对外经济贸易大学
University of International Business and Economics

2016-2017 年度科研立项
开题报告

课题名称 构建个人信用区块链

课题方向 信息科技

负责人姓名 刘金羽

负责人所在学院 信息学院

联系电话 13161130133

电子邮件 LIUJINYU1997@qq.com

提交日期 2016 年 11 月 23 日

共青团对外经济贸易大学委员会制表

填表说明

一、请课题负责人根据开题报告的内容要求认真完成填写。

二、课题负责人应根据课题设计情况实事求是填写。填写字体请用宋体五号，并用 A4 纸打印，于左侧装订成册。

三、本表一式两份，由课题负责人提交至所在学院专门负责学术科研活动相关工作的部门，并由该部门统一交学生学术科研活动管理委员会学办公室。

五、《对外经济贸易大学 2016-2017 年度科研立项开题报告》将作为项目立项的主要材料之一。

六、本表格不够可自行扩页。

<table>
<tr><td>课题名称</td><td colspan="8">构建个人信用区块链</td></tr>
<tr><td rowspan="4">课题方向</td><td>选择方向</td><td colspan="7">信息科技</td></tr>
<tr><td>管理学</td><td>经济学</td><td>统计学</td><td>马克思主义</td><td>民族学与
文化学</td><td>哲学</td><td>宗教学</td></tr>
<tr><td>教育学</td><td>语言学</td><td>社会学</td><td>港澳台研究</td><td>新闻学与
传播学</td><td>法学</td><td>体育
科学</td></tr>
<tr><td>政治学</td><td>历史学</td><td>艺术学</td><td>国际问题研究</td><td>图书馆、情报与
文献学</td><td>文学</td><td></td></tr>
<tr><td rowspan="11">参与者
（3-7 人，实践转科研团队为 3-10 人。人员若与提交的申请表有变动，需说明）</td><td>序号</td><td colspan="2">姓名</td><td>学号</td><td>学院</td><td colspan="2">联系方式</td></tr>
<tr><td>1（课题负责人）</td><td colspan="2">刘金羽</td><td>201536014</td><td>信息学院</td><td colspan="2">13161130133</td></tr>
<tr><td>2（第二课题负责人）</td><td colspan="2">周曼</td><td>201536032</td><td>信息学院</td><td colspan="2">13161127377</td></tr>
<tr><td>3</td><td colspan="2">贺玉琼</td><td>201536054</td><td>信息学院</td><td colspan="2">13611168909</td></tr>
<tr><td>4</td><td colspan="2">王泽普</td><td>201525041</td><td>信息学院</td><td colspan="2">15903658246</td></tr>
<tr><td>5</td><td colspan="2">胡庆涛</td><td>201409037</td><td>英语学院</td><td colspan="2">13161414978</td></tr>
<tr><td>6</td><td colspan="2"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>7</td><td colspan="2"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>8</td><td colspan="2"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>9</td><td colspan="2"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>10</td><td colspan="2"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>人员变动说明</td><td colspan="8">加入了英语学院的胡庆涛同学，因为区块链英文文献较多，加入英语学院的有助于我们准确了解外文文献。</td></tr>
</table>

一、课题背景

(一) 学术科研需求

(二) 社会实践需求

二、国内外研究动态

(一) 国内外发展的历史及现状

(二) 前沿发展情况

1. 相关领域现阶段已有主要研究理论、观点、技术、方法述评
2. 自己研究的内容

三、理论意义与现实意义

(一) 理论意义

(二) 现实意义

四、主要内容

(一) 相关术语的界定

(二) 课题研究的目标

(三) 课题研究的基本框架

1. 论文提纲及各部分内容间的逻辑关系
2. 拟采用的研究方法与指导思想

五、重点与难点

(一) 重点

(二) 难点

六、主要观点

七、创新之处

(一) 课题研究理论创新

(二) 课题研究方法创新

八、课题预期研究成果与表现形式

（课题研究的成果形式包括研究报告、教育论文、专著、软件、课件等多种形式）

九、课题进度安排

十、参考文献

课题设计 2000 字以上 （转下页）	**一、课题背景** （一）学术科研需求 比特币自推出以来已超过 8 年时间，没有出现过资金或用户信息被盗用的记录。其安全性得到验证，且其资金清算的效率和成本也具有明显的优势。这使得人们对比特币所运用的区块链技术的信心不断增强，而且人们也越来越清晰地认识到，区块链尽管是比特币所首创和应用的一种技术和协议，但区块链并不同于比特币，其应用也绝不会只局限于比特币。当然，区块链的应用大都刚刚起步。当前的区块链项目主要处在开发、测试阶段，是否能被广泛推广应用还需时间检验。正因为其巨大的潜力和优势，对于区块链技术场景应用的学术研究正在呈井喷式增长。 （二）社会实践需求 随着互联网的发展和广泛应用，已经使得越来越多的经济交往和交易活动转到网上进行。网络世界（或线上社会）正在快速扩展、充实和活跃，而网上交易必须解决当事人的身份验证、价值核实、交易记录、查验核实等方面的效率和安全保护问题，在这方面，传统思维和习惯做法就是顺应线下交易向线上转移的发展轨迹，讲现实（线下）社会的通行规则和做法推到网络（线上）社会，但实践中却越来越难以适应网上交易的需求，尤其在个人信用的记录和保留方面。 在政治信用方面，由于收到现实社会行政管辖的制约影响，个人信用无法流畅地跨国传递，导致许多贪官污吏在境外逍遥自在。在借贷信用方面，目前不同银行之间无法做到完全共享用户信用数据，导致部分信用较差的借款者一再拖欠账款，造成不必要的人力物力资源浪费。更有甚者凭借“内部渠道”随意篡改信用记录，自新交规颁布以来，买分卖分现象严重，扣分制度形同虚设。个人信用记录的分散化、及严重的行业、区域隔离现象不利于社会公平与效率的提升，是建设现代化社会的一大障碍。 **二、国内外研究动态** （一）国内外发展的历史及现况 国外： 历史：区块链技术起源与 2008 年由化名为“中本聪”的学者在密码学邮件组发表的奠基性论文《比特币：一种点对点电子现金系统》。后来比特币的第一个区块诞生于 2009 年 1 月 4 日，由创始人中本聪持有，一周后，中本聪发送了 10 个比特币给密码学专家哈尔芬尼，形成了比特币史上第一次交易; 2010 年 5 月,佛罗里达程序员用 1 万比特币购买价值 25 美元的披萨优惠券, 从而诞生了比特币的第一个公允汇率。此后，比特币被更多的国家和人们所承认其价值，而且其价格也在不断上涨。从而比特币所包含的区块链技术也越来越被广泛的关注。 现状：区块链将会经历以可编程数字加密货币体系为主要特征的区块链 1.0 模式，一可编程金融系统为主要特征的区块链 2.0 模式和以可编程社会为主要特征的区块链 3.0 模式。目前一般认为区块链技术正处于 2.0 模式的初期，股权重酬和 P2P 借贷等各类基于区块链技术的互联网金融应用相继涌现，然而上述模式实际上是平行而非演进式发展的，区块链 1.0 模式的数字加密货币体系仍然远未成熟，距离其全球货币一体化的愿景实际上更远更困难。而且，在美国，以高盛为代表的美国金融巨头也在积极开发区块链技术在金融方面的应用，以期在改变金融当前的发展格局。 国内： 历史：国内与世界一样在国内兴起了用大规模计算机获取比特币的热潮，从而使得比特币在国内流通。但为了保证金融的正常运转，中国央行下发了不承认比特

课题设计 2000 字以上 （转下页）	币的文件，随后比特币热潮在中国逐渐冷却，但是其区块链技术却被广泛的发掘和研究。在 2016 年 10 月，中国区块链联盟发布了《中国区块链技术和应用发展白皮书》规划了中国区块链未来的发展。 现状：目前，区块链领域已经呈现出明显的技术和产业创新驱动的发展态势，但是相关学术研究严重滞后，亟待跟进。截止到 2016 年 11 月，关于区块链的论文数量不足。而且在我们研究的区块链在个人信用的应用方面无论文的指导（根据中国知网和万方数据库的搜索记录）。 （二）前沿发展情况 1.相关领域现阶段已有主要研究理论，观点，技术 ，方法述评 主要的研究理论： 基于中本聪发表的论文《比特币：一种点对点电子现金系统》。狭义的区块链即是去中心化系统各节点共享的数据账本。每个分布式节点都可以通过特定的哈希算法和 Merkle 树数据结构，将一段时间内接收到的交易数据和代码封装到一个带有时间戳的数据区块中，并链接到当前最长的主区块链上，形成最新的区块。 观点： 在当前科学界人们已经不仅仅满足于将区块链技术运用于电子货币，由于区块链的实现，区块链拥有去中心化，加密安全，不可篡改以及可溯源的技术特点，因此可以运用于数据存储，数据鉴定，金融交易，资产管理，选举投票等与其技术特性相匹配的场景，具有很大的发展前景。但是，区块链仍然存在一些局限性，区块链虽然采用了几乎不可逆的哈希算法，但是仍然存在网络攻击 PoW 共识过程，导致区块链的存在安全性问题，而且区块链的共识需要很大的算力来实现，所以导致每笔交易的确认过程需要约 10 分钟，这一定程度上限制了区块链在小额交易和时间敏感性交易中的应用。 技术： 该过程设计区块，链式结构，哈希算法，Merkle 树和时间戳等技术要素。 方法： 探索性研究方法 信息研究方法 2.自己研究的内容： （1）建设个人信用区块链的的必要性 （2）区块链具有的独特属性分析：围绕有望打造历史不可消除、信息对称的个人信用评估体系 （3）区块链建成的个人信用评估体系的数据来源分析、数据登入激励研究和评估标准分析 （4）个人资信的保密策略和查询输出方式解决方案 （5）个人信用体系的建成后的应用和对社会整体信用的提升 （6）区块链为基础的个人信用评估体系的安全性分析 **三、理论意义与现实意义** （一）理论意义 区块链作为一个新兴的技术，其应用大都刚刚起步。当前的区块链项目主要处在开发、测试阶段，是否能被广泛推广应用还需时间检验。扩展区块链的应用，深度挖掘其在个人信用场景所能发挥的效果，是对现有理论的进一步检验和扩展，能够促进区块链应用理论体系的深化和完善。 （二）现实意义 区块链技术在个人信用方面完全可以大显身手。除了先前提到的例子，人类还

课题设计

2000 字以上

（转下页）

有诸多互动均涉及信用，如协议、小额借贷、遗嘱等。传统的信用普遍建立在中心化的的基础之上，如协议，除直接涉及的利益相关方，还涉及司法机构，如果法律不认同，则协议为无效。当然，传统社会还可以基于熟人关系建立信用，如中国的民间金融活动很多是基于家庭、宗族和朋友关系进行，但这种做法局限很大，不是现代经济所能依赖的。再如小额的跨国协议，违约的追偿成本往往高于协议标的金额，亦即建立跨境信用的成本太高，因此阻碍了全球经济的市场信用建立，使得全球市场缺乏小额的信用"毛细血管"。现在有了区块链，有了全球记账的方式，自然也可以全网执行某个协议来保证信用。如果说互联网时代，我们的自由和权利在某种程度上可以依靠代码来保护，那么区块链再推进一步，通过协议，保障我们的权益可以依靠代码来自动执行。在此意义上，区块链某种程度上可承担法院执行庭的作用，而成本则低得多，使用者支付一笔可能才相当于比特币万分之一的手续费，就可以建立自己的信用。总的来说，在个人信用场景下，区块链可以充分地发挥其公开、难以篡改、去中心化的优势，为个人信用的记录和保存提供强力的技术支持，并助力现代网络信用社会的革命性发展，极大的提升社会公平与效率。

四、主要内容

（一）相关术语的界定

1.缩略语：

缩略语	原始术语
PoW	工作量证明 (Proof of Work)
PoS	权益证明 (Proof of Stake)
DPoS	股份授权证明 (Delegate Proof of Stake)
PBFT	实用拜占庭容错 (Practical Byzantine Fault Tolerance)
P2P	点对点 (Peer to Peer)
DAPP	分布式应用 (Decentralized Application)
KYC	客户识别 (Know Your Customer)
RSA	RSA加密算法 (RSA Algorithm)
ECC	椭圆加密算法 (Elliptic Curve Cryptography)
BaaS	区块链即服务 (Blockchain as a Service)

术语表 1

术语	定义/解释
共识机制	区块链系统中实现不同节点之间建立信任、获取权益的数学算法。
智能合约	一种用计算机语言取代法律语言去记录条款的合约。
挖矿	比特币系统中争取记账权从而获得奖励的活动。
分布式账本	一个可以在多个站点、不同地理位置或者多个机构组成的网络中分享的资产数据库。其中，资产可以是货币以及法律定义的、实体的或是电子的资产。

术语表 2

术语	定义/解释
区块链	分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。
分布式	相对于集中式而言。在白皮书中，分布式是区块链的典型特征之一，对应的英文是Decentralized，完整的表达形式是不依赖于中心服务器（集群）、利用分布的计算机资源进行计算的模式。
金融科技	通过科技让金融服务更高效，通常简称为FinTech。
普惠金融	立足机会平等要求和商业可持续原则，以可负担的成本为有金融服务需求的社会各阶层和群体提供适当、有效的金融服务。
数字货币	货币的数字化，通过数据交易并发挥交易媒介、记账单位及价值存储的功能，但它并不是任何国家和地区的法定货币。

术语表 3

2.其他术语

币天销毁：币天销毁等于每笔交易的金额（币）乘以这笔交易的币在账上留存的时间（天），比如花了一笔 100 天以前收到的 10 比特币，这笔交易的币天销毁就是 1000 币天。币天销毁比每日交易量这个指标更能准确地显示市场的资金流动，因为一个人开两个账户，用 100 个比特币来回转账，这样可以把交易量做到很大，但币天销毁几乎维持不变。

电子公民：在爱沙尼亚，公民可以做政府的数据库中验证有关自己记录的完整性，并且保证记录不会被篡改，这样的安全保证使新的数字服务成为可能，爱沙尼亚政府目前正在与美国纳斯达克合作，提供基于区块链技术的网上投票服务。

课题设计

2000 字以上

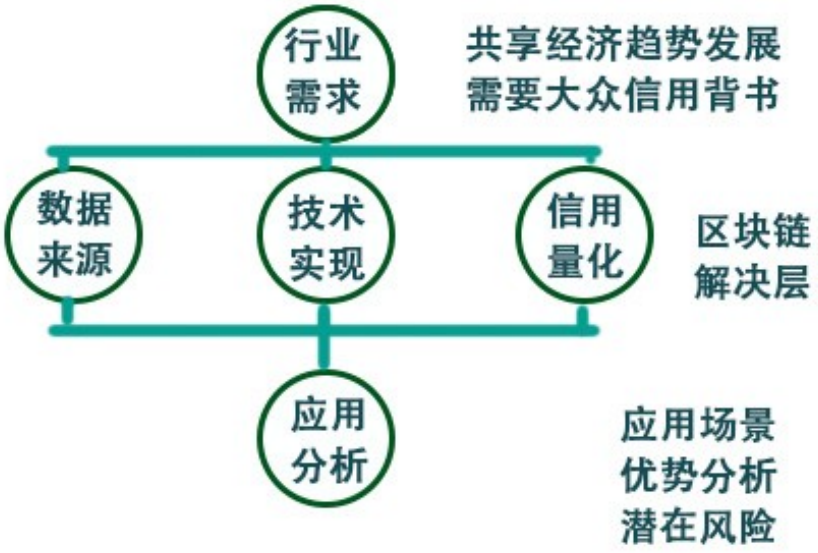
（转下页）

（二）课题研究的目标

在信誉管理和共享经济高速发展的今天，我们将探究如何运用区块链技术为个人信誉进行背书，我们将基于大众数据的可获取性，量化数据的相关性和可靠性，区块链技术可操作性和经济上的适用性进行分析，在相关研究较少的当下，做出个人信用区块链的执行框架，奠定个人信用区块链的实业基础。

（三）课题研究的基本框架

1.论文提纲及各部分内容之间的逻辑关系



课题设计 2000 字以上 （转下页）	2.拟采用的研究方法与指导思想： 采用的研究方法： 信息研究方法、量化模型方法、探索性研究方法、文献法、案例分析法 指导思想： 从实际出发，实事求是，科学分析。 **五、重点与难点** （一）重点 本课题的重点是设计相应的数据登入激励机制，将个人数据存储到区块链中，构造个人信用评估模型，并且实施有针对性的个人资信保密策略。最后运用到信用消费中，如住房按揭、汽车贷款、信用卡等各种个人消费贷款，将根据模型得出的结果与实际结果对比，以此评估模型的可行性。 （二）难点 本课题研究的难点是个人数据的存储。由于区块链具有高冗余存储、去中心化的特点，需要系统内每个节点保存所有数据的备份，所以会形成大量的数据，从而使效率下降，如何解决此问题至关重要。另外，数据登入激励机制的创建也是一个难点，因为这样会损害利用大数据赚钱的企业以及存在侥幸心理的投机主义者，势必会有很多的反对之声。除此之外，区块链个人信用评估模型的盈利模式也有待探究，只有制造相应的壁垒才能实现应有的盈利，从而促进此项应用。 **六、主要观点** 提出研究本课题的主要观点是：利用“经验主义方法论”把个人信用评估看成模式识别中的分类问题，根据历史上每个类别的若干样本，从已知数据中发现规律，从而总结出分类的规则，建立判别模型，用于对新样本的识别，此方法被称为“粗暴的经验主义方法”，存在可靠度低的风险。而引进区块链技术构建个人信用评估模型，可以较好的解决此问题，为个人信用评估带来历史性的突破。 **七、创新之处** （一）课题研究理论创新 目前，区块链在货币和金融方面的应用已经较多，尤其是比特币的应用，使区块链受到了大量的关注。在金融行业的应用有证券交易、股权众筹、P2P 网络借贷、互联网保险、跨境转账等。而区块链在信用消费所需的个人信用评估模型的应用还尚未建立完善的机制，信用评估还是依靠于原始的经验主义方法，对未来预测的准确性较低。若将区块链应用于个人信用评估，将会很大程度地拓展信用消费的规模，同时降低风险。此技术成熟后，甚至可以运用到历史学等学科，使信息的伪造成为不可能，极大地造福人类。 （二）课题研究方法创新 本课题运用跨学科研究法，将信息技术与数学建模相结合，系统的构建区块链个人信用评估模型。区块链技术的基础架构模型由数据层、网络层、共识层、激励层、合约层和应用层组成。区块链模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。构造信用评估模型用到的数学方法有神经网络、贝叶斯网络、决策树等。构造模型后通过实验法对实际情况进行模拟，运用对比法将模拟结果与实际结果相对比进行可行性分析。

课题设计 2000 字以上 （转下页）	**八、预期结果表达方式** 本课题预期将于 2016 年 7 月完成，以研究论文为研究结果。 **九、课题进度安排** 2015 年 12 月中旬-2016 年 1 月中旬 基于区块链的技术基础研究和市场研究 2016 年 1 月中旬-2016 年 2 月中旬 个人信用数据来源分析 2016 年 2 月中旬-2016 年 4 月中旬 数据量化分析 2016 年 4 月中旬-2016 年 5 月中旬 安全性和经济性分析 2016 年 5 月中旬-2016 年 7 月 论文整理发表 **十、参考文献** 2016 年中国区块链技术发展和应用白皮书 区块链技术发展现状与展望_袁勇 区块链_信任背书大数据时代的可能性_冯珊珊 基于区块链技术的信用应用设想_关莉莉

小组现有条件	（一）课题研究的组织机构和人员分工 信息学院区块链研究小组一组 刘金羽：协调统筹，整体研究 周曼： （二）小组现有条件 信息学院老师的热心指导 清华区块链技术课的文件 指导老师的技术支持
指导老师姓名： 佟强	所在单位： 信息学院
指导老师意见：（非必填）	
校团委 意见	签章　　年　月　日
科研处 意见	签章　　年　月　日
备注	

注：

1、 请不要随意更改表格格式。

该模板为开题报告最低要求，小组可增添内容。