|  |
| --- |
| 1、研究目的和意义：  茶叶质量安全问题，如农残超标，如同其他食品行业的安全问题一样，一直是亟待解决的痛点。茶叶行业有其特殊性，许多地区都会生产属于其本区域的特色名茶，比如西湖龙井、凤凰单枞等，一旦发生质量安全问题，很多时候影响的将是整个区域大范围的茶行。茶叶溯源系统记录着茶叶从生产到销售整个流程的所有必要数据，使得发生质量安全问题时，能快速定位到问题的源头以及相关负责人，及时召回问题茶叶，遏制问题蔓延的势头，这是解决目前茶叶安全窘迫现状的有效方法之一。然而对于传统的溯源系统来说，数据都是由统一的中央数据库发出，每个流程的数据在存储过程中以及日后维护时都有被篡改的可能，造成数据的真实性存在质疑，即使数据上传到权威政府机构，也同样带来中心权利过大化的问题。区块链的出现则很好地解决了数据中心化和易篡改等问题，其去中心化、不可篡改性、开发透明、机器自治和匿名性的特性，弥补了传统溯源系统的缺点。  区块链系统首先是一个分布式系统，因此在区块链技术框架的工作流程中，共识机制是一个核心问题，即如何解决Leslie Lamport等人提出的拜占庭将军问题。随着技术的发展，区块链系统在解决拜占庭将军问题实现共识这方面，出现了概率性算法PoW、确定性算法RPCA和PBFT算法等。茶叶产业链溯源在与区块链技术相结合后，共识机制这一模块在区块链技术框架的工作流程中会成为最大的性能瓶颈，特别是前期企业刚入驻平台，往系统中大量录入以前的溯源数据时。PoW算法在电子加密货币系统中每10分钟左右生成一个区块，在以太坊中每10秒左右生成一个区块，而RPCA算法和PBFT算法为3-6秒生成一个共识区块。由于数字货币在溯源系统中用处不大，故选用RPCA、PBFT等算法。即便如此，在大量数据前面，这类算法依旧无法满足系统高性能的要求，所以根据实际的场景，对现有的高效算法诸如PBFT、dBFT进行改进就显得非常重要了。  茶叶产业链溯源系统中会涉及到权限角色地位不等的各机关和企业，由此选用联盟链。联盟链与公有链的区别不仅在于系统中心化和参与者的身份，还有共识机制与激励机制上的差异。选用联盟链，意味着区块链系统中的信任机制不再是PoW或PoS，可以通过降低去中心化长度的方法，减少参与共识机制的节点以克服挖矿过程的资源浪费问题；同时，维护茶叶产业链溯源系统是联盟链中各参与节点的责任，故区块链系统的运行无需激励机制，可以不依赖数字货币，简化记录账簿，降低系统运行所需带宽，进一步提高系统性能。  2、国内外研究现状  区块链从出现到现在经历了快速的发展，1.0阶段：区块链技术主要用于支持以比特币为代表的数字货币，通过支持账户间转账、付款等支付交易操作，使得交易双方无需借助第三方机构的保证即可实现数字货币安全可信的交易。2.0阶段：区块链技术的应用场景，从单一的数字货币交易延伸到图灵完备的通用计算领域。用户不再受限于仅能使用比特币脚本所支持的简单逻辑，而是可以自行设计任意复杂的合约逻辑。出现以以太坊为代表的，将数字货币与智能合约相结合的平台，利用区块链作为底层技术，在平台上运行任意复杂的分布式程序Dapp。3.0阶段：出现以超级账本为代表的项目，进一步引入权限控制和安全保障，将区块链技术从经济领域延伸到社会管理、慈善公益、文化娱乐、医疗健康等社会各个领域中。  在1.0阶段，应用于区块链系统中的共识算法是PoW这类概率性算法，共识结果是临时的，随着时间的推移或某种强化，共识结果被推翻的概率越来越小，成为事实上的最终结果。而且其高度的去中心化，并且平均每10分钟生产一个区块。到了3.0阶段，共识算法则是PBFT这类确定性算法，且不再高度去中心化，同时形成了联盟链。  目前，世界范围内对区块链技术的研究和应用主要集中在金融领域，很多商业银行、金融机构甚至政府都在大力支持区块链相关研究。世界经济论坛报告指出，目前有超过20个国家投资区块链相关的技术领域，80%的银行在2017年开始实施一些区块链分布式账本有关的项目。  2015年12月，由开源世界的旗舰组织Linux基金会牵头，30家初始企业成员（包括IBM、Accenture、Intel、J.P.Morgan、R3、DAH、DTCC、FUJITSU、HITACHI、SWIFT、Cisco等），共同宣布了Hyperledger联合项目成立。超级账本项目为透明、公开、去中心化的企业级分布式账本技术提供开源参考实现并推动区块链和分布式账本相关协议、规范和标准的发展。Fabric是最早加入到超级账本项目中的顶级项目，由IBM、DAH等企业于2015年底提交到社区。该项目的定位是面向企业的分布式账本平台，创新地引入了权限管理支持，设计上支持可插拔、可扩展，是首个面向联盟链场景的开源项目。  **本课题针对前人的研究进行以下两部分的探索：**   1. 本课题将使用超级账本Hyperledger中的顶级项目Fabric与茶叶产业链溯源系统相结合。Fabric具备完备的权限控制和安全保障、高性能、可扩展、较低信任要求的优势，最重要的一点是，其模块化设计，可插拔的架构设计，使得我们在共识机制这块可以根据实际情况选择替换，从而让我们可以对现有的各类主流优秀的拜占庭容错算法在茶叶产业链溯源系统中的性能进行分析对比。 2. 根据Fabric项目与茶叶产业链溯源系统结合后的批量数据的录入情况，我们可以对上一步在性能对比中处于优势的算法进行优化。得益于Fabric项目中的Orderer节点提供的排序服务，且这排序服务支持多通道，所以我们并不一开始就让所有节点参与到共识之中，而是按照一定策略和条件，选择相应数量的节点参与到共识，最后再广播通知剩余节点参与共识。   参考文献：  [1] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains[J]. 2018.  [2] Sousa J, Bessani A, Vukolić M. A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform[J]. 2017:1-2.  [3] 李亚楠. 基于区块链的数据存储应用研究[D].北京交通大学,2018.  [4] Schneider F B. Implementing fault-tolerant services using the state machine approach: a tutorial[J]. Acm Computing Surveys, 1990, 22(4):299-319.  [5] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[M]. ACM, 2002. [6] Camenisch J, Herreweghen E V. Design and implementation of the idemix anonymous credential system[C]// 2002:21-30.  [7] Kemme B, Alonso G. A new approach to developing and implementing eager database replication protocols[J]. Acm Transactions on Database Systems, 2000, 25(3):333-379.  [8] Kemme B, Alonso G. Alonso, G.: A New Approach to Developing and Implementing Eager Database Replication Protocols. ACM Transactions on Database Systems 25(3), 333-379[J]. Acm Transactions on Database Systems, 2000, 25(3).  [9] Yin J, Martin J P, Venkataramani A, et al. Separating Agreement from Execution for Byzantine Fault Tolerant Services[J]. Acm Sigops Operating Systems Review, 2003, 37(5):253-267.  [10] Castro M, Liskov B. Practical Byzantine fault tolerance[C]// Symposium on Operating Systems Design & Implementation. ACM, 1999:173-186.  [11] Dijkstra E W. On-the-fly garbage collection: an exercise in cooperation[J]. Communications of the Acm, 1978, 21(11):966-975.  [12] Fischer M J. Impossibility of distributed consensus with one faulty process[J]. Acm Tocs, 1985, 32(2):374-382.  [13] Schneider F B. Implementing fault-tolerant services using the state machine approach: a tutorial[J]. Acm Computing Surveys, 1990, 22(4):299-319.  [14] Li M, Tamir Y. Practical Byzantine Fault Tolerance Using Fewer than 3f+1 Active Replicas.[C]// ISCA, International Conference on Parallel and Distributed Computing Systems, September 15-17, 2004, the Canterbury Hotel, San Francisco, California, Usa. DBLP, 2004:241-247.  [15] Benini L, Bogliolo A, Micheli G D. A survey of design techniques for system-level dynamic power management. IEEE Trans Very Large Scale Integr (VLSI) Syst[J]. IEEE Transactions on Very Large Scale Integration Systems, 2000, 8(3):299-316.  [16] 汪登, 曾小珊, 白倩兰,等. 基于区块链的食品安全溯源技术[J]. 大数据时代, 2018(3).  [17] Swan M. Blockchain: Blueprint for a New Economy[M]// Blockchain : blueprint for a new economy. O'Reilly, 2015.  [18] Swan M. Blockchain Thinking : The Brain as a Decentralized Autonomous Corporation [Commentary][J]. IEEE Technology & Society Magazine, 2015, 34(4):41-52.  [19]Calcaterra C, Kaal W A, Andrei V. Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems[J]. Social Science Electronic Publishing, 2018.  [20]Yuan Yong, Fei-Yue Wang. 区块链技术发展现状与展望[J]. Zidonghua Xuebao/acta Automatica Sinica, 2016, 42(4):481-494.  [21] Peters G W, Panayi E. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money[M]// Banking Beyond Banks and Money. Springer International Publishing, 2016.  [22]郭珊珊. 供应链的可信溯源查询在区块链上的实现[D]. 大连海事大学, 2017.  [23]吴霜, 喻朝新. 物联网和区块链技术在农产品溯源上的应用[J]. 电信工程技术与标准化, 2018(6).  [24]Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.  [25]Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4:2292-2303.  [26]Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology[C]// International Conference on Service Systems and Service Management. IEEE, 2016:1-6.  [27]Gandino F, Montrucchio B, Rebaudengo M, et al. Analysis of an RFID-based Information System for Tracking and Tracing in an Agri-Food chain[C]// Rfid Eurasia, 2007. IEEE, 2007:1-6. |