. 我国马铃薯种质资源和育种技术研究进展[J]. 种子, 2003(5): 98-100.
JIN L P, QU D Y, XIE K Y, BIAN C S, DUAN S G. Research progress on potato germplasm resources and breeding technology in China[J]. Seed, 2003(5): 98-100. (in Chinese)
- [4] 王述民, 曹永生, REDDEN R J, 胡家蓬, SHER T U. 我国小豆种质资源形态多样性鉴定与分类研究[J]. 作物学报, 2002(6): 727-733.
WANG S M, CAO Y S, REDDEN R J, HU J P, SHER T U. The morphological diversity and classification of Adzuki bean [*Vigna angularis* (Willd.) Ohwi & Ohashi] germplasm resources in China[J]. Acta Agronomica Sinica, 2002(6): 727-733. (in Chinese)
- [5] 李鸿恩, 张玉良, 吴秀琴, 李宗智. 我国小麦种质资源主要品质特性鉴定结果及评价[J]. 中国农业科学, 1995(5): 29-37.
LI H E, ZHANG Y L, WU X Q, LI Z Z. Identification and evaluation of main quality characteristics of wheat germplasm resources in China[J]. Scientia Agricultura Sinica, 1995(5): 29-37. (in Chinese)
- [6] 刘海洋, 方洵, 陈彦清, 曹永生. 区块链在农作物种质资源数据管理中的应用初探[J]. 农业大数据学报, 2019, 1(2): 105-113.
LIU H Y, FANG W, CHEN Y Q, CAO Y S. Preliminary study on the application of blockchain in data management of crop germplasm resources[J]. Journal of Agricultural Big Data, 2019, 1(2): 105-113. (in Chinese)
- [7] 刘海洋, 曹永生, 方洵, 陈彦清. 区块链技术在种业大数据中的应用[J]. 中国种业, 2019(5): 22-27.
LIU H Y, CAO Y S, FANG W, CHEN Y Q. Application of blockchain technology in big data of seed industry[J]. China Seed Industry, 2019(5): 22-27. (in Chinese)
- [8] 刘海洋, 曹永生, 陈彦清, 井福荣, 方洵. 农作物种质资源登记区块链模型研究[J]. 植物遗传资源学报, 2021, 22(1): 28-37.
LIU H Y, CAO Y S, CHEN Y Q, JING F R, FANG W. Crop germplasm resources registration blockchain model[J]. Journal of Plant Genetic Resources, 2021, 22(1): 28-37. (in Chinese)
- [9] 高阳阳, 吕相文, 袁柳, 李劼. 基于区块链的农产品安全可信溯源应用研究[J]. 计算机应用与软件, 2020, 37(7): 324-328.
GAO Y Y, LYU X W, YUAN L, LI M. Application of blockchain-based trusted traceability of agricultural products[J]. Computer Applications and Software, 2020, 37(7): 324-328. (in Chinese)
- [10] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[CP/OL].(2020-07-20)[2022-08-22]. <https://bitcoin.org/bitcoin.pdf>.
- [11] DECKER C, WATTENHOFER R. Information propagation in the Bitcoin network[C]//Peer-to-peer Computing (P2P) 2013 IEEE Thirteenth International Conference, Trento, Italy, 2013.
- [12] CROSBY M, KALYANARAMAN V. Blockchain technology: Beyond bitcoin[J]. Applied Innovation Review, 2016, 7(2): 6-19.
- [13] XU X W, PAUTASSO C, ZHU L M. The blockchain as a software connector[C]//2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, 2016: 182-192.
- [14] PILKINGTON M. Blockchain technology: principles and applications[M]. Northampton: Edward Elgar Publishing, 2016.
- [15] 安瑞, 何德彪, 张韵茹, 李莉. 基于区块链技术的防伪系统的设计与实现[J]. 密码学报, 2017, 4(2): 199-208.
AN R, HE D B, ZHANG Y R, LI L. The design of an anti-counterfeiting system based on blockchain[J]. Journal of Cryptologic Research, 2017, 4(2): 199-208. (in Chinese)
- [16] 田海博, 何杰杰, 付利青. 基于公开区块链的隐私保护公平合同签署协议[J]. 密码学报, 2017, 4(2): 187-198.
TIAN H B, HE J J, FU L Q. A privacy preserving fair contract signing protocol based on block chains[J]. Journal of Cryptologic Research, 2017, 4(2): 187-198.
- [17] METTLER M. Blockchain technology in healthcare: the revolution starts here[C]//2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom). Munich, 2016: 1-3.
- [18] 欧阳丽炜, 王帅, 袁勇, 倪晓春, 王飞跃. 智能合约: 架构及进展[J]. 自动化学报, 2019, 45(3): 445-457.
OUYANG L W, WANG S, YUAN Y, NI X C, WANG F Y. Smart contracts: architecture and research progresses[J]. Acta Automatica Sinica, 2019, 45(3): 445-457. (in Chinese)
- [19] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, 45(1): 206-225.
HAN X, YUAN Y, WANG F Y. Security problems on blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2019, 45(1): 206-225. (in Chinese)
- [20] 袁勇, 倪晓春, 曾帅, 王飞跃. 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 Y, NI X C, ZENG S, WANG F Y. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022. (in Chinese)
- [21] 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 Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494. (in Chinese)