面向农产品供应链的 DAG 式区块链共识算法研究

张 震[1]
ZHANG Zhen

摘 要 农产品安全作为食品安全的重中之重，备受社会关注。针对传统链式区块链在解决农产品供应链场景中存在的吞吐量低和可扩展性差的瓶颈，文章提出了一种建立在有向无环图（directed acyclic graph, DAG）数据结构之上的分片有向无环图 PBFT 共识算法（sharded directed acyclic graph pbft consensus algorithm, SDAG-PBFT）。传统 PBFT 算法在农产品供应链大规模节点和高并发交易场景下存在通信复杂度高、延迟显著、可扩展性差等问题，而 DAG 式区块链通过其异步通信和并行处理特性，可有效提升共识效率。通过将共识节点进行分片，该方案是兼具高效性与鲁棒性的解决方案，对农业信息化领域的区块链应用具有实践参考价值。

关键词 农产品供应链；区块链共识；DAG；PBFT

doi：10.3969/j.issn.1672-9528.2025.09.018

0 引言

食品安全是关系到国计民生的重要领域，农产品安全更是食品安全的重中之重。农产品供应链涉及的人员杂，环节多，地域分布广，在运输过程中损耗较大。区块链是一种去中心化的多方协作技术方案，可以有效解决农产品供应链中的多方数据共享，事后定责追责等问题。但是现有的区块链解决方案多是建立在传统的链式区块链结构之上，难以应对高并发，低延迟的高频交易场景。DAG 是一种有向无环图数据结构，相比于链式结构，具备较少性能约束点，支持多节点同时接入，可以达到更高的吞吐效率和扩展性。

1. 河南工业贸易职业学院现代信息技术学院 河南郑州 450053

[基金项目] 2024 年度河南省科技厅科技攻关项目（242102210188）

point transformer for robust 3D gaussian splatting[EB/OL].(2024-11-24)[2025-05-12].https://vlg.inf.ethz.ch/publications/SplatFormer-Point-Transformer-for.html.

[17]BARRON J T, MILDENHALL B, VERBIN D,et al. Mip-neRF 360: unbounded anti-aliased neural radiance fields[EB/OL].(2022-01-25)[2025-06-22].https://doi.org/10.48550/arXiv.2111.12077.

[18]KNAPITSCH A, PARK J, ZHOU Q Y,et al. Tanks and temples: benchmarking large-scale scene reconstruction[J]. ACM transactions on graphics (ToG) ,2017,36(4): 1-13.

[19]CHENG K, LONG X X, YANG K Z,et al. GaussianPro: 3D gaussian splatting with progressive propagation[EB/OL].(2024-02-22)[2025-04-23].https://doi.org/10.48550/arXiv.2402.14650.

[20]HORE A, ZIOU D. Image quality metrics: PSNR vs. SSIM[C/OL]//2010 20th International Conference on Pattern Recognition.Piscataway:IEEE, 2010[2025-06-11]. https://ieeexplore.ieee.org/document/5596999.DOI:10.1109/ICPR.2010.579.

【作者简介】

徐明强（2001—），男，河南驻马店人，硕士研究生，研究方向：计算机视觉、三维重建，email: 232100210684@gznu.edu.cn。

谢晓尧（1952—），男，贵州贵阳人，博士，教授，研究方向：网络通信、信息安全与人工智能，email: xyx@gznu.edu.cn。

刘嵩（1983—），通信作者（email:songliu@gznu.edu.cn），男，贵州贵阳人，博士，副教授，研究方向：计算机视觉、三维重建。

刘建成（1990—），男，四川成都人，硕士，馆员，研究方向：文物保护，email:liujc90@163.com。

王冲（1981—），男，四川广安人，硕士，副研究馆员，研究方向：文物保护，email:67692034@qq.com。

（收稿日期：2025-04-23 修回日期：2025-09-15）

在使用区块链解决农产品供应链领域的难题方面。Singh 等人[1]介绍了智能食品链管理系统（IBFS），该系统集成了物联网和区块链来监控食品库存并确保安全和质量。该系统使用 MQTT 代理广播和记录来自 IoT 传感器的数据。然而，它需要大量的初始投资，并且由于依赖 IoT 传感器和不断增长的数据存储需求而面临挑战。Xu 等人[2]提出了一种基于主从多链结构的粮食和食品区块链可追溯性模型，该模型比单链系统具有优势，但存在与交易存储时间相关的限制。彭松[3]为解决区块链共识算法的性能瓶颈，提出 Petrichor 算法。该方案采用分片架构和 DAG 多路径传播机制，实现交易并行处理，显著提升吞吐量。通过随机种子选举领导者区块，使分片内节点能独立达成共识，减少通信开销。岳镜涛[4]提出 ElasticDAG 共识机制，采用模块化设计分离存储与确认机制，支持轻节点快速验证。通过混合共识协议降低延迟，结合交易证明机制保障安全性。其高活性存储方案避免区块丢弃，在保证顺序一致性的同时提升吞吐量，有效适配多元化区块链应用需求。Salah 等人[5]提出了一种利用以太坊区块链及智能合约高效执行大豆农产品供应链追溯与交易业务的方法。该方案聚焦于运用智能合约来管控供应链生态系统中所有参与者之间的交互与交易。Mane 等人[6]提出了一种基于区块链的原型，旨在减少经济损失和解决农业污染问题。然而，由于交易透明，它对公共区块链的依赖限制了隐私。

1 相关技术概述

1.1 链式区块链共识算法

共识算法是区块链的灵魂，可以细分为选举类共识、证明类共识、随机类共识、联盟类共识和混合类共识[7]。选举类共识算法是以传统分布式方案中的一致性算法为主，例如 Paxos 和 Raft。证明类共识算法是区块链技术兴起之后以节点对系统的贡献度为依据进行的决策算法，通常以投入资源和资源占比为依据，例如 POS 和 POW。随机类共识算法是在缩小共识数目的指导思想下，用各种随机函数对整体节点抽样，进而提升系统共识去中心化程度，在资源投入和去中心化之间取得了平衡。联盟类共识算法是在设定系统节点准入规则的前提下，以小规模节点团体运行的共识算法，一般这类共识算法具备确定性，在节点较少的情况下，可以达到较高的吞吐量，极大提升了系统的效率，常以 PBFT 以及其各种变种为主。混合类共识算法是对多种共识算法的有机融合，是对特定行业设计的算法，借助相应行业的特性，可以在去中心化和系统低成本高效率之间达到较佳的平衡。五类共识算法的特点如表 1 所示。

表 1 五类共识算法的特点

共识算法类型	算法代表	资源消耗	容错性	交易确认方式	是否分叉
选举类共识	Paxos、Raft	非拜占庭容错			
证明类共识	PoW、PoS	多	1/2	概率性	会分叉
随机类共识	Algorand(PoS+BFT)	少	1/3	确定性	不分叉
联盟类共识	PBFT	少	1/3	确定性	不分叉
混合类共识	PoW+PoS	多	1/2	概率性	会分叉

1.2 DAG 式区块链共识算法

DAG 结构是一种有向无环图结构，在区块链领域中被用来设计为底层数据的结构，可以支持多节点同步发送交易，只需要其引用多个其他的交易。针对区块链交易构成的复杂无序的有向无环图结构，DAG 式区块链需要解决的是如何将全局顺序进行理顺，进而达到全部交易的一致性。按照是否包含一条贯穿全部有向无环图的核心主链，可以将 DAG 式区块链分为含主链的 DAG 式区块链和不含主链的 DAG 式区块链。

主链的起始点一般都是从创世交易，按照某种规则，系统可以创造新的交易或者选择已有的交易，将其纳入主链当中，用主链的有序性为其他无序的交易作为排序的基准。Byteball[8]、Conflux[9]、GHOST[10] 和 Inclusive Blockchain Protocol[11] 为该类区块链的代表。

不含主链的 DAG 式区块链一般难以用物理规则达成所有交易的全网一致性，对冲突交易使用投票的方式进行解决。DAG 首次被提议用来改进链式区块链的性能瓶颈问题就是不含主链的模式，并且每一个有向无环图节点只包含一个交易。DAGCoin[12]、IOTA[13]、HashGraph[14]、SPECTRE[15] 和 PHANTOM[16] 是该模式的代表。

2 DAGPBFT 共识算法设计

2.1 PBFT 共识算法

如图 1 所示，PBFT 算法流程共有 5 个阶段：request 请求阶段、pre-prepare 预准备阶段、prepare 准备阶段、commit 提交阶段和 reply 回复阶段。假设系统中有 n 个节点，其中存在 f 个拜占庭节点，则 f 的最大值是 $(n\text{-}1)/3$。

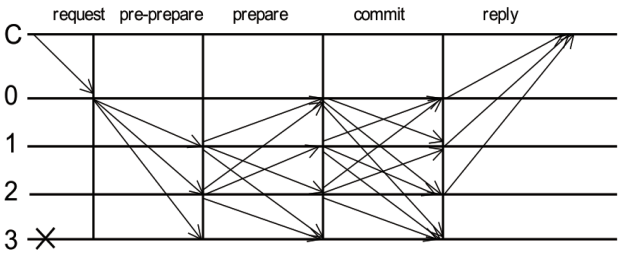

图 1 PBFT 的算法流程图

本协议中的 pre-prepare 阶段和 prepare 阶段的作用是在视图不变更的情况下保证提案间的顺序，commit 阶段的作用是在发生视图转换时保证提案间的顺序。此外，值得注意的是进入 commit 阶段的节点需要证明自己的状态才可以进入该阶段。

2.2 SDAG-PBFT 共识算法

DAG 式区块链区别于链式区块链最重要的一点是其交易数据结构的无序性，其根源在于所有节点都可以无节制地发送交易到系统中，所以针对 DAG 式区块链最重要的是达成全网一致性。因此，将节点和他们的交易进行合理分片后，再将这些小的片段进行构建有向无环图，是新算法分片有向无环图共识算法（sharded directed acyclic graph pbft consensus algorithm, SDAG-PBFT ）的基本思路。

2.3 共识算法设计

一般来说，农产品供应链中有生产节点、运输节点、监管节点、零售节点和用户节点 5 大类，其中监管节点一般固定不变，用户节点不参与共识。

简略起见，分别设定以下符号：生产节点 P_i、运输节点 T_i、监管节点 S_i 和零售节点 R_i，其中 i 取值为正整数。根据相应节点的属性，将节点进行分片。也就是说，所有的生产节点 P_i 是一个分组，在一定时间间隙内，由这些 P_i 节点进行内部构建生产方的有向无环图交易片段 $DAGP_i$。所有的运输节点 T_i 是一个分组，由这些 T_i 节点进行内部构建运输公司方的有向无环图交易片段 $DAGT_i$。所有的监管节点 S_i 是一个分组，由这些 S_i 节点进行内部构建监管方的有向无环图交易片段 $DAGS_i$。所有的零售节点 R_i 是一个分组，由这些 R_i 节点进行内部构建零售方的有向无环图交易片段 $DAGR_i$。

由于农产品供应链的业务特性，只有生产节点完成的产品才会交由运输节点转运，最后由零售节点进行售卖，产品的相关信息天然就有了时间上的先后关系。而不同批次的产品之间并没有相关性。所以，共识节点每次只需要将该批次的交易信息进行共识即可。

2.3.1 共识节点选取

采用轮流的方法，每次从相应的分组节点中选出一个节点作为共识节点，所有共识节点针对每一批次的供应链信息进行共识。如果相应片段内有错误交易，那么需要该片段内的节点重新生成一个正确的。如果无误，那么则将该片段引用当前批次的上一个片段，以及该分片节点的上一个交易片段。

2.3.2 监管交易分片

监管交易分片由监管节点分片产生，是当前批次产品信息各个环节信息的确认。由于农产品供应链的特性，从生产到消费，各个环节清晰有界限，先后关系明确，对应分片节点产生的交易经过分片内的共识后也具备较清晰的先后关系，监管节点作为参与方中的特殊节点，只需要将该生产批次对应的各个交易分片进行确认，然后将其哈希值构成的有向无环图结构保存即可。具备以下两个特性：

（1）只存储交易哈希值，减轻了节点的存储压力；

（2）便于查询。交易哈希具备快速检索一一对应的特性，所以，用户只需要对所有监管交易分片进行检索，即可获悉链上的所有信息。

2.4 共识算法流程

系统按照节点的属性对其进行分片为 P_i、T_i、S_i 和 R_i，同属一个分片的节点针对同一批产品产生的交易是各自的交易分片 $DAGP_i$、$DAGR_i$、$DAGT_i$ 和 $DAGS_i$。分片是快速提高系统性能的手段，一个完整的共识流程包含了分片内共识和分片间共识。

2.4.1 分片内共识

同属于一个分片的节点需要针对同一批次的农产品进行共识。分片内共识采用 PBFT 共识算法，能对同一批次的产品快速确认。以生产节点 P_i 为例，假设有 4 个生产节点 P_i（i=1,2,3,4），共识流程如下：

（1）request 请求阶段：P_1 向主节点 P_i 发送需要被处理的交易 $DAGP_i$，其中主节点由所有共识节点轮流担任。

（2）pre-prepare 预准备阶段：主节点 P_i 将收集到的交易打包为预准备消息提案，然后广播给其他从节点 P_i（i=2,3,4），该提案包含当前主节点的视图号 v，区块号 n，消息 m，消息摘要 d，主节点序号 i 和主节点对消息 m 的签名 s，其格式为 <<PRE-PREPARE, v, n, d, i, s>, m>。

（3）prepare 准备阶段：收到预准备消息的从节点 P_i（i=2,3,4）会首先对其进行验证，包含摘要 m 是否和消息一致，视图号 v 是否和自己一致，区块号是否满足水线限制。从节点 P_i（i=2,3,4）如果认可该提案，会对该提案进行签名产生 <PREPARE, v, n, d, i> 消息并将其广播给其他节点，如果不认可则不会发送消息。在该阶段中收到 $2f$+1 个 prepare 消息的节点被称为进入 prepared 状态。

（4）commit 提交阶段：收到准备阶段消息的节点需要对其进行验证，验证的方式与上一阶段基本相同，包含摘要 m 是否和消息一致，视图号 v 是否和自己一致，区块号是否满足水线限制。所有进入 prepared 状态的节点开始能进入 commit 阶段。本阶段中的节点将会发送格式为 <COMMIT, v, n, d, i> 的 commit 消息给其他节点，同时发送 commit 消息的节点必须证明自己已经进入 prepared 状态，证明方式是把上一阶段收集到的 $2f$+1 个 prepare 消息放入 commit 消息中。同样，收集到 $2f$+1 个 commit 消息的节点进入到 commited 状态。

（5）reply 回复阶段：达到 commited 状态的节点开始进入 reply 阶段。通过 commit 阶段的提案已经被认为是完成共识。此时，节点将自己执行的结果 <REPLY, v, t, c, i, r> 返回

给客户端，其中 v 是视图编号；t 是时间戳；i 是节点的编号；r 是请求执行的结果。若客户端收集到来自 f+1 个完全不一样的节点且执行结果是一致的消息提案，即客户端的请求将被完成。

2.4.2 分片间共识

分片间共识由监管节点 S_i 完成。纳入分片间共识的分片有生产交易图分片 $DAGR_i$，运输交易图分片 $DAGT_i$，零售交易图分片 $DAGR_i$ 和监管交易图分片 $DAGS_i$。由于农产品供应链流程中具备时间上的唯一先后顺序，所以只需要将对应片段按照实际情况引用即可，相应片段除了要引用上一业务阶段的交易图分片外，还要引用本节点分片产生的上一个交易图分片。

监管节点作为分片间共识的核心节点，产生的监管交易图分片 $DAGS_i$ 要引用该时间间隙内对应生产批次的所有分片 $DAGP_i$、$DAGR_i$、$DAGT_i$ 并将这些交易的哈希值结构图作为自己的监管交易图分片 $DAGS_i$，以表示该监管节点对这些交易片段的认可确认。

3 结语

根据农产品供应链具有短时交易量大，节点属性明显和环节间顺序固定特点，本研究提出一种分片有向无环图共识算法 SDAG-PBFT。该算法采用分片的方法，根据节点的环节属性进行节点分片，共识步骤分为分片内共识和分片间共识。节点分片内共识采用 PBFT 共识算法，将一定时间间隙内的同一批次产品交易进行共识后得到相应的交易有向无环图分片。节点分片间共识由监管节点主导，按照本间隙内各分片节点所在的业务属性对交易分片进行排序，并将这些交易纳入监管节点交易分片内。通过 SDAG-PBFT 共识算法，系统可以快速高效地进行共识，达成全部交易的一致性。但是，PBFT 算法是一种分布式系统一致性算法，当用于大量节点之间进行共识的时候，会造成系统通信量过大，堵塞网络，造成极大的通信复杂度，所以进一步的研究方向应该围绕着如何结合农产品供应链的特点对传统 PBFT 共识算法进行优化而展开。

参考文献：

[1] SINGH A, RAZA Z. A framework for IoT and blockchain-based smart food chain management system[EB/OL].(2022-11-28)[2025-04-25].https://doi.org/10.1002/cpe.7526.

[2] XU J P, HAN J Q, ZHANG X, et al. Quality and safety traceability of grains and oils based on trusted blockchain and trusted identity[J].Food science, 2323,44(3):48–59.

[3] 彭松 . 基于 DAG 的区块链异步共识算法研究与实现 [D]. 郑州 : 河南工业大学 ,2024.

[4] 岳镜涛 . 面向图式区块链的高性能共识机制研究 [D]. 武汉 : 华中科技大学 ,2023.

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

[6] EL MANE A, CHIHAB Y, TATANE K, et al.Agriculture supply chain management based on blockchain architecture and smart contracts[EB/OL].(2022-10-21)[2025-02-22]. https://doi.org/10.1155/2022/8011525.

[7] 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.

[8] CHURYUMOV A. Byteball: a decentralized system for storage and transfer of value[EB/OL].(2023-11-07) [2025-06-23]. https://www.docslides.com/samantha/byteball-a-decentralized-system-for-storage-and-transfer-of-value.

[9] LI C X, LI P L, ZHOU D, et al. Scaling nakamoto consensus to thousands of transactions per second[EB/OL].(2018-08-31) [2025-01-23].https://doi.org/10.48550/arXiv.1805.03870.

[10] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in bitcoin[C]//Financial Cryptography and Data Security. Berlin:Springer,2015: 507-527.

[11] LEWENBERG Y, SOMPOLINSKY Y, ZOHAR A. Inclusive block chain protocols[C]//Financial Cryptography and Data Security.Berlin:Springer,2015: 528-547.

[12] LERNER S D. DagCoin: a cryptocurrency without blocks[EB/OL].[2025-01-23].https://bitslog.com/2015/09/11/dagcoin/.

[13] POPOV S. The tangle[EB/OL]. 2019[2025-06-11].https://letterboxd.com/film/the-tangle/.

[14] GREEN O. HashGraph-scalable hash tables using a sparse graph data structure[J].ACM transactions on parallel computing (TOPC),2021,8(2):1-17.

[15] SOMPOLINSKY Y, LEWENBERG Y, ZOHAR A. SPECTRE: serialization of proof-of-work events: confirming transactions via recursive elections[EB/OL]. 2017[2025-06-12]. https://www.semanticscholar.org/paper/SPECTRE-%3A-Serialization-of-Proof-of-work-Events-%3A-Sompolinsky-Lewenberg/65f1613a4f1b015fc64608.

[16] SOMPOLINSKY Y, WYBORSKI S, ZOHAR A. PHANTOM: a scalable BlockDAG protocol[EB/OL].(2021-10-10) [2025-05-25]. https://eprint.iacr.org/2018/104.pdf.

【作者简介】

张震（1993—），男，河南三门峡人，硕士研究生，研究方向：区块链、云计算。

（收稿日期：2025-05-13 修回日期：2025-09-16）