附件3

项目编号：

**大学生创新创业孵化项目**

**申 报 书**

**申请者姓名： 王顺**

**所 学 专 业： 电子信息**

**孵化项目名称： 多元智能合约漏洞检测平台**

**项目所属行业： 区块链**

**项目承担单位（公章）：**

**填报日期： 年 月 日**

**浙江省大学生科技创新活动计划暨新苗人才计划实施办公室 制**

填写说明

一、凡申报本孵化项目的申请人，须认真阅读本项目有关通知，封面申请者姓名一栏填写项目负责人。

二、格式要求：申报书中各项内容以Word文档格式填写，表格中的字体为小四号仿宋体，1.5倍行距；表格空间不足的，可以扩展或另附纸张；均用A4纸双面打印，于左侧装订成册。

三、申报书由所在学校领导审查、签署意见并加盖公章后，一式1份（原件），报送浙江省大学生科技创新活动计划暨新苗人才计划实施办公室。

1. **项目简介**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项  目  概  况 | 项目名称 | | | 多元智能合约漏洞检测平台 | | | | | | | |
| 项目性质 | | | （）基础研究 （）应用研究 | | | | | | | |
| 项目来源 | | | （）自主立题 （）教师指导选题 | | | | | | | |
| 起止时间 | | | 自 2021年 12月 至 2022年 5月 | | | | | | | |
| 项目状况 | | 1、研发阶段 2、中试阶段 3、批量（规模）生产（选项打√） | | | | | | | | | |
| 申请人 | 姓名 | 王顺 | 性别 | | 男 | 出生年月 | 1996.11 | | 入学年份 | 2019.9 | |
| 所在院系 | 计算机学院 | 学号 | | 202050181 | 联系电话 | 18340877007 | | 电子信箱 | ws\_hdu@hdu.edu.cn | |
| 项 目 组  主要成员 | | 姓名 | 性别 | | 年龄 | 学院 | 专业 | 学号 | 具体分工 | | |
| 宋家豪 | 男 | | 23 | 计算机 | 电子信息 | 212050227 |  | | |
| 黄志强 | 男 | | 24 | 计算机 | 电子信息 | 212050293 |  | | |
|  |  | |  |  |  |  |  | | |
|  |  | |  |  |  |  |  | | |
| 项  目  指  导  教  师 | | 姓名 | | | 徐向华 | 性 别 | 男 | | 出生年月 | | 1965.10 |
| 主要研究方向 | | | 数据处理、数据挖掘、工业互联网安全、物联网 | | | | | | |
| 近三年获奖成果：国家级\_\_等奖\_\_\_项，省部级奖\_2\_\_项 | | | | | | | | | |
| 近三年科研经费\_\_\_\_\_\_300\_\_\_\_\_\_万元，年均\_\_\_\_\_\_100\_\_\_\_\_万元 | | | | | | | | | |
| 项  目  主  要  内  容  简  介 | | 区块链是我国当前重要发展战略，智能合约是联系区块链和应用间的重要纽带。区块链发展至今，出现过多起因为智能合约漏洞被利用而出现巨大的经济损失的案例。如著名的The Dao攻击，造成了区块链硬分叉的恶劣后果。如果智能合约漏洞在投入使用前，没有进行检测，那么潜在的漏洞可能就会被利用，造成损失。  多元智能合约检测平台可以很好的解决上述问题，该平台上集成了静态分析，动态分析，模糊测试的方法对智能合约进行测试。平台可以及时反馈智能合约潜在的漏洞。平台提供多种检测方式，如上传检测，输入检测，批量检测等。平台还提供对智能合约衍生出的文件的可视化功能，平台还能够测试智能合约部署链的效果。 | | | | | | | | | |

**二、项目的研究目的及意义**

|  |
| --- |
| 1、申请项目的必要性、目的及意义  近年来,区块链技术受到了越来越多的关注与重视,而基于区块链技术的智能合约的设计与开发也成为了热门的研究方向。一段优秀的智能合约能够提供安全可靠的服务,从而高效地解决现实生活中的问题。然而由于开发人员的技术水平参差不齐,其编写的智能合约也可能会出现安全问题,不安全的智能合约的发布使用可能会对用户造成巨大损失。因此,在正式发布智能合约之前,对其进行安全检测是尤为重要的。  多元的智能合约检测平台，提供多种方式对合约进行检测。在获得智能合约后，平台会用多种检测工具对智能合约[4]进行检测。检测完毕后反馈潜在的漏洞，使用者可以根据不同工具反馈的不同信息，对自己的智能合约进行人工审计，判断是否存在漏洞。还可以获得调用图和控制流图，根据可视化图来维护智能合约。使用者利用平台提供的私链，将智能合约部署上链，测试合约的运行情况。本项目的实现意义使得智能合约的编写者和使用者尽可能的降低因为漏洞而造成损失的可能性，更好的维护以太坊的生态系统。 |
| 2、项目的背景、主要内容、技术水平及应用范围  **项目背景：**  随着比特币受到越来越多人的关注，其使用的区块链技术也被众多开发者和学者进行研究。区块链是一个链式的数据结构，根据时间的顺序将数据组合起来，并通过密码学等相关技术来保证其安全的特性。区块链技术由于其去中心化和匿名性等特征=，已经在各行各业投入使用。区块链的阶段发展可分为三大阶段，第一阶段，区块链的表现形式主要是数字货币，其代表是比特币。第二阶段，区块链的具体表现就是智能合约，其代表是以太坊平台，有很大一部分的智能合约都是部署在以太坊平台上，目前全网已经有成千上万的智能合约在运行。第三阶段，区块链的表现为可编程的社区，区块链技术将最终运用到日常生活的方方面面，本平台主要是针对以太坊平台上的智能合约而设计。  以太坊是区块链技术的一种应用平台。以太坊不仅提供了数字货币的功能，而且允许用户编写图灵完备的智能合约。利用以太坊，用户可以进行匿名投票，拍卖等行为，用户的这些操作都需要智能合约来支持。智能合约的本质就是一段能够自动执行处理事务的代码，和其他语言相同，智能合约会因为开发者水平的参差不齐，会出现代码漏洞问题。一旦恶意的攻击者利用这些安全问题进行攻击，用户将会受到巨大的损失。2017年6月18日，恶意的攻击者利用了以太坊上发布的“The Dao”智能合约上存在的安全漏洞，成功盗取了近360万个以太坊，造成了近亿美元的损失。2018年4月22日，由于BEC智能合约中的批量转账函数存在整数溢出漏洞，攻击者成功通过转账的方式生成可很多不应存在的货币，导致最终损失了近60亿人民币，因此开发一个智能合约的检测系统非常重要[5]。  **主要内容**：  本系统拥有静态分析，动态分析，模糊测试等方式来对智能合约进行检测。本项目根据用户上传的智能合约，以及所选用的检测工具对合约进行检测。使用者无需了解检测的逻辑，只需要根据系统提示，点击相应按钮可以一键实现自动化测试[6]。并有丰富的可视化界面,将漏洞的基本信息以及危害程度相应的显示在界面上.  本系统还可以通过连接以太坊主网来同步主网中所发生的的任何事物,对可疑的事务进行告警处理,包括不限于合约重入等漏洞的提示.  本系统对于开发人员来说也是有益处的,开发人员通过上传编写的智能合约代码,系统进行一系列的检测,给与开发人员树、图、表等具体合约信息，这对于开发人员而言是可以提供巨大帮助的。  本系统可以一键部署智能合约到主网，一旦用户通过系统检测未发现漏洞的存在，用户可以选择是否立即上传到主网上，智能合约一旦上传到主网就面临着无法更改的难题，但是本系统可以在第一时间发现合约部署主网后的被攻击行为，然后智能选择是否销毁合约，从而保证合约拥有者的自身利益以及合约使用者们的自身利益。  未来打算将联盟链中的智能合约漏洞检测技术集成在本系统中，使得本系统成为一个专业，多角度的合约漏洞检测平台。  **技术水平：**  1.智能合约设计及solidity语法  2.密码学原理  3.编译原理（词法分析，语法分析）  4.模糊测试  5.系统环境搭建以及客户端设计  **应用范围：**  适用于使用solidity语言编写的智能合约。想要测试智能合约的个人或者团队都可以使用该平台来检测智能合约，提高智能合约的安全性。 |
| 3、实施该项目所具备的基础、优势和风险  **基础：**  环境方面，随着区块链的发展,以太坊[1]开始兴起,在去中心化交易的过程中体现出特有的作用。但需要智能合约的部署，而智能合约可能携带漏洞,会对以太坊安全[3]、用户造成利益损失等问题。该项目的提出就是来解决这种问题的。  技术研发方面，由于各种动静态检测工具的开源，该项目在互联网的环境上搭建一个集成各种工具并模拟区块链环境部署合约是可行的，重点在于后端逻辑，后端采用Flask框架进行编写，将各种工具集成，对智能合约漏洞进行检测[2]，并实现一定的联系，从而完成该系统的主要框架逻辑。前端采用Vue框架，配合html，js，css完成前端页面的开发。  指导老师方面，本项目指导老师现任浙江省数据存储传输技术重点实验室主任，杭州电子科技大学智能与软件技术研究所副所长，工业互联网研究中心副主任，他主持国家973项目课题1项，国家科学基金面上项目2项，浙江省重大科技专项和杭州市科技计划项目6项以及横向课题多项，作为主要成员参与国家科技支撑计划项目、国家自然基金、浙江省重大科技专项等项目10多项，涉及研究方向包括工控安全、网络安全、物联网安全、数据挖掘等多个方面，具有丰富的项目经验。  **优势：**  由于是计算机专业，具有扎实的编程能力，能够胜任本系统项目的开发工作；参与过多项项目，使用过网络爬虫、区块链技术、数据挖掘、数据可视化等技术，熟悉主流数据库，对智能合约有一定的了解。对数据的动态交互与展示有实践经验，能够承担本项目所需要的技术研发工作。本项目指导老师具有丰富的项目指导经验，能够帮助解决项目研发过程中遇到的技术和实施难题，保障项目顺利完成。  **风险：**  **系统风险：**  系统检测出的漏洞是系统可能存在的漏洞，合约并不一定具有这样的漏洞，所以检测结果可能会对使用者造成一些判断上的干扰。因为智能合约语法迭代非常快，系统检测语法更新的不及时，可能会造成漏洞无法被检测出，对使用者造成损失。系统使用时需要联网，如果遇到断网问题的话可能会造成检测结果的丢失，需要重新检测。 |
| 4、项目计划目标  项目计划实现以下目标：   1. 智能合约检测系统的前端界面开发。 2. 智能合约检测系统的后端逻辑实现。 3. 采用数据库保存用户数据。   **参考文献**   1. 赵芳煜. 基于以太坊智能合约的漏洞扫描器的设计与整合[D].北京邮电大学,2020.DOI:10.26969/d.cnki.gbydu.2020.000259. 2. 涂良琼,孙小兵,张佳乐,蔡杰,李斌,薄莉莉.智能合约漏洞检测工具研究综述[J].计算机科学,2021,48(11):79-88. 3. 倪远东,张超,殷婷婷.智能合约安全漏洞研究综述[J].信息安全学报,2020,5(03):78-99.DOI:10.19363/J.cnki.cn10-1380/tn.2020.05.07. 4. 黄凯峰. 以太坊平台智能合约漏洞检测工具研究[D].深圳大学,2019.DOI:10.27321/d.cnki.gszdu.2019.000022. 5. 谈辰. 针对以太坊智能合约代码的安全检测系统[D].电子科技大学,2019.   古涛铭. 面向智能合约的安全检测系统研究与设计[D].电子科技大学,2020.DOI:10.27005/d.cnki.gdzku.2020.002995. |

**三、预期成果、知识产权形成及经济、社会效益分析**

|  |
| --- |
| 1. 项目的预期成果及知识产权归属情况   智能合约漏洞检测系统：  申请发明专利1项；  软件著作权1项；  本项目产生的知识产权归项目团队成员和指导老师共同拥有。 |
| 1. 项目的市场前景分析   市场前景分析：虽然市场上已经存在了各种各样的检测智能合约代码的工具，但是基本上都是面向熟悉命令行工具的开发人员，对于普通用户来说就显得很不友好。基于此，开发一个面向普通用户的多工具智能合约检测系统显得意义重大，这不仅可以集成百家之长，进行对比，还能让普通用户对自己的智能合约存在的漏洞有所了解，从而进一步防范因智能合约漏洞引起的利益损失。所以该项目的出现是具有意义的。  经过调研发现，以太坊上的智能合约有其风险性，一旦部署在以太坊上的智能合约有漏洞，就可能被不法分子利用，从而来满足自己的相关利益，而在这方面的法律约束力又小，所以提前进行智能合约的检测至关重要。  该项目逻辑清晰，脉络完整，我们具有很大的信心，这是一项关于以太坊合约安全的项目，能进一步提高以太坊智能合约安全性。 |
| 1. 项目的盈利能力分析及财务预算   该项目盈利能力分析：对于此多工具智能合约检测系统，鉴于它不仅可以集成百家之长，比如Smartcheck、Slither、Oyente等检测工具，将不同检测结果进行对比，进一步让智能合约漏洞检测更加准确，还能让普通用户对自己的智能合约存在的漏洞有所了解，从而进一步防范因智能合约漏洞引起的利益损失。所以我们打算将此系统采用普通用户和会员用户的模式来达到盈利的目的，对于普通用户，只能使用Smartcheck这一种检测工具，不仅检测速度慢，而且正确率相对低下，但也能检测出一些较为大众、明显的漏洞；对于会员用户，全面开放检测工具，可以将不同检测结果进行对比，并且还能模拟在区块链上部署合约的场景，全方位增强用户体验感，从而让更多的会员用户愿意来使用我们的系统。  这项服务费用的存在，在一定程度上可以提高开发和维护人员的工作积极性，从而可以使得系统开发和维护的工作更能够顺利的进行下去。  本项目财务预算一共1万元，支出详细如下表：   |  |  |  | | --- | --- | --- | | 支出项 | 依据和理由 | 金额（万元） | | 设备材料费 | 购置处理器、内存条等用于搭建网络的配件 | 0.3 | | 差旅会议费 | 去本地或外地企业、高校进行学术调研和会议交流 | 0.4 | | 知识产权费 | 用于发表论文、申请专利和软件著作权 | 0.3 | | 总计 |  | 1.0 | |
| 1. 项目的社会效益分析   该项目的社会效益。  对于开发和维护人员而言，这让他们有了工作，解决了一些人的工作问题，让他们有一个展示自我价值的平台，从而不断为社会增加效益；  对于所有用户来说，他们能够通过此系统来检测智能合约漏洞，从而让普通用户对自己的智能合约存在的漏洞有所了解，从而对相关漏洞进行改进，进一步防范因智能合约漏洞引起的利益损失。  对于社会而言，以太坊上的智能合约有其风险性，一旦部署在以太坊上的智能合约有漏洞，就可能被不法分子利用，从而来满足自己的相关利益，而在这方面的法律约束力又小，会对整个以太坊，甚至社会带来巨大的损失，所以在部署前进行智能合约的检测至关重要。这对于社会的安全、稳定、和谐起到了一定的作用。 |

**四、项目实施进度方案**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本项目进度安排如下表所示：   |  |  | | --- | --- | | 起止年月 | 进度目标 | | 2021.12~2022.01 | 项目需求调研，关键技术研究 | | 2022.02~2022.04 | 总体方案设计 | | 2022.05~2022.11 | 系统模块开发、集成、测试 | | 2023.02 | 项目中期检查 | | 2023.02~2023.03 | 系统改进 | | 2023.04~2023.07 | 项目验收 | |

**五、项目组承诺**

|  |
| --- |
| **承 诺 书**  以上所填内容真实可靠，本项目组承诺：该项目立项后，将严格遵守有关规定、遵守本申报书和预算表中规定的条款和内容，保证按计划进度完成项目任务。  项目组全体成员（签章）：    年　　月　　日 |

**六、学校审核意见：**

|  |
| --- |
| 负责单位（公章）  年 月 日 |

**七、专家组审核意见**

|  |
| --- |
| 专家组组长签章：  年 月 日 |

**八、实施办公室审核意见**

|  |
| --- |
| 公章：  年 月 日 |