

DOI: 10.13733/j.jcam.issn.2095-5553.2024.05.016

杨欣, 赵辰, 刘瑶, 等. 基于实用拜占庭算法的区块链农产品仓储优化研究[J]. 中国农机化学报, 2024, 45(5): 104-110

Yang Xin, Zhao Chen, Liu Yao, et al. Research on blockchain agricultural product storage optimization based on practical Byzantine algorithm [J]. Journal of Chinese Agricultural Mechanization, 2024, 45(5): 104-110

基于实用拜占庭算法的区块链农产品仓储优化研究*

杨欣¹, 赵辰², 刘瑶³, 魏津瑜³

(1. 天津农学院经济管理学院, 天津市, 300384; 2. 天津理工大学中环信息学院, 天津市, 300380;
3. 天津理工大学管理学院, 天津市, 300384)

摘要: 将区块链技术嵌入农产品物流仓储可以有效解决当前农产品仓储遇到的仓储信息不对称、过程透明度低以及信息存储不安全等问题, 促进农业进一步发展。在分析区块链技术如何赋能农产品物流仓储的基础上, 提出基于实用拜占庭算法的区块链农产品仓储优化策略。该策略采用区块链数据结构管理农产品仓储信息, 利用可验证随机函数进行分组, 将 ECDSA 数字签名与可验证随机函数结合改进共识算法, 并接入 Hyperledger Fabric 中部署多个节点进行算法测试。结果表明, 本方案有效解决农产品在仓储过程中存在的安全性及效率低下等问题, 实现“区块链+农产品仓储”的新模式。

关键词: 农业物流; 农产品仓储; 区块链; 共识算法; 可验证随机函数

中图分类号: S24 文献标识码: A 文章编号: 2095-5553 (2024) 05-0104-07

Research on blockchain agricultural product storage optimization based on practical Byzantine algorithm

Yang Xin¹, Zhao Chen², Liu Yao³, Wei Jinyu³

(1. School of Economics and Management, Tianjin Agricultural University, Tianjin, 300384, China;
2. Zhonghuan Information College, Tianjin University of Technology, Tianjin, 300380, China;
3. School of Management, Tianjin University of Technology, Tianjin, 300384, China)

Abstract: Embedding blockchain technology into agricultural logistics warehousing can effectively solve the information problems encountered in the current agricultural product warehousing such as asymmetric warehousing information, low process transparency and unsafe information storage in agricultural logistics warehousing, and promote the further development of agriculture. Based on the analysis of how blockchain technology can empower agricultural logistics and warehousing, this paper proposes a blockchain agricultural product warehousing optimization strategy based on the practical Byzantine algorithm. This strategy uses the blockchain data structure to manage agricultural product storage information, uses verifiable random functions for grouping, combines ECDSA digital signatures with verifiable random functions to improve the consensus algorithm, and deploys multiple nodes in Hyperledger Fabric for algorithm testing. The test results show that, this solution effectively solves the problems of safety and low efficiency in the storage process of agricultural products, and realizes the new model of “blockchain + agricultural product storage”.

Keywords: agricultural logistics; agricultural warehousing; blockchain; consensus algorithm; verifiable random function

0 引言

农产品仓储能够实现农产品由生产地向消费地转移, 是农业在生产活动中不可缺少的环节。当前, 作为

德国“工业 4.0”战略三大主题之一的智能仓储物流, 已成为“中国制造 2025”计划智能制造的主攻方向之一^[1]。由于传统农产品物流仓储管理存在管理方式复杂、易出错, 查询困难、需第三方可信中心确保交易执

收稿日期: 2022 年 9 月 28 日 修回日期: 2023 年 2 月 21 日

* 基金项目: 2021 年天津哲学社科重点项目(TJGL21-010)

第一作者: 杨欣, 女, 1984 年生, 沈阳人, 博士, 教授, 硕导; 研究方向为企业信息化。E-mail: wing.lps@163.com

通讯作者: 魏津瑜, 男, 1968 年生, 山东乐陵人, 博士, 教授, 博导; 研究方向为区块链技术、农业互联网。E-mail: weijinyu2010@126.com

行等问题,导致农产品供应链整体产能较低、时效性较差,不能快速响应用户需求,容易产生较大损失。随着数字化时代的到来,运用新型信息技术提升农产品仓储管理效能成为未来智能农业仓储发展的主要方向。区块链作为一种由 P2P 网络、密码学等组成的具有去中心化特征的记录技术^[2],具有分布式数据存储、点对点传输、共识机制、加密算法等特点^[3],可实现去中心化可信交易,将该技术融入至农产品物流仓储可提升农产品的整体仓储效能。

随着网络信息技术的成熟,区块链与各领域的融合与研究也成为学界关注的重点。近年来,将区块链技术应用于农业物流领域的研究较多,尚杰等^[4]利用区块链技术改善生态农产品供应链内部信息不对称现象从而增加交易、节省成本,以保障生态农产品供应链稳定运行;吴晓彤等^[5]基于区块链的农产品溯源系统模型为基础,实现了农产品的可信溯源,保障农产品质量信息的安全性和可信性;张森等^[6]提出一种面向冷链物流行业的区块链技术解决方案。针对订单数据和环境数据分别设计上链系统,实现了订单数据安全上链、冷链环境数据实时上链以及物联网设备的身份认证与权限控制机制,提高了冷链物流行业的可信性和数据的安全性。通过对已有文献分析可知,区块链在农业物流方面的应用多集中在供应链与冷链领域,鲜少在仓储方面融入区块链技术。此外在现存的农产品物流仓储管理平台中,农产品仓储的安全性能较低,存储系统的性能受外界影响较大,无法避免进出农产品管控中的各种漏洞,对农产品的仓储物流效率产生影响,而基于区块链架构的共识算法能有效提高农产品仓储系统的吞吐量和信息确认效率。因此设计合理的共识算法可较好地解决货物存储中存在的问题。

近年来针对共识算法的研究,多趋向于对实用性强的实用拜占庭算法(PBFT)进行改进。Mingxiao Du等^[7]采用分层的 MBFT 网络结构,利用 LCG 对数据进行扩展,从而增加区块链系统的吞吐量,但针对 PBFT 算法通信复杂度较高的问题并没有得到更好地改善。伍星等^[8]基于 QoS 值提出了 Q-PBFT 算法,并将其匹配云制造服务场景。通过理论和试验表明该算法可以减少带宽消耗、降低共识时延,从而提升基于区块链的云制造服务平台的性能。Li 等^[9]提出了一种可扩展的多层 PBFT 共识机制以降低单层 PBFT 共识的通信量。然而,目前针对共识算法的研究多致力于共识节点模型的修改以降低通信复杂度与时延,提高吞吐量,其安全性与共识速度方面还存在一定缺陷。

鉴于此,本文通过引入 Hyperledger fabric 框架编写底层区块链,保证数据的存储与发布安全可靠,避免

因平台中心化引起的系统故障和数据丢失。同时将改进的 PBFT 算法应用至共识层,加强共识模块中对恶意攻击的检测和排除,为今后采用非传统布局仓储运作的农产品仓库管理者提供决策支持。

1 区块链嵌入的农产品物流仓储平台构建

1.1 农产品物流仓储平台需求分析

随着互联网的发展,传统农产品仓储管理系统的中心化弊端日渐显露。多数情况下使用第三方的管理系统可以提高农产品的信息处理和交易成本,但此过程会出现农产品物流信息不透明、难以追溯追责等问题,造成服务质量大幅降低。此外由于农产品种类繁多、数量庞大、存储保鲜要求各异,受自然条件的制约和影响,产量不稳定、供给与需求之间存在矛盾。为满足农产品仓储中用户的隐私保护、交易安全、数据存储等多方面的需求,本文引入以下技术:(1)引入身份认证模块与公私钥技术,保证系统的安全性;(2)引入权限模块以便拥有权限的用户可以随时随地查询农产品仓储信息;(3)引入农产品仓储管理模块负责农产品的出库、入库、移库、库存盘点、分类以及库存查询等。

此外,为确保系统的稳定性运行,提高系统的易用性,改善用户的使用体验。在安全性方面基于区块链架构的系统具有严格的访问限制,可以消除农产品在录入过程中业务活动信息和交易数据被篡改和破坏的风险,保证系统活动数据的安全性。在可靠性方面区块链技术对数据的输入有一个严格的审核过程^[10],只有当所有参与用户通过共识机制审核后,数据方能存储在区块链上,保证了数据的可靠性。

基于区块链嵌入的农产品物流仓储平台通过区块链式结构记录存储数据,智能合约定义业务逻辑^[11],共识算法对交易、合约数据进行共识,实现农产品数据存储,满足各类农产品仓储的不同需求。利用此平台可以确保信息的公平性,保证农产品信息的可追溯,强化农产品物流仓储平台的风险管控;同时采用区块链技术+智能仓储的模式,可有效提升农业仓储管理水平,增强农产品仓储的可视化,方便其进行线上、线下的售卖或调转,体现农产品仓储在调节供需矛盾以及规避风险方面的作用,为农产品物流仓储领域的发展提供新的动力。

1.2 区块链嵌入的农产品物流仓储平台设计

本文使用 Hyperledger fabric 作为农产品物流仓储平台的区块链部分,底层设计利用区块链的防篡改性和可追溯性^[12]。系统的功能模块主要分为注册和登录模块、用户管理模块、农产品仓储信息存储模块、农产品仓储信息查询、接口模块等部分。该系统整体

架构如图 1 所示。

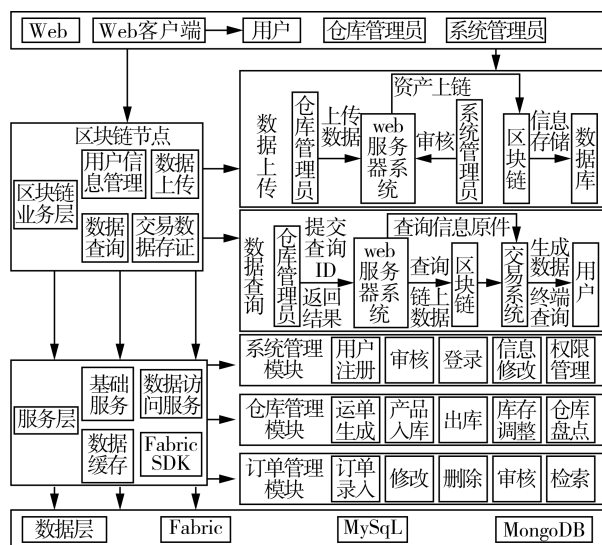


图 1 系统整体架构图

Fig. 1 Overall architecture of the system

在农产品物流仓储平台上用户首先需要注册账号,已经有账号的用户可直接登录系统。在注册成功的同时,服务器也会将用户信息在区块链注册。当用户进入系统后,可选择提交信息发布、录入、查询、存储等申请。在提交完成后,用户的信息参数将会被提交至 Hyperledger fabric 网络封装成客户端的请求。在服务模块收到申请后,将调用相关的链上代码进行交易处理,随后提交至背书节点验证。在依照背书协议进行背书后,请求会被所有共识节点按本文改进的 PBFT 进行共识,最后区块被各节点确认。此过程完成后所有的农产品数据均被部署到区块链中,可随时查询与更新。除此之外在仓储管理的环节上,由于农产品的特殊性与活性,在收获后甚至加工后还保持着一定的新鲜度。为了将农产品的生理活动减少到最低的程度,保证农产品质量,农产品仓储则成为影响商品质量的一个至关重要的因素。对于不同的农产品来说,依据其性质和特点,需要使用不同的贮存方式,以便拥有较长的贮存期。

结合分布式共识、加密算法和签名算法等技术,使用 Hyperledger 框架作为底层应用程序平台,同时使用链上代码以确保链上数据的透明性和防篡改性。此外在底层区块链的共识模块中利用改进的 PBFT 算法进行共识操作,在一定程度上提高系统的交易吞吐量、节省系统资源的消耗,保证该平台的稳定运行。

2 基于可验证随机函数的 PBFT 共识算法改进

2.1 算法改进设计

2.1.1 基于 ECDSA 的可验证随机函数

椭圆曲线数字签名算法(ECDSA)是使用椭圆曲

线密码对数字签名算法的模拟^[13],本文将 ECDSA 与可验证随机函数结合,主要过程包括系统初始化、密钥生成、随机数和证明生成、验证。过程如下:(1)设置系统参数: $GF(q)$:阶为 q 的有限域; q : A 位的大素数; E :定义在 G 上的椭圆曲线; G :椭圆曲线上的基点。(2)密钥生成:选择随机数 $x \in [1, q-1]$,生成一对椭圆曲线密钥,其中私钥为 x ,公钥为 $Y=xG$;(3)随机数和证明生成:输入消息 m ,私钥 x ;输出:随机数 v ,证明 $proof$ 。(4)验证:输入消息 m' ,证明 $proof'$;输出合法性。

2.1.2 算法优化方案

在 PBFT 算法中,达成共识所需要的通信次数会随着节点数量的增加呈现多项式级别的增加^[14],其中通信次数为 $F(n)=2n(n-1)$, n 为节点数^[15]。本文通过对节点数优化,将基于 ECDSA 的可验证随机函数算法应用于分组中,通过降低 n 值,改进算法性能。在初始阶段,将 n 个相同的共识节点分成 x 组。每组分别进行 PBFT 算法,同时每组的主节点间进行 PBFT 算法。具体分组过程的示意图如图 2 所示。

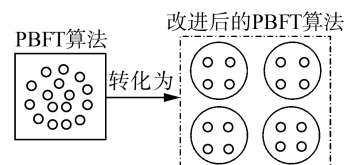


图 2 PBFT 改进算法的示意图

Fig. 2 Schematic diagram of the improved PBFT algorithm

此外,在共识过程中,当主节点故障或存在恶意为需要进行视图切换时。通常利用某一轮次视图编号 v 和副本个数 R 作为输入,即 $P=v \bmod R$ 得到新一轮次主节点。但由于 v 和 R 是公开的,其抽签结果可以被预测,节点容易遭受攻击。

本文利用基于 ECDSA 的可验证随机算法可提高安全性。该算法执行过程首先对各节点轮流进行抽签,通过各节点的私钥外加全网都知道的随机数 W 作为输入,生成一个零知识证明以及随机数。随后所有节点轮流抽签,率先抽到大于 W 的随机数则为当前轮次的打包者,并在广播的内容中加入一个零知识证明。通过零知识证明,使得全网节点只需通过公钥就可以验证并接受新一轮次的打包者。同时该过程其他节点不知道新一轮次打包者的私钥因而不会出现与其相同的结果。

2.2 算法实现流程

本文结合可验证随机函数设计随机分组算法,应用该算法将共识网络中所有无差别的节点随机分为 x 组。该算法执行流程如图 3 所示:(1)所有节点使用算法生成一对公钥 PK 和私钥 SK 。(2)输入上一步生

成的 SK 和随机生成的消息 M ,通过计算得到随机字符串 W 和证明 P ,将每个节点生成的随机字符串 W 进行广播。(3)每个节点会收到 n 个字符串,随后对其进行字典序排序,将字符串数组分为 x 组。(4)每个节点广播验证消息 $\langle verify, v, p, VK, A \rangle$, A 为节点的地址。(5)每个节点收到验证信息后,对第三步得到的 x 组字符串使用 $\langle verify, m, v, p, VK, A \rangle$ 算法进行验证。得到节点地址的数组后,各节点联系各所在组的其他节点。(6)分组完成后,所有的节点被随机的分为 x 个相同的组,等待执行共识算法。

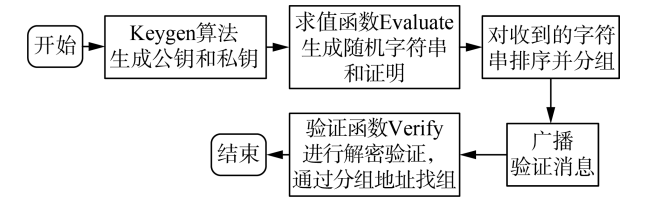


图 3 VRF 算法执行流程图
Fig. 3 Flowchart of VRF algorithm execution

当分组完成后,如若主节点故障或被恶意攻击时,需要启动视图更换协议^[16]。客户端利用在客户端及节点中引入的“发布—订阅模式”通道,订阅“主节点更换消息”得知主节点选举情况以节省等待时间。组主节点向其他节点广播视图切换消息。其他组主节点得知总主节点错误后,向分组内的所有节点发送重新执行随机分组算法的消息。

算法执行完成后会得到新的总主节点,当总主节点收到 $2f$ 个来自其他分组主节点的有效的视图更换消息后^[17]。总主节点向其他分组主节点广播新视图消息 $\langle new-view, v+1, V, Q \rangle$; V 包含主节点收到的 $2f+1$ 个有效的视图更换消息, Q 包含有效的预准备消息^[18]。如若主节点收到的 $2f+1$ 个有效的视图更换消息集合存在序号 n ,说明存在预准备消息 m ,则主节点需要向网络中其他节点广播新的预准备消息 $\langle pre-prepare, v+1, n, d \rangle$;如若都不包含序号 n ,说明不存在未提交的消息。

2.3 安全性分析

与传统的 PBFT 共识算法相比,在本文设计的改进共识算法中,是通过使用可验证随机函数随机生成主节点,其他节点可以通过随机数的输入与输出,确定其是否由该输入生成;且该过程不需要公开私钥,因此使原有共识机制的安全性能增强。除此之外,传统的 PBFT 提案人是固定的,当提案人宕机后,进行 *View change* 时通常选择节点排序,顺次成为提案人。而本文是在 *View change* 时使用上一次的 *VRF Value*+节点私钥进行 *VRF* 运算,计算出的 *VRF Value* 作为计算下次轮次提案人的因子,并将

VRF Proof、*VRF Value* 发送给其他 *Orderer* 节点做验证,其他节点验证通过后,更换新提案人。因此。引入基于 ECDSA 的可验证随机函数改进共识算法可以确保数据的安全存储和不可篡改,同时在系统故障时也能保障系统的安全运行。

3 算法测试与分析

3.1 试验环境配置与搭建

本论文采用的硬件环境 CPU 4 核,内存 2G 的计算机 4 台。超级账本的部署关系到整个系统的底层业务。在本系统中主要实现的工作是超级账本网络的联盟链架构,具体的环境配置和软件如表 1 所示。

表 1 环境配置与软件版本		
Tab. 1 Environment configuration and software version		
类别	名称	版本
操作系统	CentOS Linux release	7.9
容器环境	Docker	19.03
容器编排	Docker-compose	1.23.1
超级账本	Hyperledger	2.2.1
编程语言	Golang	1.14
运行环境	Nodejs	8.16.2

3.2 测试方法与部署

本文使用服务器 A、B、C 进行试验,下载并修改 Hyperledger Fabric 2.2.1 的源代码,通过更新 configtxgen 和 orderer 服务的相关文件,将 VRF 改进带入共识中,并在 Docker-compose 脚本中为 orderer 节点配置唯一的标识、端口和节点列表。节点的具体部署情况如表 2 所示。

表 2 服务器节点部署	
Tab. 2 Server node deployment	
服务器	部署情况
A	peer0. org1、caplier、order0、order4、order7、order10、order13
B	peer1. org1、order1、order3、order6、order9、order12、order15
C	peer0. org2、peer1. org2、order2、order5、order8、order11、order14

3.3 测试结果

3.3.1 可验证随机函数性能测试

利用天津市汉拓计算机研究所的试验环境和数据,依照本文设计的可验证随机函数进行性能测试。其实现的可验证随机函数主要分为三部分:生成密钥、生成随机数和证明、验证随机数和证明。通过试验编写代码对本方案设计的可验证随机函数进行了多次测试,得到各部分算法的平均运行时间如表 3 所示。

表 3 可验证随机函数各部分运行时间测试
Tab. 3 Running time test of each part of the verifiable random function

算法	次数	总时间/s	平均时间/s
生成密钥	10 000	0.437 237 815	0.000 044
生成随机数和证明	10 000	158.045 739 986	0.015 805
验证随机数和证明	10 000	207.735 800 654	0.020 774

由表 3 可知,可验证随机函数各部分算法的运行时间均在毫秒级,并且相较于处理交易所需的总时间,基本可以忽略其对交易处理速度的影响。

3.3.2 算法验证过程

为证明本文提出的算法效率更高,将原始 PBFT 和改进后 PBFT 的通信次数公式列举如表 4 所示。

表 4 中 n 为节点个数, x 为分组的数量。改进后

$$\frac{T}{\partial x} = \frac{(2n^2 - 2n)x^2 + (n - n^2)x^4 + (n^3 - n^2)x^2 + (2n^3 - 2n^4)x}{x^8 - 2x^7 + x^6 - 2nx^5 + (2n^2 + 2n)x^4 - 2n^2x^3 + n^2x^2 - 2n^3x + n^4} \quad (2)$$

通过式(2)可知,当斜率为 0 时,存在极值。对于 x 存在一个最优值 W 使得 T 值最大,即当改进后的 PBFT 算法中 x 的值为 W 时,通信次数最低。令式(2)的值为 0,则 $W = \sqrt{n}$,由此可知,当 x 的值小于 W 时, T 值呈现单调递增的趋势,最小值为 1,即组数的最小值为 1,进而得到 T 的取值范围为 $[0, W]$,说明利用可验证随机函数改进的 PBFT 共识算法其通信次数小于等于原始 PBFT 共识算法,因而通过该公式推导证明本次改进算法的正确性。

3.3.3 共识算法测试数据

通过对改进前后的 PBFT 算法进行测试,分别将交易量总数设置为 200,300,500,1 000 进行试验。此外分别设置 4,7,10,13,16 节点探究其吞吐量及时延的变化情况。吞吐量是指在一个共识周期下,写入区块中的数据所包含的交易数与确认时延的比值^[19],用 TPS(Transaction Per Second,每秒交易数)来表示。

$$TPS = \frac{\text{SumTranscations}_{\Delta t}}{\Delta t} \quad (3)$$

式中: SumTranscations——总吞吐量;

Δt ——时间长度。

3.3.4 同交易量不同节点对比

当交易总数为 1 000 时,不同节点下的时延以及吞吐量情况如图 4 所示。当发送量为 1 000 时,交易时延随着节点数量的增多呈现上升趋势,即同交易量下节点数量越多其处理事务消耗的时间越长。改进后的 PBFT 随着节点数量的增多其时延提升较小,基本处于同一水平。此外改进后 PBFT 在 16 节点的时延与原 PBFT 在 4 节点的时延相近,说明改进后的 PBFT 较原 PBFT 相比有较高的处理速度和效率。

的通信次数前半部分表示组内节点间的通信次数,后半部分表示各组主节点间的通信次数。

表 4 PBFT 通信次数
Tab. 4 PBFT communication times

算法名称	通信次数
PBFT	$2n(n-1)$
改进后的 PBFT	$2(n/x) \times (n/x - 1) + 2x(x-1)$

令改进前后 PBFT 的通信次数比为 T ,得到式(1)。

$$T = \frac{2x(x-1)}{2\left(\frac{n}{x}\right) \times \left(\frac{n}{x} - 1\right) + 2x(x-1)} \quad (1)$$

假设节点数 n 为常数时,组数 x 存在极值,此时,对 T 进行求导可得式(2)。

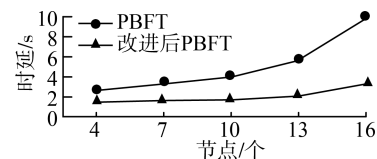


图 4 发送量为 1 000 时不同节点的时延数据

Fig. 4 Delay data of different nodes when the transmission volume is 1 000

如图 5 所示,当发送量为 1 000 时,随着节点数量增多其吞吐量也呈现出下降趋势。此外原 PBFT 在 4 节点时的吞吐量与改进后 PBFT 在 16 节点的吞吐量接近。因此可以得知改进后的共识算法,即便在较多节点的情况下其单位时间内处理交易量笔数也优于改进前的 PBFT。

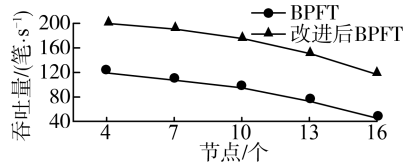


图 5 发送量为 1 000 时不同节点的吞吐量数据

Fig. 5 Throughput data of different nodes when the sending amount is 1 000

综上所述,同交易量下改进后的 PBFT 较原 PBFT 相比吞吐量较高、时延较低。除此之外随着节点数量的增多,原 PBFT 在超过其处理能力后,时延与吞吐量都有明显的下降趋势;而改进后的 PBFT 在时延与吞吐量方面影响较小。因此可以看出改进方案的性能较之前相比有所提高。

3.3.5 同节点时不同交易量对比

根据 Caliper 报告测出的数据进行分析,对 PBFT 以及改进后 PBFT 的 10 节点性能试验,其时延与吞吐

量如图6所示。由图6可知,改进后的PBFT与改进前的时延相近。但当到达一定交易量范围后,会出现明显延迟,时延差距较大。因而推知在未达到交易上限时,代表系统有能力处理,此时的延时不会过高。但当系统无法处理时,交易会发生堆积,导致延迟增加。相较于原PBFT在达到上限后时延的突增,改进后的PBFT在达到上限后的时延与未达上限前的时延差距较小,表明了改进后的PBFT具有较好的低延时性。

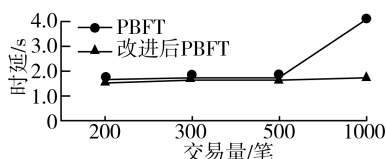


图6 10节点的时延数据

Fig. 6 Delay data of 10 nodes

由图7可知,在同节点的情况下,当交易笔数较少时,改进前后PBFT的吞吐量差别不大。但随着交易笔数增多,原方案很快到达处理上限,并会维持在某一TPS水平附近;然而改进后的方案随着交易笔数的增多其吞吐量仍继续增加。由此可知,改进后的方案较原方案相比在吞吐量上有更高的提升。特别是在交易量较多时,改进后的方案其处理事务能力更强。

综上所述,通过对10节点进行分析,可以看出在其处理能力范围内时吞吐量与时延差别较小;但当超过其处理能力范围,改进后的PBFT较最初相比有更好的处理能力。

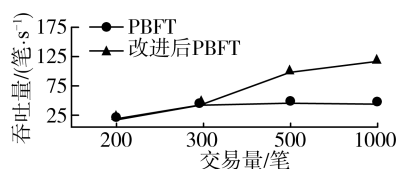


图7 10节点的吞吐量数据

Fig. 7 Throughput data of 10 nodes

4 结论

本文通过分析传统农产品仓储管理系统存在的信息不对等、安全性较差等问题,利用区块链的去中心化、分布式存储、共识机制等技术,提出基于区块链的智能农产品仓储模型。该系统对农产品仓储管理系统的优化升级主要体现在3个方面。

1) 通过对企业和农产品仓库的智能化监管实现资源的可管可控,保障各平台间的数据交互。

2) 加强对农产品储备信息的集中管理,促进数据资源的汇聚共享。

3) 有望逐步形成区域农产品联盟链,有助于完善区域农产品数据存储、处理、动态监管和协同调度,提升农产品仓储管理系统的安全性、可视性、易用性等。

相较于传统集中式农产品物流仓储系统,该系统虽然需要更多的环境配置以及调试操作,但其去中心化的设置提升了平台的安全性及实用性,方便查询与操作。

综上所述,将区块链的优良特性应用至农业可有效解决目前农产品仓储系统存在的问题,提升协作效率,实现资源的有效整合与效益的最大化。本文不仅为农产品仓储优化问题提供了新视角,同时也对农业发展起到重要作用。关于“区块链+农产品智能仓储”的模式,可以在此基础上进一步探索,形成更加透明、高效、安全的物流仓储体系。

参考文献

- [1] 刘强. 智能制造理论体系架构研究[J]. 中国机械工程, 2020, 31(1): 24-36.
Liu Qiang. Study on architecture of intelligent manufacturing theory [J]. China Mechanical Engineering, 2020, 31(1): 24-36.
- [2] 周艺华, 方嘉博, 贾玉欣, 等. 基于PBFT的联盟链共识算法[J]. 计算机科学, 2021, 48(11): 133-141.
Zhou Yihua, Fang Jiabo, Jia Yuxin, et al. Consortium blockchain consensus algorithm based on PBFT [J]. Computer Science, 2021, 48(11): 133-141.
- [3] Belhi A, Gasmi H, Bouras A, et al. Integration of business applications with the blockchain: Odoo and hyperledger fabric open source proof of concept [J]. IFAC-PapersOnLine, 2021, 54(1): 817-824.
- [4] 尚杰, 吉雪强. 区块链应用下生态农产品供应链优化[J]. 华南农业大学学报(社会科学版), 2020, 19(4): 67-75.
Shang Jie, Ji Xueqiang. Optimization of ecological agricultural supply chain based on block chain application [J]. Journal of South China Agricultural University (Social Science Edition), 2020, 19(4): 67-75.
- [5] 吴晓彤, 柳平增, 王志铎. 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.
- [6] 张森, 叶剑, 李国刚. 面向冷链物流的区块链技术方案研究与实现[J]. 计算机工程与应用, 2020, 56(3): 19-27.
Zhang Sen, Ye Jian, Li Guogang. Research and implementation of blockchain technology scheme for cold chain logistics [J]. Computer Engineering and Applications, 2020, 56(3): 19-27.
- [7] Du M, Chen Q, Ma X. MBFT: A new consensus algorithm for consortium blockchain [J]. IEEE Access, 2020, 8: 87665-87675.
- [8] 伍星, 范玉顺. 云制造服务场景下基于QoS值的改进PBFT算法[J]. 计算机集成制造系统, 2021(16): 1767-1776.
Wu Xing, Fan Yushun. Improved PBFT algorithm based

- on QoS value in cloud manufacturing service scenario [J]. Computer Integrated Manufacturing Systems, 2021(16): 1767—1776.
- [9] Li W, Feng C, Zhang L, et al. A scalable multi-layer PBFT consensus for blockchain [J]. IEEE Transactions on Parallel and Distributed Systems, 2020, 32(5): 1146—1160.
- [10] 冷基栋, 吕学强, 姜阳, 等. 联盟链共识机制研究综述[J]. 数据分析与知识发现, 2021, 5(1): 56—65.
Leng Jidong, Lü Xueqiang, Jiang Yang, et al. Consensus mechanisms of consortium blockchain: A survey [J]. Data Analysis and Knowledge Discovery, 2021, 5(1): 56—65.
- [11] 刘双印, 雷墨鹭兮, 王璐, 等. 区块链关键技术及存在问题研究综述[J]. 计算机工程与应用, 2022, 58(3): 66—82.
Liu Shuangyin, Lei Moyixi, Wang Lu, et al. Survey of blockchain key technologies and existing problems [J]. Computer Engineering and Applications, 2022, 58(3): 66—82.
- [12] Castro M, Liskov B. Practical byzantine fault tolerance [C]. OSDI. 1999, 99(1999): 173—186.
- [13] 肖帅, 王绪安, 潘峰. 无模逆运算的椭圆曲线数字签名算法[J]. 计算机工程与应用, 2020, 56(11): 118—123.
Xiao Shuai, Wang Xu'an, Pan Feng. Elliptic curve digital signature algorithm without modular inverse operation [J]. Computer Engineering and Applications, 2020, 56(11): 118—123.
- [14] Awad K M, ElNainay M, Abdeen M, et al. A secure blockchain framework for storing historical text: A case study of the holy Hadith [J]. Computers, 2022, 11(3): 42.
- [15] 高娜, 周创明, 杨春晓, 等. 基于网络自聚类的 PBFT 算法改进[J]. 计算机应用研究, 2021, 38(11): 3236—3242.
Gao Na, Zhou Chuangming, Yang Chunxiao, et al. Improved PBFT algorithm based on network self clustering [J]. Application Research of Computers, 2021, 38(11): 3236—3242.
- [16] Xing J, Fischer D, Labh N, et al. Talaria: A framework for simulation of permissioned blockchains for logistics and beyond [J]. arXiv preprint arXiv: 2103.02260, 2021.
- [17] 董振恒, 吕学强, 任维平, 等. 高性能区块链关键技术研究综述[J]. 数据分析与知识发现, 2021, 5(6): 14—24.
Dong Zhenheng, Lü Xueqiang, Ren Weiping, et al. Review of key technologies of high performance blockchain [J]. Data Analysis and Knowledge Discovery, 2021, 5(6): 14—24.
- [18] 盛守一. 基于区块链技术的供应链信息资源共享模型构建研究[J]. 情报科学, 2021, 39(7): 162—168.
Sheng Shouyi. Information sharing model construction of supply chain based on blockchain technology [J]. Information Science, 2021, 39(7): 162—168.
- [19] Hang L, Kim D H. Optimal blockchain network construction methodology based on analysis of configurable components for enhancing hyperledger fabric performance [J]. Blockchain: Research and Applications, 2021, 2(1): 100009.

(上接第 103 页)

- [13] 刘禹辰, 张锋伟, 宋学锋, 等. 基于离散元法玉米秸秆双层粘结模型力学特性研究[J]. 东北农业大学学报, 2022, 53(1): 45—54.
Liu Yuchen, Zhang Fengwei, Song Xuefeng, et al. Study on mechanical properties for corn straw of double-layer bonding model based on discrete element method [J]. Journal of Northeast Agricultural University, 2022, 53(1): 45—54.
- [14] 谢伟, 彭磊, 蒋蕙, 等. 收获期油菜茎秆双层粘结离散元模型建立与优化[J]. 农业机械学报, 2023, 54(5): 112—120.
Xie Wei, Peng Lei, Jiang Pin, et al. Discrete element model building and optimization of double-layer bonding of rape shoots stems at harvest stage [J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(5): 112—120.
- [15] 魏俊逸, 宗望远, 詹广超. 油菜茎秆径向压缩特性试验研究[J]. 江西农业大学学报, 2021, 43(1): 198—205.
Wei Junyi, Zong Wangyuan, Zhan Guangchao, et al. An experimental study of the radial compression characteristics of rape stalks [J]. Journal of Jiangxi Agricultural University, 2021, 43(1): 198—205.
- [16] 王佳, 李绍波, 陈春皓, 等. 葡萄茎秆切割装置作业参数优化与试验[J]. 中国农机化学报, 2023, 44(2): 37—45.
Wang Jia, Li Shaobo, Chen Chunhao, et al. Optimization and test of operating parameters of grape stem cutting device [J]. Journal of Chinese Agricultural Mechanization, 2023, 44(2): 37—45.
- [17] 李晓, 陈科冰, 韩明, 等. 基于质构仪穿刺模式的烟叶脆性定量评价方法[J]. 烟草科技, 2021, 54(6): 83—91.
Li Xiao, Chen Kebing, Han Ming, et al. A quantitative evaluation method for tobacco leaf brittleness based on puncture mode of texture analyzer [J]. Tobacco Science & Technology, 2021, 54(6): 83—91.
- [18] 付秋娟, 孙婷婷, 窦玉青, 等. 初烤烟叶柔软度及其与烟叶主要理化指标的关系[J]. 烟草科技, 2021, 54(5): 77—81.
Fu Qiujuan, Sun Tingting, Dou Yuqing, et al. Softness of flue-cured tobacco leaves and its relationship with main physicochemical indexes of tobacco [J]. Tobacco Science & Technology, 2021, 54(5): 77—81.