Software Engineering and Applications 软件工程与应用, 2022, 11(3), 494-503
Published Online June 2022 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2022.113052

Hans汉斯

基于区块链的可监管慈善系统设计与实现

杨铠铖[1,2]，陈玉玲[1]

[1]贵州大学计算机科学与技术学院公共大数据国家重点实验室，贵州 贵阳
[2]桂林电子科技大学广西密码学与信息安全重点实验室，广西 桂林

收稿日期：2022年4月18日；录用日期：2022年6月3日；发布日期：2022年6月13日

摘 要

近年来，中国慈善事业的快速发展带来了许多问题，现有的慈善管理系统是中心化的、慈善募捐过程不透明的，这导致了难以获得捐赠者的信任和捐赠。区块链的可信计算模型为解决上述问题提供了新思路。本文采用联盟链Hyperledger Fabric作为区块链平台实现了可监管慈善系统，制定了慈善项目发起、捐款、执行的智能合约，并设计了Charity Coin作为系统数字货币，保证捐款流向可追溯。最后，性能测试表明，该系统能够满足应用要求。

关键词

区块链，Hyperledger Fabric，慈善监管，智能合约

Design and Implementation of Blockchain-Based Regulated Charity System

Kaicheng Yang[1,2], Yulin Chen[1]

[1]State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang Guizhou
[2]Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin Guangxi

Received: Apr. 18th, 2022; accepted: Jun. 3rd, 2022; published: Jun. 13th, 2022

Abstract

In recent years, the rapid development of philanthropy in China has brought many problems. The existing charity management system is centralized and the process of charitable fundraising is not transparent, which makes it difficult to gain the trust and donation of donors. The trusted computing model of blockchain provides new ideas for solving the above problems. This paper uses the

文章引用: 杨铠铖, 陈玉玲. 基于区块链的可监管慈善系统设计与实现[J]. 软件工程与应用, 2022, 11(3): 494-503.
DOI: 10.12677/sea.2022.113052

consortium blockchain Hyperledger Fabric as the blockchain platform to implement a regulated charity system, formulates smart contracts for charitable project initiation, donation, and execution, and designs Charity Coin as the system digital currency to ensure that the flow of donations can be traced. Finally, performance tests show that the system can meet the application requirements.

Keywords

Blockchain, Hyperledger Fabric, Charity Regulation, Smart Contract

1. 引言

中共十九届四中全会上提出“重视发挥第三次分配作用，发展慈善等社会公益事业”[1]，这为中国慈善事业高质量发展指明了方向。目前，随着互联网技术不断发展，各种筹款捐助活动由传统的现金筹款转变为线上筹款。但线上筹款其不良事件也时有发生，存在的主要问题概括为以下三点：1) 信息披露不透明不规范，在现行的慈善系统中，由于人力物力等原因，每个慈善组织的信息披露和慈善项目的申请、审核标准不一，甚至产生不法分子诈捐，影响公众的捐款热情；2) 捐款流向不透明，大部分系统为中心化系统，捐款人对于捐款流向往往不清楚，容易产生内部人员挪用善款、篡改数据，造成恶劣的社会影响；3) 追责难，平台日志不规范，难以日常审计和突发事件的回溯[2]。因此，建立一套以国家监管部门及核心组织配合为主，行业自我约束为辅的慈善平台，创造有利于公益慈善健康发展的社会环境。

区块链上具有去中心化、可追溯不可篡改等特性[3] [4]，并可以通过智能合约[5]自动执行合同条款，天然适用于社会公益事业业务场景[6]。捐赠流程中的慈善项目发起、捐款流向、执行结果反馈都可以通过区块链技术进行信息上链[7] [8]，在发起项目审核通过后，将项目信息进行上链，用户可以对链上项目进行捐款，系统对非匿名用户捐款进行公开公示，方便社会公众对捐款流向进行监督，有利于慈善事业的健康发展。

2. 系统模型

为了业务完整性和数据安全，系统至少包括以下模块：身份和账户管理模块(IAM)、信息发布模块(CISM)、进展管理模块(CIPM)、慈善币管理模块(CCM)。在基于区块链的可监管慈善系统中，IAM 提供用户注册、登录、行为管理和其他功能，慈善组织和受益人使用 CISM 向区块链模块投放慈善信息，CIPM 用于记录和监管项目进展，CCM 用于用户和公益组织兑换慈善币。基于区块链的可监管慈善系统的区块链模块使用开源区块链框架 Hyperledger Fabric [9]实现，构建了慈善信息链和慈善币链。

2.1. 系统框架和需求

如图 1 所示，基于区块链的可监管慈善系统主要包括业务层和区块链层，业务层包括用户注册、发起慈善项目、项目进展管理、链上查询、慈善币管理。区块链层包括合约层、网络层、数据层，其中合约层通过共识机制和智能合约将慈善系统的业务逻辑转化为可编程合约，通过节点的共识完成慈善信息的上链存储，基于区块链的可监管慈善系统设计必须满足以下原则：

1) 个人用户和公益组织都可以发起慈善项目，但为了便于后续的监管和追责，个人用户发起慈善项目时必须先选择公益组织，公益组织先对用户发起慈善项目进行审核，项目审核通过后公益组织设计出项目执行策略，完成后其慈善信息存储在数据存储服务器中，如云存储服务 IPFS 网络[10]，签名上链后通过背书节点确认，链上记录慈善项目信息；

2) 本系统设计一种与人民币等值的加密货币 CC (Charity Coin) [11]，以便于慈善资金的监管，该货币价格不会因为市场价值进行波动，捐赠者通过人民币汇兑慈善币，不征收任何汇兑费和税，捐赠者可以向受益人捐赠准确的金额而不扣除任何费用，有效地跟踪善款流向，同时系统后续将考虑使用数字人民币 DCEP (Digital Currency Electronic Payment) [12]作为慈善系统数字货币；

3) 必须验证慈善币的交易，交易双方的钱包地址都必须有足够的慈善币，交易记录了慈善币从一个钱包到另一个钱包的过程，每次捐赠都需要通过区块链共识机制进行验证，公益组织可以通过收据、图像证据来证明慈善过程，用户可以直接向公益组织捐款并对这笔捐款流向进行跟踪。

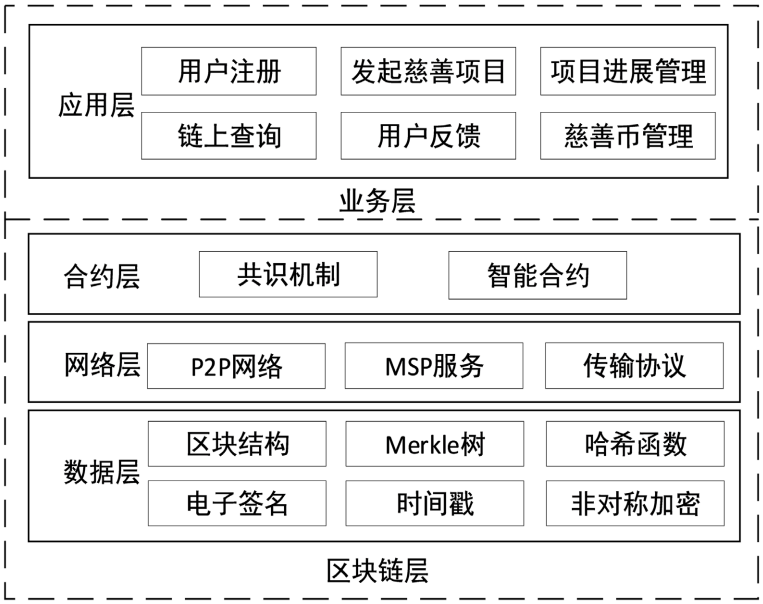

Figure 1. System architecture design
图 1. 系统架构设计

2.2. 系统算法的使用

部署基于区块链的可监管慈善系统时，可按如下方式运行：

1) 用户通过 IAM 模块进行个人用户和公益组织的认证注册，个人用户可以即时提交即时通过注册，公益组织包括基金会、社会团体、民办非企业，注册的审核时间约为两个工作日，完成注册后即可获得自己的钱包地址，并可以通过 CISM 模块发起慈善项目，提交慈善项目申请后，公益组织在五个工作日内返回项目的审核结果，组织审核通过的项目信息写入区块链；

2) 项目信息上链后进入项目筹款阶段。筹款期间，个人用户和公益组织通过 CCM 模块进行项目捐款，系统将相关捐款信息上链并实时更新项目筹款进度。筹款完成后，项目进入执行阶段，执行方按照项目发起时提交的执行计划执行，系统根据执行计划将捐款拨给项目执行方，执行方执行过程中通过 CIPM 模块更新项目进展。慈善项目执行结束后，受益人、执行方和公益组织三方共同提供项目成果报告，进行项目成果信息上链。

3. 可监管的慈善系统设计

基于区块链的可监管慈善系统由四个模块组成，包括身份和账户管理模块(IAM)、信息发布模块(CISM)、项目进展模块(CIPM)、慈善币管理模块(CCM)。如图 2 所示，收益人、公益组织和捐赠人是系统的三个主要用户，捐赠者、组织和受益人可以通过基于 web 和移动的应用程序，使用区块链网络与捐赠管理系统连接。除此之外，具有不同授权级别和管理控制的多个管理员用户也是系统的一种用户类型。

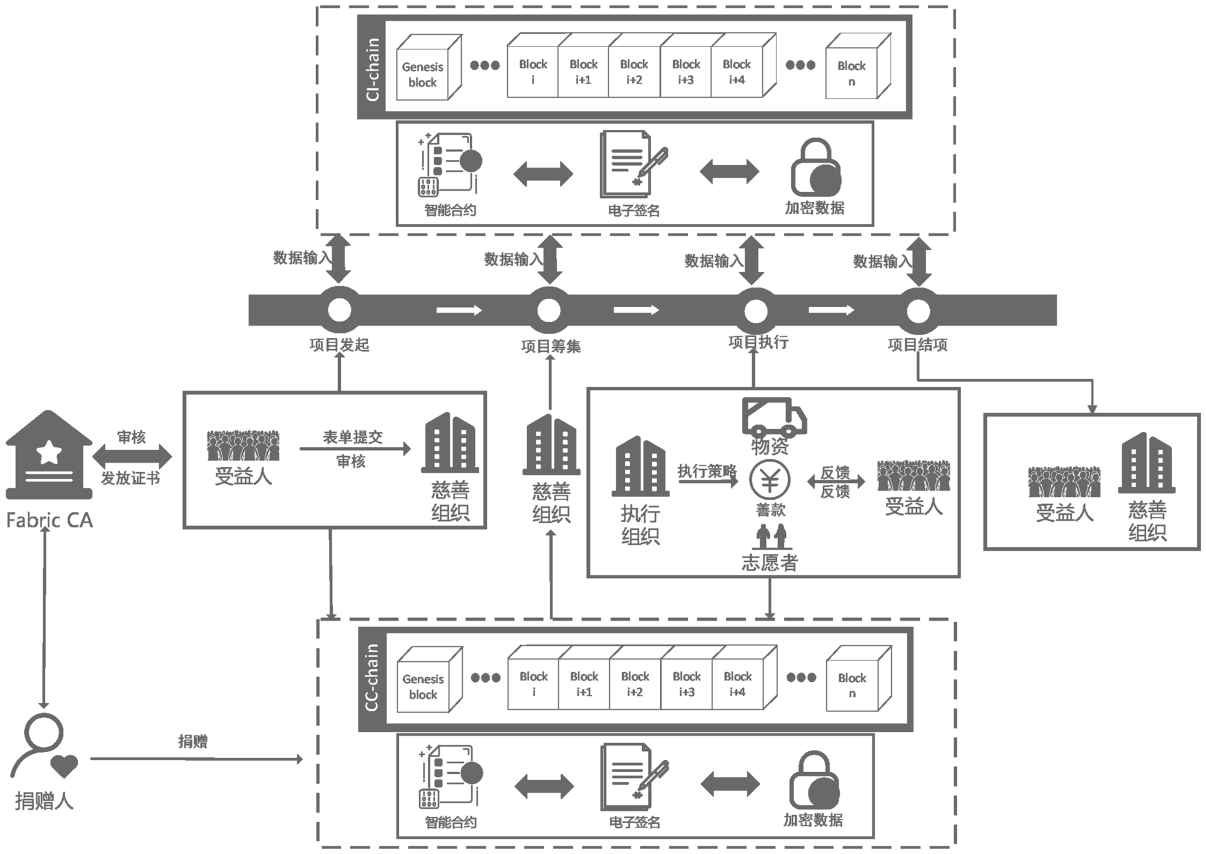

Figure 2. System model
图 2. 系统模型

3.1. 区块链实现

如图 2 所示，基于区块链的可监管慈善系统基于 Hyperledger Fabric (HLF)的多通道特性[13]设计了慈善信息链(CI-chain)和慈善币链(CC-chain)。HLF 是一个联盟许可链，所有用户都需要经过证书颁发机构(CA)的认证才能加入区块链网络，HLF 包含成员服务提供商模块、智能合约模块、分布式账本模块、交易模块。并且 HLF 在版本 1.4 中已经实现了令牌机制，使用 UTXO 模型[14]。在本系统中，其中一条链是慈善信息链，用于存储慈善项目的发起、筹集、执行、结项等慈善项目相关信息，另一条链是慈善币链系统设计了一种新的加密货币 CC。总共将有 100 亿个慈善币，每个 CC 价值 1 人民币，用户根据自己的意愿进行捐助。例如，如果用户捐赠 10 人民币，那么他将获得 10 CC 的余额。

3.2. IAM 模块

在本模块中，个人用户必须向 CA 提供注册帐户所需的信息，如姓名、身份证、地址、手机号。我

国公益组织可登记为社会团体、基金会、民办非企业(慈善法出台后改称社会服务机构)，公益组织通过提供公司信息，如组织名称、法人信息、统一社会信用代码等来完成注册。注册成功后用户将获得一个钱包地址，该地址打包在 x.509 证书中，同时作为慈善币链的账户信息，个人用户和组织都可以对 CC 币进行兑换。算法 1 说明了用户如何注册帐户。如果信息合法，将生成任何类型的用户。如果他们的信息有拼写错误或帐户已在系统中冻结，则注册将失败。

考虑到我们系统的安全性，本模块将定期检查现有账户，发现并冻结恶意账户。如果发现非法信息，相关用户的帐户将被列入失信筹款人黑名单，慈善组织将被线下追查。

算法1 注册账户

Input:*participant'sinformation p*
Output:*participant's cert c*
1: **if** *p is not correct or p has registered but still frozen* **then**
2: *c* ← *failure*;
3: **end**
4: **else**
5: **if** *p.role* == *USER* **then**
6:*c* ← *generateUserCert(p)*;
7: **end**
8: **else if** *p.role* == *foundationFD***then**
9: *c* ← *generateFDCert(p)*;
10: **end**
11: **else if** *p.role* == *social-service-agencySSA***then**
12: *c* ← *generateSSACert(p)*;
13: **end**
14:**else if** *p.role* == *social-groupSG***then**
15:*c* ← *generateSGCert(p)*
16:**end**
17: **end**
18: **if** *c* ≠ *failure* **then**
19: *save c* to CI-chain: *save(c);*
20: **end**
21: **return***c*;

3.3. CISM 模块

CISM 模块通过智能合约实现发起慈善项目。用户在进行慈善项目发起前，需填写包括受益者信息、目标金额、申请事由、联系方式、地址，背书组织等信息，在申请审核时系统初始化项目已筹金额为“0”，筹款状态为“未完成”。系统后续将考虑引入变色龙哈希函数使慈善信息是可修改的，但每个修改的记录都可追溯，以确保用户能够根据后续实际情况完善项目信息。算法 2 说明了用户发起慈善项目的智能合约。如果信息合法，将生成组织对该慈善项目的电子签名信息上链。如果信息非法或帐户已在系统中冻结，则发起慈善项目将失败。

3.4. CIPM 发布

慈善项目信息上链后显示在系统页面中，捐赠者和公益组织都可以进行捐款，并实时更新筹款进度，完成筹款目标后，筹款状态更新为“已完成”，项目进入执行阶段，执行方按照项目发起时提交的执行计划执行，执行方执行过程中通过 CIPM 模块更新项目进展。算法 3 说明了慈善进展信息上链的智能合约，如果信息合法，将生成组织对该慈善项目的进展信息上链，如果信息非法或者账户已在系统中冻结，则项目进展更新失败。

算法2 发起慈善项目

Input:*participant's cert c, charity information info,execution strategy es,charityinformation oftheorganizationin CI-chain* L_{CIs};
Output:*execuntion result r*;
1:**if** *c is not frozen and info is correct* **then**
2: calculate*info.hash* ←H(*c*,*info*,*es*);
3: get *c* and *info's* prove *p* from*Sig*(*c*|*info*, *c.prikey*);
4: insert *info* list L_{CIs}: *insert*(*info*, L_{CIs});
5: save to CI-chain:*save*(*info.hash*, *p*);
6: *r*← (*success*|*info.hash*);
7: **end**
8: **else**
9: *r*←*failure*;
10: **end**
11: **return***r*;

算法3 慈善进展管理

Input:*participant's cert c, charity information info,charityinformation oftheinfoin CI-chain* L_{infos};
Output:*execuntion result r*;
1:**if** *c is not frozen and info is correct* **then**
2: calculate*info.hash* ←H(*c*,*info*);
3: get *c* and *info's* prove *p* from*Sig*(*c*|*info*, *c.prikey*);
4: insert *info* list L_{infos}: *insert*(*info*, L_{infos});
5: save to CI-chain:*save*(*info.hash*, *p*);
6: *r*← (*success*|*info.hash*);
7: **end**
8: **else**
9: *r*←*failure*;
10: **end**
11: **return***r*;

3.5. CCM 模块

本文设计的加密货币是基于 Hyperledger Fabric，采用 UTXO 模式，用户只能使用未使用的交易输出。慈善币管理模块第一个智能合约是针对 CC 的 IEO (Initial Exchange Offerings)，智能合约初始化了系统发行货币的总数，并且规定了人民币和慈善币的汇率是 1，并设计了 CC 购买与出售的功能。算法 4 说明了 CC 的发行和 CC 的兑换功能。算法 5 说明了捐赠信息上链功能，慈善币链与慈善信息链的交互最终实现有效地善款流向可监管，防止善款滥用。

4. 实验分析

本节的第一部分介绍系统的环境配置，第二部分介绍系统主要功能实现，第三部分是对系统性能的测试与分析。

4.1. 环境设置

本系统实现在三台虚拟机 VMware Workstation Pro 中完成，操作系统为 Ubuntu18.04。虚拟机内存 2 GB，处理器核心数为 2 个，硬盘为 25 GB。其中 Hyperledger Fabric 的版本为 2.3，Golang 版本为 1.17.5，Node.js 版本为 12.9.1，Docker 版本为 19.03.2，Docker-compose 版本为 1.25.0，系统搭建的节点使用 Docker 容器封装。

算法4 慈善币管理

Require: *Initialization of the parameters*
1: *Initialization max_charitycoin = 100 billion*
2: *Initialization rmb_to_charitycoin rate = 1*
3: *Initialization total_charitycoin_bought = 0*
4:**Func**(*buy_charitycoin*)
5: **Input:** *participant's cert c, rmb_invested*
6: **if** *c is not frozen***then**
7: *charitycoin_bought = rmb_inversted * rmb_to_charitycoin;*
8: *equity_charitycoin[c] += charitycoin_bought;*
9: *equity_rmb[c] = equity_charitycoin[c]/rmb_to_charitycoin;*
10: *total_charitycoin_bought += charitycoin_bought;*
11: save to CC-chain: save()
11: **end Func**
12:**Func**(sell_*charitycoin*)
13: **Input:** *participant's cert c, charitycoin_to_sell*
14: **if** *c is not frozen and total_charitycoin_bought >= charitycoin_to_sell* **then**
15: *equity_charitycoin[c] -= charitycoin_bought;*
16: *equity_rmb[c] = equity_charitycoin[c]/rmb_to_charitycoin;*
17: *total_charitycoin_bought -= charitycoin_bought;*
18: save to CI-chain: save()
18: **end Func**
19:**end**

算法5 发起捐赠

Input:*participant's cert* c_1,*participant's cert* c_2,*charity information info*, *charitycoin_donate*, *charityinformation ofthein-foin* CI-chain L_{infos};
Output:*execuntion result r*;
1:**if** c_1,c_2*is not frozen and* c_1*.charitycoin_donate* < c_1*.total_charitycoin_boughtand info is correct* **then**
2: c_1*.total_charitycoin_bought -= charitycoin_donate;*
3: *info.fundraising+=charitycoin_donate;*
4：**if***info.fundraising*>= *info.fundtarget*
5: *info.fundstatu* = "done"
4: calculate*donate.hash* ←H(c_1, *info*);
5: get c_1 and *info's* prove *p* from*Sig*(c_1|*info*, c_1*.prikey*);
6: insert *info* list L_{infos}: *insert*(*info.fundraising*, L_{infos});
7: save to CI-chain:save(*donate.hash*, *p*);
8: *r*← (success|*donate.hash*);
9: **end**
10: **else**
11: *r*←*failure*;
12: **end**
13: **return***r*;

4.2. 系统主要功能测试

针对本系统的慈善项目发起、项目信息展示、用户捐款记录等重要功能进行了实验测试，部分重要功能实验结果如图 3~5 所示，图 3 显示了慈善项目发起和项目信息界面，图 4 显示了发起慈善项目后系统的后台记录，图 5 显示了用户的捐款记录。

4.3. 实验结果

本系统性能测试使用 Hyperledger Caliper 性能测试工具[15]进行测试，对区块链网络中交易成功率、

交易延迟、吞吐量(TPS)等指标进行测试。测试模拟三个组织各有两个节点的 Fabric 网络中发送交易请求，测试用例包括慈善项目发起合约 createCI，查询合约 queryCI 等，分别测试区块链的读写性能。测试在搭建在虚拟机中 Fabric 网络节点上，系统配置为处理器核心数为 2，内存为 4 GB，硬盘为 25 GB，网络带宽为 100 Mbit/s，启用 CouchDB 作为状态数据库。

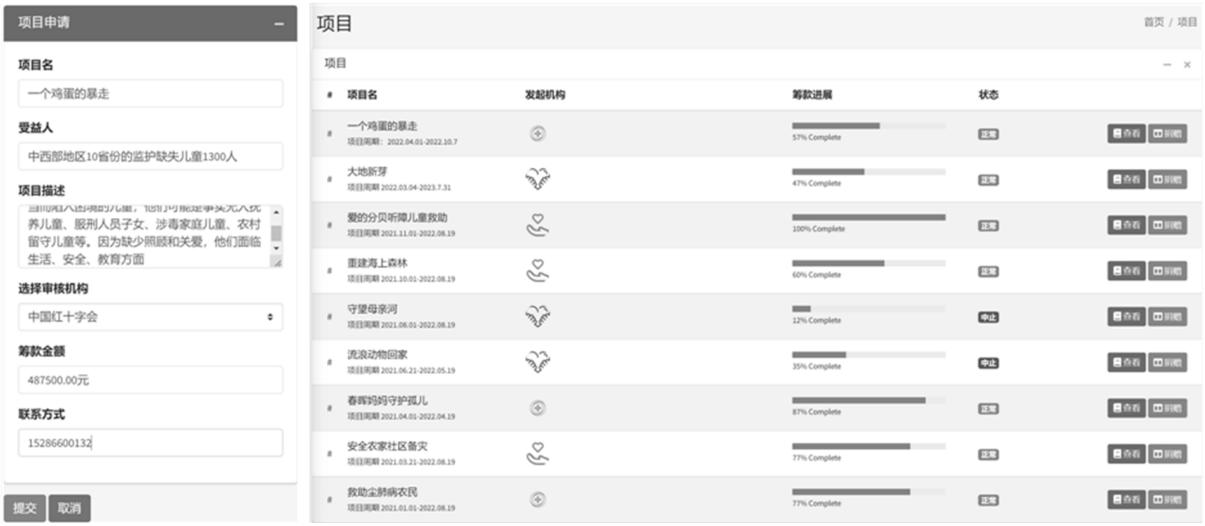

Figure 3. Project initiation function verification
图 3. 项目发起功能验证

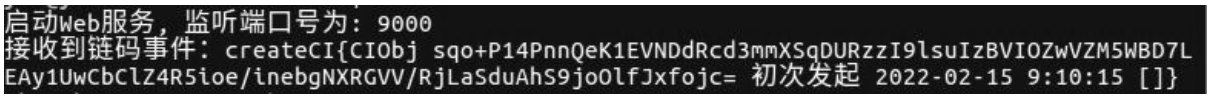

Figure 4. Background record of project initiation
图 4. 项目发起后台记录

Figure 5. Donation record query
图 5. 捐款记录查询

压力测试分为 12 轮进行，前 6 轮测试内容为慈善信息信息上链智能合约 createCI 测试，每轮测试交易量为 1000 笔，目的是测试账本写入性能。为了精准测试出区块链网络承载能力峰值，吞吐量发送速率梯度设定为 50 tps、100 tps、150 tps、200 tps、250 tps、300 tps。后 6 轮测试内容为查询链上签约信息智

能合约 queryCI 测试，每轮测试交易量为 1000 笔，目的是测试账本读取性能。吞吐量发送速率梯度设定为 100 tps、200 tps、300 tps、400 tps、500 tps、600 tps。

在测试量为 1000 次的条件下，createCI 智能合约的吞吐量与平均延迟的关系如图 6 所示，网络的交易吞吐量约为 230 TPS 左右。当发送速率达到第四轮 200 TPS，交易的平均延迟开始急剧升高，吞吐量保持在 230 TPS 左右不变，平均延迟在 3 s 左右。当发送速率更高时，交易超出链上负载，进入排队队列等待，导致延迟不断增大。

queryCI 智能合约的吞吐量与平均延迟的关系如图 6 所示，在前四轮中，因为 queryCI 智能合约的操作不需要写入链上数据，网络节点不进行共识，随着发送速率的增大，系统查询吞吐量随之增大，延迟一直稳定在 0.01 s 左右。当发送速率达到第四轮 400 TPS，交易的平均延迟开始急剧升高，吞吐量保持在 350 TPS 左右不变，平均延迟在 0.1 s 左右。当发送速率更高时，交易超出链上负载，进入排队队列等待。

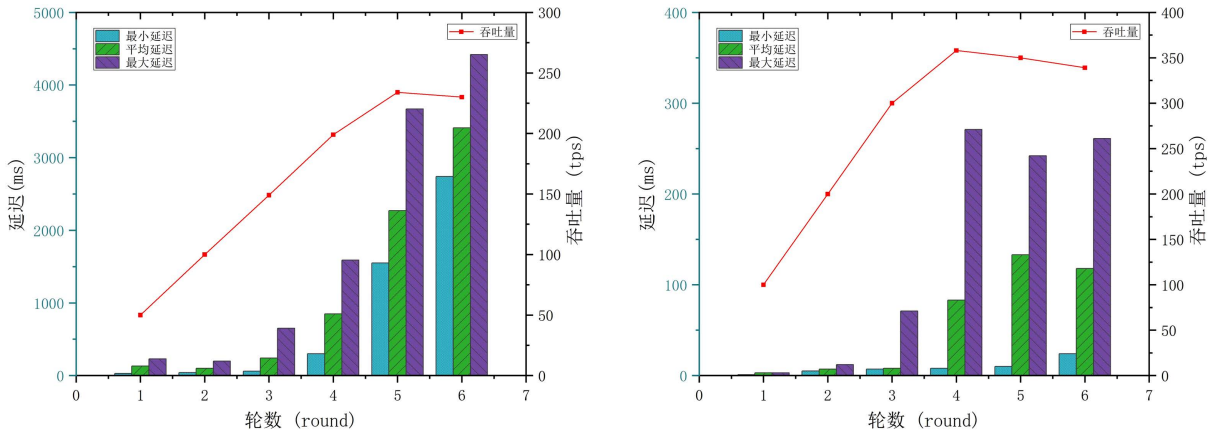

Figure 6. Blockchain reading and writing performance (left: write performance of blockchain transactions, right: read performance of blockchain transactions)
图 6. 区块链读写性能表现(左：区块链写性能，右：区块链读性能)

5. 结语

相对于传统慈善平台来说，本文通过慈善过程信息上链，并设计了一种数字货币进行善款追踪，使用智能合约和数字钱包有效解决了传统慈善平台的信任问题。本文还对该系统进行了性能测试，实验表明，该系统性能可以满足业务需要。在未来的研究工作中，将考虑引入变色哈希龙函数实现根据实际情况变更项目信息、删除风险项目等功能，优化算法提高系统效率，并与相关企业合作推广本平台。

参考文献

[1] 杨斌. 重视发挥第三次分配作用探寻中国特色公益慈善之路[EB/OL]. http://theory.people.com.cn/n1/2020/0102/c40531-31531793.html, 2020-01-02.

[2] 毕瑞祥. 我国慈善组织财务信息披露问题发现及改善[J]. 地方财政研究, 2017(5): 92-97.

[3] Bitcoin, N.S. (2008) A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[4] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.

[5] Clack, C.D., Bakshi, V.A. and Braine, L. (2016) Smart Contract Templates: Foundations, Design Landscape and Research Directions. arXiv preprint arXiv:1608.00771.

[6] 容志. 基于区块链技术的公共服务供给侧改革:运用与前瞻[J]. 上海对外经贸大学学报, 2021, 28(1): 88-102. https://doi.org/10.16060/j.cnki.issn2095-8072.2021.01.007

[7] 李琪, 李勍, 朱建明, 关晓瑶, 王慧, 郗晨梓. 基于区块链技术的慈善应用模式与平台[J]. 计算机应用, 2017,

37(S2): 287-292. https://doi.org/10.18686/bd.v2i10.1722

[8] 谭文安, 王慧. 基于智能合约的可信筹款捐助方案与平台[J]. 计算机应用, 2020, 40(5): 1483-1487.

[9] Linux (2020) Hyperledger Fabric. https://www.hyperledger.org/

[10] Benet, J. (2014) IPFS-Content Addressed, Versioned, P2P File System. arXiv preprint arXiv:1407.3561.

[11] Dai, W., Wang, Q., Wang, Z., *et al*. (2021) Trustzone-Based Secure Lightweight Wallet for Hyperledger Fabric. *Journal of Parallel and Distributed Computing*, **149**, 66-75. https://doi.org/10.1016/j.jpdc.2020.11.001

[12] 穆杰. 央行推行法定数字货币 DCEP 的机遇、挑战及展望[J]. 经济学家, 2020(3): 95-105. https://doi.org/10.16158/j.cnki.51-1312/f.2020.03.010

[13] 邵奇峰, 金澈清, 张召, 钱卫宁, 周傲英. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.

[14] 张若雪, 全骐. 基于 UTXO 和区块链的资金穿透记账系统[J]. 上海金融, 2018(4): 42-47. https://doi.org/10.13910/j.cnki.shjr.2018.04.007

[15] Linux (2020) Hyperledger Caliper. https://github.com/hyperledger/caliper