

江苏省高等学校
大学生创新创业训练计划项目申报表
(创新训练项目)

推 荐 学 校 : _____ (盖 章)
_____ 面向电子商务的区块链

项 目 名 称 : _____ 智能合约的设计与实现
_____ 重点项目

项 目 类 型 : _____ 一般项目
_____ 校企合作基金项目

所属一级学科名称 : _____ 12 管理学

项 目 负 责 人 : _____ 方泽强

联 系 电 话 : _____ 17705190086

指 导 教 师 : _____ 刘阳

联 系 电 话 : _____ 15805152685

申 报 日 期 : _____ 2019 年 4 月

江苏省教育厅 制

二〇一九年三月

填表说明

一、申报表要按照要求逐项认真填写，填写内容必须实事求是表述准确严谨。空缺项要填“无”。

二、格式要求：表格中的字体采用小四号宋体，单倍行距；需签字部分由相关人员以黑色钢笔或签字笔签名。

三、项目类型为重点项目、一般项目和校企合作基金项目等。

四、项目来源：1. “A”为学生自主选题，来源于自己对课题的长期积累与兴趣；“B”为学生来源于教师科研项目选题；“C”为学生承担社会、企业委托项目选题。
2. “来源项目名称”和“来源项目类别”栏限“B”和“C”的项目填写；“来源项目类别”栏填写“863项目”、“973项目”、“国家自然科学基金项目”、“省级自然科学基金项目”、“教师横向科研项目”、“企业委托项目”、“社会委托项目”以及其他项目标识。

五、表格栏高不够可增加。

六、填报者须注意页面的排版。

项目名称		面向电子商务的区块链智能合约的设计与实现											
项目所属一级学科		12 管理学		项目所属二级学科		1208 电子商务类							
项目类型		(√) 重点项目 () 一般项目 () 校企合作基金项目											
项目来源		A	B	C	来源项目名称		来源项目类别						
			√		基于 3 值抽象的假设-保证式 PCTL*组合随机模型检验方法/物联网环境下电子商务流程的可信验证		国家自然科学基金项目/ 省级自然科学基金项目						
项目实施时间		起始时间： 2019 年 5 月 6 日 完成时间： 2020 年 5 月 6 日											
项目简介 (限 100 字)		在全世界国家与企业加快布局区块链经济的大背景下，本项目以租赁交易流程为例，从智能合约的设计与实现入手，重构去中介的可信电子商务商业模式，为传统电子商务注入新活力。											
申请人或申请团队	主持人	姓名	方泽强	年级	2016 级	学号	21201 62016	所在院系/专业	信息工程学院 /软件工程	联系电话	17705190086	QQ 邮箱	786085698 @qq.com
		姓名	王洲程	年级	2016 级	学号	21201 61883	所在院系/专业	国际经贸学院 /电子商务	联系电话	15380428330	QQ 邮箱	424396482 @qq.com
	成员	姓名	孙卓	年级	2016 级	学号	21201 63193	所在院系/专业	信息工程学院 /软件工程	联系电话	17327764197	QQ 邮箱	1548314601 @qq.com
		姓名	王颖娴	年级	2016 级	学号	21201 61760	所在院系/专业	会计学院/会计	联系电话	18061751579	QQ 邮箱	844302769 @qq.com
		姓名	丁焯菊	年级	2017 级	学号	21201 72551	所在院系/专业	国际贸易学院/ 电子商务	联系电话	18888050093	QQ 邮箱	1135170681 @qq.com
	指导教师	第一指导教师	姓名	刘阳		单位		南京财经大学					
年龄			38		专业技术职务		教授						
主要成果		围绕安全攸关系统的分析与验证领域，做了一些有意义的探索工作：主持完成或在研国家自然科学基金、中国博士后科学基金、省自然科学基金和省高校自然科学基金重大项目各 1 项，参与完成或在研 ERC-Singapore 联合项目 1 项、国家自然科学基金项目 3 项、国家高技术研究发展计划（863 计划）和国家重点基础研究发展计划（973 计划）子课题各 1 项；以第一作者或通讯作者（协助指											

		导的博士生第一作者)发表或被录用多篇论文于 CCFA/B/C 类期刊/会议、计算机学报、软件学报和电子学报英文版等国内外著名期刊和国际会议; 相关成果被欧洲科学院院士 Prof. Katoen 研究组等或国际期刊 IEEE Transactions on Service Computing 等引用。		
第二指导教师	姓名	无	单位	无
	年龄	无	专业技术职务	无
主要成果		无		

一、 申请理由

(一) 背景分析

1. **政策支持度高，发展环境好。**区块链技术诞生初期主要运用于数字货币、金融支付等领域。从 2014 年起，国际电子商务零售业巨头亚马逊、美国联邦快递等大型公司开始研究将区块链技术运用到电子商务产业链条中;国内阿里巴巴、京东、滴滴打车等一批具有代表性的电子商务企业也开始积极研究区块链技术在电子商务行业的应用，以进一步降低成本，提高服务质量。

尽管中国对区块链技术关注相对较晚，但从 2015 年开始对区块链的关注有了质的飞跃且发展速度极快。2016 年成立了中关村区块链产业联盟、金融区块链联盟、中国区块链研究联盟等多家有影响力的区块链产业联盟。2016 年 10 月 16 日，工信部发布《中国区块链技术和应用发展白皮书》，总结了国内外区块链发展现状和趋势，分析了包含金融、供应链、文化娱乐、智能制造、社会公益、教育就业等多个应用场景的技术应用，指出了区块链的核心技术路径以及未来区块链技术标准化方向和进程。

同时，腾讯在 2017 年 4 月发布区块链方案白皮书;随后，2017 年 8 月国务院指导意见中就明确鼓励利用开源代码开发个性化软件，开展基于区块链、人工智能等新技术的试点应用;2018 年 11 月中国电子商务协会区块链技术研究院成立。可以看到，在全世界国家和企业加紧区块链技术布局与落地的背景下，中国面临着重大的历史性机遇。

2. **区块链与电子商务的结合潜力大。**二者在生活的各个领域发挥着愈发重要的作用，例如区块链+物流项目，网络不同的支付方式以及大量涌现的去中心化交易市场。这些新兴项目相比传统业务具有其独占优势，在于跨境、去信任、去中心化、低成本、交易速度快等。

在现今社会中，中心化是信息沟通和运营成本高的主要原因。而这种中心化体制正在逐步改变，互联网的出现使得通信成本显著下降。同样的，区块链将会大幅降低电子商务运营成本。例如，出售房屋就像支付订阅博客一样容易。由于新技术，人们可以在没有中间人的情况下开展电子商务业务。这种独特的区块链交易行为关键离不开智能合约，所谓智能合约，就是传统合约的数字化版本，它们是在区块链数据库上运行的计算机程序，可以在满足特定条件时自行执行。而在区块链 2.0 时代，以太坊(区块链技术开发平台)将区块链与智能合约完美结合，为行业带来无限潜力。

3. **电子商务智能合约的安全倍受关注。**目前智能合约已经发生过重大安全事件，如黑客利用漏洞入侵系统，进而对智能合约用户造成巨大损失。其中较为严重的两大事件有：①Bitfinex 在 8 月 2 日凌晨发布公告，发现了安全漏洞。该漏洞导致 Bitfinex 全面停止交易，这将导致每位用户的账户平均损失 36%；②黑客智能合约存在的漏洞攻击 The Dao，造成价值逾 5000 万美元的损失。ETH 市场价格从记录高位 21.50 美元跌至 15.28 美元。目前来看，智能合约存在四大安全风险：隐私泄露、交易异常、合约故障、拒绝服务；如何找到智能合约安全性与灵活性的平衡是行业亟待解决的重要问题。

（二） 研究意义

自 2009 年比特币诞生以来，以其为代表的区块链技术迅速崛起，经历了以数字货币为代表的区块链 1.0 时代，未来几年的区块链的研究方向将以“区块链 2.0 应用为主”，其中的智能合约将在区块链电子商务领域具有广泛的应用前景。但是，目前智能合约应用技术的发展尚处于初级阶段，如何在电子商务领域引入与构建区块链技术已成为现在众多企业正在面临的挑战。2019 年，区块链及相关行业更是处于加速发展期，国家与企业都在加紧布局区块链业务，全球正在跑步进入“区块链经济时代”，而中国也面临重大机遇。作为新时代中国学生，研究此项目不仅能结合自身优势以锻炼自身实践能力，还可放眼产业前沿，拓宽自身眼界为今后职业规划提供帮助。

本课题旨在面向电子商务的区块链中智能合约的设计与实现，通过区块链的去中心化特征和智能合约的优势来解决现在中心化电子商务交易机制中的先天性问题，如高额的交易成本、信息隐私安全问题、信用问题等。在电子商务领域中应用区块链技术，对于电子商务企业来说，不仅可以填补以前机制中的漏洞，还可以提高交易效率、降低交易成本，使企业更加迎合未来市场的需求与发展方向。项目通过以太坊智能合约开发平台，以电子商务中的租赁业务为例，进行智能合约的设计、实现与安全性验证，可以切实了解智能合约在实际应用中的优缺点，并在此基础上建立合约的优化方案，可以推动智能合约在电子商务领域的进一步发展与应用。

（三） 可行性分析

本课题研究的是面向电子商务的区块链智能合约的设计与实现。中国作为全球最大的互联网市场，截止 2018 年 12 月，我国网民规模已达 8.29 亿，且仍在持续增长。区块链智能合约技术，作为新产业技术，已被大部分电子商务企业关注，然而现在的智能合约发展还处于初级阶段，不正确的使用仍会导致非常严重的后果。因此，如何解决在电子商务领域构建区块链技术俨然成为了电子商务领域的一大挑战与任务，而本课题的研究具有普遍的现实意义和研究价值。

(1) 理论可行

有效的设计原理。狭义的智能合约就是用以实现商业逻辑算法的程序代码段，设计智能合约主要包含共同协商合约、制定合约规范、验证合约规范性、编写合约代码 4 大环节。具体理论涉及由合约参与者进行协商，确认各方的权利和义务，确定合约文本并进行规范性检验等过程，先运用流程图绘制工具如 **ProcessOn**，最后运用高级语言 **Solidity** 将智能合约前期设计模型转化成标准合约代码，此设计原理已运用于各个领域不同工具，因此是行之有效的。

可靠的实现机制。智能合约的实现本质上是将对象程序化并通过平台发布到区块链上，成为全网共享资源，再通过外部数据的触发，智能合约将自动执行从而改变区块链中对象的状态和数值。例如用智能合约实现房子租赁：房主将制定好的合约代码通过平台发布到区块链上，如果有人转账付款租金，则触发合约，将待出租房子变为已出租房子，这样一来便实现了房屋租赁。这次课题将使用目前最热门的智能合约平台——以太坊进行智能合约的实现。

易读的验证理论。智能合约是对某领域专业知识的程序语言描述，因此必须保证合约文本与合约代码的一致性，而合约验证是保证这些要求的重要途径。目前，形式化验证是智能合约领域的主流验证方法，它是基于数学的描述和推理计算机性质的技术，智能合约的形式化验证原理主要包括 4 个部分：代码生成、形式化描述、形式化验证与一致性测试。

(2) 技术可行

强大的设计软件。现有结构图绘制工具 **Visio** 或 **PowerDesigner** 两大工具将助力智能合约的前期设计部分，其可视化的操作界面和敏捷的开发模式可以绘制思维导图，流程图，概念模型图，层次结构图，业务逻辑图等，使我们团队能更好地理解并设计电子商务特定业务的智能合约。

敏捷的实现工具。区块链 2.0 时代，依托以太坊官方的在线编译工具 **Remix**，即可省去本地环境繁琐的环境搭建步骤，使团队开发者能更加专注于合约开发本身。此外，配合高封装度编程语言 **Solidity**，使得合约代码易于理解。

可靠的验证系统。重视系统安全的现代社会，模型检验工具已十分常见；命令行工具如 **NuSVM**，与带有可视化界面的软件如 **Prism**，**Uppal** 结合，可以帮助我们团队顺利地完 成电子商务业务中智能合约的安全性验证，并依据实验数据形成报告，为成果报告提供强有力的数据支撑。

良好的实验设备。团队成员拥有全平台操作系统电脑，如 **macOS**、**Windows**、**Linux** 等，而南财的电子商务实验室拥有高性能的计算机设备，支持大型数据的计算与演示，这些为我们进行电子商务与区块链结合的智能合约开发与验证提供了坚实的硬件基础。

(3) 资料来源可行

完成智能合约安全验证需要大量的数据、资料以及相应设备。南京财经大学配有江苏省重点电子商务实验室，为我们提供相应的设备和空间环境。同时，途牛、京东、苏宁和实验室的密切合作，又为我们验证智能合约安全提供了大量的有效数据。南京财经大学刘阳教授，本身研究安全攸关软件的可信验证：基于模型/智能搜索的定量方法，能为我们提供专业的技术指导。

(4) 团队实力可行



方泽强：南京财经大学信息工程学院软件工程专业 1601 班学生，在班级任职班长，常年获得一等奖学金。曾赴加州伯克利大学参与暑期项目，有厦门建发集团实习经历。校内实践丰富，主持过如“电子商务数据分析”，“基于 Javapathfinder 模型检验”等项目。自身还熟练掌握 Weka, SPSS, Echarts 等数据分析工具，Visio 等逻辑结构图绘制工具，擅长制作 PowerPoint 进行概念可视化传达。



王颖娴：南京财经大学会计学院会计专业 1606 班学生，在班级任职学习委员。曾任职于过南京财经大学学生会文艺部，组织能力强，举办过中国大学生音乐节校园十佳歌手大赛，学生会内各大文艺活动。在校期间参加过“2018 悦诗风吟绿色营销大赛”，取得全国第二名并获爱茉莉太平洋集团 1 万奖学金。学习成绩优秀，常年获得学习优秀奖学金，素质拓展奖学金，先进个人奖等。擅长商业分析，参与哈斯商学院“Annaly 资本管理公司年报分析”项目获导师满分评价。



孙卓：南京财经大学信息工程学院软件工程专业 1601 班学生，多次获优秀奖学金，曾获全国五一建模三等奖和全国大学生建模省三等奖。数据分析与自学能力强，善于用 Python 编写爬虫和数据处理，熟练掌握 Java 语言；通晓 html，CSS 等前端知识，能轻松设计与搭建网站，有个人博客搭建经验；擅长算法实践应用，有推荐系统项目实践经历。



丁烨菊：南京财经大学国际经贸学院电子商务专业 1701 班学生，现任南京财经大学大学生创新创业联合会宣传部部长，能熟练使用 Ai、Ps 等平面设计软件。学习认真，专业课知识功底强，能够使用简单的 Java 编程语言和前端 html5/CSS 网站开发语言。做事认真，善于与人交际，有不错的组织才能。



王洲程：南京财经大学国际经贸学院电子商务专业 1602 班学生，在班级担任班长，曾获优秀共青团员及奖学金等荣誉。自主性强，做事认真负责，有条理，善于处理与分析问题，有较强组织能力与领导能力。综合素质较强，熟悉掌握 Ps、Pr 等软件和 Java、VBA 编程语言及 Excel、Access 软件的数据处理能力。曾实习于网络科技公司，参与开发远程教育平台软件及前端网站设计与开发。

二、项目方案

（一） 研究目标

项目将以以太坊作为区块链开发平台，重构去中介的可信电子商务商业模式，以租赁电子商务交易流程为例，专注于智能合约的设计、实现、安全性验证等方面，在此基础上进一步提出智能合约优化方案，并将其拓展到其它电子商务应用场景。

（二） 创新特色

本次项目研究的创新之处共体现在三个方面：

1. 研究对象的独特。本次项目以新兴技术区块链中的智能合约为研究对象，聚焦于当前热点问题——智能合约的安全性。随着区块链技术的不断发展，其技术的应用领域逐渐扩展并得到更多人关注，因此对智能合约安全方面的研究分析，有利于推动智能合约的逐步完善与发展。

2. 研究工具的新颖。为实现智能合约的 solidity 代码化，根据相关开源社区提供的一系列的开发工具，本次项目将选用 Remix 在线开发工具。Remix 工具基于 Web 浏览器，用户能够在网页中编写合约代码，并且能够将编译成的二进制字节码部署到相应的区块链网络中，最终使本次项目顺利的完成电子商务智能合约实现阶段。

3. 研究方法的创新。本次研究主要采用模拟法，即先依照原型的主要特征，创造一个相似的模型，然后通过模型来间接研究原型的方法。在该项目中，主要体现为根据实际案例设计电子商务交易机制并在此基础上建立模型进行分析。通过这种研究方法，不仅可以简化算法，便于理解和分析，还可以保障数据的客观性，提高准确性。

（三） 技术路线

在已有的资料文献为理论的基础上，通过实地考察、专家访谈、社区数据挖掘、项目开发实践的形式得到大量资料与数据，利用当代计算机工具，结合理论进行项目研究，提出优化方案和应用场景。

资料调研

（1）**实地考察：**充分利用信息工程学院优势，在老师的协助下，对本校江苏省重点电子商务实验室进行实地考察，依托密切合作的电子商务企业如苏宁和途牛，通过录像，录音等记录方式再结合实验室提供的数据与文档，为后期实践提供知识背景。

（2）**专家访谈：**在各大高校中采访老师和电子商务企业相关负责人，了解最近几年区块链与电子商务行业发展的整体现状，以及他们对此前景的看法建议，展开关于课题的技术讨论。

(3) **社区资料挖掘**：充分利用图书馆，期刊电子库，知网等寻找相关书籍与文献，了解行业现状；此外到区块链相关社区如巴比特上搜寻有关技术博文，教程，了解电子商务从业者对区块链与电子商务结合的看法与智能合约实现技术。

开发实践

(4) **电子商务交易合约机制的设计**：通过知识的学习与相关资料文献的查找显示，智能合约是电子商务的基础与核心，但是目前的智能合约并不完善，其中的许多问题反而制约了电子商务交易机制的发展，主要体现在安全性问题上。我们基于电子商务领域的租赁业务来设计一个适用于该情景下的电子商务交易机制，并在这个机制的基础上进一步分析智能合约在安全性方面的应用，切实了解智能合约需要优化的内容。

(5) **智能合约的 Solidity 代码化的实现**：基于对苏宁、途牛公司实地考察与调研数据资料分析，智能合约仍未成熟，合约中代码的漏洞可能引起交易问题，甚至是恶性连锁反应。因此我们基于设计的电子商务交易机制，结合租赁业务的现实状况分析智能合约的优化问题。通过形式化检验的相关方法，验证在租赁业务中的智能合约安全性，使得合约的生成和应用有了规范性的约束，保证了合约的可行性和可信性。

(四) 研究进度安排

时间	工作内容	阶段性成果
2019.05-2019.07	通过纸质/网络等方式调研电子商务企业关于智能合约方面的研究内容	形成调研报告
2019.07-2019.08	智能合约的设计	电子商务交易合约模型完成
2019.08-2019.09	用 Solidity 语言实现智能合约	实现合约的 Solidity 代码化
2019.09-2019.10	以太坊开源工具 Remix 在线编译合约	形成编译结果报告
2019.10-2019.11	将编译后的机制形式化与符号化	总结出符号化合约内容，选择验证方法并制订验证计划
2019.11-2020.01	智能合约的形式化验证 (NuSVM) 与模型检验 (Prism/Uppal)	安全性验证分析报告
2020.01-2020.02	根据验证结果分析提出合约优化分案	文档形式的优化方案
2020.02-2020.04	整理所有数据与资料并结合导师指导建议，完成研究报告	形成研究报告和论文
2020.04-2020.05	搭建项目博客进行成果展示	项目成果多媒体展示

（五）项目组成员分工

方泽强：负责本次“面向电子商务的区块链智能合约的设计与实现”课题的总体协调与总体统筹工作，负责与组员做充分的沟通与任务的分配。主要工作是整合各项资料，并明确每个成员的任务，同时协调好指导老师与本组成员的有效沟通，保证项目的高效高质量完成。

王洲程：负责本次“面向电子商务的区块链智能合约的设计与实现”课题的总体实施工作，负责攻克项目难关和编译程序代码，同时做好项目的详细策划，组织每一步的工作，保证项目的切实可行。

孙卓：负责本次“面向电子商务的区块链智能合约的设计与实现”课题的资料查找与搜集，为项目的研究做好理论知识的准备，同时参与攻克编码编译，解决技术性难题，为项目的研发提供技术层面的可靠保障。

王颖娴：负责本次“面向电子商务的区块链智能合约的设计与实现”课题的数据整理统计与分析工作，检验资料与数据的正确性。同时跟进项目的研究，记录进度与过程中的零碎资料，为项目的进一步发展以及数学层面的逻辑性与准确性提供保障。

丁烨菊：负责本次“面向电子商务的区块链智能合约的设计与实现”课题的文案编辑与经费预算估计，负责项目进行过程的经费记录，保证项目的正常发展。同时，整合各项资料形成书面文案，为课题的汇报呈现做好准备。

三、学校提供条件

1.南京财经大学拥有江苏省级重点电子商务实验室，与苏宁、途牛、京东等大型电商企业有着密切的合作，从而为研究提供充分的数据支持与科研条件。同时，学校一向支持和鼓励大学生创新创业工作和理论与实践相结合，创造了优质的创新学习环境，为课题的产生与发展提供了坚实的基础。

2.南京财经大学一直致力于推动高等教育教学改革，促进人才的培养和教学方法的创新,鼓励支持大学生积极参与科学研究、技术开发和社会实践等创新活动，不断激发学生的创造性、积极性和主动性，提高大学生的科学素质和文化素养，培养大学生的创新创业精神和实践能力。学校一直高度重视大学生实践创新项目训练，根据具体项目的实施情况，给予充足的配套经费，保证研究的顺利进行。

3.南京财经大学设有针对学生的实践创新平台，组织专业老师指导大学生实践创新训练活动，全程指导学生进行实践创新训练，能够给课题调研的学生提供合理建议，帮助课题的调研，营造良好创新环境。同时，学校还设有创业园，为大学生的创业实训提供物质基础与设施基础。

4.为进一步培养社会所需人才，南京财经大学近年来非常重视“互联网+”领域的人才培养与发展，多次开展与“互联网+”相关的知识培训和各种竞赛，因此该课题的研究可以得到学校的相关帮助与重视。

四、预期成果

1.设计的合约可提供给开源社区。合约包括源代码与文档说明，为区块链开发者提供实际案例。

2.验证的智能合约漏洞可上传至以太坊平台官方，帮助官方排除现存的合约漏洞与潜在危险因素。

3.优化方案与智能合约设计方案也可以为电子商务企业与从业者提供特定的解决方法，促进其布局电子商务与区块链业务。

4.将前期调研与项目实践成果形成论文发表，或申请相关专利。

5.搭建项目专属博客，上传团队研究成果（包括模型，源代码，优化方案），将自己的项目开源，使更多电子商务区块链开发者或从业者受益。

五、经费预算

总经费（元）	10000	财政拨款/企业资助（元）	0	学校拨款（元）	0
--------	-------	--------------	---	---------	---

注：总经费、财政拨款、学校拨款按照规定金额填写，校企合作项目企业资助金额不少于 5000 元。

费用名称	资料费	材料费	调研费	其他	合计
金额	3000	1500	4500	1000	10000

具体预算项目：资料费包括查阅文献费用、购买软件、海外服务器租赁及打印资料等；材料费涉及购买计算机外围设备如 U 盘，云存储数据托管费；调研费用具体为实验室调研费以及电子商务企业实地考察；其他费用包括交通费及形成论文发表费用。

六、导师推荐意见

同意推荐

区块链拥有去中介化、可溯源、可信任和公开透明等诸多优势，区块重构电子商务是电子商务发展的重要趋势和必然。智能合约是电子商务区块链的关键和核心，其重要性不言而喻。本项目立意新颖、研究目标明确、技术路线详实可行，有很好的理论价值和实践意义。

签名：

2019年4月16日

七、院系推荐意见

同意推荐

院系负责人签名：

学院盖章：

2019年4月16日

八、学校推荐意见：

同意推荐

学校负责人签名：

学校公章：

2019年4月29日