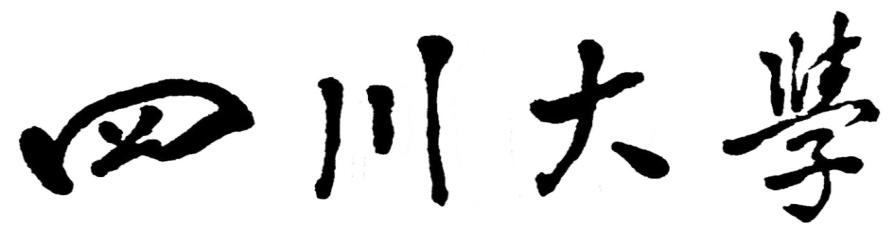
****

**大学生创新训练计划**

**项目申报书**

**项目名称：基于区块链的公益众筹平台**

**项目负责人：黄振洋**

**所在学院：软件学院**

**专业年级： 2015级**

**学 号： 2015141463062**

**手 机： 17760471603**

**电子邮箱： 745125931@qq.com**

**指导教师： 王鹏**

**项目起止年月： 2016.12—2017.12**

**项目参与学生人数： 4**

**四川大学教务处制**

二零一四年十二月

填写说明

一、凡申报**四川大学“大学生创新训练计划”**必须填写本申报书。创新训练计划项目是本科生个人或团队，在导师指导下，自主完成创新性研究项目设计、研究条件准备和项目实施、研究报告撰写、成果（学术）交流等工作。

**二、“项目所属一级学科”**是指教育部1998年颁布的“普通高等学校本科专业目录”中的哲学、经济学、法学、教育学、文学、历史学、理学、工学、农学、医学和管理学11个一级学科门类中的一种或多种(跨学科)。

三、“**项目开展支撑平台“**指支撑本项目开展的校、院级教学实验中心、科研实验室等，表中填写有关实验室名称，可以多个。

四、**“项目组成员”**人数原则上不超过五人。

五、报送本申报书时，一式2份，并报送申报书电子文档。

六、本书应该填写完整、内容详实、表达准确，数字一律填写阿拉伯数字。

七、打印格式与装订

（1）纸张为A4大小，双面打印；

（2）文中小标题为四号、仿宋、加黑；

（3）栏内正文为小四号、仿宋；

（4）左侧距边界1厘米装订。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | 基于区块链的公益众筹平台 | | | | | | | |
| 申请经费 | 10000元 | | 起止时间 | | | 2016年 12月 至 2017年 12月 | | |
| 项目所属 一级学科 | 计算机科学与技术 | | | | | | | |
| 项目开展 支撑平台 | 软件学院实验室 | | | | | | | |
| 项目负责人基本信息 | | | | | | | | |
| 姓名 | 学号 | | | 专业年级 | | | 所在学院 | |
| 黄振洋 | 2015141463062 | | | 2015 | | | 软件学院 | |
| 性别 | 手机 | | | 电子邮箱 | | | 身份证号 | |
| 男 | 17760471603 | | | [745125931@qq.com](mailto:745125931@qq.com) | | | 350681199703201012 | |
| 项目组成员基本信息 | | | | | | | | |
| 序号 | 1 | 2 | | | 3 | | | 4 |
| 姓名/性别 | 魏昊妤 | 王雅雯 | | | 徐遵杰 | | |  |
| 学号 | 2015141463180 | 2015141013125 | | | 2015141463203 | | |  |
| 专业年级 | 2015 | 2015 | | | 2015 | | |  |
| 所在学院 | 软件学院 | 经济学院 | | | 软件学院 | | |  |
| 手机 | 15528202656 | 18224454987 | | | 18692077799 | | |  |
| 电子邮箱 | 740602798@qq.com | wyw9743@foxmail.com | | | 1194953762@qq.com | | |  |
| 身份证号 | 370305199710156249 | 130503199704030627 | | | 430405199808293032 | | |  |
| 签名 |  |  | | |  | | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 指导教师基本信息 | | | |
| 姓名 | 所在学院或单位 | 研究方向 | 职称/职务 |
| 王鹏 | 软件学院 | 医学图像处理和医学大数据 | 讲师 |
| 性别/年龄 | 手机 | 电子邮箱 | 签名 |
| 男/29 | 15281079513 | 744727686@qq.com |  |

**项目内容概述(限200字以内)**

|  |
| --- |
| 本项目研究的是基于区块链的公益保险众筹以解决当前各类公益众筹平台的钱款流向和信任度问题，利用区块链技术使每笔善款所对应的保单及理赔状况反馈给捐助者并建立受捐人征信系统以取得信任，并与慈善机构和保险公司合作，根据推荐算法按与用户的相关度推荐受捐人和符合受捐人情况的保险，将善款以保险的形式帮助特定贫困人群预防、缓解致贫事件，以小额成本起到更精准扶贫作用。  我们希望能通过这个平台实现对受捐人最大的守护。 |

**项目特色创新点概述（限50字以内）**

|  |
| --- |
| ●区块链使善款去向透明化；  ●推荐算法按相关度推荐受捐人；  ●互联网+金融+社会公益；  ●精准扶贫； |

**项目组成员分工**

|  |  |
| --- | --- |
| **姓名** | **主要研究工作** |
| 黄振洋 | 区块链，Android编程 |
| 魏昊妤 | 算法设计与实现，界面设计与美化 |
| 王雅雯 | 金融领域知识支持，界面设计与美化 |
| 徐遵杰 | Android编程，客户端，服务端 |

**一、项目简介（研究内容、目的意义、具体目标、国内外研究现状分析及评价等）**

|  |
| --- |
| **【研究内容】**  **1．项目背景**  党的十八届五中全会中，建立健全农村留守儿童和妇女、老人关爱服务体系；实行医疗、医保、医药联动......这些事关解决人民群众最关心最直接最现实利益问题的政策，无不引来全国人民热议。会议进一步要求，实施脱贫攻坚工程，实施精准扶贫、精准脱贫，分类扶持贫困家庭，探索对贫困人口实行资产收益扶持制度，建立健全农村留守儿童和妇女、老人关爱服务体系。  “空巢老人”与贫困地区儿童的问题是我国现阶段伴随着经济发展产生的特殊群体问题。他们生产、生活、学习等问题的妥善解决涉及到千家万户的幸福，更关系着全民族素质，关系着国家的前途未来。因此，要从他们的当前真正亟需解决的实际问题入手，分类扎实做好各项工作，使他们能够像正常人一样快乐生活，健康成长。  **1.1 目标群体的生活现状分析**  1.1.1贫困地区儿童  从贫困地区儿童所处的外部环境分析，由于他们缺乏及时、有效的家庭监护，而祖父母等临时监护人因年老体弱、安全保护意识不强等原因无法认真行使监护权，加之他们年幼，辨别是非以及自我保护能力低下，很容易受到伤害，导致贫困地区儿童患病不能及时医治和受到意外伤害的事件屡有发生，他们的安全状况存在诸多隐忧。   此外，从他们自身角度分析，儿童往往从他们的长辈那里继承了贫穷。营养不良的妇女生下低体重婴儿。这些婴儿长到幼儿时期，微量营养素缺乏会使他们发育迟缓，家庭和学校恶劣的卫生状况也导致他们经常生病，这就是贫困带来的恶性循环。  1.1.2空巢老人  老年人病痛多，看病花销大，引起的相应问题也多。一是花销大无力承担。“空巢老人”绝大部分都参加了新农合，但他们仍存在着自费部分无力承受的问题。同时他们小病不断，需经常吃药，门诊费用又不能报销，因此他们只能“小病拖、大病熬”，不到万不得已不去就诊、买药、住院；二是就诊困难。偏远山区乡村山大人稀，加之他们年老行动不便，看病十分不易；三是生病在家无人护理。60岁以上“空巢老人”在家生病后，只能由老伴照顾，老伴年纪大，为患者熬药、喂药等都很困难，帮患者翻身、照顾起居等就更困难了，而独身的“空巢老人”倘若生病，生活条件更为艰苦。  **1.2 目标群体的公益现状分析**  纵览公益组织的慈善项目，会发现它们也大量集中于助学、大病救助、营养改善等领域。弱势群体例如孤儿、罹患大病儿童、残障儿童、孤寡老人等，既是民政部门的救助对象，也是众多公益组织的帮扶群体。而像大病医疗、营养补给、基础教育等领域，既是财政投入的领域，也是公益组织引导社会爱心资源进行支持的领域。  **1.3 公益众筹需求分析**  在贫困地区的很多地方都是儿童与老人相依为命，上述的生活条件及社会背景使他们的一些意外和疾病的发生率远远高于正常家庭的老人和儿童。再加上他们的人身安全得不到有效的保障，一旦出现健康方面的威胁，相关费用对于他们来说几乎不可能负担。健康问题永远是放在第一位的，所以要解决他们的问题，摆在首位的就是他们的健康需要有所保障，防患于未然，不能等到事情发生才想办法补救。  贫困地区儿童的教育问题，空巢老人的心理问题等已经引起了社会各界的广泛关注和帮助，然而医疗保险等基本的保险作为进一步的预防措施，却少有关注。当下大多数人致力于解决当前身患重病或各种事故需要大量资金的贫困人群，然而我们更希望这样的事情少发生，发生后得到更及时有效的治疗，那么一个公益众筹平台则满足了这样的需求。  **2． 研究主要内容**  本项目主要研究基于区块链的公益保险众筹平台，为了实现公益善款去向透明化和的善款的最高效利用，目前针对特定贫困人群——留守儿童和空巢老人募集公益善款并为他们投保。与其痛心于悲剧发生后补救，我们更希望能防患于未然，能给他们更多前置、及时、温暖的关怀。  **2.1该平台主要分为以下功能：**  **2.1.1爱心计划**  用户在登录平台后选择制定爱心计划，定下一个小目标，并签订爱心合约，预付自定义数额的爱心押金，通过每日打卡方式监督自己，目标完成则可随意支配这笔押金：选择是否捐赠或退回；目标未完成则自动将押金捐赠，但仍可自主选择捐赠对象。捐赠成功获得一定爱心值。爱心值累计至一定数量可向慈善机构申请捐赠票据或证书。  **2.1.2爱心捐款**  用户在捐款前可以自主选择捐赠金额及受捐人，该善款会以与保险公司协定后的保险的形式落实给受捐人。本平台会用推荐算法根据用户信息推荐与用户相关度（地区、兴趣等）较高的受捐人。受捐人信息由慈善机构提供，保证信息的真实性；本平台利用区块链技术做到每一笔善款去向的透明化和可追踪，并及时反馈给捐款人。  **2.1.3 爱心活动**  用户在本平台里可以选择参与由公益组织或慈善机构组织的爱心活动。让用户切身参与到爱心行动当中，愿意花时间帮助那些需要帮助和关怀的人。同时，用户的参与会记录在他/她的个人记录中。  **2.1.4 爱心项目发布**  公益组织或者慈善机构可以发布爱心项目进行众筹，不仅如此，用户可以通过发现身边的需要帮助的人，发布爱心项目，在通过审核以后即可发布到平台里。   * 1. **关键技术：**   **2.2.1 区块链技术**  区块链是由区块链网络中所有节点共同参与维护的去中心化分布式数据库系统，它是由一系列基于密码学方法产生的数据块组成，每个数据块即为区块链中的一个区块。根据产生时间的先后顺序，区块被有序地链接在一起，形成一个数据链条。区块链的核心，是一个全球性的分布式数据库，这个技术平台是开放的、可编程的，它不仅能够记录金融交易，还可以记录几乎所有有价值的东西：出生证明、死亡证明、结婚证、教育程度、财务账目、医疗过程、保险理赔、投票等任何可用代码来表示的东西。  **2.2.2 推荐算法**  推荐算法是计算机专业中的一种算法，通过一些数学算法，推测出用户可能喜欢的东西。我们想通过推荐算法，向用户推荐可能与其有一定关系的公益保险众筹项目。  本项目中涉及了两种类型的相似推荐：用户与受捐人信息的相似度、用户历史参与项目的相似度。  可能用到的算法有：  **☆基于协同过滤的推荐算法**  协同过滤推荐算法是诞生最早，并且较为著名的推荐算法。主要的功能是预测和推荐。算法通过对用户历史行为数据的挖掘发现用户的偏好，基于不同的偏好对用户进行群组划分并推荐品味相似的商品。协同过滤推荐算法分为两类，分别是基于用户的协同过滤算法(user-based collaborative filtering)，和基于物品的协同过滤算法(item-based collaborative filtering)。简单的说就是：人以类聚，物以群分。 协同过滤算法主要是通过对未评分项进行评分预测来实现的。不同的协同过滤之间也有很大的不同。  **☆组合推荐**  由于各种推荐方法都有优缺点，所以在实际中，组合推荐（Hybrid Recommendation）经常被采用。研究和应用最多的是内容推荐和协同过滤推荐的组合。最简单的做法就是分别用基于内容的方法和协同过滤推荐方法去产生一个推荐预测结果，然后用某方法组合其结果。尽管从理论上有很多种推荐组合方法，但在某一具体问题中并不见得都有效，组合推荐一个最重要原则就是通过组合后要能避免或弥补各自推荐技术的弱点。  虽然协同过滤推荐算法在信息过滤方面呈现出了极大的优势，但随着电子商务和社交网络的快速发展和相互间的不断融合，算法在不同领域中的应用也凸显出一些问题：①冷启动问题；②稀疏性问题；③最初评价问题。为解决这些问题，引入用户相似度概念，重新定义社交网络中相似度属性，相似度构成及其计算方法，提出一种改进的协同过滤推荐算法，并给出推荐质量与用户满意度评价方法。也成为个性化推荐研究的一个重要议题。  传统的相似度有皮尔逊相关系数法、向量余弦法、调整的向量余弦法、约束的皮尔逊相关系数法、斯皮尔曼相关系数法等，在不同的应用领域中，选  取不同的相似度计算方法。由于社交网络的特殊场景，本文重新定义了相似度及其计算方法。算法中的相似度由用户属性决定的用户属性相似度构成，通过计算用户间的距离DA−B度量，距离值越小，用户间的属性相似程度越高；  仿真实验结果表明，与2 类经典协同过滤推荐算法相比，基于用户属性相似度的协同过滤推荐算法有优点：相似度Sim\_(A-B)=(∑\_(i=1)^n[ω\_i d\_i ]+(ω\_num ) ̅D\_HM )在O(n2) 时间内即可执行完算法，为用户产生推荐；算法取得较好的推荐效果，有着较高的基线成功率和覆盖率。且按用户相似度的Top-N 排序算法在社交网站中得到推荐集有较好的推荐质量。  在基于用户属性的协同过滤推荐算法的基础上，我们加入了用户的实时行为（包括搜索、筛选、关注、浏览、捐款等）的数据分析，识别用户意图并将符合用户意图的相关项目推荐给用户。同时，对于部分新用户或者历史行为不太丰富的用户，使用一些替补策略（如热门或者同城）进行填充。最后通过候选集重排序，提高推荐策略的覆盖度和精度，并实现过滤功能。  **【目标意义】**  本项目致力于通过众筹等方式，为偏远地区的留守儿童和空巢老人提供公益保险，让他们的健康得到基本的保障。这些保险包括但不仅限于大病医保、意外伤害险、教育险等。通过这些保险，能够有效地将留守儿童、空巢老人患病后的巨额费用风险以保险的方式得到解决或缓解。   1. **社会意义：**   公益保险包括但不仅限于大病医保、意外伤害险。通过这些保险，能够有效地将留守儿童、空巢老人患病后的巨额费用风险以保险的方式得到解决或缓解。且一份保险所需的金额远远小于巨额的医疗费用，以小额成本防患于未然，也正起到了精准扶贫的作用。  现在，互联网上的关于医疗费用的众筹平台有很多，但针对这些高危人群的公益保险领域还尚未完全开发。一份保险所需的金额远远小于巨额的医疗费用，以小额成本防患于未然。一份保险的金额，很难帮助这些老人和儿童解决什么实际问题，但通过保险的金融杠杆作用，这份保险却能让因意外事故而陷入困境的人获得较大的补偿。所以我们认为，这完全是一种更精准的扶贫方式。  同时，对于奉献爱心的公民来说，一方面通过打卡系统，他们能够获得良好的生活习惯；同时通过捐款等形式积累爱心值，他们能够获得慈善机构颁发的荣誉证书等奖项。   1. **科研意义：**   由于长期以来习惯了不透明的操作模式，很多机构的工作人员的行为模式有很多地方不符合日益觉醒的现在公众的期待与要求不少公益基金会大做无具体指向的公益筹款，到具体花费的时候，很难让大家知道，也很少有基金会主动晒自己的账单。而我们的项目使用了区块链技术，这使得每个捐款的人都能看到自己资金的去向，整个过程完全透明。用户是可以溯源和查证这些记录的，也就保证了资金去向的公开透明化，从而保证了平台的可信度以及加大用户对平台的监管等。  **【具体目标】**  在项目实施的过程中，我们希望尽力实现如下目标：   1. **创建一个安全、完整的公益众筹平台**   通过我们的自主学习，利用一些技术，完成一个安全、有效、公开透明的公益众筹平台。打造人人可参与、可信赖的一个平台。通过这个平台，为偏远地区的留守儿童和空巢老人提供公益保险，让他们的健康得到基本的保障。   1. **利用区块链得到善款的追踪以及捐款的公开透明化**   探索通过区块链技术解决慈善事业中的善款透明度的问题，让善款的生命周期可以透明，做有情有义的“耐心资本”。  **【国内外研究现状分析及评价】**  **【国内外研究现状】**   1. **国外**   国外的社会公益研究一般是指服务于公共利益，不带任何商业目的的研究活动，是广义的社会公益研究概念。基础研究、应用和开发研究中都包含社会公益研究。所以国外的社会公益研究范围比较宽泛。  在众筹方面，从全球首个众筹网站 Kickstarer （2009）在美国上线以来，网络众筹就表现出巨大的生命力。到 2012 年，全球的众筹平台已超过 700 个，融资额从 2011 年的 14.7 亿美元飙升至28 亿美元。2013 年，全球众筹融资平台达到 536 个，较 2012 年增长了 38.7%。而国外的众筹平台主要集中在文化、艺术、科技等领域的创意。    图1：全球众筹市场增长图   1. **国内**   目前，中国公益组织还是以国字号的公益筹款机构为主，它们在引导行业发展中起到了非常明显的规范作用，并基本形成合乎规范的接受资助和合作、监督模式。根据中国慈善联合会29日在京发布《2015年度中国慈善捐助报告》显示，除了企业在捐助额方面同比持续增长之外，个人捐赠也呈现同步上升趋势。据统计：2015年个人捐赠总额达到169.30亿元，较2014年上涨53.72亿元。其中个人小额捐赠（单笔金额在人民币1万元以下）总额从2014年的58.6亿上升为75亿元。报告认为，普通民众进行小额捐赠的规模不断扩大，说明中国社会的慈善氛围愈发浓厚，全民参与慈善的形势日渐成熟。  近年来，我国的网络众筹业也是发展迅猛。自从内地第一个众筹网（“点名时间”）2011 年在北京上线以后，众筹融资一直是迅速发展。到 2014 年上半年，全国众筹行业的融资总额就达1.88 亿元，参与众筹融资的规模超过了 10.9 万人。众筹融资爆发式的增长现状，让人视 2014 年为“众筹元年”。发起者、支持者和众筹平台的协同推进，使众筹融资形成了多种发展趋势。  但是，国内利用区块链与公益众筹平台结合进行一些安全方面以及进行善款去向透明化的研究和项目还比较少。因此，我们认为本项目具有创新性以及很大的意义。  **【分析评价】**  可以看出，网络众筹的兴起打破了传统金融的融资模式，使普通的社会个体都能享有获得项目资金支持的机会。公益与众筹平台结合并加上区块链则是一种有意义的尝试。区块链技术是一种促进信任、增强开放透明的新型技术。利用区块链技术，让每一笔款项的生命周期都记录在区块链上，用户可以持续追溯。由这件“小事”出发，未来可能解决整个中国社会的公益透明度和信任度问题，带来的是无法估量的社会价值。 |

**二、研究技术路线及可行性分析**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **【技术路线分析】**   1. **系统总体功能设计**   **【系统功能设计】**  C:\Users\huang zhen yang\AppData\Local\Microsoft\Windows\INetCacheContent.Word\大创系统功能图 (1).png  图2：系统功能描述图  此图为系统功能描述图。用户在进入该软件之后，可以选择进行注册操作或者已有账户的用户可以直接登录。用户能进行的操作大概有用户信息查看、项目捐款、发布项目、制定爱心计划等。而在服务端方面，服务端需要对客户端的请求等做出响应。服务端的功能大概有发布项目、管理用户、对接慈善机构、资金管理等。  C:\Users\huang zhen yang\AppData\Local\Microsoft\Windows\INetCacheContent.Word\大创系统模块构架图.png  图3：系统模块图  此图为系统模块图，由主系统分支下来，主要涉及的三个模块：界面、算法、技术和数据库。各个模块之间交互形成我们软件的整个系统。在我们开发的过程中将按照各个系 统模块分别开发，以及开发各个模块间的接口。  **【服务端功能设计】**  大创服务端基本流程图  图4：服务端时序图  这是服务端时序图，主要是根据手机端用户发送的请求做出相应的逻辑处理，并且将对数据库进行添删查改，除此之外，服务端还将为客户端提供接口以及对用户进行消息广播等功能。  **【客户端功能设计】**  C:\Users\huang zhen yang\AppData\Local\Microsoft\Windows\INetCacheContent.Word\客户端功能图.png  图5：客户端功能描述图  这是客户端能描述图，用户注册/登陆进入系统，在主界面中可以查看到一些正在进行中的项目并自行选择是否捐助，系统将根据推荐算法向用户智能推荐用户可以会关心的项目；用户可以为自己制定爱心打卡计划，旨在帮助用户完成自己目标或者养成好的生活习惯，同时献出自己的爱心。此外用户如果发现自己身边有需要帮助的人，可以提交材料，申请项目，经审核后将在平台上发布；用户在的个人信息、捐款记录、发布新的项目、爱心值、钱包等信息都可以在“我“这一功能模块中查看。  图6：客户端具体功能描述图C:\Users\huang zhen yang\AppData\Local\Microsoft\Windows\INetCacheContent.Word\系统构架图.png  这是客户端能描述图，用户注册/登陆进入系统，在主界面中可以查看到一些正在进行中的项目并自行选择是否捐助，系统将根据推荐算法向用户智能推荐用户可以会关心的项目；用户可以为自己制定爱心打卡计划，旨在帮助用户完成自己目标或者养成好的生活习惯，同时献出自己的爱心。此外用户如果发现自己身边有需要帮助的人，可以提交材料，申请项目，经审核后将在平台上发布；用户在的个人信息、捐款记录、发布新的项目、爱心值、钱包等信息都可以在“我“这一功能模块中查看。  **【用例图】**  大创系统用例图  图7：用例图  此图为根据项目提出研究问题，以及功能模型，从开发者的角度根据软件功能绘制的软件用例图，作为项目开发过程中需求分析的参考资料。   1. **系统开发环境**   ****主要开发语言：JAVA, JavaScript, Solidity  ****开发工具：Eclipse, VisualStudio2015, AndroidStudio1.0.  ****建模工具：rational rose 2010  ****文档工具：Office 2010  ****数据库：MySQL   1. **项目关键技术**   **【区块链】**  **1.区块链概述**  区块链（BlockChain) 技术是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案。因此，我们打算利用区块链技术的透明性来实现用户善款的去向公开透明化。  **2.相关概念**  ☆区块链：区块链以区块为单位组织数据。全网所有的交易记录都以交易单的形式存储在全网唯一的区块链中。  ☆区块：由header和body组成。Header:链接到前面的块并且为区块链提供完整性； Body:包含验证了块创建过程中的比特币交易的记录。  ☆区块形成过程：在当前区块加入区块链后：  a.把在本地内存中的交易信息记录到区块主体中；  b.在区块主体中生成此区块中所有交易信息的Merkle树，把Merkle树根的值保存在区块头中  c.把上一个刚刚生成区块的区块头的数据通过SHA256算法生成一个哈希值填入到当前区块的父哈希值中；  d.把当前时间保存在时间戳字段中；  e.难度值字段会根据之前一段时间区块的平均生成时间进行调整以应对整个网络不断变化的整体计算总量，如果计算总量增长了，则系统会调高数学题的难度值，使得预期完成下一个区块的时间仍在一定时间内。  ☆哈希值要求：  a.包括前面块的header的哈希值；  b.小于或等于目标数；  c.包括一个称为随机数的数字；  d.包括所有交易的Merkle根。  ☆随机数：随机数是只能使用一次的密码数字。如果产生一个超过目标数的大哈希值，那么需要选择一个新的随机数然后再试一次。一个新的随机数会改变所得到的散列。  ☆Merkle根：Merkle根是header部分的SHA256哈希值，代表了区块body部分所有交易。当交易被接受写入散列body,互相串联在一起，在一个二叉树（binary tree）中再次散列。所有此散列和串联的结果，在所有在它之前的哈希的单一“根”哈希中结束。每一笔被接受的新交易都会改变Merkle根。由于Merkle根是大家试图找到的哈希值的header的一部分，每笔新交易的产生会使得需要解决新的哈希散列问题。非叶子节点value值的计算方法是将该节点的所有子节点进行组合，然后对组合结果进行hash，计算所得出的hash value。叶子节点的value是数据集合的单元数据或者单元数据HASH。  **3.具体分析**   |  |  |  |  | | --- | --- | --- | --- | | **字段** | **子字段** | **大小** | **描述** | | **区块头** | 区块大小 | 4字节 | 本区块字节大小 | | 版本号 | 4字节 | 标示区块协议版本 | | 父区块哈希值 | 32字节 | 上一区块（父区块）的区块头部哈希子 | | 默克尔树根 | 32字节 | 本区块中所记录交易的默克尔树根哈希值 | | 时间戳 | 4字节 | 本区块的产生时间 | | 难度目标 | 4字节 | 产生本区块所进行的工作量证明计算的难度目标 | | 随机数 | 4字节 | 用于工作量证明算法的随机数 | | **区块内容** | 交易数量 | 1-9字节 | 本区块记录的交易数量 | | 交易 | 由交易数量决定 | 本区块的所有交易 |   图8：区块数据结构图    图9：区块链结构与要素示意图  区块链技术主要让参与系统中的任意节点，使用密码学方法产生相关联的数据块（ Block ），每个数据块中包含了一定时间内的系统全部交易数据，并且生成秘钥用于验证其数据的有效性和链接下一个数据块。其中，每个节点由一系列存储全网信息的数据区块链接而成。  具体分析， 每个数据区块由四个关键要素构成，分别是前一区块的哈希值、本区块的时间戳、一个随机数和本区块的哈希值树。 其中，前一块的哈希值用于将本区块与前一区块构建对应关系， 头尾对应，构成一条链；时间戳用于记录存储模块的时间段 ; 随机数可用于挖矿奖励， 保证大家有动力做这个事情，同时也提供了系统需要的计算能力；而哈希值树则是该模块下各类存储信息的秘钥阵列，客户只有密码才能获取数据区块下的某部分信息。 总之，区块链技术以加密算法为基础，通过去中心化的链条相通、时间有序，构建起记录和更新交易信息的全球分布式可信网络数据库。    图10：中心化模式和去中心化模式对比  具体分析，区块链技术具有四个主要特点。 一是去中心化，没有中心核心系统，没有一个中央的支付清算机构，节点间直接信息交互，任一节点损坏（或管制）不会影响全网行，交易效率高，成本低，业务连续性大大提升。二是去信任化。 不同于传统基于政府信用或法律法规强制的信任模式，而是借助开源算法，使得系统运作规则公开透明。 在这种模式下，每个节点之间进行数据交换是无需互相信任，可以匿名，同时每笔交易都会被真实记录，以防止数据被控制和篡改，可以有效避免信任主体的违规行为。 三是集体维护。四是安全数据库。单个节点可能会被暴力修改，但因为交易数据是分散到全网各个节点，单个节点数据修改不被全网认可的。 理论上分析，只要不是控制超过全系统 50% 以上的计算能力数据是无法篡改的。  **4.初期设想的区块链在本项目中的应用**  目前，公益事业方面存在着捐款去向追踪困难等问题，即经常有用户捐出几元到几百元不等的善款，捐款进入公益项目账户之后就无法追踪。利用区块链技术，让每一笔款项的生命周期都记录在区块链上，用户可以持续追溯。    图11：项目初期预想解决方案  **4.1捐款可信化**  我们项目初期的预想是将我们的平台作为区块链网络中的一个节点成为受信任的中央实体，推进捐款以及结算流程并承担重要责任。这样，即使不需要激进的变革，我们也能做到善款的去向追踪公开透明化以及更好地监督和管理系统。  举一个简单的例子，假设A要向B捐助x元。那么，A首先会向全网区块链广播这个消息；平台中心结点收到后确认这条消息并向全网广播；继而A向B捐款，全网结点都能收到这个消息和记录，并在区块链中记录；最后B向全网结点广播收到捐款的消息。通过这种方式来实现资金去向的双重认证，提高可信度。    图12：双重确认过程    图13：交易信息记录过程  **4.2 善款生命周期公开透明化**  区块链中每一笔交易都通过密码学方法与相邻两个区块串联，也就是说，资金去向会记录在区块链的区块中。  因此，用户是可以溯源和查证这些记录的，也就保证了资金去向的公开透明化，从而保证了平台的可信度以及加大用户对平台的监管等。  而我们的想法是我们这个平台节点作为区块链系统中的一个节点，从而，与上述类似，我们可以对系统中发生的所有交易做到完全监督，并且实时接收透明的交易数据。  **【推荐算法】**  **1.推荐算法概述**  推荐算法是计算机专业中的一种算法，通过一些数学算法，推测出用户可能喜欢的东西。我们想通过推荐算法，向用户推荐可能与其有一定关系的公益保险众筹项目。  **2.推荐算法的实现**   * 框架：     图14：推荐算法框架图  从框架的角度看，推荐系统基本可以分为数据层、触发层、融合过滤层和排序层。数据层包括数据生成和数据存储，主要是利用各种数据处理工具对原始日志进行清洗，处理成格式化的数据，落地到不同类型的存储系统中，供下游的算法和模型使用。候选集触发层主要是从用户的历史行为、实时行为、地理位置等角度利用各种触发策略产生推荐的候选集。候选集融合和过滤层有两个功能，一是对出发层产生的不同候选集进行融合，提高推荐策略的覆盖度和精度；另外还要承担一定的过滤职责，从产品、运营的角度确定一些人工规则，过滤掉不符合条件的item。排序层主要是利用机器学习的模型对触发层筛选出来的候选集进行重排序。  同时，对与候选集触发和重排序两层而言，为了效果迭代是需要频繁修改的两层，因此需要支持ABtest。为了支持高效率的迭代，我们对候选集触发和重排序两层进行了解耦，这两层的结果是正交的，因此可以分别进行对比试验，不会相互影响。同时在每一层的内部，我们会根据用户将流量划分为多份，支持多个策略同时在线对比。   * 数据应用   用户主动行为数据记录了用户在平台上不同的环节的各种行为，这些行为一方面用于候选集触发算法中的离线计算（主要是浏览、付款），另外一方面，这些行为代表的意图的强弱不同，因此在训练重排序模型时可以针对不同的行为设定不同的回归目标值，以更细地刻画用户的行为强弱程度。此外，用户对deal的这些行为还可以作为重排序模型的交叉特征，用于模型的离线训练和在线预测。   * 基于用户相似度的协同过滤推荐算法   用户属性相似度计算  由用户属性决定的用户属性相似度，通过计算用户间的距离度量，距离值越小，用户间的属性相似程度越高。社交网络中用户属性包括用户个人信息和其他选填项。用户属性分为2类：一类是数值型属性（如年龄、身高、收入等）；一类是名称型的属性（如体型、教育水平、婚否等）。  1）对于数值型属性，计算不同用户之间数值型属性的绝对差值ZGTSP``]E)%~GS6@DGGGO}N。不同属性绝对差值的最小和最大差距为)OPZ2402%)4)JXZ60)SOH25，将这个区间平均划分成n−1 个等距的小区间PJK69`N7V65SZF6H(%[9FFNKLO0][Z7W_9M$H91~F@9MWQ，当用户间的数值型属性的绝对差值落在其中的某个小区间，对每个小区间依次给定数值型属性距离{0，1，2，⋯，n−1，n}（这里只划定3 个区间），针对不同的区间，得到用户间的数值型属性距离DNum；对于每个名称型属性，根据每个名称型属性先前设定的取值数N，确定编码的位数n =lbN，然后对不同的取值进行格雷编码并依次串连起来，计算不同用户间格雷编码之间的海明距离，得到不同用户间的名称型属性距离DH。若定义用户A与B间的距离来度量用户间的属性相似度，每一个属性的权重为$Z11KJQSA}P$MF@SA@6OS_6，则所有属性权重值满足WDJR0PJASK]X)@@{VOBMIYP。  对于数值型的属性距离DNum，根据前面的说明，定义不同的取值区间：  若{P98%LI[LGR85NL`45VFGFI，则IV33)LFRXU6N)I0MD]`)%XX；  若LL%GB9}PTAGBHZKQC84LEWE，则MP3RMHU1{~Y9CCF$Q)CAEU3；  ……  若83TO5U$[7(R]O5[63}7~BQ8，则1}U70{~1NZ~I6DE9EQ__RW4。  针对数值属性，用户间的距离计算为  `[KSKX`})RNIQRI3IEMU(]R (1)  一般情况下，只划分为3 个区间。  若L{AX8}V)}}TN4P$%5ZYTKQ9，则[V7H~TI`[U03RULM5DK7_IU；  若2{TZ$4QQGEO[R{GMV{7HYMU，则UCHRCW49KZM]QR7QMUUY`77；   1. 对于名称型的属性距离dNum，对不同的取值进行编码。因名称型属性的取值范围较为单一，可采用二进制编码来表示，比如名称型属性中体型可描述为：瘦、匀称、胖，对应的二进制编码可描述为：00、01、11，其他属性可以此类推。最终将用户的全部名称型属性编码串联起来，形成一个二进制串BNom；采用计算二进制串BNom 的海明距离来度量用户间名称型属性的距离；其权重是n 个名称型属性的权重的平均值：   VWDQB%0Q(CWI1L2CEQ@KVY6  则AM(IG285{11[7)]N]0@U(YH (2)   1. 最终得到2 个用户A 与B 的信息属性距离为：   ZNB0900{[~@R8@$@)H%G32F (3)  即OSK]WXVO5)(N8L{`HEWK6OE。  DA-B越小，相似度越大，而DA-B 越大，相似度越小。  计算示例：若A={23，183 cm, 0101000000}，B={26, 176 cm, 1100010100}，则用户A 与B 间的距离DA-B =1(0+1+4)=5。  综合前面的论述，算法1 给出了为目标用户U0 产生推荐集合的过程。  算法1 A&I\_CF(U0, U, int N)  //算法为目标用户U0 产生其推荐集C；  //算法最后输出目标用户U0 的推荐集C。  输入：目标用户U0，备选用户集U，产生推荐个数N。  Begin：  1) 相似度计算  ① 用户属性相似度计算。  根据]{O9JWA]57R3JVVTO00[O6V计算用户U0 的数值型属性距离DNum。  对于用户U0 名称型属性，对属性取值进行格雷编码，将用户名称型取值格雷码串连，计算出海明距离DH。  根据FTC`QY8U~~[MZ@506AGAYLL计算用户U0 与其他用户间的距离，用来度量用户U0 与其他用户间属性相似度，即用户间的距离DA-B。  2) 产生推荐集  ① 确定候选集C。根据用户间的互动信息，找出和目标用户U 相似用户KD8D~9PTCVOD$JPN{FVD3AJ产生互动的用户集7OPDK5JP}K5SSFB`0_4]@80。  ② 产生推荐集。上一步产生的候选集求并集IA[``N9HC}LQGDZJ6D}P{}F。  将候选集C 里的用户按照相似度进行排序，得出最后的推荐集合BY`Z1%X0BUL]XAZMV5AF}ELSWRHQV@{4)XT5WX@46]JRXK，按照Top-N 排序算法为用户产生推荐。  输出：目标用户U0的推荐集L@T1~VP73MKUQ@)DHF)G`(K。  基于用户相似度的系统过滤推荐算法通过计算用户相似度，计算得到用户相似度值越小，表明用户间相似程度越高，按照相似度降序对用户排序，产生推荐候选集，再使用Top-N 方法取到候选集排在前N 位的用户推荐给目标用户。  算法复杂度分析  算法复杂度是衡量算法效率的标准，通常可分为时间复杂度和空间复杂度。随科技的发展，算法执行所需的存储空间对于算法的影响逐渐弱化。通过对上述用户相似度算法分析，算法执行过程只需要存储用户属性信息、交互信息、推荐集信息，存储空间的占用较小；且随用户的增加，存储空间线性增加，数量级上没有变化；此外，当前硬件发展使得较小的代价即可获得较大的存储容量，因此，该算法中时间复杂度成为衡量算法效率的重点，本文聚焦于此算法的时间复杂度分析。  该算法执行的时间开销集中在相似度计算公式 中，可见算法时间复杂度由相加的2 部分构成。若用户属性中有M 个数值型属性和N 个名称型属性，用户集数量级为n。则有以下分析：  for(in i=0; i<n; i++){ //执行n+1 次  for(int j=0; j<n; j++){ //执行n (n+1)次  //用户属性相似度计算  a:数值型 //执行M×n (n+1)次  b:名称型 //执行lbN×n(n+1)次  a+b //执行n (n+1)次  }  //按照用户间的相似度对用户进行排序  Rank\_Users By Similarity //执行n+1 次  }  //为用户产生推荐  Generate Recommendations //执行N0 次  算法执行总次数：  f(n)= n+1+ n(n+1) + M×n(n+1) + IbN×n(n+1) + n(n+1) + n+1+  f(n)= (M+IbN+2)× + (M+ lbN)×n + (+2)  其中，M、N、α、β、N0 均为常量，利用时间复杂度计算原则，忽略常量、低次幂和最高次幂的系数，  计算得出算法的时间复杂度：  T(n)=T()+T(n)+T(1)  T(n)=O()  从上述分析可知：本文中算法时间复杂度在O()内，在不增加额外存储空间的前提下，其时间复杂度与文中引用2个经典推荐算法处于同一数量级，未增加过多的时间开销。  在不增加算法额外存储空间的情况下，实验证明基于用户属性和互动信息的推荐算法精确度、基线成功率、覆盖率都优于基于全部互动的推荐方式（包括积极、成功和消极、不成功的互动）。实验还表明，按用户相似度的Top-N 排序算法在社交网站中得到推荐集有较好的推荐质量。   * query-based   搜索是一种强用户意图，比较明确的反应了用户的意愿，但是在很多情况下，因为各种各样的原因，没有形成最终的转换。尽管如此，我们认为，这种情景还是代表了一定的用户意愿，可以加以利用。具体做法如下：  1)对用户过去一段时间的搜索无转换行为进行挖掘，计算每一个用户对不同query的权重。  2)计算每个query下不同deal的权重。  3)当用户再次请求时，根据用户对不同query的权重及query下不同deal的权重进行加权，取出权重最大的TopN进行推荐。   * 实时用户行为   目前我们平台业务会产生包括搜索、筛选、关注、浏览、捐款等丰富的用户行为，这些是我们进行效果优化的重要基础。我们当然希望每一个用户行为流都能到达转化的环节，但是事实上远非这样。  当用户产生了捐款行为上游的某些行为时，会有相当一部分因为各种原因使行为流没有形成转化。但是，用户的这些上游行为对我们而言是非常重要的先验知识。很多情况下，用户当时没有转化并不代表用户对当前的item不感兴趣。当用户再次到达我们的推荐展位时，我们根据用户之前产生的先验行为理解并识别用户的真正意图，将符合用户意图的相关deal再次展现给用户，引导用户沿着行为流向下游行进，最终达到下单这个终极目标。  目前引入的实时用户行为包括：实时浏览、实时收藏。   * 替补策略   虽然我们有一系列基于用户历史行为的候选集触发算法，但对于部分新用户或者历史行为不太丰富的用户，上述算法触发的候选集太小，因此需要使用一些替补策略进行填充。  热门项目：在一定时间内收到捐款最多的item，可以考虑时间衰减的影响等。  同城项目：满足基本的限定条件，在用户的请求城市内的。   * 候选集重排序   如上所述，对于不同算法触发出来的候选集，只是根据算法的历史效果决定算法产生的item的位置显得有些简单粗暴，同时，在每个算法的内部，不同item的顺序也只是简单的由一个或者几个因素决定，这些排序的方法只能用于第一步的初选过程，最终的排序结果需要借助机器学习的方法，使用相关的排序模型，综合多方面的因素来确定。  1. 模型  非线性模型能较好的捕捉特征中的非线性关系，但训练和预测的代价相对线性模型要高一些，这也导致了非线性模型的更新周期相对要长。反之，线性模型对特征的处理要求比较高，需要凭借领域知识和经验人工对特征做一些先期处理，但因为线性模型简单，在训练和预测时效率较高。因此在更新周期上也可以做的更短，还可以结合业务做一些在线学习的尝试。  非线性的树模型Additive Groves[4]（简称AG），相对于线性模型，非线性模型可以更好的处理特征中的非线性关系，不必像线性模型那样在特征处理和特征组合上花费比较大的精力。AG是一个加性模型，由很多个Grove组成，不同的Grove之间进行bagging得出最后的预测结果，由此可以减小过拟合的影响。  http://www.36dsj.com/wp-content/uploads/2015/01/1031.jpg  图15：非线性模型  每一个Grove有多棵树组成，在训练时每棵树的拟合目标为真实值与其他树预测结果之和之间的残差。当达到给定数目的树时，重新训练的树会逐棵替代以前的树。经过多次迭代后，达到收敛。  2. 数据  采样：对于点击率预估而言，正负样本严重不均衡，所以需要对负例做一些采样。  负例：正例一般是用户产生点击、捐款等转换行为的样本，但是用户没有转换行为的样本是否就一定是负例呢？其实不然，很多展现其实用户根本没有看到，所以把这样样本视为负例是不合理的，也会影响模型的效果。比较常用的方法是skip-above，即用户点击的item位置以上的展现才可能视作负例。当然，上面的负例都是隐式的负反馈数据，除此之外，我们还有用户主动删除的显示负反馈数据，这些数据是高质量的负例。  去噪：对于数据中混杂的刷单等类作弊行为的数据，要将其排除出训练数据，否则会直接影响模型的效果。  3. 特征  在我们目前的重排序模型中，大概分为以下几类特征：  deal(即捐款单)维度的特征：主要是deal本身的一些属性，包括险种、捐款额、已捐赠数量、类别、点击率等；  user维度的特征：包括用户属性等；  user、deal的交叉特征：包括用户对deal的点击、关注、捐款等  距离特征：包括用户的工作地、居住地等距离。  对于非线性模型，上述特征可以直接使用；而对于线性模型，则需要对特征值做一些分桶、归一化等处理，使特征值成为0~1之间的连续值或01二值。     1. **初期设想的推荐算法在本项目中的应用**   推荐算法通过研究用户的喜好和兴趣，为用户推荐其所需的各种资源。在本项目中，我们通过分析用户填写的基本资料为其推荐与其相关性较大的受捐人（如地区、兴趣爱好、梦想……）以此来提高用户的满意度和体验。  基于用户相似度的协同过滤推荐算法在原有的协同过滤推荐算法上有了很大的改进：原有的协同过滤推荐算法在不同领域中的应用凸显出一些问题：①冷启动问题；②稀疏性问题；③最初评价问题。为解决这些问题，文献[7]引用了用户相似度概念，重新定义社交网络中相似度属性，相似度构成及其计算方法，提出一种改进的协同过滤推荐算法，并给出推荐质量与用户满意度评价方法。  本项目计算用户与受捐人属性相似度，通过计算用户间的距离DA−B度量，距离值越小，用户间的属性相似程度越高。  除了基于用户属性相似度的推荐算法，由用户在使用期间进行的主动的行为（浏览、关注）也是非常高质量的参考数据，我们根据用户的搜索意愿，用到query-based、实时用户行为、替补策略等方法，与上述推荐算法结合，为用户（包括新用户）推荐高质量有效的众筹项目。  **参考文献:**  [1] 吴 慧，卞艺杰，赵 拮，马瑞敏. 基于信任的协同过滤算法.计算机系统应用20 14 年 第 23 卷 第 7 期：131-135  [2] 彭 安.网络众筹的金融现状及发展趋势.财经论坛2016 年 9 期：127-128  [3] 张 波.国外区块链技术的运用情况及相关启示.技术应用2016年·第5期：35-38  [4] 温晓桦. 区块链，金融场景应用. WEALTH  [5] 顾彦. 区块链+金融：未来更多向智能合约领域发展.CSEI  [6] 王 硕. 区块链技术在金融领域的研究现状及创新趋势分析. 上海金融 2016 年第 2 期  [7] 荣辉桂，火生旭，胡春华，莫进侠. 基于用户相似度的协同过滤推荐算法. 通信学报  [8] O’Donovan J． Smyth B ． Eliciting trust values from recommendation errors． Proc. of the 18th Int.Florida Arti-ficial Intelligence Research Society Con ference,20 0 5．28 9- 294 ．  [9] 郭艳红．推荐系统的协同过滤算法与应用研究[学位论文]．大连：大连理工大学，2008  [10] 杨博, 赵鹏飞. 推荐算法综述. 山西大学学报(自然科学版)34(3):337～ 350, 2011  [11] Connor MO, Herlocker J L. Clustering Items for Collaboreative Filtering[ C]//Process of the ACM SIGIR Workshop on Recommender Systems, 1999.  [12] 陈健 , 印鉴.基于影响集的协同过滤推荐算法[ J] .软件学报, 2007, 18(7):1685-1694  [13] Pearl J. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference[ M] .San Francisco :M organ Kaufmann, 1988  [14] Linder G, Smith B, York J.Amazon.com Recommendations: Item-to-Item Collaborative Filtering[ J] .IEEE Internet Computing, 2003, 7(1):76-80.  [15] 宋湘燕，黄珊. 区块链技术在商业银行的应用前景[N]. 金融时报，2015-12-21（7）.  **【可行性分析】**   1. **可行性分析**   **◆技术可行性**  区块链最早作为比特币的底层“账本”记录技术。经过几年的发展和改进，逐渐成为了一种新型的分布式、去中心化、去信任化的技术方案。特别是近两年以来，区块链已逐步脱离比特币，独立地成为技术创新的热点，开创了一种新的数据分布式存储技术，引导了系统与程序设计理念的变化，并可能颠覆现在商业社会的组织模式，其应用受到了越来越多的关注。而且，现在一些区块链的社区也相当活跃，资料文档等也很丰富。因此，可以通过不断地学习、对资料的查阅以及对优秀论文的研究来解决关于学习区块链遇到的问题，并通过区块链解决本项目的一些问题。  推荐系统在各种系统中广泛使用，推荐算法则是其中核心的技术点。推荐系统算法通常是某类推荐模型的实现，它负责获取数据，例如用户的喜好和可推荐项的描述，以及预测给定的用户组会对哪些选项感兴趣。目前，推荐算法通常被分为四大类（1-4）：  1.协同过滤推荐算法  2.基于内容的推荐算法  3.混合推荐算法  4.流行度推荐算法  虽然这些算法模型不一定适用于我们问题的解决，但相信随着研究的深入，一定可以找到解决的办法，并且这些算法相关的论文以及研究资料也很有参考价值。  **◆人员可行性**  本小组成员来自软件学院、经济学院。团队成员学习能力强，专业知识掌握良好，都能够独立完成课程所需项目以及任务，有着充分的知识储备和相关课程的学习。成员各有所长，优势互补，并具有一定的项目开发经验。成员的技术知识储备，时间分配均可满足本项目开发需求。  **◆社会效益**  当前，贫困地区儿童、空巢老人等弱势群体急需帮助，并且政策提倡精准扶贫。本项目针对这些问题提出了良好的解决方案。本项目若获得成功将可很好的帮助这些弱势群体，获得社会爱心人士的广泛关注和大力支持。所以，本项目具有良好的社会可行性以及社会效益。   1. **项目发展预期步骤**     图16：项目发展预期步骤图  **各阶段阶段性成果：**  1. 需求分析：软件需求规格（功能，性能和运行环境约束）。  2. 系统设计：概要设计规格说明书；数据库和数据结构说明书；集成测试计划  3. 程序设计：详细计划规格说明书；单元测试计划。  4. 编码：源程序代码  5. 单元和集成测试测试：单元测试报告，系统集成测试报告。  6. 验收测试：可供用户使用的软件产品（文档、源程序）  7. 运行和维护 |

**三、对项目的参与兴趣和已有的知识积累或实践基础**

|  |
| --- |
| 经过我们的分析，公益对于流程透明性有极强的需求，而通过区块链做到公益透明化，来实现捐款信息的公开，资金去向有限的可追溯，意义重大，因而我们所有组员都有极大的兴趣和热情投入到该项目的研究中去。  下面是项目团队成员介绍：  黄振洋：2015级软件学院创新班成员，有一定的编程能力，对本系统有一个总体的认识以及了解。自学能力较强，能够运用C, JAVA, Python等语言，自行编写过一些程序。  魏昊妤：2015级软件学院，有独立编程能力，热衷程序开发，自主学习能力和创造力强，熟练运用C，C++, JAVA等语言，对金融方向有一定了解和研究，且能运用PS等软件对系统的美工设计方面起到帮助。  王雅雯：2015级金融双语专业。自学并通过了证券从业资格考试。对金融市场的运行和金融产品的应用有一定的认识和了解。成绩优秀，自学能力强。是本项目成功的关键之一。  徐遵杰：2015级软件学院创新班成员，成绩优秀，对数据结构与算法的研究有一定的优势，学习能力强，数学知识比较丰富，编程能力强，熟练运用C，C++, JAVA等语言，在编程竞赛中获奖，有助于本系统的总体设计和功能实现。 |

**四、研究计划和进度（可就文献查询、社会调查、方案设计、实验研究、数据处理、研制开发、撰写论文或研究报告、结题和答辩、成果推广、论文发表、专利申请等工作逐项进行安排）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **项目研究（研制开发）进度安排表**   |  |  |  |  | | --- | --- | --- | --- | | **阶段** | **时间** | **具体任务** | **阶段成果** | | **文献查询**  **社会调查** | 2016.11-  2016.12 | 提出问题  需求分析  分析可行性 | 可行性报告  项目申请书  项目初步开发计划  软件需求规格书 | |  | 2017.1 | 总体设计 | 概要设计规格说明书  数据库和数据结构说明书  集成测试计划 | | 2017.2-  2016.3 | 详细设计 | 详细计划规格说明书  单元测试计划 | | **实验研究**  **数据处理**  **研制开发** | 2017.4-  2017.8 | 编码  单元测试 | 源程序代码  单元测试报告 | | 2017.9-  2017.11 | 综合测试 | 统集成测试报告  软件产品  用户使用文档 | | **撰写提交**  **研究报告** | 2017.11-  2017.12 | 撰写报告 | 研究报告 | | **结题答辩**  **成果推广**  **专利申请** | 2017.12 | 结题答辩  成果推广  专利申请 | 结题答辩  成果推广  专利申请 | |

**五、项目研究支撑条件**

|  |
| --- |
| **一、系统开发环境**  ****主要开发语言：JAVA, JavaScript, Solidity  ****开发工具：Eclipse, VisualStudio2015, AndroidStudio1.0.  ****建模工具：rational rose 2010  ****文档工具：Office 2010  ****数据库：MySQL  **二、工作环境**  软件学院创新实验室 |

**六、预期提供的成果形式**

|  |
| --- |
| 1.□文献资料综述 2.□调查报告 3.□研究论文 4.√开发软件  5.□设计 6.□硬件研制； 7.□申请专利  8.√其他 名称： 项目开发文档 |

**七、项目经费概算(包括调研、耗材、资料、发表论文、印刷等费用)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 在整个项目完成后，我们力求提供下面的研究成果：   1. 各阶段的开发文档 2. 能提供用户使用的软件 3. 主要源代码 4. 研究论文  |  |  | | --- | --- | | **使用项** | **金额（元）** | | 调研费 | 1000.00 | | 软件费用 | 1000.00 | | 书籍资料 | 1500.00 | | 会议组织、交通 | 1000.00 | | 耗材 | 1000.00 | | 宣传费用 | 500.00 | | 开发工具 | 1000.00 | | 阿里云服务器 | 2000.00 | | 论文发表 | 1000.00 | | 合计 | 10000.00 | | |

**八、评审情况**

|  |
| --- |
| **指导教师意见：** |
|  |
| **指导教师（签名）： 年 月 日** |
| **学院推荐意见：** |
|  |
| **主管院长签名： 年 月 日** |
| **学校专家评审意见：** |
|  |
| **组长签名： 年 月 日** |
| **学校认定意见及批准经费：** |
|  |
| **学校负责人签名： 年 月 日** |