DOI:10.13652/j.issn.1003-5788.2020.11.011

基于区块链的食品供应链数据双链存储优化模型

Optimized model of dual-chain storage of food supply chain data based on blockchain

高圣乔[1,2] 刘新亮[1,2,3] 高彦平[1,2]

GAO Sheng-qiao[1,2] *LIU Xin-liang*[1,2,3] *GAO Yan-ping*[1,2]

(1. 北京工商大学电商与物流学院,北京 100048;2. 农产品质量安全追溯技术及应用国家工程实验室,北京 100048;3. 中国农业大学信息与电气工程学院,北京 100083)

(1. *School of E-commerce and Logistics, Beijing Technology and Business University, Beijing* 100048, *China*; 2. *Agricultural Engineering Quality Safety Traceability Technology and Application National Engineering Laboratory, Beijing* 100048, *China*; 3. *School of Information and Electrical Engineering, China Agricultural University, Beijing* 100083, *China*)

摘要:区块链的出现,为食品供应链管理提供了一种去中心化整合资源、消除信息不对称的解决方案,但目前区块链解决方案中大多面临性能和存储瓶颈。针对此问题,文章提出了一种基于区块链的食品供应链数据双链存储优化模型。模型构建了主链、摘要链双链结构,用户可以根据需求选择适当的存储模式,缓解了区块数据存储膨胀问题;模型采用改进的委托权益证明与拜占庭容错共识机制,加入信誉积分机制选举记账节点,防止女巫攻击的同时,减少了交易确认和区块验证时间。通过仿真试验,验证了该方案能很好适配食品供应链,大幅优化存储资源,提高共识出块速度,提升区块链系统性能和吞吐量。

关键词:食品安全;区块链;供应链;共识机制;存储膨胀

Abstract: The emergence of blockchain provides a solution of decentralized integration of resources and elimination of information asymmetry for food supply chain, but most of the current solutions are facing performance and storage bottlenecks. In response to this problem, this paper proposes a dual-chain storage optimized model for food supply chain data based on blockchain. The model builds a double-chain structure of the main chain and the digest chain. Nodes can choose the appropriate storage mode according to their needs, which alleviates the problem of block storage expansion. By adopting the improved Delegated Proof of Stake and Byzantine fault tolerance consensus mechanism with the credit system to elect accounting nodes, to prevent witch attacks at the same time to reduce transaction confirmation and verification time of blocks. Finally, through simulation experiments, it is verified that the solution can adapt well to the food supply chain, greatly optimize the storage resources, increase the speed of block generation, and improve the performance and throughput of the blockchain system.

Keywords: food safety; blockchain; supply-chain; consensus mechanism; storage expansion

食品供应链通常由监管机构监管,上下游企业串联而成,链上企业的数据都由企业自己维护,容易造成供应链上的信息孤岛[1-2]。由于商业竞争,上下游企业篡改、伪造信息十分常见,导致不同企业与消费者之间的信息不对称[3]。尽管中国很早就着手构建追溯平台,通过加大监管力度,让食品供应链各个环节的数据透明,从而解决不对称问题[4],但企业中心化的管理方式存在着极大的信息自主权,无法保证信息的完整性和准确性,同时还存在供应链不同环节数据结构难以统一,难以整合的问题,因此,信息不对称问题一直未得到有效解决[5]。

随着比特币的持续升温,区块链因其去中心化和不可篡改的特性进入人们视野[6],区块链的特性不仅可以有效解决当前供应链数据中心化存储带来的诸多问题,同时也为跨机构溯源提供技术支持[7-8]。但是,区块链技术带来诸多优势的同时也存在一些问题,最明显的就是存储膨胀:截至 2020 年 1 月,比特币区块链账本总容量约为 220 GB,这一数字还在持续高速增加。比特币全节点约有 10 000 个,这些节点提供的总容量高达 2 PB,却

基金项目:科技部重点研发课题(编号:2016YFD0401205);北京市科委计划项目(编号:Z191100008619007);北京市教委面上项目(编号:KM201510011008)

作者简介:高圣乔,男,北京工商大学在读硕士研究生。

通信作者:刘新亮(1972—),男,北京工商大学副教授,在读博士研究生。E-mail:liuxinl@btbu.edu.cn

收稿日期:2020-06-04

只存储了 220 GB 的数据。高昂的空间需求也造成了入网的巨大门槛，随着数据的持续膨胀，能负担得起的节点越来越少[9-10]。此外，由于共识算法的制约，一些交易确认时间延长，导致性能也存在瓶颈[11]。为解决区块链自身存储膨胀以及性能低的问题，文章拟提出基于区块链的食品供应链数据双链存储优化模型。利用区块链的不可篡改和去中心化的特点，来解决食品供应链存在的信息篡改和不对称的顽疾；采取主链—摘要链模式缓解存储膨胀；通过改进的委托权益证明（Delegated Proof of Stake，DPoS）＋拜占庭容错（Byzantine Fault Tolerance，BFT）共识机制，配合候选节点信誉积分机制，提高交易吞吐量和性能，同时增强系统的稳定性和安全性。

1　区块链

区块链的本质是去中心化的分布式账本[12]，运用非对称加密[13]、哈希函数、时间戳[14]、点对点网络、共识机制等技术。区块是存储交易信息的数据结构，将其盖上时间戳，首尾相连，形成有时间顺序的链式结构就是区块链。共识机制维护分布式一致性，使区块数据不可篡改；哈希和非对称加密等技术保证交易的安全可验证。

图 1 是比特币区块链的链式结构：其本质是一个单向链表，包含一个指向前驱区块的指针；区块头中包含时间戳、版本号等信息，其中默克尔根连接了一棵记录着所有交易的完全二叉树，逐层哈希得到默克尔根[15]。

1.1　区块链的技术特点

（1）去中心化：区块链网络中不存在中心化节点，所有节点是平等的。这是因为其底层采用了 P2P 网络（图 2），节点间可以任意通信、交易，无需第三方审核[16]。

（2）不可篡改：区块按时间顺序生成，通过前驱区块的头哈希连接。一旦交易被篡改，默克尔根和头哈希都会改变，与后继区块的记录不符，从而该区块后的所有区块都要重新共识，这需要全网大部分算力来重新完成工作量证明，因此数据几乎无法被篡改。

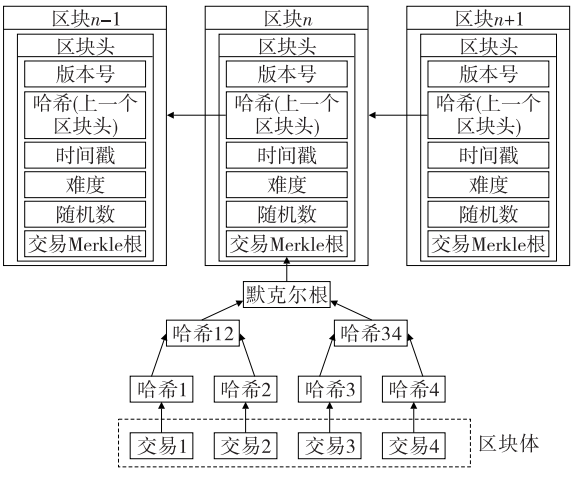

图 1　比特币中区块链的链式结构

Figure 1　The blockchain structure in Bitcoin

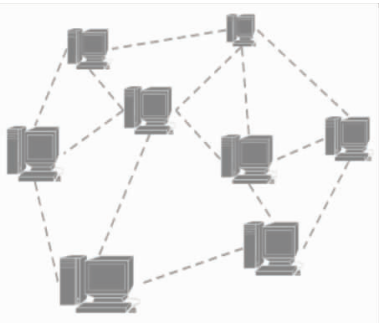

图 2　P2P 网络结构

Figure 2　P2P network structure

（3）性能低：网络中一笔交易和每个新区块都要通过全网节点的验证，为防止分叉导致的欺诈行为，一笔交易只有上链并在其上方累积若干区块后，才被认定完成。

（4）存储膨胀：用户的不断增加导致交易量日趋庞大，因此区块数据量快速膨胀。由于不存在第三方可信机构，信任构建于完整的历史交易，所以区块链系统普遍面临存储瓶颈，准入门槛高的问题。

1.2　共识机制

目前有几大主流的共识算法：比特币的工作量证明机制（Proof of Work，PoW）[17]；以太坊的权益证明机制（Proof of Stake，PoS）[18]；委托权益证明 DPoS[19] 以及实用拜占庭容错机制（Practical Byzantine Fault Tolerance，PBFT）[20]。

DPoS 通过社区投票选举 witness（见证人）节点记账出块。通过减小记账节点数量，缩短区块间隔，增加吞吐量。但其存在投票惰性、恶意贿赂等问题，且过分依赖社区自治，有中心化的风险。

PBFT 主要用于联盟链，由于主节点多次广播，因此需要尽可能少的节点参与来保证效率。

2　食品供应链数据双链存储优化模型

鉴于食品供应链现存的问题以及区块链应用的瓶颈，提出基于区块链的食品供应链数据双链存储优化模型，模型的整体架构见图 3。参与方包括食品供应链的主要成员：消费者、核心企业和监管机构；产生的数据分为链上和链下两部分存储；P2P 网络中依据参与方的功能进行节点类型划分；最底层是主链—摘要链的双链存储模式。

按区块链的技术架构（如图 4），将模型拆分成数据层、网络层、共识层和应用层单独设计。

2.1　数据层

数据层用于存储食品供应链产生的数据。区块链依赖分布式系统，单位存储成本极高，模型根据数据的敏感程度和重要性，将其分为链上和链下存储[21]：链上只存放敏感且重要的小型数据，包括产品信息、交易参与方信息、证书和凭证的哈希值等。哈希值是通过哈希函数对

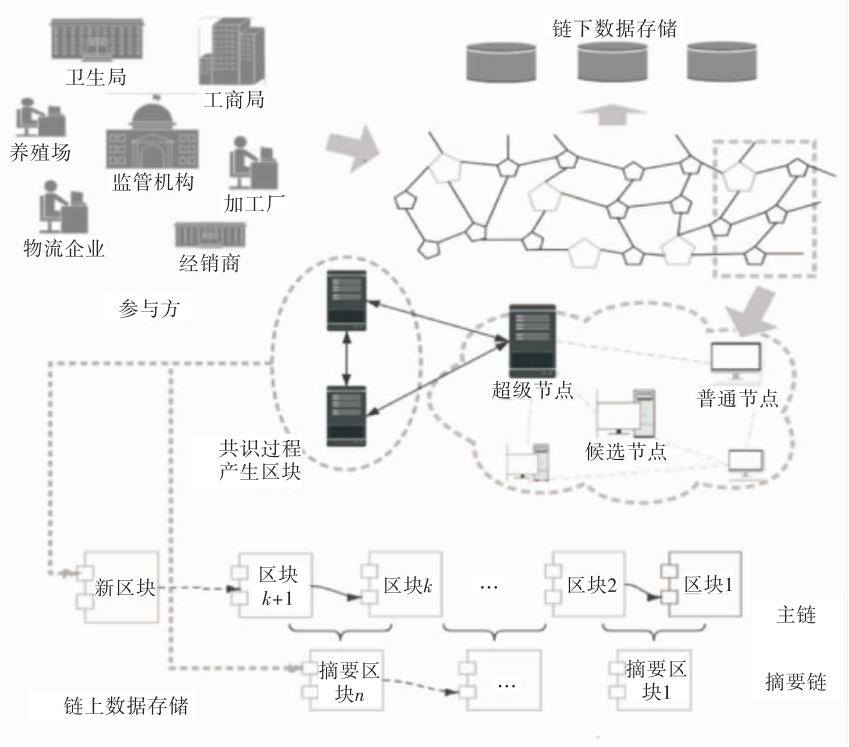

图 3　食品供应链双链存储优化模型整体结构

Figure 3　Food supply chain dual-chain storage optimized model

目标内容生成的固定长度以十六进制表示,具有输入敏感的特性,可验证数据一致性[22]。链下即为企业和监管机构各自的数据库,主要保存企业信息、产品信息、检疫数据、证书及合同完整信息、转账装载凭证等交易源数据、物流追溯信息等非敏感内容。这样可以很好地利用区块空间,杠杆化区块链的性能[23]。

2.1.1　食品供应链交易信息结构　区块链上链的数据不可篡改,而要保证源头可信则需其他技术,例如通过射频识别(radio frequency identification,RFID)、物联网等对加工生产进行数据实时采集,确保源头可信[24]。

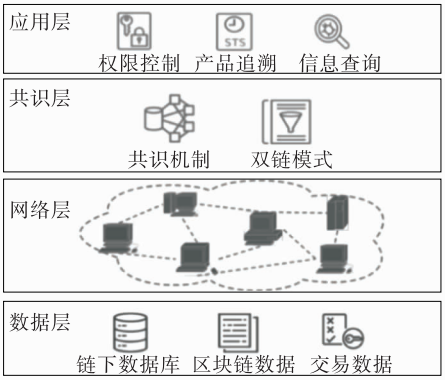

图 4　区块链食品供应链体系分层结构图

Figure 4　Food supply chain system layered structure based on blockchain

为了更高效地存储供应链数据,设计了如表 1 的全新交易信息结构,对于某类食品,其在供应链上流通所生成的交易信息包括但不限于:食品编号 Id,食品名称 Name,操作信息(Operating Information,OI),时间戳 TimeStamp,交易参与方 P,数字签名 $Sign_p$,源数据地址 Url(s),源数据哈希值 Hash(s),前一步骤地址 Url(ls),交易信息哈希值 Hash(t)。

食品在供应链经过每一步骤都需负责人签名。若超级节点验证发现问题,根据签名及时定责,同时阻断产品流通。源数据即为链下数据,提供地址和哈希值,确保未

表 1　交易信息数据结构

Table 1　Transaction information data structure

名称	描述
Id	食品唯一编号
Name	食品名称
OI	该交易阶段经过的操作
TimeStamp	交易发生时间字符串序列
P	交易的参与方
$Sign_p$	交易参与方的私钥签名
Url(s)	源文件链下存放地址
H_s	源文件哈希值
Url(ls)	前一步交易数据地址
H_t	整条交易信息哈希值

篡改;前一步交易信息地址用来回溯交易过程;提供整条交易哈希值供验证。每笔交易审核通过且上链即交易达成。

2.1.2　主链—摘要链区块结构　主链记录全网的所有交易信息,为缓解存储膨胀,在主链的基础上生成摘要链,记录主链部分信息以及系统运行产生的关键数据。为适配食品供应链,配合信誉积分机制,模型对区块结构进行改进。如图 5 所示,主链区块头新增了区块生产者签名。

如图 6 所示,摘要链区块头除主链区块头内容外,还包括对应主链区块高度、数量。区块体包含:主链区块高度、头哈希、默克尔根;该轮超级节点信誉积分变动情况。

2.2　网络层

网络层设计了节点身份认证规则、不同角色以及竞争记账权的规则。

2.2.1　网络搭建与节点类型　食品供应链包含监管机构、核心企业及消费者等参与者。首先由监管机构组建 P2P 许可区块链网络,其他参与者需申请入网。为避免女巫攻击,申请时需提供相应的营业许可、检疫记录、法人信息等,通过监管机构 CA 认证(Certificate Authority)。通过后会授予数字证书和公私钥,允许参与交易[25]。

图 5　主链区块结构图

Figure 5　Block of main chain

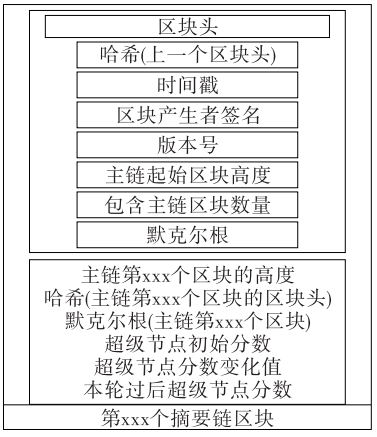

图 6　摘要链区块结构图

Figure 6　Block of digest chain

节点按功能分为 3 类:超级节点、候选节点和普通节点。

超级节点是区块链记账节点,负责验证交易、生成账本并维护一致性;超级节点分常任和轮换两种:组建网络的监管机构为常任超级节点;其他参与者竞争轮换超级节点。超级节点数目固定。

候选节点从全网节点选出,作为超级节点的候选域;候选节点意味着有意愿参与全网共识过程,履行维护网络稳定的义务,并保存主链账本数据;候选节点根据信誉积分机制竞争超级节点。详见 2.2.3。

普通节点仅参与交易,不参与共识过程。无需保存主链数据,只需记录摘要链。供应链成员在认证入网后,可以根据自身需求,选择成为候选节点或普通节点。

2.2.2　交易广播及验证　参与方对交易签名并转发给临近的超级节点,超级节点先利用公钥验证数字签名,然后利用哈希值验证交易内容是否被篡改。验证无误后加入本地交易池,并转发给其他超级节点。

以 s(source)代表源数据,SN(SuperNode)代表超级节点。伪代码:

算法 1　超级节点验证交易

Input:交易数据 t(transaction)

Output:void

1) boolean flag1 = SN.check($Sign_p$);//验证交易签名

2) s = SN.getSource(Url(s));//通过地址获取源数据

3) boolean flag2 = H_s == Hash(s)? true:false;//验证源数据准确性

4) boolean flag3 = H_t == Hash(t)? true:false;//验证交易数据准确性

5) If(flag1 && flag2 && flag3)

6) SN.SendtoAll(t);//发送给其他超级节点

7) SN.addToLocal(t);//加入本地交易池

8) else:

9) SN.SendtoSupVision();//发送给监管部门确权定责

2.2.3　信誉积分机制　节点入网后,若选择候选节点,则会得到初始积分。经过不同的行为,分数会产生变化,详见表 1。根据预设的超级节点数量,系统会按照积分降序从候选节点中补齐轮换超级节点。若候选节点积分相同,则参考达成的有效交易数量。每轮双链共识完成后,根据积分实时替换超级节点:积分不足者成为候选节点,积分高者顶替其位置。

2.3　共识层

2.3.1　改进的 DPoS+BFT 共识机制　传统的 DPoS 共识机制存在投票惰性,恶意贿赂,过度依赖社区自治等问

题,节点投票率仅为 40%[26]。因惩罚机制不完善,作恶成本低,恶意节点甚至采取贿赂手段争取记账权,损害公平性的同时,对系统的安全稳定造成巨大威胁。此外,DPoS 中区块不可逆的条件是该区块上方累积 2/3 * 见证节点个区块,导致交易确认时间非必要延长,造成性能瓶颈;共识过程取消了全网验证,系统稳定性遭到弱化,更易受攻击或出现分叉。

该模型采用候选节点信誉积分机制,舍弃 DPoS 的投票机制,规避了恶意节点的行为以及社区投票惰性。根据候选节点在系统运行期间的累积信誉积分,选出对系统贡献最大的 n 个超级节点,参与记账出块。信誉积分由节点平时交易等行为积累,因此超级节点都是系统的

表 2　候选节点积分细则

Table 2　Candidate node details

节点行为	加分	扣分
经过身份认证入网,并成为候选节点	100	
作为主节点,在规定时间内出块,且区块内容通过验证上链	+2	
作为超级节点参与共识时,未按时出块		−5
作为超级节点参与共识时,提议区块未通过		−3
共识过程中,未在规定时间内对其他超级节点提议作出响应		−5
作为超级节点致使非法交易通过验证		−3
参与一笔合法交易,且交易通过验证上链	+0.1	

最大权益节点,维护系统稳定的同时保护自身利益。BFT 算法根据当前视图编号 v 计算出主节点,将客户端请求发给不同的副本节点进行验证,判断副本节点返回消息数量,当即决定请求是否通过。这一点弥补了 DPoS 的缺陷,区块验证更充分,省去了区块上链到不可逆的过程,从而缩短交易确认时间,性能得到提高。因此该模型形成改进的 DPoS+BFT 共识机制,双链共识流程图如图 7。

2.3.2　主链及摘要链生成　经上述步骤即生成主链区块,由所有超级节点参与共识而成。

以 bi 表示第 i 个副本节点,m 为区块内容,P 表示主节点,v 表示视图编号。伪代码表示:

算法 2　生成主链区块

Input:N(本轮超级节点集合);t(交易数据集合)

Output:主链区块

1) While(! N.isEmpty()) do//存在超级节点未提议区块

2) v =0;//进入初始视图

3) P=N.getRandom() //随机选取主节点

4) m=p.CreateBlock(T)//从本地交易池打包区块

5) p.Sign(m)//生产者签名

6) D_m=p.Hash(m);//计算区块摘要

7) req=p.generate(view,D_m,m);//打包消息

8) p.SendtoAll(req);//发送 request 消息

9) for b_i in N: //Backup 节点验证:

10) If(check(sign)&&(Dm==Hash(m)))

11) return resp;//返回 response 消息

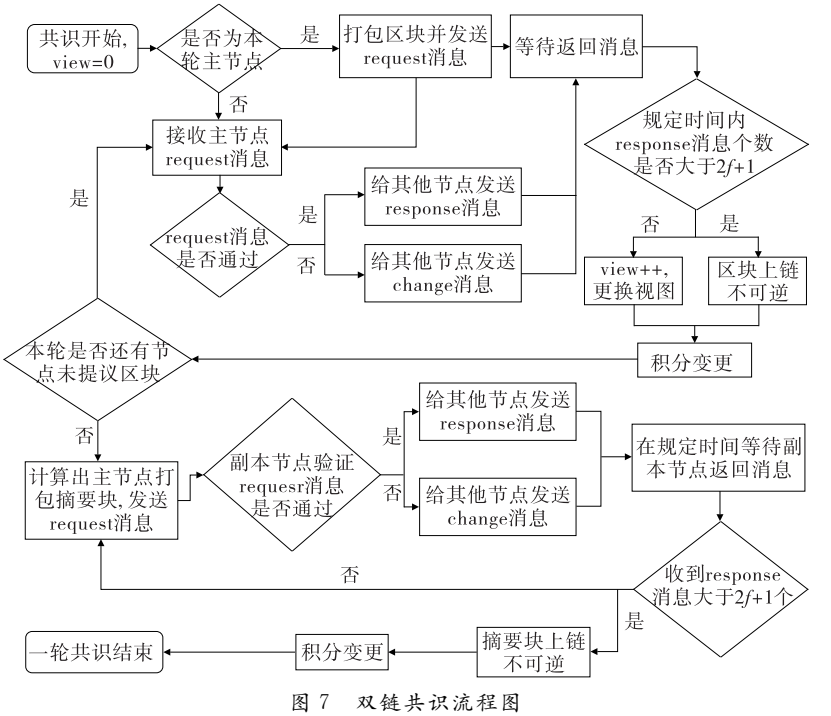

图 7　双链共识流程图

Figure 7　Dual-chain consensus flow chart

12）else：

13）return change；//返回更换视图消息

14）for b_i in N：//超级节点判断 response：

15）If(！(check(resp)&&(resp＞2/3))||change＞2/3）//验证内容和数量

16）addBlock(m)；//上链，等待下次共识

17）else：

18）view＋＋；//更换视图

19）PointChange()；//积分变更

20）end while；

摘要链生成周期和主链一致，主链经过一轮共识生成不大于超级节点个数 n 个区块，摘要链生成一个区块。摘要链同样采用改进的 DPoS＋BFT 共识机制，据式(1)选出主节点，打包摘要区块，重复一轮共识过程，若成功则本轮摘要链出块结束；否则，发起更换视图请求，重新选取主节点打包区块。

$$DigestP=(v+T_{stamp})\bmod n, \tag{1}$$

式中：

$DigestP$——下轮超级节点编号；

v——视图编号；

T_{stamp}——时间戳，ms；

n——主链超级节点编号。

2.4 应用层

应用层主要是监管机构、食品企业以及消费者的前端入口，用户可以访问企业和监管部门的网站查询数据。还包含基于区块链的供应链追溯 Web 应用，提供用户交互功能，包括数据查询、追溯等业务。消费者的商品到手后，可凭借其产品 Id 进行溯源信息查询，过程源数据对消费者可见。

虽然区块链数据是公开的，但是针对企业之间恶意竞争问题，为数据设置访问权限：所有交易信息均通过公钥加密，需私钥解锁查看；在应用层的访问端口，未经授权的用户无法查询交易商品的源数据、企业信息等敏感数据。

3 仿真试验与分析

3.1 试验环境与参数设置

利用以太坊部署食品供应链双链模型，模拟 110 个节点，包括监管节点 10 个，核心企业 95 个，消费者组织5 个，在本地局域网实现多机互联。为便于试验数据的收集，开始前在企业节点部署源数据，模拟生产、加工、屠宰、运输等不同阶段的数据，通过不同的 url 记录访问地址。设网络内每 5 s 随机发生交易，单个节点每笔交易量为 1。设超级节点个数为 23 个。试验相关环境和参数如表 3。

试验过程中会生成两条链，表 4 截取了摘要链的部分区块数据，反映双链结构以及两条链之间的关联。

3.2 模型性能分析

3.2.1 存储性能分析　试验选取了两个指标来衡量存储性能，分别是存储增长率(Storage growth rate，SGR)，以及存储利用率(Storage utilization rate，SUR)。存储增长率指的是单位时间内区块链数据量的增长，如式(2)；存储利用率指的是单位存储空间中，包含的有效交易个数，如式(3)。

表 3 试验环境和参数表

Table 3 Experimental environment and parameter

软硬件参数	详细信息
操作系统	MacOS 10.15.4
CPU	2.6 Hz Intel Core i7
内存	32 GB 2 666 MHz DDR4
局域网带宽	100 Mbps
编程语言	Solidity

表 4 摘要链区块部分数据表

Table 4 Partial data of digest chain

参数名称	参数数值
哈希	0x53735dbb612447b54de066b8b6682445 27f767b44664f794fa03679e90b5ae02
时间戳	03-21-2020 18:41:09
播报方	1PdNVV71qNbHxchKiRrxqoR8Johpa LfoMX
默克尔根	d74546eef705418e60eb89c6c925b8a5d5b 4348c35dc773a5eccf53eda8e740f
大小	1,103,729 bytes
包含主链区块数量	23
包含主链起始高度	579
前驱摘要块	0xcc3fcdde77568b1088d1652dc00cd6b9 592b42dc4f481ac40463e15ed4a5a258
后继摘要块	0x3a3c24df02c5e40675b26be80cb33306 2761aa1d3f60a5dd02494d9d58bfca5f

$$R_{SG}=\frac{Size_{t1}-Size_{t2}}{\Delta t}, \tag{2}$$

式中：

R_{SG}——存储增长率，MB/s；

$Size_{t1}$——t_1 时间区块链大小，MB；

$Size_{t2}$——t_2 时间区块链大小，MB；

Δt——时间增量，s。

$$R_{SU}=\frac{\Delta transaction}{\Delta size}, \tag{3}$$

式中：

R_{SU}——存储利用率，笔/MB；

$\Delta transaction$——交易增量，笔；

$\Delta size$——区块链大小增量，MB。

选取系统运行 20，40，60，80，100，120 min 的时间点采集数据，统计主链和摘要链的大小，得到的对比数据如表 5。首先，共识机制决定了两条链存储增速比较稳定，

但摘要链占用空间同比远低于主链,仅为主链的 1/20 左右。且通过计算,摘要链的存储增长率明显低于主链,增速缓慢。这得益于摘要链的生成机制,几乎没有冗余。说明普通节点的存储压力较低,证明了模型入网门槛低的优势。

为了验证模型的 SUR,选取文献[25]中的水产品追溯区块链作对比试验,试验环境和条件均设为相同,包括节点数、交易时间间隔和单次交易量等参数。交易达到不同数量时,分别记录两个模型区块链大小,并计算 SUR。统计的交易次数为 100 000 的整数次,共统计 6 次,对比结果如图 8。通过式(3)计算出模型主链 SUR 为 877.96 笔/MB,水产品追溯区块链 SUR 为 790.51 笔/MB;主链要好于水产品追溯链,说明相同大小的区块数据中,主链包含更多有效交易。这得益于全新的交易信息结构以及链上链下存储模式,不存在冗余和较大的源数据。

3.2.2　系统性能分析　试验选取两种指标来衡量模型的性能,一是吞吐量(Transaction Per Secod,TPS),指模型在单位时间内能够处理请求的数量,是衡量模型解决短时间高并发问题能力的重要指标,如式(4)。二是平均交易确认时长,即一笔交易从广播到上链不可逆所需时间。

$$TPS=\frac{\Delta transaction}{\Delta t}, \tag{4}$$

式中:

表 5　主链摘要链占用空间对比

Table 5　Comparison of space occupied by main-chain and digest-chain

时间/min	摘要链大小/MB	主链大小/MB
20	10.6	238.5
40	20.5	478.6
60	30.5	719.5
80	41.2	960.2
100	51.5	1 201.6
120	62.1	1 443.1

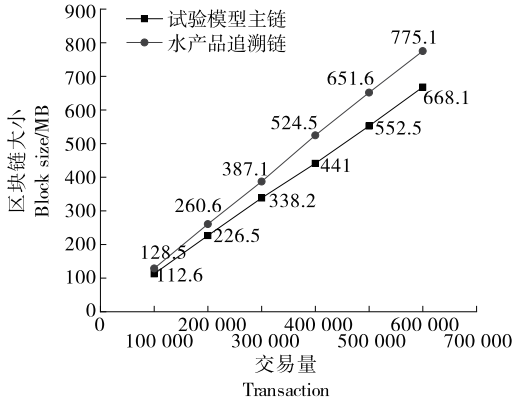

图 8　区块链存储利用率对比图

Figure 8　Blockchain storage utilization comparison

TPS——每秒交易数量,笔/s;

$\Delta transaction$——交易增量,笔;

Δt——时间增量,s。

TPS 方面,模型的改进 DPoS+BFT 共识机制,配合信誉积分机制,通过试验获取的交易数量与运行时间,计算出 TPS 为 185.4 笔/s。为证明模型效率方面的优势,选取相对成熟的共识机制对比,结果如图 9。PoW 中设置挖矿随机数解为以 5 个 0 开头的 8 位十六进制数,由于全网参与广播和工作量证明,吞吐量仅为 6～7 笔/s;PoS 难度值与 PoW 相同,由于币龄的加权,所需工作量更小。由于出块间隔和交易确认条件未发生变化,其 TPS 表现与 PoW 接近,前两者都无法支持短时间高并发交易。后两者的表现明显好于前两者,PBFT 由于每次切换视图前对请求作出判断,确认时间短,提升了吞吐量;模型的共识机制在请求确认的处理方面加以改进,能一直保持较低的确认时限,维持较高的吞吐量。

图 10 对比了 DPoS、PBFT 和试验模型共识机制中,不同节点数量下的交易确认时长。分别模拟 40,60,80,100,120 个节点组网的情况,测试出一笔交易从产生到上链的平均时间。由图10可知,DPoS中随着节点的增加,

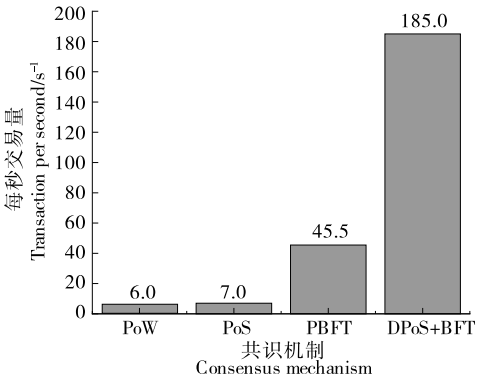

图 9　4 种共识机制 TPS 对比图

Figure 9　Comparison of four consensus mechanisms TPS

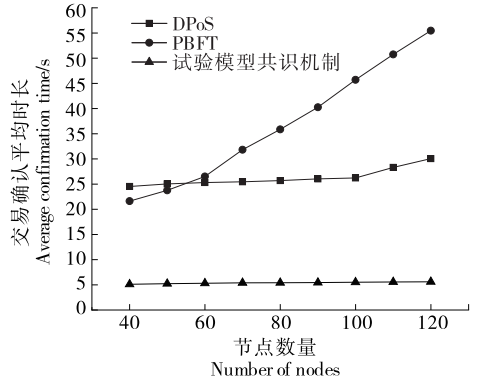

图 10　3 种共识机制交易确认时长对比

Figure 10　Comparison of transaction confirmation time of three consensus mechanisms

见证节点随之增加，而达到不可逆需要大于 2/3 的见证节点出块，因此交易确认时间也在增加。PBFT 中，当节点个数保持在 100 以内时，表现良好，而一旦超过 100，消息传播会受制于网络带宽，无法达到最佳速度。相同网络环境下，模型的超级节点个数会随全网用户数量的增加而改变，不过由于改进了区块不可逆的确认条件，能够使交易的确认保持在一个稳定的时间，性能随节点增加一直保持在较高水准。

4 结论

文章提出了食品供应链双链存储优化模型，在解决供应链固有顽疾的同时，还对区块链落地项目中普遍存在的低吞吐量、低性能、存储膨胀等问题加以优化解决。对于食品供应链企业，为其提供极低的门槛，就能够参与企业间的点对点交易，且能满足企业对于高频交易、快速确认的需求，同时为企业数据安全和隐私提供保护；对于消费者而言，模型满足其购买食品的每一项数据安全可追溯，保证数据完整性、真实性。区块链技术仍在高速发展中，下一步研究方向主要是线上交易、网络传输的消息丢失、延迟、重复或乱序问题，以及智能合约技术的引入研究。

参考文献

[1] 郭菊娥，陈辰. 区块链技术驱动供应链金融发展创新研究[J]. 西安交通大学学报(社会科学版)，2020，40(3)：46-54.

[2] 杨建亮，侯汉平. 冷链物流大数据实时监控优化研究[J]. 科技管理研究，2017，37(6)：198-203.

[3] 刘瑞明，段雨玮，黄维乔. 中国转型期的食品安全治理：基于行为法经济学的分析[J]. 中国工业经济，2017(1)：100-118.

[4] 杨明，吴晓萍，洪鹏志，等. 可追溯体系在食品供应链中的建立[J]. 食品与机械，2009，25(1)：146-151.

[5] 谢康，肖静华，赖金天，等. 食品安全"监管困局"、信号扭曲与制度安排[J]. 管理科学学报，2017，20(2)：1-17.

[6] NAKAMOTO S. Bitcoin：A peer-to-peer electronic cash system[EB/OL]. (2018-11-01)[2020-04-19]. http://www.bitcoin.org/bitcoin.pdf.

[7] 工业和信息化部. 中国区块链技术和应用发展白皮书[EB/OL]. (2016-10-18)[2020-04-19]. https://www.jianshu.com/p/6ac84516a4c5.

[8] 曾小青，彭越，王琪. 物联网加区块链的食品安全追溯系统研究[J]. 食品与机械，2018，34(9)：100-105.

[9] 贾大宇，信俊昌，王之琼，等. 区块链的存储容量可扩展模型[J]. 计算机科学与探索，2018，12(4)：525-535.

[10] 朱立，俞欢，詹士潇，等. 高性能联盟区块链技术研究[J]. 软件学报，2019，30(6)：1 577-1 593.

[11] EYAL I，SIRER E G. Majority is not enough：Bitcoin mining is vulnerable[J]. Communications of the ACM，2018，61(7)：95-102.

[12] 李明佳，汪登，曾小珊，等. 基于区块链的食品安全溯源体系设计[J]. 食品科学，2019，40(3)：279-285.

[13] JOHNSON D，MENEZES A，VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security，2001，1(1)：36-63.

[14] HABER S，STORNETTA W S. How to time-stamp a digital document[J]. Journal of Cryptology，1991，3(2)：99-111.

[15] TSCHORSCH F，SCHEUERMANN B. Bitcoin and beyond：A technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials，2016，18(3)：2 084-2 123.

[16] CHRISTIDIS K，DEVETSIKIOTIS M. Blockchains and smart contracts for the internet of things[J]. IEEE Access，2016，4：2 292-2 303.

[17] NGUYEN G T，KIM K. A survey about consensus algorithms used in Blockchain[J]. Journal of Information Processing Systems，2018，14(1)：101-128.

[18] HOUY N. It will cost you nothing to 'kill' a proof-of-stake crypto-currency[J]. Economics Bulletin，2014，34(2)：1 038-1 044.

[19] 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)：2 011-2 022.

[20] CASTRO M，LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. Acm Transactions on Computer Systems，2002，20(4)：398-461.

[21] LIU Bin，YU Xiao-liang，CHEN Shi-ping，et al. Blockchain based data integrity service framework for IoT data[C]// 2017 IEEE International Conference on Web Services (ICWS). [S.l.]：IEEE，2017：468-475.

[22] YU Hong-bo，HAO Yong-lin，BAI Dong-xia. Evaluate the security margins of SHA-512，SHA-256 and DHA-256 against the boomerang attack[J]. ence China Information ences，2016，59(5)：1-14.

[23] XU Xi-wei，LU Qing-hua，LIU Yue，et al. Designing blockchain-based applications a case study for imported product traceability[J]. Future Generation Computer Systems，2019，92：399-406.

[24] 李宣，柳毅. 基于双区块链及物联网技术的防伪溯源系统[J/OL]. 计算机应用研究. [2020-05-08]. https://doi.org/10.19734/j.issn.1001-3695.2019.08.0291.

[25] 洪坤明，刘新亮，高圣乔. 基于联盟区块链的水产养殖品质量追溯系统的设计与实现[J]. 科学技术与工程，2019，19(35)：79-86.

[26] 陈梦蓉，林英，兰微，等. 基于"奖励制度"的 DPoS 共识机制改进[J]. 计算机科学，2020，47(2)：269-275.