计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190900055

区块链技术在信托行业的应用研究

可雨憬　敬茂华　郑涵尹
东北大学秦皇岛分校计算机与通信工程学院　河北 秦皇岛 066004
(1378117826@qq.com)

摘　要　现有的信托平台因其高度的中心化模式导致了交易不透明、易受攻击等诸多问题和安全风险,无法与当前信托业的快速发展相匹配。区块链所具有的去中心化、开放性、独立性、安全性和匿名性等特点,能够很好地解决信托业所面临的问题。基于区块链技术,文中提出了双链架构模型,并基于该模型设计并实现了一个双链信托业务底层平台。该平台一方面采用关系型数据库和区块链信息交互双链设计模式,实现了对信息权限的严格控制,增强风险管理;另一方面,采用联盟链、私有链双链交互设计模式,实现了信托业务模式构建。在此基础上,文中设计并实现了建立信任、信托应用链功能模块、以及基于应用链的应用接口 API,最后对区块链技术在信托业务中的应用所具有的优势和挑战进行分析总结。

关键词:区块链;智能合约;信托
中图法分类号　TP315

Application Research of Blockchain Technology in Trust Industry

KE Yu-jing,JING Mao-hua and ZHENG Han-yin
School of Computer and Communication Engineering,Northeastern University at Qinhuangdao,Qinhuangdao,Hebei 066004,China

Abstract　Due to its highly centralized mode,the existing trust platform has many problems and security risks,such as opaque transactions and easy to be to attacksed,and cannot match the rapid development of current trust industry. Blockchain has the characteristics of decentralization,openness,independence,security and anonymity,and can well solve the problems faced by the trust industry. Based on the blockchain technology,a dual-chain architecture model was proposed,and a dual-chain trust business underlying platform was designed and implemented based on it. On the one hand,the platform adopts the interactive double-chain design model of a relational database and blockchain information,to realize strict control of information permissions and enhance risk management;on the other hand,the platform uses a dual-chain interaction design mode containing an alliance chain and a private chain to achieve the establishment of trust business model. On this basis,the trust building,trust application chain functional modules,and application chain-based application interface APIs are designed and implemented. Finally,the advantages and challenges of the application of blockchain technology in trust business are analyzed and summarized.

Keywords　Block chain,Smart contract,Trust

1　引言

随着我国金融行业的不断发展与进步,金融产业已成为我国市场经济的支柱产业。信托业务是支撑金融产业发展的核心业务[1]。

如今,信托业已经正式跨入“20 万亿时代”,稳居资管行业规模第二的位置。2016 年底,信托行业管理规模已达到 20.22 万亿元,同比增长 24%,四季度环比增速分别为 1.70%,4.25%,5.11%和 11.29%,行业增长势头明显。信托资产规模的快速增长对信托行业的风险管控提出了更高的要求。然而,现有的信托平台因其高度的中心化模式导致其存在交易不透明、易受攻击等诸多问题和安全风险,无法与当前信托业的发展相匹配。

区块链是一种集分布式数据存储、点对点传输、共识机制、密码学等技术于一体,具有去中心化、开放性、独立性、安全性和匿名性等几大特点的新兴技术,目前已经在数字代币[2]、电子商务[3-4]、物流业[5]和能源互联网[6]等众多领域得到了应用[7-10]。区块链技术与信托的信任基础、多元主体、中低频交易等特性高度契合,在信托业务领域应用[11]中具有相当大的优势,受到国内外金融领域的广泛重视[12]。2016 年 8 月,美国银行、汇丰银行联合新加坡政府确立了基于超级账本协议的区块链供应链项目[13];10 月,沃尔玛、IBM 和清华大学共同创建了一个产业供应链的项目[14];2017 年 3 月,IBM 和马士基合作提出了基于超级账本的区块链解决方案,可见区块链技术在供应链金融中具有重要研究价值[15-18]。但目前具体应用区块链技术发展信托业的普适性方法尚未被提出。本文结合相关研究,利用区块链去中心化、不可篡改性、可追溯等技术特性构建基于区块链的信托业务底层支持框架[19],通过共识算法、智能合约、双链交互等技术实现信托业务信息搜集、信息存证、安全交易、高效支付等过程,能够有效降低信托风险,提高交易效率并降低成本,实现信托业务高数据化转型。

通信作者:敬茂华(jingmaohua@nequ.edu.cn)

2 区块链技术在信托业中的优势和具体应用

缺乏高效、透明的信息流通手段是桎梏当前信托业发展的重要原因，而区块链技术自身特性对解决信托平台信息高度中心化和低效流通问题具有天然的优势[10]。

优势一：区块链本质上是一个不可篡改的分布式账本，按照严格的规则和共识机制由每一个区块链参与者共同维护更新，有效地去中心化且防伪性极高，保证了信托交易信息的真实性和交易的公开透明。

优势二：区块链的信任机制建立在非对称秘钥密码原理的基础上，具有交易溯源等技术特点，能够有效地降低交易风险。使用特殊加密系统，只有通过交易私钥才能读取信息，可对客户身份信息进行识别；利用可追溯的特性，实现链内共享交易违约记录。

优势三：通过区块链技术与数字资产相结合的大胆突破，充分挖掘数据潜力，提高效益。使用区块链技术可大大减少人力物力的浪费，有效规范市场行为，引导信托行业健康有序的发展。

在信托领域引入区块链技术，可在信息存证、风险识别和简化支付3方面应用，创新。

(1)信息存证：应用区块链对信托项目的相关资料进行存证，保证资料内容真实可信，同时也为信托公司受托人对业务的管理行为提供证明。区块链的时间戳包含了原始文件、签名参数及签名时间等信息，可广泛应用于信托存证场景。

(2)风险识别：区块链存证所有相关资料，确保有查询权限的人员可以通过区块链平台一键查询交易信息，及时管控风险。区块链技术还可以增强担保措施，在线分布式账本能够让参与者更加容易追踪特点资产的所有权信息。

(3)简化支付：区块链底层技术可以实现点对点的价值转移，通过资产数字化和重构金融基础设施架构，可以大幅提升金融资产交易流程效率并降低成本。

3 基于区块链的信托业务应用框架设计与实现

3.1 基于区块链的信托业务模式构建

基于区块链技术，智能合约以代码形式预置在服务器中并完成对区块链数据的操作，利用区块链和智能合约实现信托业务立项阶段、方案阶段、合同阶段、实施阶段、投后阶段及终结阶段的存证、管理和维护，构建基于区块链的信托业务模式，如图1所示，实现信息高度透明化、信息不可篡改性。

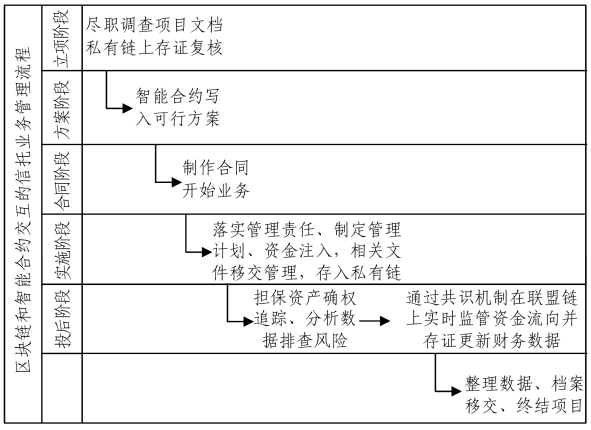

图1 应用区块链技术的信托业务管理流程

Fig. 1 Trust business management process using blockchina

具体业务开展层面，在项目立项阶段后信托计划设立前，信托公司需要在方案阶段业务进行尽职调查，系统全面地评估各种已有及潜在风险，并将评估报告通过共识机制以区块链技术存证，从技术层面上保证资料内容的真实可靠、不可篡改，加强信托机构风险管理规范性，后经风险合规部和风险总监复核，根据调查结果判断这一信托产品可行性。

项目审议批复后，项目组制作合同协议，信托资金注入信托项目，信托机构履行投后管理的职责，通过区块链平台对资金流向进行实时监控管理，确保信托财产以预定计划完成拟投资项目，避免资金被恶意挪用造成投资方损失。对担保措施这一有效的风险控制手段，区块链技术可以通过完成对担保资产确权和追踪，减轻动产抵押业务长期存在的局限性。

在投后管理阶段，信托机构需要完成建立项目管理台账，参与资金管理，更新财务数据，分析排查风险等工作，以区块链技术链接各方可保障信托相关信息能够第一时间在链上存证并对信息加盖时间戳，信托机构有查询权限的人员和委托人可以实时查询信托资金具体流向及已存证的信托项目相关信息。通过智能合约对具体项目设定特定规则，实时跟踪风险变化，加强风险识别能力，提高风险防范能力，可以有效保障投资者财产安全。

基于上述分析，本文提出基于区块链的信托业务服务框架，如图2所示。

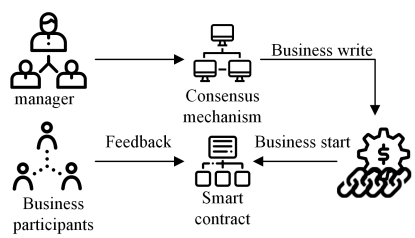

图2 基于区块链的信托业务服务框架

Fig. 2 Blockchain-based trust service framework

该服务框架采用类拜占庭共识算法(Practical Byzantine Fault Tolerance，PBFT)的联盟链和私有链创建整个网络的信任共识，使得委托方、信托机构和受益方可以通过区块链的技术特性保障信任关系，两者通过智能合约产生、存证、管理和追踪新的交易，并将交易信息对全网进行广播，接收到信息的节点通过共识机制对交易进行验证，验证通过后将交易写入区块链。

3.2 建立信任

以区块链技术优化信托业务，代替传统人工管理、存证及监控信托客体的根本原因是区块链去中心化、不可篡改、公开透明的自身特性。区块链技术提供了一个值得信赖的环境进行服务交互，底层算法的不可篡改性从技术层面上保障了业务交易信息的真实性，去中心化的共识算法可以保证信托机构运营的公开透明，也能防止外界的恶意攻击。同时，区块链技术可以进行担保资产的确权和追踪，实时保障委托方及受益方权益。在区块链网络中，所有规则都以预先设定的算法进行表述，摒弃了高度中心化的传统信托业务中第三方机构的信任背书，将对业务人员的信任转移到对机器和算法的信任上，只需信任算法就可以建立互信，也节省了人力资源在账

簿更新、验证过程的浪费，同时保障了对信托业务交易活动的记录存证、传输管理和信息追踪。区块链技术通过集体维护的特性，公开透明的共享服务信息，从而降低运营成本，提高服务效率，也减轻了信托机构作为第三方管理平台的不可靠性。因此，传统信托业务使用区块链技术优化可以提供一种稳固的可信服务交互。

3.3 信托应用链双链框架及其功能模块设计

根据区块链的访问权限开放程度，区块链可分为公有链、私有链和联盟链。公有链上的每个节点可以自由加入和退出网络，并参加链上数据的读写，不存在任何中心化的服务端节点；私有链中的节点写入权限由内部控制，而读取权限可视需求有选择性地对外开放；联盟链的各个节点通常有与之对应的实体机构组织，通过授权后加入与退出网络，联盟链由联盟内成员节点共同维护。信托平台若要实现去中心化，公开管理记录和交易信息，则要求参与信托业务的各节点平等且能进行数据互操作，联盟链可以赋予每个节点平等的读写权限以实现完全去中心化，但无法保护用户信息私密性且易产生冗余数据影响交易速度。为同时保障重要信息的安全性和最大程度的信息共享，本文采用联盟链和私有链双链交互架构。其中，不同用户私密信息被分割成多条私有链由不同的计算机（服务器）托管，同时记录存储用户信息、交易敏感信息并进行密钥管理和安全认证，联盟链用来创建交易区块。记录管理交易、存储数据，双链之间通过验证节点进行交互。

信托业务平台应用链主要包括 4 个模块：平台管理模块、智能合约模块、区块链管理模块、通信管理模块，其模块组织方式如图 3 所示。

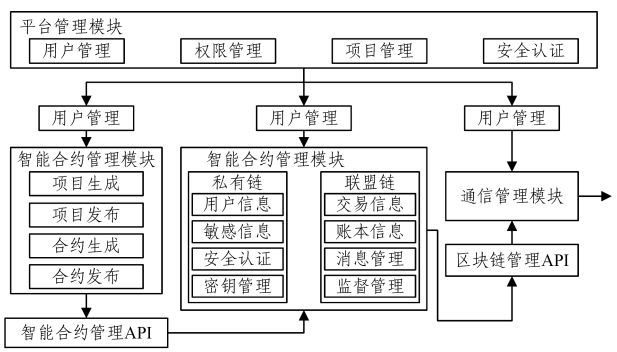

图 3 模块组织图

Fig. 3 Module organization char

（1）平台管理模块，用于提供查询管理服务的公共服务模块。为避免区块链上数据冗余，使用关系型数据库和区块链交互作为平台运维数据支持，定期进行更新，对普通用户提供基础的管理服务和非实时查询服务，支持用户注册、账户管理、权限管理、项目管理、数据管理。同时，在区块链参与计算的各个节点中严格控制不同用户的操作权限。

（2）智能合约管理模块，用于管理各类信托项目的全周期活动，项目完整的生命周期包括信托项目的生成和发布，信托合约生成和执行，信托项目投后管理及资产担保。

（3）区块链管理模块，双链交互架构，通过验证节点连接私有链和联盟链，用于管理区块链的运行，存证平台所有交易数据，包括区块链管理、一致性模块、区块链存储和通信协议。

（4）通信管理模块，保障用户和服务器、服务器和服务器之间通信的安全性和实时性。

3.4 应用链接口设计

应用链将提供统一的应用编程接口，通过这些接口支撑实现信托服务应用。

（1）生成资产地址

初始化基于区块链的信托业务平台时，首先要生成资产注册登记和进行交易管理的区块链总地址，在之后调用区块链各接口时，都要先传入该地址，然后再进行交易。生成资产地址的接口如表 1 所列。

表 1 生成地址接口

Table 1 Generate address interface

接口方式	生成资产地址接口
接口定义	List(String) getNewAddress(String symbol, int number)
参数定义	symbol：资产发行符号 number：获取资产地址列表数量
返回值	返回某种资产类型的地址列表

（2）用户注册登记

用户首先要在平台注册登记，然后平台会给用户分配相应的资产地址，并将二者在区块链关联起来。接下来，返回与用户关联的资产地址，存储在平台。后续在进行交易时，可以根据用户的登录账号和密码来返回分配给用户的资产地址，然后再进行各类操作。该接口如表 2 所列。

表 2 用户注册登记上链接口

Table 2 User registration chain interface

接口名称	用户注册登记链接口
接口定义	String registerAccount(String userID, String userPswd)
参数定义	userID：用户登录名 userPswd：用户登录密码
返回值	userID：用户登录名 rescultCode：返回值代码，0：成功，其他失败。 Txid：用户在区块链上注册的交易 id； assetsAddress：用户资产地址列表； symbol：资产类型符号 address：用户资产地址

（3）用户资金存入

刚注册登记完成的账户内是没有资产的，需要用户自行存入后再进行交易。用户将资金存入区块链信托平台中，存入成功后，区块链平台和全网将会更新资金余额，此次存入过程将被写入区块链中，返回区块链查询 ID，可以供后期查询交易结构详情时使用。该接口如表 3 所列。

表 3 资金存入接口

Table 3 Fund deposit interface

接口方式	资产存入接口
接口定义	String plusCredit(String userID, String userAddress, String userPswd, String metadata)
参数定义	userID：用户登录名 userAddress：用户资金地址 userPswd：用户登录密码 metadata：用户登记的元数据
返回值	txid：用户存入资金区块链查询 ID

（4）资金扣除

用户在区块链平台上进行信托交易，确认交易成功进行

后，平台将从余额中扣除相应的资金，然后将扣除后的资金余额在区块链平台和全网进行更新，同时将此次交易写入区块链中，返回区块链查询 ID。接口如表 4 所列。

表 4 资金扣除接口

Table 4 Fund deduction interface

接口方式	资产扣除接口
接口定义	String subCredit (String userAddress, double number)
参数定义	userAddress：用户资金额度地址 number：用户扣除资金数量
返回值	txid：用户扣除资金区块链查询 ID

(5)查询交易记录详情

用户如果对某次交易有疑问或想查询过往某次交易的具体结果，可以给平台提供交易后的区块链交易 ID，然后平台将会返回此次交易的交易信息详情。接口如表 5 所列。

表 5 查询交易详情接口

Table 5 Query transaction details interface

接口方式	查询交易详情接口
接口定义	DecodeRawTransaction getRawTransaction(Stringtxid)
参数定义	txid：区块链交易 ID
返回值	DecodeRawTransaction：交易结构详情

4 特点和创新

(1)使用区块链的高度数据化信托平台可降低营业成本。信托行业资产体量庞大，但公司层面的利润水平相对偏低，一方面由于国内大量低技术含量、低回报率的通道类业务，另一方面由于国内信托机构粗放式发展忽视对成本的控制。优化成本管理是信托发展的必然途径，通过区块链技术搭建信托业务平台可以将信息高度数据化，很大程度上解放信托机构的人力成本，降低营业支出和管理费用，节约大量资本，促进信托经济更有效地运转。

(2)通过关系型数据库交互双链设计严格控制信息权限可增强风险管理。信托业暴发风险的部分原因来自信托公司内控的流程不完善，以关系数据库交互双链设计可将整个业务流程信息按权限划分，区别管理。关系数据库存储基本信息，实现面向普通用户的基础服务和平台运维，公有链存证线上数字材料和交易信息的真实性和准确性可以被实时验证，技术特点杜绝了伪造的可能性，同时私有链设计保障机要信息安全完整。整个业务流程按用户权限严格划分，降低了由管理机制不健全带来的风险，即使必须人为处理的环节产生纰漏，也会因为流程公开透明、信息权限严格控制而更容易被发现解决，最大程度减轻损失，极大地完善信托业务风险控制机制。

(3)联盟链、私有链双链设计。区块链技术以资产数据化等方式进行金融机构间点对点的价值转移，信托计划相关企业组建联盟链，其开放程度弱于公有链，强于私有链，实现“部分去中心化”，链上各个节点对应相关实体机构或者组织，参与者通过授权加入网络并组成利益相关联盟，以共同维护区块链的运行。同时，采用私有链来支持区块链关键敏感数据的存储，以双链存储结构，私有链存储用户个人信息、信托敏感信息，联盟链存储可公开的信托交易信息，实现公开透明的同时保障隐私和机要文件的信息安全。

(4)关系数据库与区块链交互设计。因为区块链是一个不断增长、可追溯的分布式数据库，将所有系统数据存入区块链会导致数据冗余、延迟增高等问题，严重影响计算速度所以本文使用关系数据库与区块链进行交互。将用户信息、业务数据(合约、交易)通过区块链存储，平台数据(运维)使用一般关系数据库存储，并定时与区块链交互更新数据库。

结束语 本文回顾了现有研究中区块链在金融业的发展和应用，进一步分析了未来研究方向。针对传统信托业务固有的缺陷和当前信息化数据化潮流，分析了区块链技术在信托业务中的应用优势和具体应用手段，提出基于区块链技术的信托业务框架，并具体分析引入区块链技术后信托业务信息管理的设计方法和实现模式，在此基础上，设计并实现了信托业务平台管理应用链。但是本文的研究仅提出了应用区块链的信托业务框架和基本设计，与完全实现的可具体应用于现实生活的信托业务应用链还有一定距离，未来将进一步研究实际环境应用区块链技术的存储、性能等相关问题，以实现完整的信托业务应用链。

参 考 文 献

[1] MENG J, YUAN X F. Analysis on the Restrictive Factors of the Development of China's Trust Industry and Countermeasures [J]. Marketing Management Review, 2018(3): 118-120.

[2] ZHANG P, LUO X X. A Limited Tracing Method Based on Blockchain Digital Tokens[J]. Systems Engineering-Theory & Practice, 2019(6): 1469-1478.

[3] DING Q Y, ZHU J M. Product information traceability and anti-counterfeiting model of B2C e-commerce platform from the perspective of blockchain [J]. China Business and Market, 2017(12): 41-49.

[4] HU X B. Construction and Application of E-commerce Platform System Based on Blockchain Perspective[J]. Modern Marketing, 2019(7): 200.

[5] NING Z, LI M Y. Logistics Information Platform LIP-Chain Based on Alliance Blockchain[J]. Computer Technology and Development, 2019(8): 6.

[6] CHENG D L, SHEN C, PANG L. Research on the Application of Alliance Blockchain in Energy Internet[J]. Mechanical and Electrical Information, 2019(24): 155-157.

[7] YU W J, WU Y. Research on Network Transaction System Based on Blockchain Technology[J]. Modern Electronics Technique, 2019, 42(12): 25-28, 32.

[8] YIN Z C, LI H. Electronic contract solution based on superbook technology[J]. Modern Electronics Technique, 2018(11): 86-90.

[9] HUANG J H, GAO L C, XU Y Z, et al. Smart Contract Design on Crowdfunding Blockchain[J]. Journal of Information Security Research, 2017, 3(3): 211-219.

[10] UNDERWOOD S. Blockchain beyond bitcoin [J]. Communications of the ACM, 2016, 59(11): 15-17.

[11] LU J N. Application of blockchain technology in the trust industry [D]. Jinan: Shandong University, 2018.

[12] HAWLITSCHEK F, NOTHEISEN B, TEUBNER T. The limits of trust-free systems: A literature review on blockchain techno-

logy and trust in the sharing economy [J]. Electronic commerce research and applications,2018,29(1):50-63.
[13] ZHOU J,LI W Y,GUO G. Patent Situation Analysis of Blockchain Technology[J]. Telecommunications Network Technology,2017(3):37-42.
[14] WANG C L,WANG Y D,QIN Q,et al. Supply chain logistics information ecosystem model based on blockchain [J]. Information Studies:Theory & Application,2017(7):115-121.
[15] CHEN L,SUN W,LI H L. Research on Financial Risk Prevention of Supply Chain Based on Blockchain Technology[J]. Hebei Enterprise,2018(2):32-33.
[16] ZHANG J L,LUN Z W. Research on the Combination of Blockchain Technology and Supply Chain Finance[J]. Co-Operative Economy & Science,2017(21):58-59.
[17] WU J. The Application of Blockchain Technology in Supply Chain Finance-Based on the Perspective of Information Asymmetry[J]. Logistics Technology,2017,36(11):121-124.
[18] ZHU X X,HE Q S,GUO S Q. Application of Blockchain Technology in Supply Chain Finance [J]. China Business and Market,2018,32(3):111-119.
[19] ZHAO M H,ZHANG L,QI J. Blockchain-based social Internet of things trusted service management framework [J]. Telecommunications Science,2017,33(10):19-25.

KE Yu-jing, born in 1999, bachelor. Her main research interests include network and information security, and block chain technology.

JING Mao-hua, born in 1977, Ph.D, lecturer. Her main research interests include automata principle, network and information security.

(上接第 566 页)

[2] LATTNER C,ADVE V. LLVM:A compilation framework for lifelong program analysis & transformation[C]// Proceedings of the International Symposium on Code Generation and Optimization:Feedback-directed and Runtime Optimization. IEEE Computer Society,2004:75.
[3] ZHAO J,NAGARAKATTE S,MARTIN M M K,et al. Formalizing the LLVM intermediate representation for verified program transformations[C]// Acm Sigplan Notices. ACM,2012,47(1):427-440.
[4] PANDEY M,SARDA S. LLVM cookbook [M]. Packt Publishing Ltd.,2015.
[5] FRASER C W. A compact,machine-independent peephole optimizer[C]// Proceedings of the 6th ACM SIGACT-SIGPLAN symposium on Principles of programming languages. ACM,1979:1-6.
[6] SPRADLING C D. SPEC CPU2006 benchmark tools[J]. ACM SIGARCH Computer Architecture News,2007,35(1):130-134.
[7] GUOBIN Y E. Getting to know the LLVM compiler[D]. Master's thesis,The University of Edinburgh,2011.
[8] LATTNER C. Introduction to the llvm compiler infrastructure [C]// Itanium Conference and Expo. 2006.
[9] PANDEY M,SARDA S. LLVM cookbook [M]. Packt Publishing Ltd,2015.
[10] CYTRON R,FERRANTE J,ROSEN B K,et al. Efficiently computing static single assignment form and the control dependence graph[J]. ACM Transactions on Programming Languages and Systems (TOPLAS),1991,13(4):451-490.
[11] CALLAHAN D,COOPER K D,KENNEDY K,et al. Interprocedural constant propagation[C]// ACM SIGPLAN Notices. ACM,1986,21(7):152-161.
[12] COCKE J. Global common subexpression elimination[J]. ACM Sigplan Notices,1970,5(7):20-24.
[13] LATTNER C,ADVE V. The LLVM instruction set and compilation strategy[J]. CS Dept.,Univ. of Illinois at Urbana-Champaign,Tech. Report UIUCDCS,2002.
[14] HOKENEK E,MONTOYE R K,COOK P W. Second-generation RISC floating point with multiply-add fused[J]. IEEE Journal of Solid-State Circuits,1990,25(5):1207-1213.
[15] OSMIALOWSKI P. How The Flang Frontend Works:Introduction to the interior of the Open-Source Fortran frontend for LLVM[C]// Proceedings of the Fourth Workshop on the LLVM Compiler Infrastructure in HPC. ACM,2017:1.

HU Hao, born in 1994, postgraduate. His main research interests include information security.