计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(11):112−117 [doi: 10.15888/j.cnki.csa.008169]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链的新型存储模型慈善系统①

于金刚[1,2], 王海汀[1,2], 赵培培[1,2], 李　姝[3]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 沈阳计算技术研究所, 沈阳 110168)
[3](沈阳理工大学 装备工程学院, 沈阳 110159)
通讯作者: 李　姝, E-mail: lishucx@163.com

摘　要: 现如今的慈善领域总会面临着数据无法公开透明的问题, 人们无法对不公开数据的慈善组织报以信任, 即使公开了数据, 也要面临着数据造假的质疑. 针对现有慈善组织存在的公信力不足、便捷性低, 以及善款流向不透明等问题, 本系统采用区块链技术, 通过设计新型数据存储模型, 将上传的项目数据按照所需的要求进行加解密等操作, 使得数据具有保密性; 同时将交易数据进行链上存储, 利用区块链不可篡改可追溯等特性, 将所有经过本系统的交易数据进行上链操作, 使得交易数据变得公开透明, 同时无法对已经完成的交易的数据进行修改, 从而使整个系统具有足够的公信力, 有效地弥补了传统慈善系统的数据不公开, 同时可能存在数据造假的不足.

关键词: 区块链; 以太坊; 慈善; 智能合约; 安全

引用格式: 于金刚,王海汀,赵培培,李姝.基于区块链的新型存储模型慈善系统.计算机系统应用,2021,30(11):112–117. http://www.c-s-a.org.cn/1003-3254/8169.html

Charity System with New Save Module Based on Blockchain

YU Jin-Gang[1,2], WANG Hai-Ting[1,2], ZHAO Pei-Pei[1,2], LI Shu[3]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)
[3](School of Equipment Engineering, Shenyang Ligong University, Shenyang 110159, China)

Abstract: The charity field is always faced with the problem that the data cannot be open and transparent. People cannot trust the charitable organizations that do not disclose the data. Even if the data is disclosed, they have to face the question of data fraud. Aiming at the problems existing in charitable organizations, such as lack of credibility, low convenience, and opaque flow of money, this system adopts the blockchain. By using a new data storage model, the uploaded data is encrypted and decrypted according to the required requirements, so that the data has confidentiality. At the same time, the data in the public chain can not be modified to make up for the transaction in the public chain At the same time, there may be insufficient data fraud.

Key words: Blockchain; Ethereum; charity; smart contract; security

如今我国的慈善事业的总体进度以及发展情况较之世界上先进国家的水平有较大的差距, 如今我们经常会在新闻中见到诈捐、贪污善款等丑闻的发生, 这样对于慈善领域的发展可以说是一种打击[1,2]. 在爆发一系列事件之后, 国内慈善事业也经历了前所未有的信任危机. 许多慈善基金会、机构在一时间流失了许多捐赠, 部分慈善人士更是选择绕过机构, 向受助群体直接提供“一对一”帮助. 虽然那些顶着“慈善”旗号的不法组织、个人最后受到了法律制裁, 但这依旧难以重拾国人对于慈善事业的信心[3].

① 收稿时间: 2021-01-25; 修改时间: 2021-02-23; 采用时间: 2021-03-11; csa 在线出版时间: 2021-10-22

在慈善领域公信力的问题上, 传统的慈善组织会因为透明度不高且监管难以到位[4], 无论多么详细的账目报表, 都是中心化的产物, 都是 (慈善) 机构的一家之言, 自然缺乏信任度. 这样就导致这些组织的公信力不足, 群众无法得知善款的具体用处, 对这些组织缺少信任. 现在的捐款的主流方式是通过网上募捐, 区块链作为比特币的底层技术, 因为其具有的不可篡改和可追溯的特性而被人所知, 于是, 将区块链技术应用在慈善领域, 通过网上募捐, 记录善款的流动方向, 随时可以查询善款的去向, 针对应用在慈善领域的区块链系统可以做到善款追踪, 公开慈善账目, 提升慈善组织的透明度, 提升公众的信任感.

近年来, 国内外学者也提出了一些基于区块链技术的慈善系统, 如文献 [5], 本文与传统的基于区块链的系统的区别在于, 传统的区块链系统应用主要使用的是在系统内设计专属于系统的 token 或者以积分的形式供使用者使用, 并且系统要上传到区块链网络中的内容大多会采用全部上传的方式; 而本文所设计的慈善系统采用了具有监管职能的第三方监管机构身份——监督者, 系统会将收集到的信息自动地识别和分类, 监督者在审核通过后, 会将提取出的信息凭证上传到区块链网络中, 从而节省出区块的使用空间, 节约成本.

1 相关领域及技术介绍

1.1 传统慈善系统

传统的慈善系统更多的是采取本地存储的方式, 通过系统内部链接的数据库进行信息的存储, 其中涉及到的交易记录也大多由系统的所属方来保存, 这样的中心化管理就不可避免的涉及到信息是否公开透明的问题, 尤其是对于交易数据来说, 捐助者无法确定自己所捐助的款项是否被使用在自己所期待的方向上, 无法做到实时的监控, 可能会造成一些贪污的问题, 这些就需要用到区块链交易数据可溯源、不可篡改的特性[6].

1.2 区块链

区块链技术源自于比特币的创造, 区块链作为一个新兴技术, 具备去中心化、防篡改、可追溯等特性, 这些特性在金融领域中都具有非常突出的效果, 它可以适应多种情况下的金融交易, 同时也为金融交易提供了一个具备公信力的合理的平台, 区块链技术是开放的, 同时也是一个能高效地分配资源的技术, 为金融交易提供了新的手段, 区块链技术为商业领域的快速发展, 带来了更多的成长空间. 与分布式结构相比较而言, 传统的中心化结构有两点比较突出的问题: 一是因为如今的交易方式会使交易双方产生信息不对称的问题; 二是在交易的时候难免会产生资金安全的问题. 区块链技术可应用于优化支付体系和构建高效安全的金融科技. 其中, 根据区块链技术的发展, 演化出了很多区块链技术的底层平台, 其中的以太坊平台是最为人熟知的平台之一, 以太坊平台具有完备的图灵机制, 对于实现智能合约的目的来说已经具备很成熟的环境.

1.3 以太坊

对于以太坊来说, 可以看作是区块链技术与智能合约的结合, 以太坊是区块链 2.0 的产物, 以太坊对于智能合约来说具有更加成熟的环境, 可以帮助智能合约更稳定的运行. 以太坊可以看作是一个为交易服务的状态机, 他通过读取一系列的输入, 通过这些输出产生一个新的状态, 其中, 对于如何执行某种功能或者某种需要的状态, 我们需要根据具体的要求来编写符合规定的智能合约, 实现不可篡改可追溯的功能.

2 基于区块链的慈善系统模型与合约设计

2.1 采用新型存储模式的慈善系统模型设计

为了满足慈善系统对数据的安全性、存储量、不可篡改等方面的需求, 采用了区块链技术与慈善相结合的方式, 满足了数据的可追溯、不可篡改的要求, 本系统的重点放在了区块链的信息存储能力的问题上, 因为区块的存储能力有限, 所以为了节省上链存储的成本, 本系统设计了一种新型的结合了区块链的存储模型. 通过信息的重要程度对等级的信息进行筛选, 从而将所需的特定信息进行加密上链, 将非必要信息进行本地存储, 从而减轻区块所要保存的任务量. 系统通过 4 个层次进行设计[7], 具体结构如图 1 所示.

具体步骤如下:

(1) 搭建以太坊平台环境, 可以正常编写、运行智能合约, 同时按照所需的需求来设计智能合约应当遵守的规则.

(2) 慈善系统中, 最主要的是智能合约层的设计, 智能合约层主要设计了 3 种角色, 分别应该具备以下能力:

受助人: 提供受助信息, 提交受助计划, 包括所需的款项或者所需的物资等.

捐款人: 提供资金以及待捐赠项目所需的物资等, 将其信息提交至监督者, 在得到确认的信息后, 可以得到反馈信息.

监督者: 审核受助信息以及捐助信息, 查询善款动态.

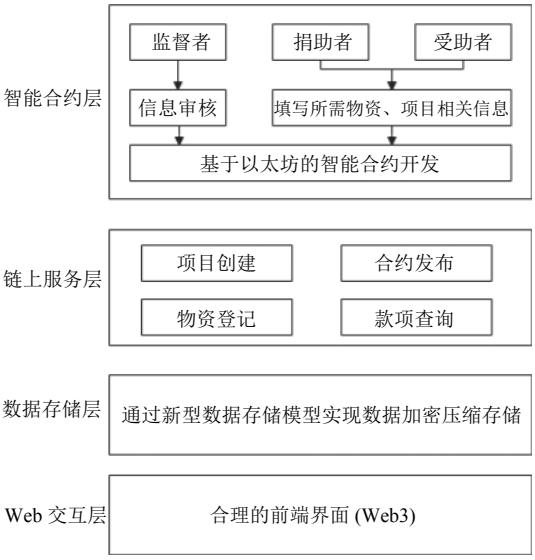

图 1 慈善系统模型设计图

在设计慈善系统的同时, 重点设计对于链上信息进行加密保存的存储模型.

(3) 对智能合约进行打包封装, 通过 Web3 来设计系统的前端界面, Truffle 框架实现前后端的交互功能.

2.2 智能合约层设计

首先根据搜索的资料以及相关方向上的一些实际的慈善系统的调研情况, 来总结出在慈善领域使用区块链技术的突出优势, 在这些优势方向上加以设计, 提出创新, 从而将理论中的设计在现实中得以实现[8].

在设计系统的整体架构上, 要趋于简洁明了, 将系统按照设定的思路为其中的使用者设计为 3 个角色: 捐款者、受助者以及监督者. 这 3 个模块互相独立, 但在某些功能上又会有相互照应的关系, 具体代码设计如下:

```
function numberOfCampaigns() public returns(uint numCampaigns){
        return numCampaigns;
    }
    function Beneficiary(uint campaignID)view public returns(string memory bname){
        return campaigns[campaignID].bname;
    }
    function ProjectDescription(uint campaignID)view public returns(string memory description){
        return campaigns[campaignID].description;
    }
    function FundingGoal(uint campaignID) view public returns(uint fundingGoal){
        return campaigns[campaignID].fundingGoal;
    }
    function NumberOfFunders(uint campaignID)view public returns(uint numFunders){
        return campaigns[campaignID].numFunders;
    }
    function AmountRaised(uint campaignID)view public returns(uint amount){
        return campaigns[campaignID].amount;
    }
```

其中, 捐款者需要有可以捐款以及查询属于自己的捐款的流向动态的功能; 受助者需要有提交受助信息, 选择受助计划的功能; 监督者当然要履行监督的职能, 需要有监督受助信息, 同时可以监督捐款流向的功能. 所有的功能都围绕着系统为上传至系统内的项目所分配的 *ID* 而进行, 通过 *ID*, 使用者可以进行查询、登记、增加或者修改等操作, 具体功能设计如图 2 所示.

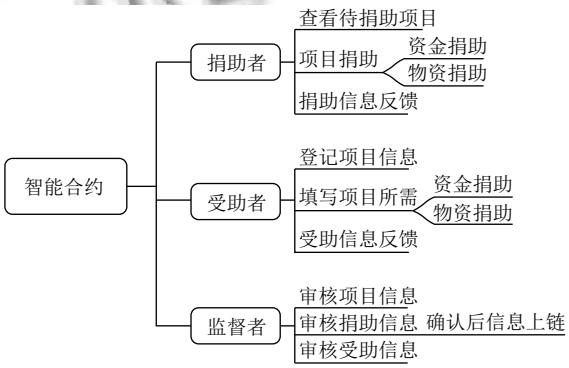

图 2 智能合约功能图

2.2.1 合约内角色属性分配

慈善项目登记功能是这个慈善系统最核心的部分, 其各项属性信息如表 1, 其内部的每一个属性通过登记者输入, 或是经过不同的计算方式录入到系统中, 系统会自动收集当前账户的地址信息, 在登记项目信息的

时候, 会将当前提取的使用者地址自动设置为受益地址, 当监督者使用合约的摧毁机制时, 会将所筹集的善款打向指定账户.

表 1 项目登记合约属性

属性名	类型	描述
beneficiary	address	Beneficial address
bname	string	Name
description	string	Project description
fundingGoal	uint	Target amount raised
numFunders	uint	Number of donations
amount	uint	Unpaid amount
id	uint	Project ID
getFrom	string	Project source
historyAmount	uint	Total amount raised

2.2.2 功能模块设计

(1) 受助者模块

对于受助人来说, 受助人首先需要注册自己的信息, 因为要更多的涉及到组织与组织之间的联系, 所以对于受助者模块的设计时, 要更多的贴近针对组织的特性来进行设计, 受助人分为很多种类, 比如针对孤寡老人、贫困学生、重病患者、留守儿童等; 这些不同的对象所要登记提交的信息有些许不同, 以后可以设计为多个入口, 从不同的入口进行信息的登记; 同时可以设计一个阈值, 当受助金额达到这个阈值的时候, 会将筹集到的善款转向填写的地址.

(2) 捐助者模块

首先, 对于捐助者来说, 这个身份可以查看所有的受助者的信息, 通过查找不同的分类, 查询到受助者所需的金额, 以及捐助人本身的地址信息 (交易地址) 的登记, 同时拥有选择是否进行匿名捐助的功能, 捐助者当然还要查看自己的善款的流向以及使用记录.

(3) 监督者模块

基于区块链本身的特性, 对于链上的信息是不可进行篡改的, 所以监督者更多的监督是对于信息的审核功能, 因为需要下到实地去考察资料是否符合真实情况, 对于资料正确性的审核, 以及其本身要具有发布合约的功能, 由监督者来判断合约的使用期限.

2.3 链上服务层设计

以太坊平台环境的搭建: 以太坊作为区块链 2.0 时代最突出的代表之一, 它可以平稳的运行智能合约以及足够的空间来为节点提供投票等功能, 使用智能合约的目的是确保系统在运行中保证严格按照代码所描述的功能来运行, 而不会因为后续的修改对系统的结果造成影响.

2.4 数据存储层设计

在慈善领域的数据存储过程中, 可能会涉及到项目的资料过于隐私, 不方便公开, 同时要注意数据资料保存的完整性, 不能丢弃数据, 会导致原始的存储模式无法实现这样的目的, 所以根据以上需求, 设计采用了新的数据存储以及访问模型[9,10], 如图 3 所示.

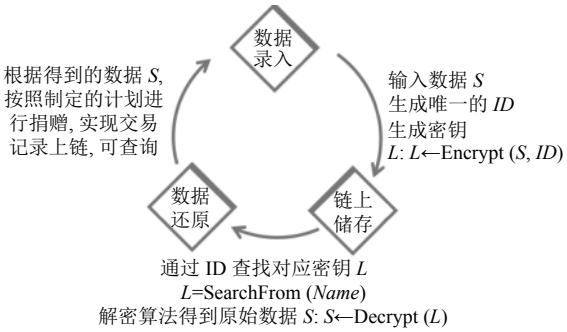

图 3 新型存储模型

整个数据存储模型包含 3 个部分: 数据录入, 数据还原, 链上存储; 首先信息记录者会进入项目登记界面, 按照项目需求填写有关信息, 同时系统会为该项目生成唯一的 *ID*, 将每一个项目所对应的数据进行加密计算, 得到属于这个项目的密钥. 我们会在链上存储根据加密计算得到的项目密钥 *L*, 这样可以在不暴露登记资料的情况下, 进行数据的链上存储. 在数据还原部分, 我们会根据项目名称查询项目所对应的密钥 *L*, 在得到了密钥 *L* 之后, 根据解密算法对已加密的数据密钥 *L* 进行解密, 得到我们所需的数据, 之后再根据计划由解密方对上传方进行捐赠.

具体的步骤为:

(1) 输入数据 *S*;

(2) 对每个项目进行标记, 生成唯一的 *ID*;

(3) 对每一个输入的数据 *S* 与 *ID* 共同进行加密计算, 生成对应的密钥 *L*: *L*←Encrypt(*S*, *ID*);

(4) 将密钥 *L* 和对应的 *ID* 标记存在链上;

(5) 当进行读取数据操作时, 首先通过项目名称进行密钥查找: *L* = SearchFrom(*Name*);

(6) 得到密钥 *L* 后, 通过解密算法对密钥 *L* 进行解密, 得到所需的数据 *S*: *S*←Decrypt(*L*);

(7) 最后根据数据还原得到的项目 *ID* 进行捐款等一系列操作.

2.5 Web 交互层设计

系统采用了 Web3 来进行智能合约与底层功能的

交互, 主要是根据不同的功能设计了不同的页面, 实现了功能和界面的链接交互, 构成了完整的系统架构.

3 慈善系统的界面设计与实现

该系统基于以太坊平台来搭建智能合约, 在 Windows 10 系统下进行测试, 在智能合约的编写上使用 Solidity 语言, 采用的 Solidity v0.5.12 版本, 同时使用 Ganache v2.0.1 可视化客户端搭建私有链, 默认将系统搭建在 7545 端口, 可以通过客户端提供的私钥公钥对系统进行操作测试, 首先进行 Truffle 的部署, 之后再运行程序, 通过 Ganache 客户端提供的私钥, 将账户导入到 Metamask 钱包中, 从而实现实验环境的搭建;

3.1 应用界面设计

受助者首先需要在指定的页面进行项目登记, 如图 4 所示, 涉及到的信息包括要登记的项目名称, 项目的具体描述以及项目所要筹集的金额; 系统会根据当前登录的地址自动提取受益账户地址, 将发布项目的地址设置为最后善款发放的接收方.

图 4 项目登记界面

在输入项目的基本信息的同时, 会为这个项目分配独属于项目本身的 *ID*, 这个 *ID* 用于后续的项目查询以及捐款的过程. 系统会提取项目的 *ID* 以及地址信息进行加密操作, 生成用于存放于区块链网络的密钥. 得到密钥后, 会将密钥代替项目信息存放于区块链网络中, 从而节省了区块链存储的空间, 提高了区块的空间使用率.

当以捐助者的身份登录时, 可以根据已知的项目名称进行项目查询, 系统会根据输入的项目名称, 在区块链网络上查找符合条件的项目 *ID*, 再通过特定的数据还原算法, 将密钥进行解密, 从而获得项目的完整信息. 具体查询界面如图 5 所示.

其他功能界面和项目查询界面类似, 分别通过项目 *ID* 或者项目所对应的受益方地址来进行查询或者交易操作.

受益地址	Insufficient permissions
项目名称	困难住户补助项目
项目登记ID	1
项目描述	Insufficient permissions
项目筹集目标(eth)	20
已捐款次数	0
已筹集善款(eth)	Insufficient permissions
平台已登记项目数量	2

图 5 项目查询界面

3.2 数据保密性测试

系统为需要隐私保护的用户设置了专门的私密信息加密功能, 会将用户上传的信息设置为项目捐助者以及监督者才可以查看. 我们采用了 Ganache 客户端通过廉价 Metamask 的方式模拟节点来发起交易, 数据查询结果如图 6 所示, 显示了在不同权限的情况下查询数据的结果.

受益地址	0xb69e659bb249d62b9ced5ebeddca6079a1d56f1c
项目名称	困难住户补助项目
项目登记ID	1
项目描述	用于疫情时期，困难用户的衣食住行捐助款项
项目筹集目标(eth)	20
已捐款次数	0
已筹集善款(eth)	0
平台已登记项目数量	2
受益地址	Insufficient permissions
项目名称	困难住户补助项目
项目登记ID	1
项目描述	Insufficient permissions
项目筹集目标(eth)	20
已捐款次数	0
已筹集善款(eth)	Insufficient permissions
平台已登记项目数量	2

图 6 数据查询测试

3.3 数据存储量测试

为了节约在区块上的存储空间, 我们采用了新型存储模型来进行数据的存储, 以每个区块可以存储 2 MB 数据为例, 我们测试对于小、中、大型数据规模的存储过程中, 新型存储模型与传统存储模型性能上的区别; 传统存储需要将所有的项目信息打包保存, 实现全部信息上链的存储方式, 其中我们得到了 3 种规模下的信息大小: 178 B、496 B、1022 B; 而在新型存储模型中, 我们只需要通过对特定信息的分离, 对分离出的信息进行加密上链即可, 这样得到的 3 种规模的数据都只需要 128 B, 那么在同一区块下的存储数量形成了明显的对比.

3.4 系统应用区块链的前后可信度对比

区别于传统的中心化管理的慈善系统, 采用了区块链技术的新型慈善系统更具有可信性, 我们通过网上的评测与问卷的形式采集了人们对于慈善系统的可信程度的分析, 我们选择了 20–40 岁年龄段的工作者进行样本采集, 在发放的 1000 份调查问卷中, 收到了 847 份有效回复, 分析结果表明, 当采用区块链时的慈善系统可信度要远高于传统的中心化管理的慈善系统[11], 如图 7 所示, 其中实虚线表示区块链慈善系统的可信度, 轻虚线表示传统慈善系统可信度.

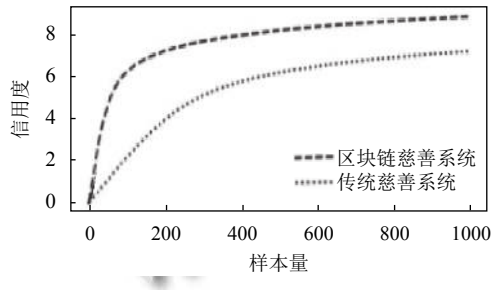

图 7 可信度对比图

3.5 交易数据可视化

在交易数据可视化的实现上, 我们可以通过查询区块上存储的交易数据来查看属于捐助人的款项的流动去向, 交易数据的查看可以通过以太坊区块查询网页或者本地测试所使用的的 Ganache 进行查询, 其中在 translation 页面中包括转账地址和接受地址, 以及时间信息等.

在涉及到物资捐助的时候, 系统设计了一套通过监督者权限才能使用的账本功能, 监督者通过得到捐助和受助两方对于捐助信息的确认后, 将捐助者提交的有效捐助信息进行上传, 将物资的有关信息全部打包提交到链上, 后续对于物资的处理过程全部需要将信息提交到监督者的手中, 这样就可以记录物资的使用情况的完整流程, 之后将上传到链上的信息同步到系统的主页面, 从而实现物资信息的可追溯和查询的功能.

4 总结

区别于具有中心化职能的慈善系统, 基于区块链的慈善系统更加具有公信力. 首先分析了传统的慈善组织或系统在捐款、项目审核以及资金流动等过程中的缺陷以及漏洞, 然后对目前区块链与慈善领域结合的应用研究进行说明; 之后介绍了本系统在数据存储上的创新, 为信息登记之后的保密性提供了可靠支持. 系统实现了慈善捐款的全部流程都可以在链上进行查询和审核, 同时提供了信息的加密存储. 最后通过 Ganache 等测试工具验证了该系统的可行性以及信息的安全性, 证明了在捐款过程中交易数据的可溯源, 可查询, 不可篡改的特性; 以及针对用户私密信息加密的安全性, 在读取用户信息时还原数据的可行性, 通过两者实现了系统的数据可使用的循环, 然后通过测试模块的存储性能, 验证了该系统可以在保障信息安全的同时, 增加了可存储量, 为信息的存储提供了更加便利的条件, 从而实现交易数据可溯源、信息安全有保障的慈善系统.

参考文献

1 易勤, 欧嵬, 刘威, 等. 基于区块链的慈善系统的研究与实现. 计算机时代, 2020, (2): 62–66.
2 王嘉, 陈海峰. 区块链技术在中国慈善事业中的应用分析和研究. 电脑与信息技术, 2017, 25(6): 57–59. [doi: 10.3969/j.issn.1005-1228.2017.06.016]
3 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494.
4 任锦鸾, 蔡霖. 基于区块链的数字资产价值开发模式研究. 现代传播, 2019, 41(2): 127–131. [doi: 10.3969/j.issn.1007-8770.2019.02.024]
5 李贺. 基于区块链技术的慈善系统模式研究. 电脑与信息技术, 2019, 27(4): 40–44. [doi: 10.3969/j.issn.1005-1228.2019.04.012]
6 何飞, 傅继晗. 基于区块链技术的慈善捐助系统设计. 信息系统工程, 2019, (3): 44–46. [doi: 10.3969/j.issn.1001-2362.2019.03.024]
7 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展. 计算机学报, 2018, 41(5): 969–988. [doi: 10.11897/SP.J.1016.2018.00969]
8 李琪, 李勍, 朱建明, 等. 基于区块链技术的慈善应用模式与平台. 计算机应用, 2017, 37(S2): 287–292.
9 Buterin V, Reijsbergen D, Leonardos S, *et al*. Incentives in Ethereum's hybrid casper protocol. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Seoul: IEEE, 2019. 236–244.
10 Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. International Conference on Financial Cryptography and Data Security. Barbados: Springer, 2016. 142–157.
11 管晓永, 任捷. 区块链技术对传统征信的变革研究. 征信, 2020, (3): 45–50. [doi: 10.3969/j.issn.1674-747X.2020.03.008]