同行专家业内评价意见书编号：20240854202

附件1

浙江工程师学院（浙江大学工程师学院）
同行专家业内评价意见书

姓名： 邹鑫

学号： 22160282

申报工程师职称专业类别（领域）： 电子信息

浙江工程师学院（浙江大学工程师学院）制

2024年04月01日

一、个人申报

（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1.对本专业基础理论知识和专业技术知识的掌握情况

作为计算机技术专业的学生，我对计算机科学的基础理论知识有扎实的掌握，包括数据结构、算法、计算机网络、操作系统等方面的知识。在专业技术知识方面，我熟悉多种编程语言，如Java、JavaScript、C++，我了解数据库管理系统的基本原理，掌握常用的开发工具和技术。此外，在学习过程中，通过完成项目、参与实习等实践活动，我更好地巩固和应用所学知识，同时对于软件开发流程、系统设计和架构等方面的能力得到了锻炼，具备扎实的基础理论知识和实践能力，以及持续学习和适应新技术的能力。

2. 工程实践经历

在参加工程实践的过程中，我在导师的带领下参与校外企业的合作项目，主要从事数字资产的托管系统的开发，同时硬件钱包的研发工作也结合了我本科所学知识，在这个过程中，我的软件工程、金融相关能力都有较大的提高，并且在合作过程中，一直有论文的产出。

3. 在实际工作中综合运用所学知识解决复杂工程问题的案例

曾经参与了一个资产托管项目，其中一个关键的任务是开发一款硬件钱包，以解决资产的密钥存储安全问题。这项工程涉及到机械设计、单片机编程、软件开发以及图像处理等多方面的知识，是一个综合运用所学知识解决复杂工程问题的典型案例。在数字资产管理领域，私钥的安全存储一直是一个备受关注的问题。为了提高用户资产的安全性，我们决定设计和开发一款硬件钱包，该钱包能够在离线状态下安全存储用户的私钥，并且具备便捷的使用体验。在硬件钱包外观的设计中，运用了机械设计相关知识，考虑了材料选择和机械结构，确保了硬件钱包的外壳具有足够的强度和抗摔性，同时提供了合适的按键和连接口。在硬件钱包内部搭载了一块嵌入式单片机，用于管理私钥的生成、存储和交易签名等功能。通过单片机编程的相关知识的应用，实现了与硬件的高效通信，同时确保了私钥的安全性，防范了各种攻击。除了硬件层面，还开发了配套的软件，用于用户与硬件钱包的交互。这包括了设备连接、签名生成、交易确认等功能。通过软件开发，实现了用户友好的界面和流畅的操作体验。为了增加硬件钱包的安全性，我们采用了图像处理技术用于信息交互，主要通过扫描二维码的形式进行信息传输，避免了触网带来的各种风险。

在项目的开发过程中，首先，进行了需求分析，与甲方产品团队和安全专家深入沟通，了解用户需求和安全标准，明确了硬件钱包需要满足的功能和性能要求。然后再进行系统设计，进行了系统分析和模块化设计。确定了硬件和软件之间的接口，考虑了系统的可扩展性和灵活性。项目开发的周期中，采用敏捷开发方法，通过不断的迭代和测试，逐步完善硬件和软件的功能。导师每周会带领我所在的开发团队与甲方公司的产品团队开展例会，沟通需求与项目进度，每个迭代周期中团队成员都充分协作，确保了项目的整体进展。项目验收前进行了安全性测试，进行了多层次的安全性验证，包括代码审查、黑盒测试和模拟攻击，确保了硬件钱包在面对各种威胁时能够保持安全。最后从用户的角度收集反馈，不断优化用户界面和体验，确保硬件钱包符合用户期望。

最终，我们成功开发出一款硬件钱包，能够安全地存储用户的私钥，同时提供了一个以多方签名技术为基础的资产托管的平台，提供了便捷的数字资产管理解决方案。通过这个项目，我深刻理解了在实际工作中，用不断迭代的敏捷开发方式解决复杂工程问题的必要性，也对多学科知识的应用有了更深刻的认识，同时，这个项目让我拥有了更加丰富的团队协作经验，锻炼了我参与团队协作的技能，使我的专业能力也得到了集中的提升。

（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】

1.
公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】

成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/授权或申请时间等	刊物名称/专利授权或申请号等	本人排名/总人数	备注
Blockchain Multi-Signature Wallet System Based on QR Code Communication	会议论文	2022年12月23日	CCF CBCC 2022	2/4	EI会议收录\导师第一作者

2.其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

（三）在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 85 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 1.5 年（要求1年及以上） 考核成绩： 85 分（要求80分及以上）
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！ **申报人签名：** 邹鑫	

22160282

二、日常表现考核评价及申报材料审核公示结果

日常表现考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： ☑优秀 ☐良好 ☐合格 ☐不合格 德育导师/定向生所在工作单位分管领导签字（公章）朱辰 2024年 10月 1日
申报材料审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： ☐通过 ☐不通过（具体原因： ） 工程师学院教学管理办**公室**审核签字（公章）： 年 月 日

浙 江 大 学 研 究 生 院

攻读硕士学位研究生成绩表

学号：22160282	姓名：邹鑫	性别：男	学院：工程师学院	专业：计算机技术	学制：2.5年
毕业时最低应获：24.0学分	已获得：25.0学分			入学年月：2021-09	毕业年月：2024-03
学位证书号：1033532024602235			毕业证书号：103351202402600461		授予学位：电子信息硕士

学习时间	课程名称	备注	学分	成绩	课程性质	学习时间	课程名称	备注	学分	成绩	课程性质
2021-2022学年秋季学期	研究生英语基础技能		1.0	免修	公共学位课	2021-2022学年夏季学期	物联网信息安全技术与应用基础		2.0	89	专业学位课
2021-2022学年冬季学期	计算机安全		2.0	88	专业选修课	2021-2022学年夏季学期	工程伦理		2.0	83	公共学位课
2021-2022学年秋冬季学期	中国特色社会主义理论与实践研究		2.0	85	公共学位课	2021-2022学年夏季学期	大数据与人工智能工程应用		2.0	82	专业学位课
2021-2022学年秋冬季学期	研究生论文写作指导		1.0	82	专业学位课	2021-2022学年春夏季学期	优化算法		3.0	98	专业选修课
2021-2022学年秋冬季学期	电子与信息工程技术管理		2.0	93	专业学位课	2021-2022学年夏季学期	移动互联网智能设备应用设计与实践		3.0	81	专业学位课
2021-2022学年冬季学期	研究生英语		2.0	免修	公共学位课	2022-2023学年冬季学期	大数据可视化的前沿技术		2.0	91	专业选修课
2021-2022学年春季学期	自然辩证法概论		1.0	84	公共学位课						

说明：1. 研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2. 备注中“*”表示重修课程。

学院成绩校核章：

成绩校核人：张梦依

打印日期：2024-04-02

Blockchain Multi-signature Wallet System Based on QR Code Communication

Hongxin Zhang[1], Xin Zou[1], Guanghuan Xie[1], and Zhuo Li[2(✉)]

[1] College of Computer Science and Technology, Zhejiang University, Hangzhou 310058, China
{zhx,22160282,looper}@zju.edu.cn
[2] Global Technology Service, State Street Technology (Zhejiang) Ltd., Hangzhou 310013, China
lizhuo@zju.edu.cn

Abstract. In order to avoid the risk of theft and loss of the private key of the blockchain wallet, a novel secure and stable blockchain multi-party signature system combining software and hardware is proposed. First, at the software level, multi-party key management method is adopted to divide the blockchain wallet key into multiple fragments for multi-point storage. Threshold signature technology is adopted to provide key escrow and retrieval services. Then a cold wallet for storing keys is designed at the hardware level. In order to avoid the risk of being attacked by hackers through network contact, a visible light communication method based on Quick Response Code is proposed. The Base45 coding scheme is adopted to improve the coding efficiency of QR Code, and the GG18 multi-party signature process is optimized. Finally, this paper analyzes the security of visible light communication, and verifies the efficiency of this method by experiments.

Keywords: Blockchain · Secure multi-party computing · Hardware wallet · QR Code encoding · Visible light communication · Digital asset escrow

1 Introduction

In blockchain transactions, users need to use the key for transaction signature, which is independent of the real identity. Therefore, the key controls the whole life system of the wallet, and the leakage of the key will cause irreparable loss to the assets stored in the wallet address. Key management includes storage, backup, recovery, and transaction review, and it requires high security and standardization. For common users, there is a need to digital asset escrow service.

Digital asset escrow services refer to digital currency escrow and trading services provided by third parties. There are various forms of escrow, such as wallets, custodians, etc. The core service is to provide digital currency deposits and withdrawals. Since the development of digital asset custodians, the leading

Y. Sun et al. (Eds.): CBCC 2022, CCIS 1736, pp. 31–48, 2022.
https://doi.org/10.1007/978-981-19-8877-6_3

经检索“Engineering Village”，下述论文被《Ei Compendex》收录。（检索时间：2023 年 8 月 11 日）。

<RECORD 1>
Accession number:20225313322366
Title:Blockchain Multi-signature Wallet System Based on QR Code Communication
Authors:Zhang, Hongxin (1); Zou, Xin (1); Xie, Guanghuan (1); Li, Zhuo (2)
Author affiliation:(1) College of Computer Science and Technology, Zhejiang University, Hangzhou; 310058, China; (2) Global Technology Service, State Street Technology (Zhejiang) Ltd., Hangzhou; 310013, China
Corresponding author:Li, Zhuo(lizhuo@zju.edu.cn)
Source title:Communications in Computer and Information Science
Abbreviated source title:Commun. Comput. Info. Sci.
Volume:1736 CCIS
Part number:1 of 1
Issue title:Blockchain Technology and Application - 5th CCF China Blockchain Conference, CBCC 2022, Proceedings
Issue date:2022
Publication year:2022
Pages:31-48
Language:English
ISSN:18650929
E-ISSN:18650937
ISBN-13:9789811988769
Document type:Conference article (CA)
Conference name:5th CCF China Blockchain Conference, CBCC 2022
Conference date:December 23, 2022 - December 25, 2022
Conference location:Wuxi, China
Conference code:287889
Publisher:Springer Science and Business Media Deutschland GmbH
Number of references:25
Main heading:Blockchain
Controlled terms:Efficiency - Personal computing - Signal encoding - Visible light communication
Uncontrolled terms:Block-chain - Digital asset escrow - Digital assets - Encodings - Hardware wallet - Multi-signature - Private key - QR code encoding - QR codes - Secure multi-party computing
Classification code:716.1 Information Theory and Signal Processing - 717.1 Optical Communication Systems - 723.3 Database Systems - 723.5 Computer Applications - 913.1 Production Engineering
DOI:10.1007/978-981-19-8877-6_3
Database:Compendex

注：
1. 以上检索结果来自 CALIS 查收查引系统。
2. 以上检索结果均得到委托人及被检索作者的确认。

教育部科技查新工作站（Z09）
检索人（签章）：朱佩
2023 年 8 月 11 日