华南农业大学

硕士研究生中期考核与学位论文开题报告

学号: 20173078011

姓名: 苏锐佳

学院: 数学与信息学院

专业(领域): 计算机技术

研究方向: 区块链溯源

导师姓名: 杜治国

攻读学位: 工程专业学位硕士

|  |  |  |  |
| --- | --- | --- | --- |
| 论文题目 |  | | |
| 选题来源 | 其他 | 论文类型 | 基础研究 |
| 开题日期 | 2017-09-17 | 涉密 | 否 |
| **一、立题依据（包括研究目的、意义、国内外研究现状和发展趋势，需结合科学研究发展趋势来论述科学意义；或结合国民经济和社会发展中迫切需要解决的关键科技问题来论述其应用前景。附主要参考文献目录）**  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。  2017年12月14日，沃尔玛、京东、IBM、清华大学电子商务交易技术国家工程实验室共同宣布成立中国首个安全食品区块链溯源联盟，旨在通过区块链技术进一步加强食品追踪、可追溯性和安全性的合作，提升中国食品供应链的透明度。  **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] Mason B J.Clouds,rain and rainmaking[M].Cambridge University Press,1975:86-87.  [5] Wang T,Clifford S F.Use of rainfall-induced optical scintillations to measure path-averaged rain parameters[J].Journal of the Optical Society of America,2004,65(8):927-937. [6] Starik S,Weman M.Simulation of rain in videos[C]//Texture Workshop.Nice,France:IEEE Press,2003,2:406-409.  [7] Garg K, Nayar S K. Detection and removal of rain from videos[C], Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Columbia, NewYork, USA, 2004: 528-535.  [8] BrewerN,Liu Nianjun. Using the shape characteristics Pattern of rain to identify and remove rain from video[J]. Lecture NotesinComputerScience, 2008,(5342):451-458.  [9] Barnum P, Narasimhan S G, Kanade T. Analysis ofrain matrix factorization and sparse coding[J]. Journal of Machine Learning Research, 2010, 11: 19-60.  [10] Kang L W,Lin C W,Fu Y H.Automatic single-image-based rain streaks removal via image decomposition[J].IEEE Transactions on Image Processing.2012,21(4):1742-1755.  [11] Fu Y H,Kang L W,Lin C W.Single-frame-based rain removal via image decomposition[C].//Iternational Conference on Acoustics.Speech and Signal Processing,2011:1453-1456.  [12] Chen D Y,Chen C C,Kang L W.Visual depth guided image rain streaks removal via sparse coding[C].//International Systems on Intelligent Signal Proceccing and Communications Systems,2012:151-156  [13] Kang L W,Lin C W,Lin C T.Self-learning-based rain streak removal for image/video[C].//International Symposium on Cricuits and Systems,2012:1871-1874.  [14] Olshausen B A,Field D J.Sparse coding with an overcomplete basis set:A strategy employed by V1[J].Vision research,1997,37(23):3311-3325.  [15] Zakzeski J,Bruijnincx P C A,Jongerius A L.The catalytic valorization of lignin for the production of renewable chemicals[J].Chemical reviews,2010,110(6):3552-3599.  [16] Joachims T,Making large scale SVM learning practical[R].Universital Dortmund,1999.  [17] Y. Luo, Y. Xu, and H. Ji, Removing rain from a single image via discriminative sparse coding, In IEEE Int’l Conf. Computer Vision, 2015.  [18] Zhou Yuan, Han Yusheng, Zhou Pucheng, A Method for Removal of Rain in Single Image[J], JOURNAL OF GRAPHICS, Vol.36,No.3, June 2015,pp.439-443  [19]Wu Q,Zhang W,Vijaya Kumar B V K.Raindrop detection and removal using salient visual features[C].//International Conference on Image Processing,2012:941-944.  [20]Bertalmio M,Sapiro G,Caselles V.Image inpainting[C].//Proceedings of the 27th annual conference on Computer graphics and interactive techniques,2000:417-424.  [21] Jin-Hwan Kim, Chul Leey, Jae-Young Simz, and Chang-Su Kim. SINGLE-IMAGE DERAINING USING AN ADAPTIVE NONLOCAL MEANS FILTER.in Proc IEEE CVPR, June 2013, pp. 528–535.  [22]Y. Li, R. T. Tan, X. Guo, J. Lu, and M. S. Brown, Rain Streak Removal using Layer Priors, In IEEE Conf. Computer Vision and Pattern Recognition, 2016.  [23]石晓晴, 单幅图像中雨滴检测与去除方法的研究[D].北京交通大学,2016.  [24]Eigen D,Krishnan D,Fergus R.Restoring an image taken through a window covered with dirt or rain[C].Proceedings of the IEEE International Conference on Computer Vision,2013:633-640.  [25]Hinton G E,Osindero S,The Y W.A fast learning algorithm for deep belief nets[J].Neural computation,2006,18(7):1527-1554.  [26]Burger H C,Schuler C J,Harmeling S,Image denoising:Can plain neural networks compete with BM3D[C].IEEE Conference on Computer Vision and Pattern Recognition,2012:2392-2399.  [27]Dabov K,Foi A,Katkovnik V.image denoising with block-matching and 3D filtering[C].International Sociaty for Optic and Phtonics,2006:412-427. | | | |

|  |
| --- |
| **二、研究内容和目标（说明课题的具体研究内容，研究目标和效果，以及拟解决的关键科学问题。此部分为重点阐述内容）**   1. **本课题主要研究内容分为两部分：**   1）茶叶产业链溯源系统与区块链系统结合。  在溯源系统中，每一样商品都在区块链网络中被数字化，这样信息维护者方可全面具体的维护产品信息，避免溯源信息割裂问题，利用产品和参与者的标识，认证授权中心可以通过智能合约的方式自动对产品当前担责节点开发权限，保证数据维护的有序性和可靠性，防止非相关节点违规操作。被授予权限的参与者维护信息时需以私钥连接到网络中，而一旦参与者发起产品转移，比如茶叶从存储仓库转移到加工场，系统通过内嵌的智能合约进行相关的审核，通过后将参与者之前提供的信息打包录入区块链中。由此可见，数据打包成区块的时间节点是可控的，从而保证内部溯源数据不会与外部溯源数据被封装进同一个区块，造成区块信息访问权限发生矛盾（为保护企业隐私，内部溯源信息的访问权限必然高于外部溯源信息）。  2）拜占庭容错共识算法在系统中的性能分析对比与大量数据录入时系统生成区块的性能优化  一般情况下，在系统中一旦参与者发起产品转移，将会有区块产生，而区块加入到区块链之前，则需要经由框架选用的共识机制达成共识才行。Fabric在共识机制上可拔插的架构设计，让我们可以将目前主流的共识算法分别应用其中，并进行性能分析和对比，以此选出更适合本系统的算法。Fabric框架的共识机制默认为PBFT算法，因此在把Fabric框架和茶叶产业链溯源系统结合在一起之后，我们无需做任何修改即可使用PBFT算法。Tenermint算法是PBFT算法的简化版，PBFT为3阶段共识过程的异步协议，Tenermint则是2阶段共识过程的弱同步协议。RPCA算法使用一种子网络内部相互信任并构成大网络的方案。本课题打算使用这三种算法进行性能分析与对比，不过我们无需分开进行测试，Fabric框架中的Orderers节点提供的排序服务支持多通道，这意味着我们可以在所有节点里面同时生成三条区块链，并且彼此之间的消息沟通互不干涉，少了每次测试都要重置系统的麻烦，这有助于提高测试的效率。  有些企业在刚入驻系统时，需要录入大量的历史数据，如果按一般情况的做法去生成区块，那么最终完成所有的区块生成将要花费大量时间。在此，我们可以参考一下RPCA算法的思路：RPCA算法为了降低节点间同步沟通的成本，使用了一种子网络内部相互信任，由这些内部信任的子网络构成大网络的方案，只要子网络之间的连接度不低于一个阈值即可。由于Fabric具备成员管理服务，成员必须被许可才能加入网络，因此在本系统中我们无需像RPCA那样长期维护一个可信任的子网络。对于需要生成大量区块的节点（暂时成为节点A）来说，节点A可以在最开始使用Fabric的Orderer节点服务，获取网络中至少80%以上的短期内不会进行任何区块生成请求的节点，然后和这些节点直接进行区块的共识，省略交易共识过程。  **2.拟解决的关键问题**  1）不同拜占庭容错算法在结合了区块链技术的茶叶产业链溯源系统中的性能分析和对比。  2）企业在茶叶产业链溯源系统中录入大量数据时生成区块的性能优化。 |

|  |
| --- |
| **三、研究方案设计及可行性分析（包括：研究方法，技术路线，理论分析、计算、实验方法和步骤及其可行性）**  **1、研究方法：**  在课题的设计最初阶段通过文献研究法、调查法不断积累相关知识，拓展对各类共识算法的认知，进而粗略设计出整个方案的框架。然后继续通过文献研究法、实验法、经验总结法对方案进行具体化，优化各部分框架。再通过文献研究法和实验法、经验总结法完成各部分的设计，实现各模块的有机结合。  **2、技术路线：**  系统实现：由于主流的容错算法在网上都能找到现成实现，为了做性能分析和对比，故需先结合Fabric项目与茶叶产业链溯源系统  性能分析与对比：利用Fabric项目的模块化设计和可拔插架构，将RPCA、PBFT等主流的容错算法分别应用于系统中，在相同数据集上进行测试，并对结果进行分析和对比  系统性能优化：优化一类特殊的情况，即在大量数据录入而引起区块生成时间过长造成系统性能下降 |

|  |
| --- |
| **四、本研究课题的特色与新颖之处**  本课题是区块链与茶叶产业链溯源系统的结合以及共识算法在系统中的应用与优化，与现有的技术和研究成果相比，特色先进性体现在以下方面：   1. 将区块链技术有机地结合进茶叶产业链溯源系统中，解决传统溯源系统的缺点和弊端。 2. 解决在大量数据录入而引起区块生成时间过长造成系统性能低下的问题。 |
| **五、研究基础与工作条件（1.与本项目相关的研究工作积累基础 2.包括已具备的实验条件，尚缺少的实验条件和拟解决途径）**  **1、工作积累基础**  已实现了完整的茶叶产业链溯源系统，并有多家企业已入驻。  **2、实验条件**  1）开发工具：Laravel、NodeJS、VueJS、Fabric等   1. 开发环境：CentOS 7.5、windows   3）开发语言：NodeJS、PHP、JavaScript  4）服务器  **3、尚欠缺的条件** |

**学位论文工作计划**

|  |  |  |
| --- | --- | --- |
| 时间 | 研究内容 | 预期效果 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**经费开支情况表**

|  |  |  |
| --- | --- | --- |
| **开支项目** | **数量** | **金额(万元)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **导师意见**（根据该生的政治表现、思想道德、学习成绩、学习态度、科研能力、遵纪守法和执行学校规章制度等提出是否同意继续攻读硕士学位）  导师签名： 日 期： 年 月 日 |
| **中期考核意见**（优秀、良好、及格、不及格）  **开题报告指导小组意见**（包括对以下各参考项目的评价、提出开题报告是否通过的意见。）  请在相应栏目内画“√”   1. 选题与导师研究方向符合度 符合( ) 一般( ) 不符合( ) 2. 选题与专业（领域）符合度 符合( ) 一般( ) 不符合( ) 3. 选题的新颖性 强( ) 一般( ) 不明显( ) 4. 研究的可行性 可行( ) 一般( ) 不可行( ) 5. 研究的工作量 充足( ) 一般( ) 不足( ) 6. 总体评价 优( ) 良( ) 中( ) 差( )   对开题报告是否通过的意见： |
| 小组成员签名：  日 期： 年 月 日 |
| **学科意见**（请对开题报告的选题与专业符合度作出评价，并提出是否同意开题的意见。）  学科带头人签名： 日 期： 年 月 日 |
| **学院意见：**  学院负责人签名： 学院公章： 日 期： 年 月 日 |

硕士研究生成绩单

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学号 |  | | 姓名 | | |  | | | | 性别 | 男 |
| 学院 | 数学与信息学院 | | | 专业 | | 计算机技术 | | | | 学制 | 2 |
| 导师 | 王美华 | | | | | | | | 入学日期 | | 2016-09-08 |
| 类别 | 课程名称 | | | | 学时 | | 学分 | 学期 | | 成绩 | 备注 |
| 学  位  课  程 |  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
| 非  学  位  课  程 |  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
|  | | | |  | |  |  | |  |  |
| 总学分 | |  | | | | | 学位课学分 | | |  | |

打印日期：2017-09-22

、