基于双层架构的溯源许可链共识算法设计

丁庆洋[1] 朱建明[1]* 高胜[1] 张瑾[2] 许艳静[1] 贾传昌[1] 高政[1]

（1 中央财经大学 信息学院,北京 100081 2 中央财经大学 保险学院,北京 100081）

摘 要：区块链中的区块按照时间历史顺序进行排列，同时通过数据加密技术以及共识机制使得区块链具有不可篡改性，这使得产品溯源成为区块链的重要应用场景.选择产品信息追溯技术不仅要考虑技术的可行性同时要考虑产品以及生产者的市场属性，这使得许可链代替公有链成为产品信息溯源的重要部署方式.现有研究成果中对溯源许可链的研究多停留在机制设计和框架建构上，少有对适用于产品信息溯源的共识算法进行研究.在技术工程实践过程中,联盟链中多选用实用拜占庭容错(Practical Byzantine Fault Tolerance，PBFT)作为溯源链的共识机制（如超级账本项目，Hyperledger)，但伴随着参与节点数量的增加，溯源链的运行效率将明显下降，延迟时间明显提高，致使多数项目依然处于试验阶段.基于此，本文提出基于双层架构的溯源许可链共识机制（DLPCM）.本文首先将参与者在垂直维度上化分两层，其次在不同层次上根据区块链的不同部署方式采用不同的共识机制；最后，对该共识机制下的溯源信息查询机制进行介绍.本文为基于许可链的溯源系统的开发和设计提供了重要借鉴.

关键词：许可链、溯源、双层架构、共识机制

Design of Traceability Permissioned Chain Consensus Algorithm Based on Double -Layer Architecture

DING Qing-Yang[1] ZHU Jian-Ming[1] GAO Sheng[1] Zhang Jin[2] XU Yan-Jing[1] JIA Chuan-Chang[1] GAO Zheng[1]

(1 School of Information, Central University of Finance and Economics, Beijing 100081

2 School of Information, Central University of Finance and Economics, Beijing 100081)

Abstract: The blocks in the blockchain are arranged in chronological and historical order, and the blockchain is incapable of modification through data encryption technology and consensus mechanism, which makes product traceability to be an important application scenario of blockchain. To choose product information traceability technology, we should consider not only the feasibility of the technology but also the market attributes of the product and the producer, which makes the Permissioned chain replace the public chain as an important deployment method of product information traceability. In the existing research results, the research on the traceability license chain mainly focuses on mechanism design and framework construction, and the consensus algorithm applicable to product information traceability is rarely studied. In the process of technology of engineering practice, choose Practical more Byzantine Fault Tolerance in league chain (Practical Byzantine Fault how PBFT) as the consensus of traceability chain mechanism (such as Hyperledger), but with the increasing number of participating nodes of the traceability chain efficiency will be significantly reduced, and the delay time will be significantly improved, resulting in most of the project is still in the stage of experiment. Based on this, this paper proposes a traceability license chain consensus algorithm based on double-Layer Architecture (DLPCM), and analyzes its security. In this paper, participants are divided into two layers on the vertical dimension, and different consensus mechanisms are adopted at different levels according to different deployment modes of blockchain. Finally, the traceability information query mechanism under the consensus mechanism is introduced, This paper provides an important reference for the development and design of traceability system based on license chain.

Keywords: Permissioned chain, traceability, Double -Layer Architecture, consensus mechanism,

---

基金项目：国家重点研发计划基金资助项目（NO.2017YFB1400700）；国家自然科学基金资助项目（NO.U1509214）.
Foundation item: National Key R&D Program of China (NO. 2017YFB1400700); National Natural Science Foundation of China (NO.U1509214).

*通信作者

1 引言

区块链最初作为数字货币-比特币的底层支撑技术进入人们的视野，并以其良好的分布式存储、点对点传输机制、数据可追溯性、数据防篡改性逐渐为人们所认可. 在经历作为数字加密货币底层支撑技术的区块链 1.0 时代，以及以以太坊为代表的区块链 2.0 时代，区块链技术不断成熟，其应用场景不断扩展，实践落地的项目也越来越多（诸如，国内的百度区块链，美图链，阿里慈善溯源链等），区块链已经迎来了区块链 3.0 的时代.同时，在国家战略层面，中共中央总书记、国家主席习近平同志，在 2018 年 5 月召开的中国科学院第十九次院士大会、中国工程院第十四次院士大会上讲话上也首次将区块链技术与人工智能、量子信息、移动通信、物联网并列为新一代的信息技术，从国家战略高层的角度对区块链技术的未来发展进行了肯定.国家工信部也发布了《2018 中国区块链产业白皮书》对区块链未来的发展做出了展望.可以预见，在未来一段时间内区块链技术将取得长足进步，也将会有更多的应有落地.

在诸多应用场景中，产品信息溯源已经成为一种重要的应用场景，国内外的应用实践也逐步增多，诸如国外的超级账本 Hyperledger 的锯齿湖项目，国内的京东产品溯源项目，这些项目也都取得一定的成果，其适用的产品也在逐渐地扩展.但在实践过程中以及理论研究中依然存在诸多问题，例如吞吐量、延迟时间等，阻碍着区块链技术应用场景的进一步扩展.在诸多问题中，一个较为核心和底层的技术问题便是溯源链的共识机制设计.现阶段理论研究中，关于区块链用于产品溯源的研究大多以区块链用于溯源的可行性、追溯机制的设计、产品信息溯源的模型框架建构以及区块链技术应用于不同产品溯源的具体场景分析等.针对溯源链共识机制具体设计的研究较少.同时，在国内溯源实践过程中，企业多以借鉴国外成熟的开源项目并加以利用为主，涉及到原创性、基础性的创新较少，因而对于溯源链共识算法的创新关注度不高.这就使得基于区块链技术的溯源链的共识机制研究存在较多空白.

同时，溯源尤其是产品生产信息的溯源，不仅是一个技术问题也是一个经济问题，甚至是一个国家行政管理问题，存在诸多利益相关者.对于消费者而言，可溯源的产品信息有助于甄别假冒伪劣商品，提升消费效用，其对于产品可溯源系统的要求在于溯源信息的准确性、全面性和便捷性；对于国家行政机关而言，可溯源的产品信息有助于维护良好的市场氛围，净化市场环境，便于其行政管理工作的开展，其对于产品可溯源系统的要求在于溯源信息的不可伪造性和易于获知性以及便于监管性.对于企业而言，可追溯的产品信息有利于其提高产品附加值，提升产品竞争力，作为系统的投入者，企业也要考虑成本、技术可行性，最为重要的是企业商业数据的保密性.以区块链技术作为底层支撑的溯源链具有较好的数据可追溯性、数据防篡改性以及分布式共享性，同时区块链技术的不断进步也使得其实际应用性逐渐提高.但在实际应用过程中也需要对区块链的部署形式加以考虑.公有链虽然在加密数字货币中得到了广泛应用，但其完全的去中心化、较低吞吐量以及延展性使得其自主可控性较低，并不完全适用于溯源的业务场景.以联盟链和私有链为具体部署形式的许可链具有区块链数据的分布式共享性、数据历史时序性以及数据不可篡改性，同时许可链中的存在类（准）中心节点，可以对参与者的权限进行控制，加之部署的智能合约可以较好的满足相关利益方对追溯系统的要求，本文所论述的溯源链以许可链为底层构架，具体形式则为基于私有链的溯源链和基于联盟链的溯源链.因而，本文所探讨的基于双层架构的溯源链的共识机制由部署于不同层次上的基于私有链的溯源链的共识算法和基于联盟链的溯源链的共识算法组成.

本文的创新点为结合溯源的实际业务流程，将溯源链划分为部署私有链的辅助层和部署联盟链主层，并介绍了相对应的共识机制.本文的后续章节安排如下：第二部分为相关工作介绍，第三部分为溯源链的双层架构体系，第四部分为溯源链的共识机制设计，第五部分为信息溯源以及查询机制，第六部分为安全性分析.

2 相关工作

基于双层架构的溯源链共识机制设计相关的研究主要包括：对基于区块链技术进行溯源的机制论证、对国内外共识算法的梳理、不同产品具体的溯源机制设计、基于公有链和私有链的溯源机制设计等具体如下：

对基于区块链技术进行溯源的机制论证.丁庆洋等（2017）研究指出伴随着我国电子商务的飞速发展，产生了一系列制约我国网络零售市场长远发展的难题，特别是 B2C 销售中存在的信息不对称、产品信息追

溯和防伪问题等，更是难以依靠常规网络零售市场治理手段予以彻底解决. 鉴于区块链技术能够凭借分布式存储架构、区块链式连接、“瀑布效应”，利用密码学、共识算法、智能合约等技术，在信息收集、流转、共享等过程中解决信息追溯难题，弥补产品防伪漏洞，防止信息篡改，而区块链上传信息的真实性、可用性、完整性问题，也可借助物联网技术加以解决，即能够通过接入物联网信息采集终端，确保信息客观公正动态地传输到电商平台产品信息区块链，实现对产品性状等信息的实时跟踪记录，因此可利用区块链技术实现对产品信息的追溯并防止篡改，进而结合物联网技术解决产品防伪问题[1]. Abeyratne 基于 Regattieri 的研究展望了将区块链技术应用于供应链管理的远景,并分析了在供应链管理中可能会遇到的问题[2-3]..Huertas 讨论了如何在其设计的 Eximchain 上使用智能合约来进行供应链管理[4].

对国内外共识算法的梳理研究.袁勇等（2018）系统性地梳理和讨论了区块链发展过程中的 32 种重要共识算法, 介绍了传统分布式一致性算法以及分布式共识领域的里程碑式的重要研究和结论, 提出了区块链共识算法的一种基础模型和分类方法，并总结了现有共识算法的发展脉络和若干性能指标[5].

不同产品具体的溯源机制设计.汪登等（2018）指出近年来，食品安全案件屡次发生，亟需采用安全、可信、透明的食品安全溯源系统来加强对食品产业链的监管与效率，提高食品安全水平，保障国民饮食健康，而目前的食品溯源系统主要面临着信息采集不标准、数据存储不安全、中心系统易受攻击和企业间信息交换过程隐私不能保障等问题.区块链技术具有分布式容错、不可篡改与隐私保护的特点，可以针对性地解决目前食品溯源系统中面临问题.基于区块链的食品安全溯源系统通过技术架构的分析提出将区块链恰当植入食品溯源体系的方案，即区块链技术应用于系统的数据库层与通信层，并对采用方案后的食品溯源体系的运行机制进行分析，结合具体应用场景与实际案例来论证设计方案的有效性[6].高峰等（2018）提出了一种针对比特币交易的溯源机制，能够追踪交易信息在网络层的传播路径，从而将交易中的匿名比特币地址和发起交易节点的 IP 地址相关联. 通过设计一种基于主动嗅探的邻居节点识别方法，溯源机制支持轻量级监测，而且相比现有溯源技术具有更好的实用性. 文中针对比特币系统开发了溯源程序，从有效性、准确率、适用范围等方面对其进行测试与分析评估. 实验结果表明，比特币网络中有 69.9%的服务器节点适用于这种溯源机制，能够获得召回率 50%、准确率 31.25%的溯源精度，优于现有的交易溯源方法，具有较强的实践意义和使用价值[7]. 陶启等（2018）论述了区块链应用于食品质量安全管理的可行性，并针对大米建立了去中心化、低成本高效率、信息可靠的执行环境，构建从农田到餐桌的大米全产业链质量全息数据库，采用基于危害因子的食品风险与安全溯源技术，设计了多角色、多环节和多要素的智能管理系统[8].

基于公有链和私有链的双链溯源机制设计.刘家稷等（2018）利用区块链分布式存储、去信任化和不可篡改的特性设计了一个基于区块链技术的防伪溯源系统(Traceability System Using Publicand Private Blockchain,TSPPB).TSPPB 使用公有链和私有链两套区块链,该溯源系统能够确保获得的溯源信息的真实可靠不可篡改并解决传统产品溯源系统存在的产品标签复制、滥发和产品质量问题相关责任人及问题环节定位困难的问题.在确保溯源信息安全性并解决传统溯源系统隐患的同时, TSPPB 还能够高效且保持低成本的运行[9].但同时，该论文在系统设计之初并未考虑到监管部门在整个溯源体系中的作用，也为对共识机制进行详细论述.Feng Tian 构建了一个基于 RFID 技术与区块链技术的溯源系统 Agri-food Supply Chain Traceability System,以防止溯源系统的信息被篡改并用于防止标签复制,引入了 BigchainDB 的概念,以解决区块链需要存储现实世界中的大量数据时可能存在的扩展性不足的问题[10-11].沃尔顿链是一种结合了RFID 技术与区块链技术的溯源系统,防止溯源系统的信息被篡改并通过 RFID 防止标签复制.

通过梳理相关工作，可以发现基于区块链实现溯源的相关研究已经取得丰硕的成果，但针对基于私有链和联盟链双层架构的溯源机制研究并不多见，同时论述其中共识机制的文献更是少见.

3 双层架构体系以及组网机制

溯源链的功能和性质，意味着其有诸多参与者，要求其有较高开放性，而现有以 Hyperledger 为代表的联盟链并不能满足较多参与者的高并发应用需求.因而本文在此提出双层架构体系，在纵向将其划分为主层和辅助层.主层用于溯源信息的共享和查询并在主层部署联盟链，辅助层用于收集存储溯源信息并在辅助层部署私有链，将数据存储量大、涉及产品具体生产销售的敏感信息部署于私有链中，并通过哈希指针的

方式与主层联结，主层则对数据的合规性进行审查并进行数据的共享，这种部署方式以产品溯源的具体业务场景为基础，不仅有利于减轻主层的负载有利于保护企业的隐私数据同时满足各方对溯源系统的要求.

溯源链涉及到利益相关者主要包括企业、消费者以及国家监管机构.而企业根据其在产品的流通环节中位置又可以划分为生产企业、物流企业、销售企业.国家监管机构根据其职能又可以划分为工商行政管理机构、卫生检疫机构、税务征收稽查机构、海关出入境管理机构、质量监督管理机构等.消费者则是最终购买商品并具有产品信息溯源需求的消费人群.在双层架构体系下，每一个企业和国家监管机构都建立自身范围内的私有链.不同的企业和国家行政管理部门私有链的具体数据内容不尽相同.生产企业主要存储生产产品的原材料信息、生产加工环节信息、产品批号生产时间、相关国家部门的批准和鉴定信息.物流企业则主要存储产品物流时间、物流存储方式、物流批号、物流通道信息.国家监管部门根据其履行法律职权的需要存储不同的信息，主要为产品审批信息、抽查检验信息、卫生检疫信息、出入境审批信息等等.这些私有链以及存储信息构成了主层的数据基础，各个私有链的数据通过哈希指针与主层联盟链相联结.主层通过共识后的数据，以提供外部接口的方式为消费者进行溯源信息的查询提供便利.在主层采用点对点组网机制，各个节点之间可以共享数据信息.在辅助层采用星型拓扑的组网机制，以参与主层共识的节点作为中心组网点.具体参见图 1 双层架构体系图.

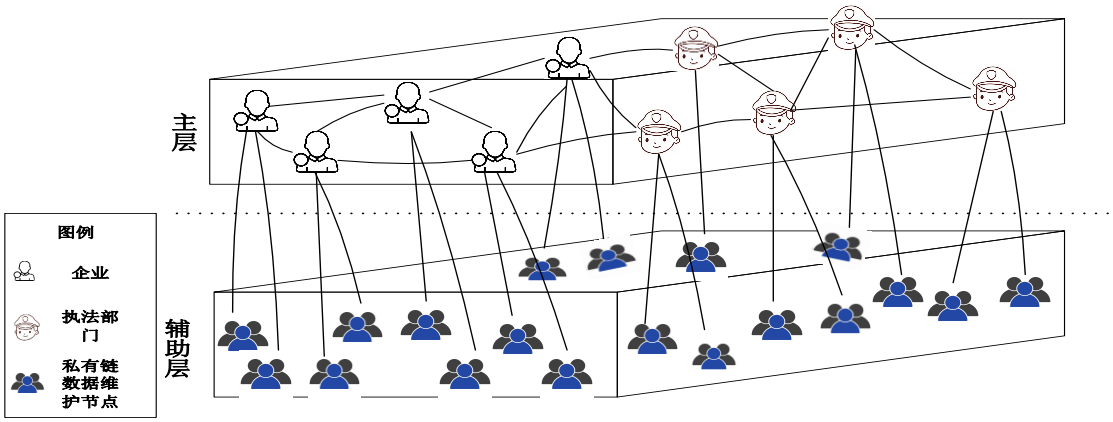

Figure 1 Double-layer architecture diagram

图 1 双层架构体系图

4 基于双层构架的溯源链共识机制

基于双层架构的溯源链整合了辅助层的私有链和主层的联盟链，因而在不同层次中需要采用不同的共识机制.结合溯源业务实际，本文提出在主层联盟链采用改进的实用拜占庭容错（Improved Practical Byzantine Tolerance，IPBFT）共识机制，在辅助层私有链采用强领导式 Raft（Raft of Strong Leadership，RSL）共识机制.该共识机制主要分为四个阶段：第一阶段为用户节点角色设置，第二阶段为数据区块构造，第三阶段为审核共识阶段以及数据上链更新.

4.1 溯源链中参与者角色设定

溯源链基于许可链的数据结构形式，因而无论是基于联盟链的溯源链还是基于私有链的溯源链都有类（准）中心节点.类（准）中心节点拥有记账权，负责收集交易数据、建造数据区块，同时对进入许可链中的参与者进行审核，对参与者的权限进行控制.具体到溯源链的主层中，类（准）中心节点一般是生产企业或是具有一定信息技术基础的大型销售企业，这些企业负责整体溯源链的规划与建设，负责溯源链参与节点的审核并进行权限管理，向消费者提供溯源信息的查询服务.在溯源链的辅助层中，类（准）中心节点一般为生产企业中的质监部门或是产品流通环节中其他企业的信息技术部门，这些部门负责私有链的运行与维护，并负责与联盟链的信息传输.除类（准）中心节点外，还包括验证节点.验证节点参与共识，对区块数据进行验证.在主层中，验证节点一般为国家执法部门和流通环节中非类（准）中心节点的企业，这些部门对职责范围内的相关产品信息进行审核，并验证数据区块参与共识.在辅助层中，验证节点为参与产品生产和销售的企业中的其他部门，他们负责将产品信息发送至私有链的中心节点，并保存区块链的数据备份.具

体如下表 1 所示.

Table 1 participant role settings in the traceability chain

表 1 溯源链中参与者角色设定

	主层		附加层	
	类（准）中心节点	验证节点	类（准）中心节点	验证节点
职责	规划、建造维护溯源链，收集交易数据、建造数据区块、对参与者进行审核，提供外部查询接口	维护溯源链，参与验证	私有链的运行与维护，与联盟链的信息传输	维护溯源链，参与验证
权限	记账权、参与者权限管理	审核信息的合规性，数据查询，溯源链信息备份	记账权、参与者权限管理	审核信息的合规性，数据查询，溯源链信息备份
实体执行部门	是生产企业或是具有一定信息技术基础的大型销售企业	国家执法部门和流通环节中非类（准）中心节点的企业	生产企业中的质监部门或是产品流通环节中其他企业的信息技术部门	参与产品生产和销售的企业中的部门

4.2 数据区块结构

溯源链中的类（准）中心节点负责建造区块，其中产品生产、物流等各个环节的具体产品溯源信息存储于辅助层的私有链中，而主层中联盟链中的数据只是私有链区块的哈希值. 因而，大量数据存储于辅助层，主层共识过程中的数据传送量将大大降低，进而提高数据的吞吐量降低延迟时间.

辅助层中的私有链是溯源机制的基础. 其数据区块由区块头和区块体两部分组成. 区块头中主要封装当前区块哈希值、前置区块头哈希值、产品生产或流通中涉及到的部门哈希值、版本号、Merkle 根、时间戳，其中当前区块的哈希值是对经过验证节点验证之后的区块利用 Hash256 算法计算等到的函数值，前置区块头哈希值为父区块的哈希值，产品生产或流通中涉及到的部门哈希值是产品在具体生产或是流通中涉及到有关部门的哈希值，版本号为整个区块链系统的版本编号，Merkel 根则是对区块体中的数据进行 Merle 计算后得到的，时间戳为经过验证节点共同验证后由类（准）中心节点设置. 区块体主要封装产品生产或流通信息或是销售信息，不同企业的由于其所处供应链条的环节不同存储的信息不尽相同，如生产企业数据区块体主要包括的事项有：产品批号、生产时间、加工工艺、原材料信息、生产线编号、数字签名等. 图 2 给出了生产企业私有链数据区块结构的示例.

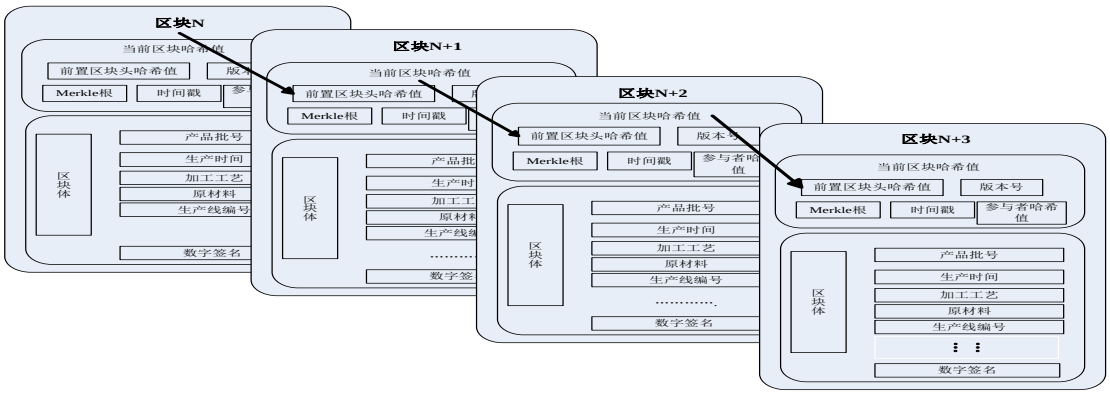

Figure 2 Example of the production block private block data block structure

图 2 生产企业私有链数据区块结构的示例

溯源链主层中的联盟链以主要实现数据在不同企业以及执法部门中的共享，同时对外实现溯源信息的查询. 因而，在联盟链中的区块体中的数据并没有必要存储详细信息，只要在数据区块中存储用于溯源的数据路径以及相关企业私有链的区块的哈希值即可. 其数据区块由区块头和区块体两部分组成. 区块头中主要封装的数据信息与私有链中区块头中的数据类似，包括当前区块哈希值、前置区块头哈希值、产品生产或流通中涉及到的部门哈希值、版本号、Merkle 根、时间戳，区块体中主要封装的是不同企业私有链当前时间点上的区块哈希值、数字签名. 图 3 为主层联盟链的数据结构图.

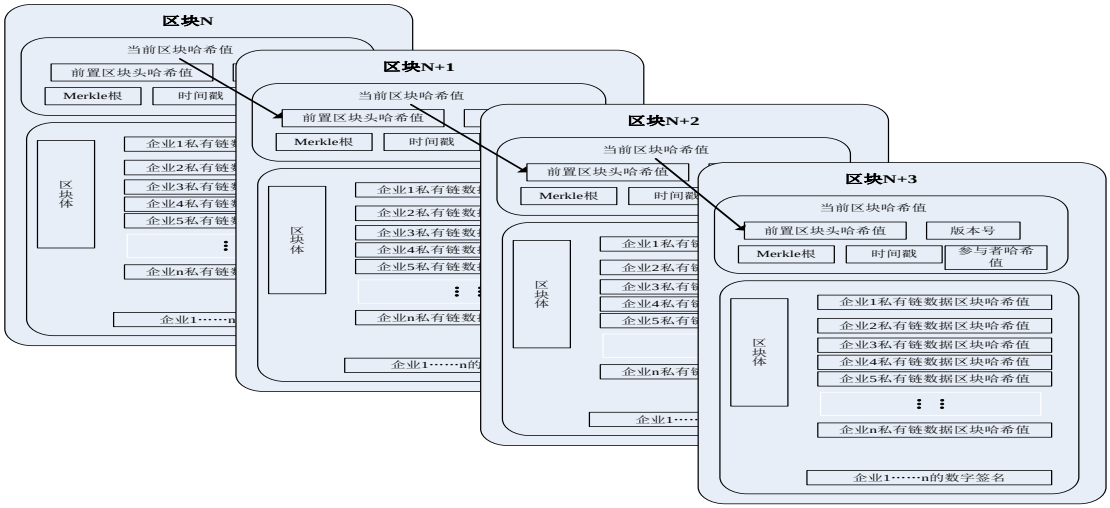

Figure 3　Data structure diagram of the main layer alliance chain

图 3 主层联盟链的数据结构图

4. 3 共识机制

4.3.1 相关定义

为便于清晰阐释共识算法的核心思想，本文将对共识机制涉及到的主体以及客体进行定义，相关定义具体内容如下：

定义 1：企业 E、国家监管部门 R 和企业中的具体部门 $S.Ei \in (E_1 \cdots\cdots En)$表示溯源链中涉及到的各个不同企业.$R_i \in (R_1 \cdots\cdots Rn)$ 表示溯源链中涉及到的各个不同的监管部门.$S_1 \in (S_1 \cdots\cdots Sn)$ 表示溯源链中涉及到的企业中的不同的部门. $E_{S_i} \in (E_{S_1} \cdots\cdots E_{S_n})$表示溯源链中涉及到同一企业中的不同部门.$E_{S_i}^{i} \in (E_{S_1}^{1} \cdots\cdots E_{S_n}^{n})$ 表示溯源链中涉及到的不同企业的不同部门.

定义 2：企业私有链 P 和联盟链 A. $P_{E_i} \in (P_{E_1} \cdots\cdots P_{E_n})$ 表示不同企业的私有链.*Center node* 表示私有链中心节点角色的承担部门.*Center node* $_A$ 表示公有链中心节点角色的承担部门.

定义 3：具体产品 D，产品信息 F 和执法部门的相关审批信息 $Appr.Di \in (D_1 \cdots\cdots Dn)$表示不同产品.$E_{D_i}^{i} \in (E_{D_1}^{1} \cdots\cdots E_{D_n}^{n})$ 表示溯源链中不同企业的不同产品.$D_i \to F_{E_i} \in (D_1 \to F_{E_1} \cdots\cdots D_n \to F_{E_n})$ 表示溯源链中不同企业的不同产品信息.$Appr_{R_i} \in (Appr_{R_1} \cdots\cdots Appr_{R_n})$ 表示溯源链中不同执法部门的审批信息.$Appr_{R_i} \to D_i \to F_{E_i} \in (Appr_{R_1} \to D_1 \to F_{E_1} \cdots\cdots Appr_{R_n} \to D_n \to F_{E_n})$ 表示溯源链中不同执法部门针对不同信息的不同审批信息.

定义 4：数字签名 $Sig.Sig_{E_i} \in (Sig_{E_1} \cdots\cdots Sig_{E_n})$ 表示不同企业的数字签名.$Sig_{R_i} \in (Sig_{R_1} \cdots\cdots Sig_{R_n})$ 表示不同执法部门的数字签名.$Sig_{E_{S_i}^{i}} \in (Sig_{E_{S_1}^{1}} \cdots\cdots Sig_{E_{S_n}^{n}})$ 表示不同企业不同部门的数字签名.

定义 5：哈希值 h 由哈希算法 $H_{(\cdot)}$，即 $H_(P_{E_1}) \cdots\cdots H_(P_{E_n}) \to\to h_{P_{E_1}} \cdots\cdots h_{P_{E_n}}$，$h_{P_{E_i}} \in (h_{P_{E_1}} \cdots\cdots h_{P_{E_n}})$.

定义 6：时间戳 $T.T_{P_{E_i}}$ 表示私有链的时间戳，T_A 表示联盟链的时间戳.

4.3.2 共识算法

基于双层架构的溯源链共识机制的核心思想为审核即验证，线下对产品信息进行审核，线上即通过验证.通过验证则意味着共识完成.由于用于溯源的产品信息存储于辅助层的企业私有链中，私有链的数据完整以及可靠性至关重要.以私有链的溯源信息为为基础，主层中的联盟链负责将企业私有链的信息共享给其他企业和执法部门.通过信息的共享实现数据存证，一旦发生产品质量问题，为企业厘清责任具有重要意义，这也是溯源链的重要功能之一.基于此，本文将首先介绍私有链的强领导式 Raft（Raft of Strong Leadership，RSL）共识算法，继而介绍主层联盟链采用改进的实用拜占庭容错（Improved Practical Byzantine Tolerance，IPBFT）共识算法.

（1）RSL 算法

算法描述：RSL 算法中类（准）中心节点具有控制权，通过将各个部门提交的产品溯源信息进行审核，

并将信息向其他私有链的参与部门推送审核结果信息，其他部门进行复验，复验完成后数据上链.

算法 1：类（准）中心节点进行数据审核

输入：各部门提交的产品信息

输出：审核结果

Algorithm：Center node auditing data

Import：$D_i \rightarrow F_{E_i}$ []

Outport：Result of Auditing []

for i in $D_i \rightarrow F_{E_i}$[]: //加载产品信息数据

check($D_i \rightarrow F_{E_i}$) //查验信息完整性

check($Sig_{E_{S_i}^i}$) //查验数字签名

check($Appr_{R_i} \rightarrow D_i \rightarrow F_{E_i}$) //查验生产过程中相关执法部门的审批是否完备

if checked $D_i \rightarrow F_{E_i}$ []

then append(Result of Auditing []) //生成合规信息集

end if

end for

send Result of Auditing [] to E_{S_i}

end

算法 2：企业中的相关部门进行复验

输入：类（准）中心节点审核信息

输出：复验结果

Algorithm2：Center node Reauditing data

Import：Result of Auditing []

Outport：Result of Reauditing []

for i in $E_{S_i}^i$ []: //企业中除类（准）中心节点外的其他部门

check(Result of Auditing []) //查验信息完整性

check($Sig_{E_{S_1}^i} \cdots\cdots Sig_{E_{S_n}^i}$) //查验数字签名

if checked Result of Auditing []

then append(Result of Reauditing []) //生成合规信息集

end if

end for

send Result of Auditing [] to Center node

end

算法 3：私有链中类（准）中心节点构造区块并主层发送哈希值

输入：复验结果

输出：生成数据区块以及发送哈希值到主层联盟链中

Algorithm3：Center node Reauditing data

Import：Result of Reauditing []

Outport：block of Result of Reauditing [] and $h_{P_{E_i}}$

Get Result of Reauditing [] //收集复验结果

Block（Result of Reauditing []） //构造区块

$H_{(\text{block of Result of Reauditing []})} \rightarrow\rightarrow h_{P_{E_i}}$ //生成哈希函值

$Sig_{E_i}(h_{P_{E_i}})$ //对哈希函数值进行签名

Send $h_{P_{E_i}}$ to E_i //将区块哈希值发送到各个企业

Send $h_{P_{E_i}}$ to R_i //将区块哈希值发送到各个执法部门

end

（2）IPBFT 算法

算法描述：主层中的类（准）中心节点将收集到的信息进行打包，并建立数据区块，将数据区块发送到每一个参与节点，每个节点对数据区块进行验证，所有节点验证通过后将数据区块联结到联盟链上.

算法 1：主层节点对数据进行收集建造区块

输入：每一个节点的区块哈希值

输出：数据区块

Algorithm： The central node of the main layer collects the data and builds the block

Import：$h_{P_{E_i}}$

Outport：block（Ture$h_{P_{E_i}}$[]）

Get $h_{P_{E_i}}$[]

for i in $h_{P_{E_i}}$[]: //加载全网私有链数据区块哈希值

check($h_{P_{E_i}}$) //查验每一个哈希值

check(Sig_{E_i}) //查验数字签名

check($T_{P_{E_i}}$) //查验私有链时间戳

if $T_{P_{E_i}}$ >=T_A:

then send back false to *Ei* //如果私有链时间戳晚于当前时间则报错

else if check($h_{P_{E_i}}$)and check(senF) = false:

then send back false to *Ei* //如果任意一个被查验项不合规则报错

else append(Ture$h_{P_{E_i}}$[]) //生成合规数据集

end if

end for

block（Ture$h_{P_{E_i}}$[]） //建立合规数据集的区块

send block（Ture$h_{P_{E_i}}$[]）to *Ei* //发送区块到非中心节点的企业

send block（Ture$h_{P_{E_i}}$[]）to *Ri* //发送区块到执法部门

end

算法 2：收集审核结果并建立联结到联盟链

输入：收集审核结果

输出：联结到联盟链上的新区块

Algorithm2: Collect audit results and establish a link to the alliance chain

Import：Collect audit results

Outport：New blocks attached to the union chain

Get Collect audit results of *Ei*[] //收集非中心节点的验证结果

Get Collect audit results of *Ri*[] //收集执法部门的验证结果

for i in *Ei* ∈(E_1……*En*):

for i in R_i ∈（R_1……*Rn*）:

check Audit results of *Ei* //查验非中心节点的验证结果

check Audit results of *Ri* //查验非中心节点的验证结果

end for

end for

if result of check() = right

then generate block[] //若查验结果都为正确，生成新区块

end if

link block []to alliance chain{} //联结区块到主链

broadcast alliance chain{}　　//广播主链最新进展

end

5　信息追溯以及查询机制

除通过信息的共享实现数据存证，为企业厘清责任外，为消费者提供便利的产品信息溯源也是溯源链的重要功能.在溯源链中，消费者通过向企业提出产品溯源的请求，主层中的中心将对其请求进行判定，判定合法的请求，中心节点将向溯源请求涉及到的企业发送查阅私有链数据的请求，溯源信息涉及到的企业将向中心节点返回具体信息，中心节点进一步将该信息发送到消费者.如果中心节点判定消费者请求不合法将返回拒绝请求的信息.具体如图 4 所示.

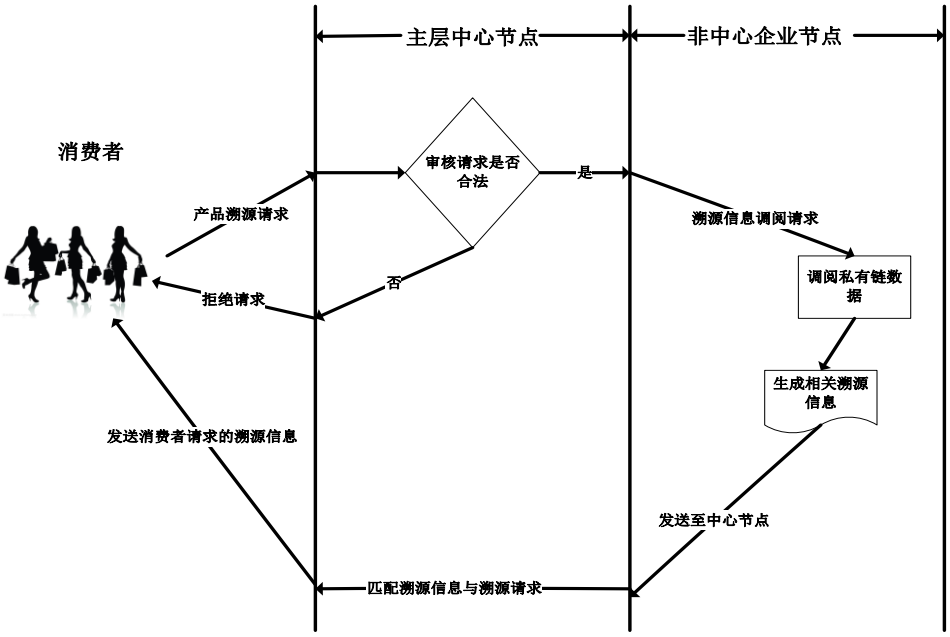

Figure 4 Schematic diagram of traceability information query mechanism

图 4 溯源信息查询机制示意图

6 结语

本文，结合产品溯源业务场景的实际，提出了基于双层架构的溯源链的共识机制. 针对区块链本身难以加载大量数据的技术瓶颈，本文提出双层数据架构的数据体系，即主层和辅助层. 将大量信息产品具体信息存储于附加层的私有链上，并通过哈希指针以及数字签名与主层联结. 在主层部署联盟链，并进行跨企业的共识，通过共识后的数据将实现跨企业的共享. 同时通过哈希指针的方式有效实现了数据的防篡改也满足了企业商业数据保护的需求. 本文提出在辅助层的私有链和主层的联盟链，分布采用 RSL 和 IPFT 的共识机制，并对共识算法进行了具体介绍，同时也给出了不同部署形式区块链的区块数据结构. 最后，本文介绍消费者实现产品溯源的具体路径. 本文的研究内容对基于区块链建立溯源系统的相关研究进行了扩展，也为实际项目落地提供了参考和借鉴.

参考文献

[1] 丁庆洋，朱建明.区块链视角下的 B2C 电商平台产品信息追溯和防伪模型[J].中国流通经济，2017（12）：41-49.

[2] Abeyratne, Saveen A., and Radmehr P. Monfared., “Blockchain ready manufacturing supply chain using distributed ledger ,” International Journa lof Research in Engineering and Technology, 2016(9) 1-10,September

[3] Regattieri, A, Gamberi, M, and Manzini, “Traceability of food products: General framework and experimental evidence,”. Journal of food engineering 2007(81):347-356.

[4] Eximchain: Supply Chain Finance solutions on a secured public, permissioned blockchain hybrid, ” https://eximchain.com/ Whitepaper%20-%20Eximchain.pdf, March. 2018

[5] 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, (9):1-12.

[6] 汪登,曾小珊,白倩兰,等. 基于区块链的食品安全溯源技术[J]. 食品科学, 2018(2).1-10

[7] 高峰, 毛洪亮, 吴震, 等. 轻量级比特币交易溯源机制[J]. 计算机学报, 2018(5).899-1004.

[8] 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[J].中国粮油学报，2018（8）：44-52.

[9] 刘家稷,杨挺,汪文勇.使用双区块链的防伪溯源系统[J]. 信息安全学报, 2018, 3(3).17-29.

[10] Tian, Feng, “An agri-food supply chain traceability system forChina based on RFID & blockchain technology,” IEEE International Conference on Service Systems and Service Management(ICSSSM).,January 2016.

[11] Feng T, “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things, ” IEEE International Conference on Service Systems and Service Management (ICSSSM)., January 2017.