基于区块链的物联网卡安全流转方法研究

韩宇龙[1],肖 青[2],柳耀勇[1],孙东昱[1],王政宏[1]
(1.中移物联网有限公司 集成电路创新中心,北京 100037;2.芯昇科技有限公司,江苏 南京 210018)

摘 要:针对物联网卡非法流通现象严重、监管溯源工作困难的问题,运用区块链为核心技术,结合物联网技术,设计物联网卡安全流转方法和系统。该系统由区块链系统、信息系统、区块链终端、微信小程序组成,安全流转过程包括卡信息初始录入、转出申请、转入确认和溯源查询。该系统采用智能合约实现流转过程规则,分布式存储信息摘要和物权变更信息,数据库集中式存储物联网卡 ICCID 号段和信息摘要对应关系,SE-SIM 实现终端密钥存储和数字签名。经试点验证和分析,该系统能够保证溯源数据安全可信,兼顾批量并发性能,并提高监管效率。

关键词:区块链;物联网卡;安全流转;信息摘要;SE-SIM
中图分类号:TN914;TP302.1 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.211395

中文引用格式:韩宇龙,肖青,柳耀勇,等. 基于区块链的物联网卡安全流转方法研究[J].电子技术应用,2021,47(12):110-115.
英文引用格式:Han Yulong,Xiao Qing,Liu Yaoyong,et al. IoT card secure transfer method research based on blockchain[J]. Application of Electronic Technique,2021,47(12):110-115.

IoT card secure transfer method research based on blockchain

Han Yulong[1],Xiao Qing[2],Liu Yaoyong[1],Sun Dongyu[1],Wang Zhenghong[1]
(1.IC Innovation Center,China Mobile IoT Company Limited,Beijing 100037,China;
2.Xinsheng Technology Company Limited,Nanjing 210018,China)

Abstract:Aiming at the problems of IoT card, such as serious illegal circulation, difficult supervise and traceability, an IoT card secure transfer method and system are designed. The system includes a blockchain subsystem, an information subsystem, some blockchain devices and a WeChat applet, and its secure transfer procedure includes initial entry of card information, transfer out application, transfer in application and traceability queries. Blockchain smart contract is used to implement circulating traceability rules, blockchain is used to implement distributed storage of message digest and possession change information, database is used to implement centralized storage of correspondence between IoT card ICCID number range and message digest, and SE-SIM is used to implement device key storage and digital signature. Through actual pilot application and analysis, the system can ensure the safety and credibility of traceability data, consider the batch concurrency performance, and improve the efficiency of supervision.
Key words:blockchain;IoT card;secure transfer;message digest;SE-SIM

0 引言

根据 GSMA 和 Machina 统计和预测,2020 年全球物联网连接数量达 126 亿,未来 5 年平均增长率达 15%,而中国物联网连接数增长率高于世界水平。蜂窝通信(2G/3G/4G/5G、NB-IoT、eMTC 等)物联网作为一种广域通信物联网技术,已经成为运营商大连接战略背景下的物联网未来发展主要形式[1]。物联网卡作为蜂窝通信物联网接入网络的媒介,开卡规模和用户规模与日俱增,用户涉及行业极其广泛[2]。但是,物联网卡在基本功能设计上相对于普通电信卡并无明显差别,且流量资费优惠力度明显,导致功能滥用和违规倒卖等情况频发。

为有效管理物联网卡风险监控和使用安全,国内诸多专家学者进行了一定的研究和探索[3-5]。然而,研究方向集中在业务滥用、机卡分离等运营方面,而从源头风险管控、准确流转溯源方面的研究较少。因此,通过技术手段解决物联网卡流转过程规则实现、转移登记、数据存储、安全分享,有助于物联网卡安全管理实现闭环。

区块链技术是具有去中心化、支持多元参与、信息防篡改、高度自治等特点的集成应用;基于区块链的身份认证、敏感数据传输安全保护、用户数据安全和跟踪核实存证、多组织协作等应用探索逐渐成熟[6-9]。因此,应用区块链支撑物联网卡安全流转具备潜能。本文基于区块链的分布式账本技术以及物联网安全技术,提出一种物联网卡安全流转方法和系统实现,保证物联网卡交易流转相关信息能够可靠登记上链、精准高效溯源,并降低监管难度。

1 区块链技术与 SE-SIM

1.1 区块链技术

区块链技术最初作为比特币应用的底层技术，起源于文献[10]。区块链对传统商业业务流程引入了突破性变革，因为传统商业业务流程的应用和交易需要中心化机构或可信第三方来验证，而区块链采取去中心化的方式实现了同样的信任级别。区块链技术架构和设计的固有特性提供了透明性、健壮性、可审计性和安全性等属性[11-13]，因此，区块链能够改变传统的社会信任机制和社会生产关系。

智能合约是一种用数据算法和软件程序来编制合同条款、部署在区块链上且可按照规则自动执行的数字化协议，起源于文献[14]。智能合约初期由于计算条件的限制和应用场景的缺失，并未受到研究者的广泛关注，直到区块链技术出现，智能合约被重新定义。区块链实现了去中心化的存储，智能合约则在其基础上实现了去中心化的计算[15]。

1.2 SE-SIM

SE-SIM 是中移物联网有限公司自研的物联网安全芯片，拥有安全单元 SE[16]、抗紫外线安全存储、硬件加密模块和真随机数发生器等特点，较传统的软件加密和可信执行环境(Trust Execution Environment，TEE)方案具有显著更高的安全等级，能够抵抗实验室级软件及物理攻击。同时，SE-SIM 具有 SIM 的载体功能，通过将两种能力结合，为客户提供数字签名、通信加密、终端保护的功能。

2 物联网卡安全流转系统设计

2.1 物联网卡流转特点分析

(1)ToB 和 ToC 场景

物联网卡流转根据最终环节不同，可以分为 ToB-企业消费者和 ToC-个人消费者 2 种场景。

(2)集成电路卡识别码唯一标识

物联网卡使用集成电路卡识别码(Integrate Circuit Card Identity，ICCID)作为唯一物理标识，运营商掌握 ICCID 与国际移动用户识别码(International Mobile Subscriber Identity，IMSI)和移动用户号码(Mobile Subscriber International ISDN，MSISDN)对应关系。

(3)批量连续 ICCID 流转

物联网卡 ToB 场景所有流转环节，以及物联网卡 ToC 场景除最终环节外的所有环节，通常为批量连续 ICCID 形式流转。流转载体通常以“箱”或“盒”为单位，且其包装上会印有起止 ICCID 号生成的条形码标识。

(4)流通隐私保护

物联网卡流转过程中，隐私数据(ICCID 明文、物权所有者身份等)不适合分布式存储。每个参与方应只能访问自身经手的物联网卡流转的一级上游和一级下游，监管方能够访问所有物联网卡全流程流转信息。

2.2 系统设计思路

物联网卡安全管理主要针对的是物联网卡运营商运营、代理商/分销商销售、设备制造商装配、个人使用等过程间流转的安全监管问题。通过区块链技术、平台技术、数字密码技术、物联网技术等实现物联网卡初始数据存证、物权流转变更、角色权限控制、数据溯源查询等功能。

经过对物联网卡流转特点分析，系统设计思路如下：使用 Hash 算法对批量 ICCID 进行标识；使用中心化数据库存储 Hash 值和批量 ICCID 对应关系；使用区块链存证 Hash 值所有权和流转信息；使用智能合约实现流转过程的确权验证、物权转移、溯源查询权限规则；使用终端实现批量卡 ICCID 信息自动化采集和交易申请；使用 SE-SIM 保证终端身份安全和信息安全；使用微信小程序支持 C 类消费者。

2.3 系统架构设计

本文提出的物联网卡安全流转系统主要包括区块链系统、信息系统、区块链终端、物联网卡流转助手微信小程序，如图 1 所示。其中，区块链底层框架使用 Hyperledger Fabric，选择 3 个背书节点部署智能合约(身份管理、物权流转)，外部通过区块链网关 API 访问区块

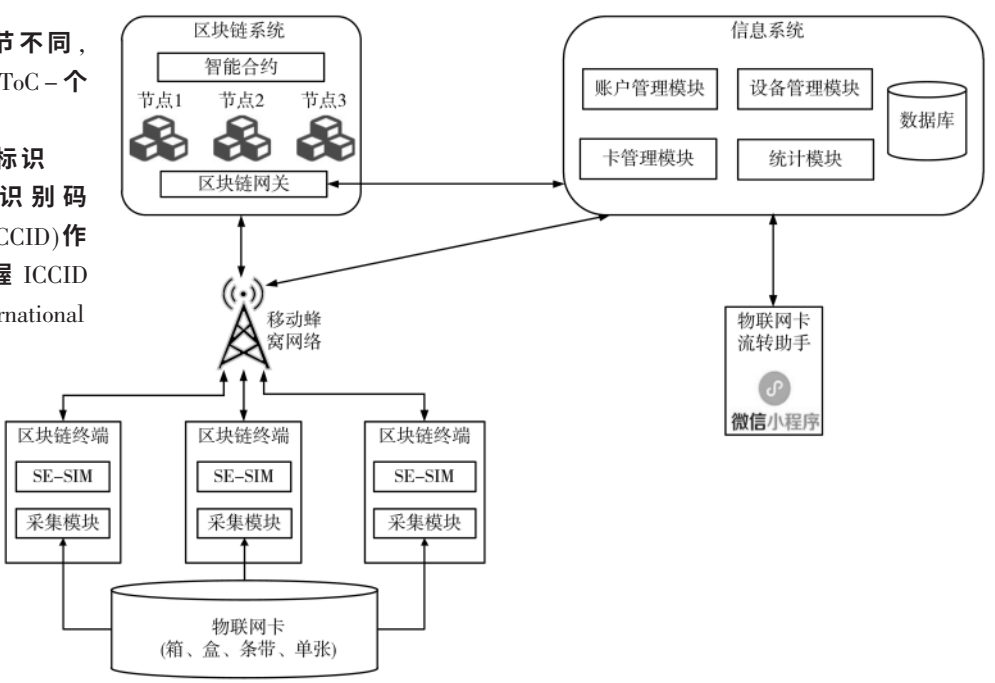

图 1 物联网卡安全流转系统架构图

《电子技术应用》http://www.chinaaet.com

链服务；信息系统主体功能模块包括账户管理模块、设备管理模块、卡管理模块、统计模块，通过平台技术实现用户可视化操作界面、账户区块链秘钥托管、物联网卡批量信息和物权 Hash 的对应关系生成和维护；区块链终端为安装有 SE-SIM 和客户端 APP 的移动通信设备，用于运营商和企业用户执行物联网卡信息自动化采集、流转申请、确认和权限验证等操作；微信小程序用于个人用户执行流转确认操作。

2.4 系统业务逻辑

物联网卡安全流转方法业务逻辑包括卡信息初始录入、转出申请、转入确认、溯源查询 4 个层级，如图 2 所示。

2.4.1 卡信息初始录入

运营商登录信息系统，通过导入.xls 列表或者人工录入的方式录入卡信息(ICCID、IMSI 和 MSISDN)。信息系统本地数据库维护卡信息表，内容包括 ICCID、IMSI、MSISDN、

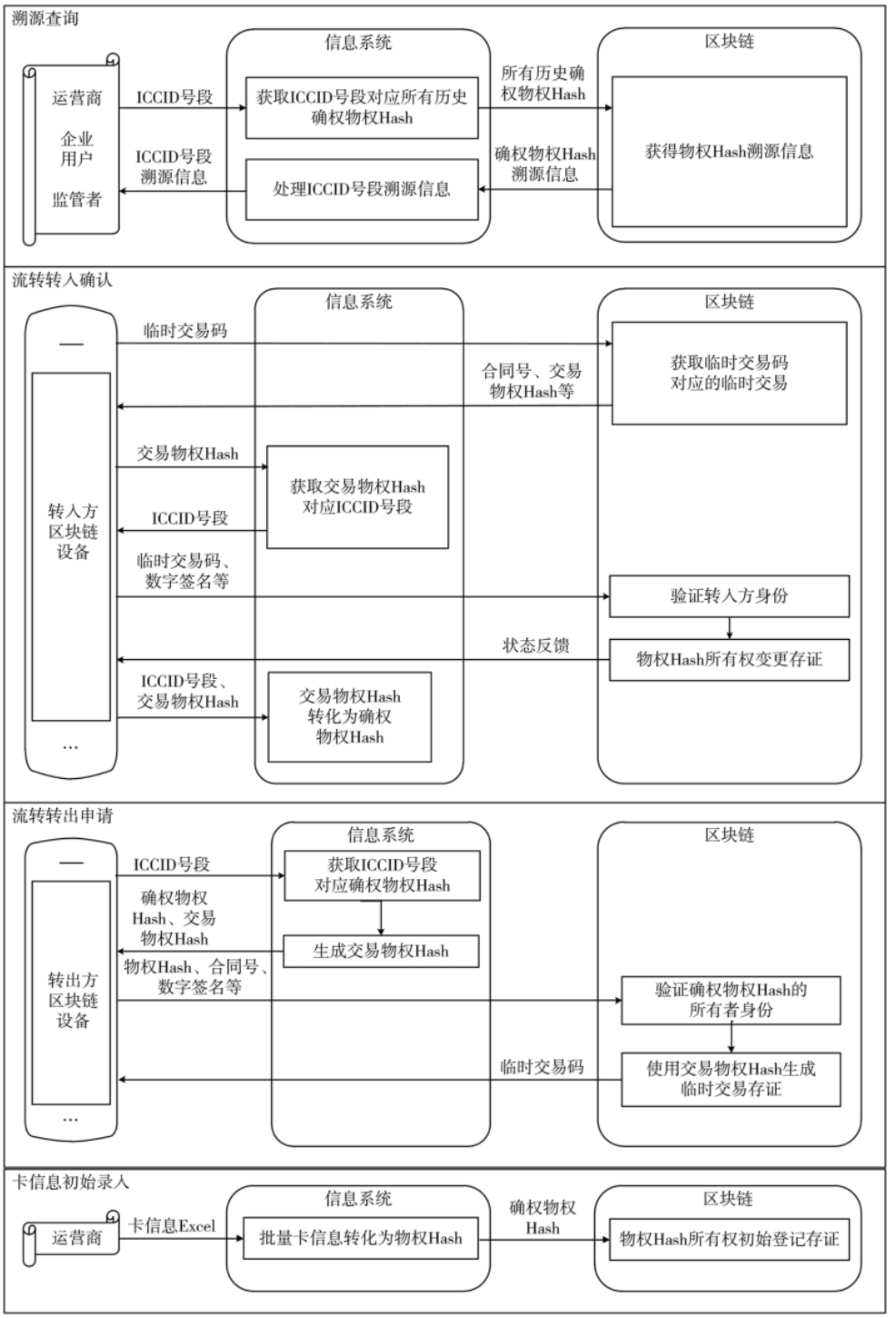

图 2 物联网卡安全流转方法业务逻辑图

所属运营商、组织号、导入时间等。

信息系统通过 SHA256 算法对 ICCID 号段进行计算，获得确权物权 Hash。ICCID 号段的组织方法为：连续号将首末两个号通过“-”相连，其他单独枚举号通过“,”相连，形式如“A1-An，B1，C1-Cm”。信息系统本地数据库维护交易历史信息表，内容包括 ICCID、当前位置组织号、确权物权 Hash、创建时间等。

信息系统调用区块链智能合约 API 接口，将确权物权 Hash-其所有权信息的键值关系存证在区块链分布式账本。

2.4.2 转出申请

转出方(运营商或企业用户)使用区块链终端采集需要流转的 ICCID 号段(通过二维码扫描、条形码扫描、人工录入等方式)，然后调用信息系统 API 接口 transRecenthash，将 ICCID 号段转化为交易物权 Hash，同时获得 ICCID 号段在交易历史信息表中对应的最近 1 次的所有确权物权 Hash。信息系统本地数据库维护交易当前信息表，内容包括 ICCID、当前位置组织号、交易物权 Hash、创建时间等。

区块链终端调用区块链智能合约 API 接口，首先验证自身是所有确权物权 Hash 的当前拥有者身份；通过验证后，区块链智能合约使用 CRC 算法对包括转出申请时间戳、转出者 ID、交易物权 Hash 等内容做运算，获得长度不超过 8 B 的临时交易码。将临时交易码-物权变更内容的键值关系存证在区块链分布式账本。

2.4.3 转入确认

转入方(企业用户)使用区块链终端调用区块链 API 接口，从区块链分布式账本查询临时交易码对应的临时交易(交易物权 Hash 和物权变更内容)，调用信息系统API 接口 transConfirm，将交易物权 Hash 转化为 ICCID 号段。通过验证线下实物，转入方选择是否对临时交易做确认。

区块链终端调用区块链智能合约 API 接口，验证自身是交易物权 Hash 物权变更转入者身份；通过验证后，将交易物权 Hash-物权变更内容的键值关系存证在区块链分布式账本，同时删除临时交易码-物权变更内容的键值关系。

区块链终端调用信息系统 API 接口 transSuccess，将交易物权 Hash 转化为确权物权 Hash。信息系统随即将对应当前交易从交易当前信息表中删除，并添加到交易历史信息表。

此外，如果转入方是个人用户，使用微信小程序实现相近过程，微信小程序直接与信息系统后台对接，信息系统后台托管公共用户的身份密钥。

2.4.4 溯源查询

运营商、企业用户、监管者登录信息系统，通过多种过滤条件(ICCID、组织号、登记时间等)选中需要进行溯源查询的物联网卡 ICCID。信息系统从本地维护的交易历史信息表获得该 ICCID 对应的所有历史确权物权 Hash。

信息系统调用区块链智能合约 API 接口，获取每个历史确权 Hash 对应的溯源信息(生命周期中所有物权变更信息)；然后处理和拼接 ICCID 溯源信息并展示。通过权限控制，保证每个角色只能访问其自身经手的物联网卡流转的一级上游和一级下游。溯源查询流程如图 3 所示。

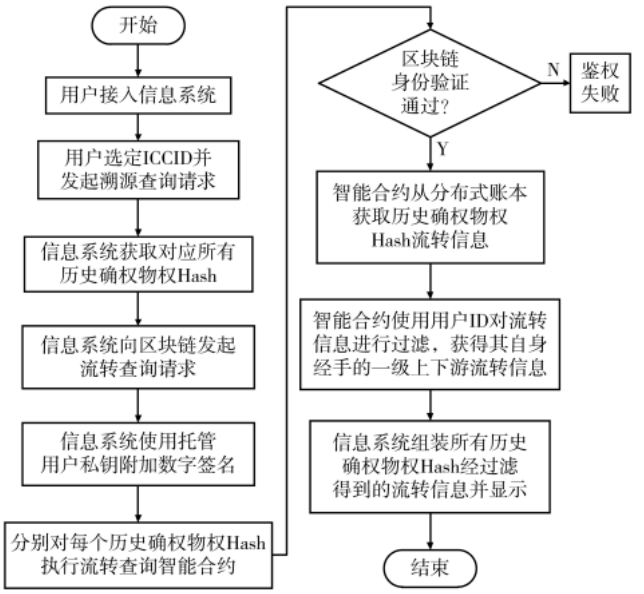

图 3 溯源查询流程图

2.5 智能合约设计

分布式应用(DAPP)程序的开发最重要一环是智能合约的开发和处理。本系统智能合约功能逻辑划分为身份管理合约和物权流转合约两部分，如图 4 所示。其中，身份管理合约负责所有参与角色的区块链身份创建、查询、更新以及智能合约调用签名验证机制；物权流转合约负责物权存证、查询、验证、更新以及物权流转变更机制。身份管理合约和物权流转合约两者处于同一通道 channel，之间通过 InvokeChaincode 跨合约调用机制连接。

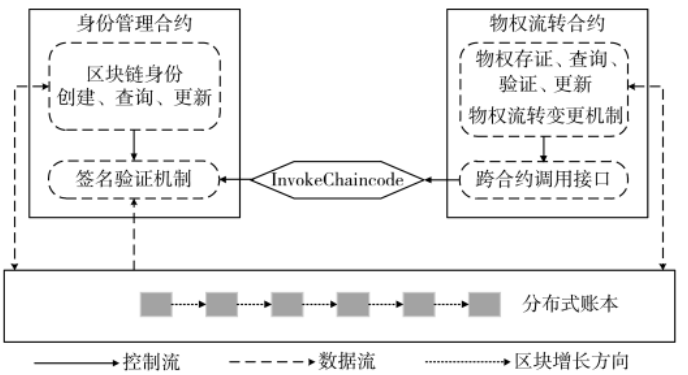

图 4 智能合约功能逻辑设计图

2.6 安全接入设计

所有业务参与实体调用区块链服务都需经历通信加密和身份验证环节。具体地：(1)业务端与区块链网关

之间采用 HTTPS 通信协议，保证通信安全；(2)业务端使用国密 SM2 数字签名，智能合约进行签名验证，保证数据完整性和来源可信。其中，HTTPS 保证通信安全已是成熟方案，以下重点介绍数字签名密钥分发设计，如图5所示。

SE-SIM 内部使用 SN 号作为信任根进行密钥分散，生成设备身份公私钥对；SE-SIM 对设备身份私钥进行防护留存(外部无法读取)，将设备身份公钥吐出并存证到区块链分布式账本。信息系统内部通过软件方式生成账号身份公私钥对；信息系统本地托管账号身份私钥并保存与账户名对应关系，将账号身份公钥存证到区块链分布式账本，从而实现业务端在区块链智能合约的合法调用身份。同时，SE-SIM 和信息系统本地应保存区块链网关身份公钥并对区块链响应中附加的数字签名进行验证，实现区块链服务申请和响应的双向身份认证。

3 物联网卡安全流转系统实现

3.1 系统部署和展示

基于上述物联网卡安全流转系统架构和业务逻辑设计，实现了基于区块链的物联网卡安全流转系统，并展开实际部署工作：区块链系统部署于 BSN 北京、苏州、武汉 3 个城市节点，每个城市节点创建 3 个对等节点。信息系统部署在中移物联网有限公司的 4A(认证 Authentication、授权 Authorization、账号 Account、审计 Audit)私有云资源池中。为验证流转追溯系统技术和方案可行性，使用部署的系统开展试点应用。试点应用针对天津消防的对讲机物联网卡使用场景对 100 张真实物联网插拔卡的流通进行存证和溯源。

监管者登录信息系统，能够查询任一张物联网卡的“流转详情”，如图 6 所示。界面会展示所选定物联网卡物权流转变更的所有历史信息，包括登记单位、登记时间、转出申请和转入确实的时间和所使用的区块链设备编号，以及每一步操作的区块链 TXID(交易唯一标识号)。选中 TXID 则可以查看对应区块链交易和区块信息。

图 6 物联网卡流转详情展示

3.2 性能分析

运行于 BSN 城市节点性能参数为：并发量为 10 TPS、硬盘容量为 10 GB；信息系统性能参数为：核心数 4Kernel、内存为 8 GB；区块链终端性能参数为：处理器为高通骁龙 730G、运行内存 6 GB 的试点系统环境下，对 ICCID 为连续号并且卡数量分别为 1、10、100、1 000、5 000、10 000 的不同场景进行卡信息初始录入、转出申请、转入确认等操作，测试时间消耗。最终获得连续号批量处理性能

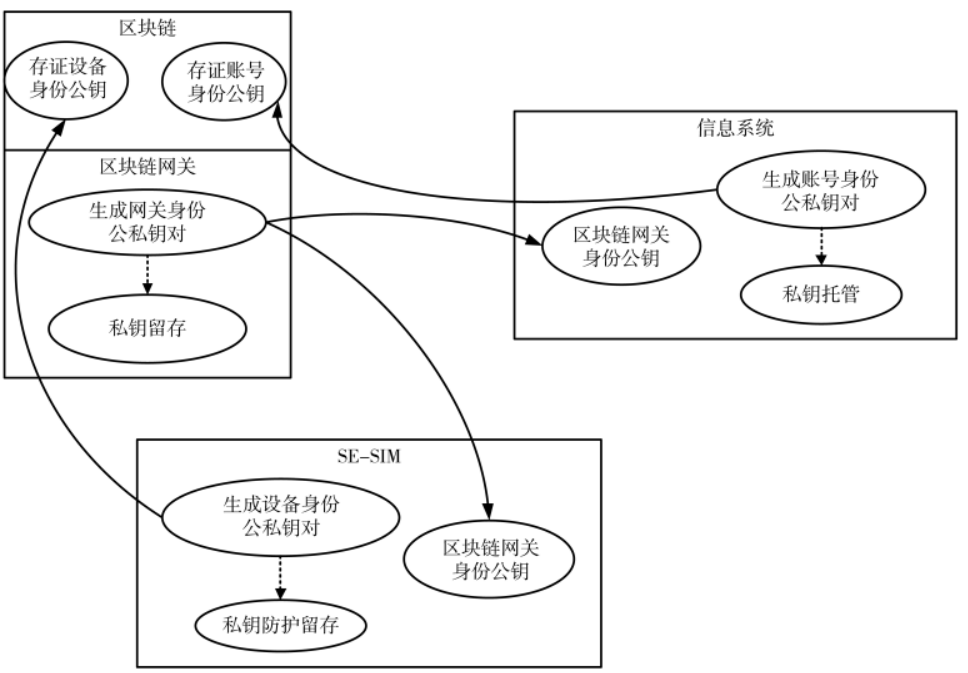

图 5 智能合约身份密钥分发设计

曲线图，如图 7 所示。其中，横坐标表示对单次处理的连续号卡数量进行以 10 为底数的对数值，纵坐标表示对应操作所消耗的时间。

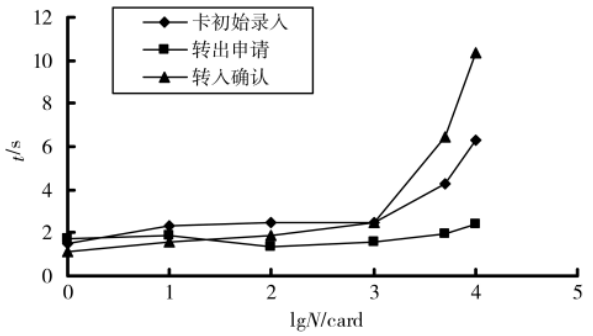

图 7 连续号批量处理性能曲线图

实验结果表明：(1)在操作 ICCID 为连续号且卡数量不超过 1 000 张时，系统整体性能趋于稳定；(2)在操作 ICCID 为连续号且卡数量超过1 000 张时，系统整体性能明显出现耗时长的现象，并且转入确认操作性能衰退最为明显，卡信息初始录入次之，转出申请影响极小。因此，在给定的试点试点系统环境下，为了追求良好系统使用体验，建议连续号批量操作保持在 1 000 张之内。

4 结论

本文针对当前物联网卡流转和使用过程中各种违规问题和危害影响进行分析，总结出通过技术手段解决物联网卡流转过程规则实现、转移登记、数据存储、安全分享等的重要解决途径，提出了以区块链技术为核心、结合物联网技术设计的物联网卡安全流转方法和系统实现。系统采用区块链智能合约实现流转过程规则、分布式存储信息摘要和物权变更信息、集中式存储物联网卡 ICCID 号段和信息摘要对应关系、SE-SIM 实现终端密钥存储和数字签名等方式，保证数据存储和数据来源安全可信性，同时兼顾系统批量大并发性能。最后，通过试点实例对物联网卡安全流转系统进行展示。结果表明，本文提出的方法和系统能够重塑信任体系，提高溯源精度并降低监管难度。

参考文献

[1] 秘俊杰，王超，卢凤晖，等.蜂窝物联网无线网络规划建设[J].电信科学，2018，34(S1)：98-103.
[2] 安宁宇，马东洋，粟栗，等.基于机器学习算法的物联网卡安全风险监测系统研究与实现[J].信息安全研究，2020，6(12)：1133-1138.
[3] 刘利军，赵蓓，张双.物联网卡安全监测模型及实践[J].电信工程技术与标准化，2020，33(5)：48-52.
[4] 赵俊，刘浩明，王伟杰.物联网卡业务运营风险监控系统的研究[J].电信工程技术与标准化，2019，32(1)：67-72.
[5] 刘宁宁，樊建勋.物联网卡违规应用浅析[J].网络空间安全，2019，10(1)：86-88.
[6] 黑一鸣，刘建伟，管晔玮.基于区块链的身份信息共享认证方案[J].密码学报，2020，7(5)：605-615.
[7] 许重建，李险峰.区块链交易数据隐私保护方法[J].计算机科学，2020，47(3)：281-286.
[8] 陈孝莲，虎啸，沈超，等.基于区块链的电力物联网接入认证技术研究[J].电子技术应用，2019，45(11)：77-81.
[9] 张金龙，赵德政，韩庆敏.一种基于区块链技术的工业数据安全性保护方法[J].电子技术应用，2019，45(7)：85-88.
[10] NAKAMOTO S.Bitcoin：a peer-to-peer electronic cash system[EB/OL].(2019-12-01)[2021-02-09].https://bitcoin.org/bitcoin.
[11] FRAN C，THOMAS K，DASAKLIS，et al.A systematic literature review of blockchain-based applications：current status，classification and open issues[J].Telematics and Informatics，2019，36：55-81.
[12] ZHENG Z B，DAI H N，CHEN X P，et al.Blockchain challenges and opportunities：survey[J].Int. J.Web and Grid Services，2018，14(4)：352-375.
[13] PRIMAVERA D F，MORSHED M，WESSEL R.Blockchain as a confidence machine：the problem of trust & challenges of governance[J].Technology in Society，2020，62：101284.
[14] SZABO N.Formalizing and securing relationships on public networks[EB/OL].(1997-09-01)[2021-02-09].http://dx.doi.org/ 10.5210/fm.v2ig.548.
[15] CHRISTIDIS K，DEVETSIKIOTIS M.Blockchains and smart contracts for the Internet of Things[J].IEEE Access，2016，4：2292-2303.
[16] 魏贵鹏，谢演，刘陟，等.基于移动设备 TEE 和 SE Java-COS 的安全解决方案的研究[J].通信技术，2020，53(12)：3056-3064.

(收稿日期：2021-02-09)

作者简介：

韩宇龙(1988-)，男，硕士，工程师，主要研究方向：区块链技术和应用。

肖青(1979-)，男，硕士，高级工程师，主要研究方向：物联网技术专家。

柳耀勇(1986-)，男，硕士，工程师，主要研究方向：物联网技术和安全技术。

扫码下载电子文档

版权声明