同行专家业内评价意见书编号：20250854421

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： 王晨皓

学号： 22260291

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

2025年03月24日

填表说明

一、本报告中相关的技术或数据如涉及知识产权保护、军工项目保密等内容，请作脱密处理。

二、请用宋体小四字号撰写本报告，可另行附页或增加页数，A4纸双面打印。

三、表中所涉及的签名都必须用蓝、黑色墨水笔，亲笔签名或签字章，不可以打印代替。

四、同行专家业内评价意见书编号由工程师学院填写，编号规则为：年份4位＋申报工程师职称专业类别(领域)4位+流水号3位，共11位。

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掌握情况(不少于200字)

本人在计算机技术领域有较好的基础理论知识和专业技术知识掌握能力。

1.基础能力方面：在数学层面，通过离散数学、概率统计、线性代数等课程，掌握了算法复杂度分析、密码学原理、图形学矩阵运算等核心数学工具；硬件层面，重点学习了计算机组成原理、数字逻辑等硬件理论；在软件层面，系统掌握了数据结构与算法设计、数据库系统、编译原理、计算机网络、操作系统等核心课程。

2.专业技术知识方面：本人主攻区块链技术应用方向，基础及专业知识方面，深入掌握密码学核心理论（如哈希函数、椭圆曲线加密、零知识证明）、分布式系统共识算法（PBFT、PoW、PoS等）、默克尔树数据结构等，应用能力方面，本人熟悉HyperledgerFabric区块链平台相关开发，擅长联盟链网络构建与部署和智能合约开发部署，同时熟悉常见访问控制策略和分布式数字身份架构与实现。

2.工程实践的经历(不少于200字)

1.本人在杭州云象网络科技有限公司有长达半年的实习经历，参与实验室与云象合作的基于区块链的BIM项目资料管理系统横向课题，主要研究内容为（1）研究基于区块链的文档资料共享服务的主客体身份认证与识别技术：结合生物特征识别、数字水印等技术，研究基于区块链的工程资料共享服务主客体身份链构技术和主客体身份识别方法，为构建安全共享环境奠定技术基础。（2）研究基于区块链的文档资料数字资源确权与侵权追踪技术：针对传统集中化的数据库技术在构建数字资源服务平台时，面临侵权且难以追踪的问题，研究基于区块链数字资源确权与侵权追踪技术。（3）研究面向区块链的文档资料数据共享服务敏感信息隐私保护技术：由于区块链的公开、透明特性，以及服务提供商联盟链、多链之间跨链数据共享的场景，将增加共享数据隐私泄露的风险。

2.本人在上海腾讯网络科技有限公司有3个月的实习经历，主要工作为（1）修改redis用户排队队列存储结构，优化用户排队机制；增加基于地域就近的用户设备分配策略。（2）开发效率工具，统计工单系统中开发人员工时数据，显示在自定义卡片中，用cron定时任务实时刷新。（3）完成虎牙渠道商需求，开发SDK接口赋予云游戏接入能力，包括回调鉴权、设备分配、设备回收等。

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（不少于1000字）

本人有长达半年全程参与实验室与杭州云象网络科技有限工作合作的基于区块链的BIM项目资料管理系统横向课题，并在其中负责需求分析、后端开发、区块链开发和前端的联调工作。

由于BIM具备非结构化、规模大、产权保护需求高的特性，经过调研，我发现传统的BIM数据共享平台通常将BIM保存在中心数据库中，采用中心化的身份体系控制用户对数据的访问权限，存在用户身份信息不互通、权限控制细粒度不足等痛点。因此，我凝练了两条技术路线，其一是针对用户身份不互通、身份中心存储易受单点攻击等问题，提出了一种基于联盟链的去中心化数字身份管理架构与方法；其二是针对BIM访问控制细粒度不足、数据流通

过程中易被篡改侵权的问题，提出了一种基于属性加密和可验证凭证的细粒度访问控制方法

1.基于联盟链的去中心化数字身份管理架构与方法

该方法包含架构设计、管理方法流程实现和安全性分析三部分。

在架构设计部分，受W3C提供的去中心化数字身份规范启发，我基于MVC模式，设计了一个包含四层的架构，自下而上分别为：a.区块链层：选用HyperledgerFabric作为底层区块链基础设施。该层主要负责存储DID文档、VC索引和去中心化密钥索引等小容量关键数据，并在各个节点部署智能合约供上层安全访问区块链账本数据。b.扩展存储层：选用IPFS构建了私有节点集群，用于存储一些大容量加密数据或存在分布式存储需求的数据如加密VC文档和用户私钥分片等。c.服务层：包括DID解析器、去中心化身份管理SDK和去中心化密钥管理SDK等关键组件。DID解析器支持多种DID方法，是BIM-DID水平扩展的保障，其主要用于解析建筑部门用户传入的JWS并验证DID的归属有效性，负责获取DID文档中的字段并转发给对应的SDK服务模块。向上提供身份管理接口和密钥管理接口，包括DID的注册与更新、DID注销或转移、可验证凭证签发等；向下与区块链账本和IPFS交互，获取数据并作逻辑处理。d.应用层：包括三类参与方：发证方、用户、验证方。用户和验证方包括建筑领域设计方、施工方、监理方下的相关个体用户，发证方为具备能力验证用户申请凭证信息的可靠建筑部门。提供JWS模块，用于封装可验证凭证、DID文档等相关数据，实现与服务层的加密通信；提供选择性披露模块，为用户提供最小化暴露属性服务，提升用户属性的隐私性。

在管理方法流程实现部分，基于需求分析，我设计了一个包含DID申请、VC申请与颁发和VP生成与验证的三阶段流程实现。a.DID申请阶段：包含用户提出申请、公私钥生成、DID和DID文档生成三个阶段。b.VC申请与颁发阶段：包含用户提出申请、申请材料转发、VC颁发三个阶段。c.VP生成与验证阶段：包含VP生成与VP验证两个阶段。

在安全性分析部分，我发现在现有的去中心化身份管理架构与方法中，不同建筑项目参与方如施工方、设计方等需要验证用户的某些属性以确定其访问某些敏感数据的资格和权限，例如设计方需要验证某建筑部门用户是否属于特定单位、施工方需要验证某建筑部门用户是否具有特定施工资质等，这些验证方通常只需要验证某些关键信息，但用户的一个完整VC文档中通常包含一些不必要的敏感信息，如果用户直接提供完整的VC供验证方验证，可能导致其他无关敏感信息被泄露的问题。因此，我补充了基于默克尔树的选择性披露方法，该方法主要分为三个阶段：默克尔树生成、选择性披露属性、选择性披露验证。同时，在本方法中，用户私钥承担着签名VC、生成VP以及注册DID等关键职责，需要一个良好的保存方案。经过调研，我发现传统的用户私钥管理模式一般分为两种：集中式管理和用户自行管理。然而，这两种方式都存在一定的风险。集中式的私钥管理方案存在明显的单点故障风险，一旦私钥管理平台遭受攻击或崩溃，用户的私钥可能被盗取或丢失，导致身份管理方案崩溃。用户自行管理的方案存在设备丢失导致的私钥泄漏等风险。因此，我提出了一种基于Shamir秘密共享的去中心化私钥管理方案。

2.基于属性加密和可验证凭证的细粒度访问控制方法

该方法包括架构设计、实施流程两个部分。

在架构设计部分，基于提出的去中心化数字身份管理架构与方法，设计了一个包含数据提供方（Data Provider, DP）、数据请求方（Data Requester,DR）、BIM元数据链及访问控制智能合约、可信执行环境（TEE）、星际文件系统（IPFS）和去中心化身份管理系统的整体架构并编写了相关智能合约。

在实施流程部分，我设计了一个包含了方法初始化、BIM侵权校验、BIM数据上传、BIM数据请求四个阶段的流程，主要是基于CP-ABE属性加密算法属实现了一套完整的细粒度的BIM访问控制流程。特别的，我在流程中还提出了一种针对OBJ格式的BIM数据侵权检测算法，并通过智能合约实现了用户级的可撤销机制，保障了BIM数据在共享过程中的安全性与隐私性。然后，通过与其他相关研究的功能性对比和方案的安全性分析，验证了本方案在细粒度访问控制与数据安全性方面的优势。最后，通过性能测试验证了本方法的可行性。

最后，我基于设计的去中心化数字身份管理架构与方法和基于属性加密和可验证凭证的细粒度访问控制方法，提出并实现了一个面向建筑领域的BIM可信共享系统。首先是对系统需求进行分析，包括功能性需求分析和非功能性需求分析两类；随后，明确了系统的架构设计和技术路线，技术路线包括前端、后端和区块链三类。最后对系统的功能作了完备的测试，包括JMeter压力测试、功能测试、Caliper区块链性能测试等，最后结果表明，该原型系统在具备充分安全性的同时，具备相当的可用性。

（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
一种基于 SGX 和 CP-ABE 的区块链 BIM 数据共享系统及方法	发明专利申请	2024年08月26日	申请号：202411174670.5	2/7	已进入实质审查
一种支持抗女巫攻击的可追溯去中心化数字身份认证方法及系统	发明专利申请	2024年08月30日	申请号：202411206207.4	4/6	已进入实质审查

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： 86 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 年（要求1年及以上） 考核成绩： 81 分
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：**	

2226029

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）：2022年3月24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：22260291	姓名：王晨皓	性别：男	学院：工程师学院	专业：电子信息	学制：2.5年
毕业时最低应获：24.0学分		已获得：27.0学分		入学年月：2022-09	毕业年月：
学位证书号：			毕业证书号：		授予学位：

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
2022-2023学年秋季学期	数值计算方法		2.0	90	专业选修课	2022-2023学年秋冬学期	高阶工程认知实践		3.0	82	专业学位课
2022-2023学年秋季学期	研究生英语基础技能		1.0	免修	公共学位课	2022-2023学年冬季学期	产业技术发展前沿		1.5	80	专业学位课
2022-2023学年秋季学期	研究生英语能力提升		1.0	免修	跨专业课	2022-2023学年秋冬学期	研究生论文写作指导		1.0	88	专业选修课
2022-2023学年秋季学期	工程技术创新前沿		1.5	90	专业学位课	2022-2023学年春季学期	自然辩证法概论		1.0	91	专业学位课
2022-2023学年秋季学期	研究生英语		2.0	免修	专业学位课	2022-2023学年春夏学期	优化算法		3.0	92	专业选修课
2022-2023学年秋季学期	新时代中国特色社会主义理论与实践		2.0	89	专业学位课	2022-2023学年夏季学期	机器学习		2.0	83	跨专业课
2022-2023学年秋季学期	数据科学技术与软件实现		2.0	90	专业学位课		硕士生读书报告		2.0	通过	
2022-2023学年秋冬学期	工程伦理		2.0	94	专业学位课						

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：2025-03-20

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119150350 A
(43)申请公布日 2024.12.17

(21)申请号 202411174670.5

(22)申请日 2024.08.26

(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号

(72)发明人 陈建海 王晨皓 董冬 王奕涵 刘振广 沈睿 何钦铭

(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 郑海峰

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/64(2013.01)
G06F 21/60(2013.01)
G06Q 40/04(2012.01)
H04L 9/00(2022.01)

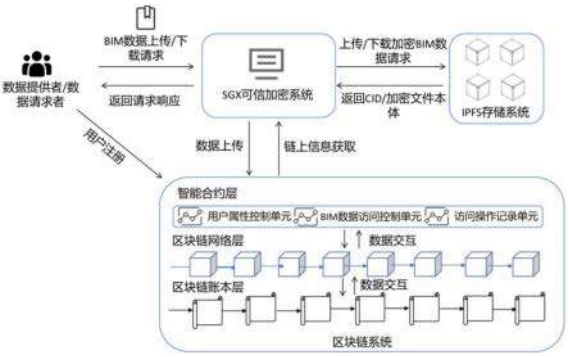
权利要求书2页 说明书7页 附图5页

(54)发明名称

一种基于SGX和CP-ABE的区块链BIM数据共享系统及方法

(57)摘要

本发明公开了一种基于SGX和CP-ABE的区块链BIM数据共享系统及方法,属于区块链技术领域。系统包括SGX可信加密系统、IPFS存储系统和区块链系统;进行用户注册时,区块链系统接收外部输入的用户属性信息并存储;接收BIM数据上传请求时,所述加密系统会接收待上传的数据并进行加密,将加密后的数据上传至所述存储系统进行存储,并接受所述存储系统返回的CID,再将该CID输入至区块链系统;接收BIM数据下载请求时,所述加密系统基于区块链系统获得待下载的数据的CID,再基于该CID从所述存储系统获得待下载的数据并输出。本发明的共享系统可为工程部门提供BIM数据细粒度共享服务,并可保证在共享过程中BIM数据和密钥不泄漏和被篡改。



CN 119150350 A

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118900182 A
(43)申请公布日 2024.11.05

(21)申请号 202411206207.4
(22)申请日 2024.08.30
(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号
(72)发明人 陈建海 薛凤泽 黄恩浩 王晨皓 何钦铭 刘振广
(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 郑海峰
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 9/00(2022.01)
H04L 9/30(2006.01)
H04L 9/40(2022.01)

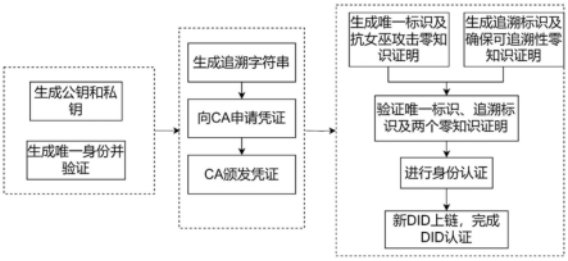
权利要求书3页 说明书8页 附图4页

(54)发明名称

一种支持抗女巫攻击的可追溯去中心化数字身份认证方法及系统

(57)摘要

本发明提出了一种支持抗女巫攻击的可追溯去中心化数字身份认证方法及系统,包括监管委员会模块、用户模块、CA模块和区块链模块,监管委员会模块生成公钥和私钥,用户模块获得待进行身份认证的用户的追溯字符串、唯一字符串和用户属性信息,并对追溯字符串进行加密,CA模块基于用户属性信息和加密后的追溯字符串生成凭证;用户模块生成唯一标识、追溯标识、抗女巫攻击零知识证明和确保可追溯性零知识证明;区块链模块对两个零知识证明进行验证,若验证成功,则进行去中心化数字身份认证;若验证失败,则不进行去中心化数字身份认证,身份认证失败。本发明保证了用户的隐私安全、保证DID不可篡改且不受第三方中心机构的控制。



CN 118900182 A