Journal of Computer Applications
计算机应用, 2020, 40(5): 1483 - 1487
ISSN 1001-9081
CODEN JYIIDU
2020-05-10
http://www.joca.cn

文章编号:1001-9081(2020)05-1483-05
DOI:10.11772/j.issn.1001-9081.2019111999

基于智能合约的可信筹款捐助方案与平台

谭文安[1,2*],王　慧[1]
(1. 南京航空航天大学 计算机科学与技术学院,南京 211106; 2. 上海第二工业大学 计算机与信息工程学院,上海 201209)
(*通信作者电子邮箱 wtan@foxmail.com)

摘　要:传统筹款捐助平台的集中式管理难以满足高可信机制的需求,筹款信息真假难辨,善款流向不透明。区块链技术的去中心化、数据不可篡改、可溯源、点对点交易等特点为构建可信捐助平台奠定了基础。由此以区块链技术为基础,提出了一种基于以太坊智能合约的捐助方案。首先,将筹款信息和捐款交易事件等存储在以太坊区块链上,并利用保证金机制保证了数据的真实性和可溯性;同时,阐述了该方案的架构模型,提出智能合约算法Donate代替人工操作,防止善款挪用和久未到账问题;最后,通过基于智能合约的可信筹款捐助平台验证了该方案的可行性。将所提平台与传统筹款平台比较分析,证明了该平台能安全有效地防止虚假筹款和善款挪用。

关键词:区块链;智能合约;筹款捐助;防欺诈;善款跟踪
中图分类号:TP391　　**文献标志码**:A

Scheme and platform of trusted fund-raising and donation based on smart contract

TAN Wenan[1,2*], WANG Hui[1]
(1. *College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Jiangsu Nanjing* 211106, *China*;
2. *School of Computer and Information Engineering, Shanghai Polytechnic University, Shanghai* 201209, *China*)

Abstract: The centralized management of traditional donation platforms is difficult to meet the needs of highly trusted mechanism. The truth of fund-raising information is difficult to distinguish, and the flow of funds is not transparent. Blockchain technology has characteristics of decentralization, data not being tampered, traceability, and peer-to-peer transaction, which lays a foundation for building a trusted donation platform. Therefore, based on the blockchain technology, a donation scheme based on the Ethereum smart contract was proposed. Firstly, the fund-raising information and donation transaction events were stored on the Ethereum blockchain, and the margin mechanism was used to ensure the authenticity and traceability of the data. Meanwhile, the architecture model of the scheme was described. The smart contract algorithm Donate was proposed to replace the manual operations in order to prevent the misappropriation and long-term non-payment problems of funds. Finally, the feasibility of the scheme was validated by the trusted fund-raising and donation platform based on smart contract. Compared with the traditional fund-raising platform, it is proved that the proposed platform can prevent false fund-raising and fund misappropriation safely and effectively.

Key words: blockchain; smart contract; fund-raising and donation; fraud prevention; fund tracking

0　引言

近年来,互联网+技术的不断发展,促进各种筹款捐助活动演变成各种线上模式,虽说这种方式带给人们极大便利,让筹款捐助跨越了空间障碍,但随着各种数据的爆炸增长,人们难以辨别孰真孰假,不法分子利用这种弊端,通过不法手段从中牟利,置筹款捐助这一善事于尴尬境地。出现以下问题:1)筹款信息缺乏可信度;2)善款流向不透明;3)善款到账不及时。区块链技术和智能合约为解决上述问题提供了技术支撑,本文将区块链技术和筹款捐助相结合,提出了一种可信筹款捐助方案,并基于此方案搭建了一个可信平台,以验证上述方案的有效性。

1　相关工作

1.1　区块链

区块链是从比特币底层技术衍生出来的新技术体系,是一种按照时间顺序将数据区块以链条的方式组合而成的特定数据结构,并以密码学方式保证其不可篡改、不可伪造的去中心化公共总账[1]。区块链的特点主要包含以下三方面:1)开放共识:任何用户都可以参与到区块链中,参与其中的节点都可以获得一份完整的账本;任何用户都可以通过公开的接口查询区块链上的数据。2)去中心化:区块链是由参与节点组成的P2P(Peer to Peer)网络,不存在中心化的硬件或管理机构,任何节点在网络中都是平等的。3)不可篡改性:区块链是一个公开的账本,区块通过节点的验证后会被永久存储,区块

收稿日期:2019-11-05;**修回日期**:2019-12-03;**录用日期**:2019-12-09。
基金项目:国家自然科学基金资助项目(61672022,61272036);上海第二工业大学校重点学科资助项目(XXKZD1604)。
作者简介:谭文安(1965—),男,湖北荆州人,教授,博士生导师,博士,CCF高级会员,主要研究方向:软件服务工程、可信服务计算与组合、协同计算、业务过程智能技术;　王慧(1995—),女,安徽安庆人,硕士研究生,主要研究方向:区块链。

中含有上一个区块的hash值，如果修改其中某一个区块，在这之后的所有区块都要重新计算，除非能控制系统中超过51%的节点，否则单个节点对数据库的修改是无效的。基于区块链的这些特性，每个节点都存有区块链上的完整信息，每笔筹款申请或善款捐助信息都是公开透明的。

1.2 以太坊和智能合约

比特币是区块链1.0技术，开创了数字货币的先河。比特币协议使用基于堆栈的脚本语言，不能构建更高级的应用，以太坊[2]则对比特币系统进行了扩展，构建了新一代智能合约和去中心化应用平台，被称作区块链2.0技术。以太坊旨在为去中心化应用实现一个在区块链之上的图灵完备的计算平台，作为具有智能合约[3]功能的开源公共区块链平台，它引入以太坊虚拟机(Ethereum Virtual Machine，EVM)，允许开发人员利用智能合约在其上创建基于任意数量彼此陌生的网络节点的分布式应用。

目前，绝大多数Web应用模式可以认为是“中心化”的。“去中心化应用程序”(Decentralized Application，DApp)是将数据保存到“基于点对点网络的时间戳服务器”，即区块链，而不是由中心化的公司或组织控制其服务，由这样的“去中心化服务”来提供具体的业务数据计算应用。DApp也可以简单地理解为是基于智能合约进行状态追踪和计算的一种应用程序。

1.3 研究现状

区块链作为新兴技术，其去中心化、防篡改、可溯源等特点使其应用于医疗[4]、金融[5]、物联网[6]、能源[7]等诸多领域。文献[8]将区块链技术应用于投票系统中实现匿名投票系统，减少人工干预保证其公正公平；文献[9]将区块链技术应用到数字内容的版权保护上，利用其可溯源特点改善传统模式；文献[10]通过使用区块链和数据交互审计平台来完成乘客隐私信息的保护。

区块链技术使社会公益慈善事业的系统设计有了新的方向。文献[11]为慈善平台开发提供了一种应用模式，将布比公司开发的区块链作为底层技术，通过限制受助人只能在慈善机构规定的其他机构处使用善款来防止受助人滥用善款，但未对善款挪用或到账不及时等问题提出有效的解决措施；国内的蚂蚁金服公司将区块链技术用于记录支付宝捐赠的具体流向，实现了善款使用的公开透明、可追溯和不可篡改；文献[12]利用蚂蚁区块链平台帮助听障儿童重获新生、和再障说分手等慈善项目实现善款筹集；文献[13]提出了众筹业务的私有区块链架构(Crowdfunding Private Block Chain，CPBC)以满足众筹业务需要，加强金融数据安全和公信力；文献[14]将区块链技术用于灾区援助的资金筹集，将整个平台搭建在以太坊之上，其交易均通过智能合约进行并存储在区块链上；文献[15]探讨了如何在慈善领域利用区块链，建立以区块链技术为基础的比特币慈善平台。这些研究给区块链在筹款捐助领域的应用提供了启示，本文方案保证了筹款信息真实可靠，杜绝了欺诈的筹款行为，同时结合智能合约技术，有效防止了善款挪用及到账不及时问题发生。

2 系统业务模型

将区块链技术引入款捐助平台设计，基于以太坊智能合约进行DApp研究与设计，实现筹款信息真实可靠以及善款去向透明化。功能包括筹款申请、筹款信息展示、捐款操作、捐款记录查询。为了保证筹款信息的真实性，除了各方调查监督外，系统还设置了保证金罚没机制，促使所有节点都能遵循系统规则，以此确保信息真实可靠，避免弄虚造假；同时，利用智能合约明确收款方地址并完成自动转账操作，捐款人和受助人直接联系，避免善款挪用或久未到账问题。

2.1 业务模型

图1展示了基于智能合约的可信筹款捐助系统中受助人提交数据进行链上存储以及捐款交易的业务模型。

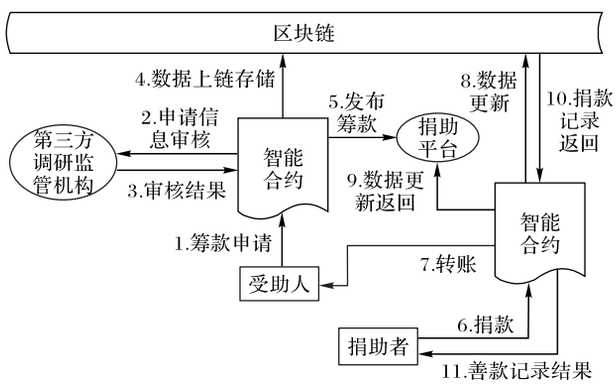

图1 业务模型

Fig. 1 Business model

首先受助人根据自身情况填写筹款申请信息，同时缴纳一定的保证金，暂存在筹款申请智能合约里，等待第三方调研机构调查审核：审核通过，智能合约才自动将受助人信息存储到区块链上，并将保证金返还给受助人，同时将审核通过的筹款信息展示在捐助平台上；若审核未通过，智能合约自动罚没受助人保证金，不予退还。

捐助者浏览捐助平台的筹款信息，选择受助对象进行捐款，后台通过智能合约自动进行交易操作，交易完成后转账交易信息将上链存储，以便后续善款查询跟踪，同时更新受助者已筹善款金额。

2.2 系统架构设计

系统架构如图2所示，包含3个部分：Web前端模块、中间模块、区块链模块。

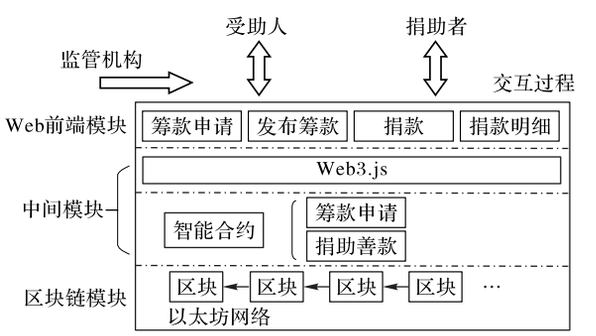

图2 系统架构

Fig. 2 System architecture

底层区块链模块提供数据和交易的存储功能，负责存储智能合约代码和执行智能合约，并将执行结果打包成区块，经过共识后写入区块链账本。基于开源区块链系统以太坊进行搭建，使用以太坊客户端构建一个去中心化的网络，用以支持智能合约交互操作和信息的存储。

中间模块主要由智能合约和Web3组成，智能合约为数据的存储查询和捐款交易提供交互接口，智能合约代码保存

在区块链模块中。当进行筹款申请或善款明细查询时,数据存储查询智能合约自动被调用,完成相应的区块链数据存储查询操作;当有捐助者进行捐款时,捐助合约被调用,自动存储转账交易信息,当达到目标金额时,自动完成交易操作。与传统的基于Web服务的HTTP API(Application Program Interface)中间件不同,智能合约是一个部署在以太坊网络上的协议,规定了用户能够执行的操作以及操作规范,用户操作全都按照合约内容进行。本文选择使用Solidity语言编写智能合约,实现筹款捐助系统的各项功能。Web3是一套和以太坊节点进行通信的API,通过Web3来获取节点状态、获取账号信息、调用合约、监听合约事件等,实现上层应用与智能合约和以太坊区块链的沟通和连接。

应用层Web前端模块为用户提供友好的互动界面,提交各参与方主体的请求,通过智能合约提供的接口与区块链进行交互,选择要调用的智能合约,执行具体的筹款申请和转账交易功能。

3　功能模块与合约设计

针对前面所提出的基于智能合约的可信筹款捐助系统架构,讨论其功能模块设计及其实现,详细介绍合约设计,讨论如何使用智能合约技术实现筹款捐助系统的可信平台。

3.1　Web前端模块

Web前端界面主要分为筹款申请、筹款信息展示、捐款、捐款明细等四部分,采用Html+Css+Javascript进行界面设计;通过Web.js库与以太坊节点的RPC接口连接来调用智能合约;运行以太坊节点的仿真器软件Ganache-cli来模拟真实的以太坊网络环境;使用谷歌浏览器提供的MetaMask插件(以太坊轻钱包)来连接以太坊节点,生成并发送交易信息到以太坊区块链网络,并进行交易费用的付款和捐款的转账操作。

钱包在以太坊网络中起着管理私钥、地址和区块链数据的作用,根据区块链数据维护方式,钱包可分为全节点钱包和轻钱包两种:全节点钱包需要同步所有区块链数据,对容量要求较高;轻钱包仅需同步与账户自身相关的数据,无需下载全部的、庞大的以太坊节点数据,帮助用户方便地管理自己的以太坊数字资产。

系统应用层基于以太坊中最受欢迎的Truffle框架开发,有效实现从智能合约编译、部署到发布的整个流程集约化操作,采用Bootstrap框架开发用户页面。

3.2　智能合约模块

智能合约(Smart Contract)这个词最初是由美国计算机科学博士尼克·萨博(Nick Szabo)在1994年提出来的[16]。智能合约指的是一种基于计算机技术实现的,可以免除人工干预而自动执行、自动校验、自动基于外部指令给出回应的具有交互性或者互操作性的合约。智能合约不仅仅是一个可以自动执行的计算机程序,更像是一个可信的第三方,可以临时保管资产,严格按照事先约定好的规则执行操作。在以太坊中,所有的交易都按照合约定义的操作有条不紊地执行,且改变着区块链的状态。支持多方合作,消除潜在的人为错误和腐败风险,对于每个参与用户来说都是透明的。

3.2.1　筹款申请

筹款申请是本系统的主要功能之一,受助人首先需要提交筹款申请信息,受助者结构体见表1。为了防止受助者填写虚假的筹款信息,所有提交的信息都需经过审核并缴纳一定的保证金,结构体中要包含审核是否通过的状态标志,只有审核通过,筹款信息才能在捐助平台进行展示;如果最后审核没有通过,不仅无法在平台上发布筹款,还会被罚没保证金。以此惩罚机制来保证系统的可信性,让所有节点自觉遵守智能合约规则。

表1　受助者结构体

Tab. 1　Recipient structure

字段	名称	类型
name	受助者姓名	string
goalamount	目标金额	uint
amount	已筹金额	uint
suffering	所患疾病	string
phone	联系方式	string
passed	审核状态	bool
raised	筹款状态	bool

第三方调研机构一旦点击审核通过按钮,智能合约就会自动将受助者信息存储到区块链上,以备后续查询和交易。将受助者信息存储到区块链上的合约算法addTarget如下所述。

算法1　addTarget。

输入　筹款申请者姓名,目标金额,所患疾病,联系方式,已筹金额初始化为"0",筹款状态初始化为"未完成"。

输出　返回成功存储到区块链的受助者信息。

步骤1　监听审核通过事件;

步骤2　审核通过,触发存储筹款申请智能合约;

步骤3　智能合约自动将申请人信息存储到区块链上,并调用发布筹款信息合约;

步骤4　返回保证金到受助者地址;

步骤5　若审核未通过,则罚没保证金。

3.2.2　善款捐助

捐助人浏览所有筹款信息展示页面,点击捐款按钮后,就会调用捐款合约,记录交易详情。善款可暂时存放在合约里,等达到目标金额,智能合约自动将善款转入受助者账户,避免善款到账不及时;未达到目标金额时,受助者也可自行提取到自己的账户中,前提是地址需保持一致,否则智能合约拒绝转账,防止善款被随意挪用。捐助者进行善款捐助的合约算法Donate如下所述:

算法2　Donate。

输入　捐款者地址,受助者序号,捐款金额。

输出　返回捐款成功信息。

步骤1　获取捐助者地址、受助人序号、捐助金额等输入信息;

步骤2　判断捐助对象是否存在、审核状态是否为通过、筹款状态是否为未完成;

步骤3　若满足步骤2),则在捐助者结构体里记录下受助者序号;

步骤4　触发捐赠事件,记录受助对象和捐赠者地址及捐助金额;

步骤5　判断是否达到目标金额;

步骤6　若满足步骤5),智能合约自动将善款转给受助者,同时将筹款状态设置成已完成;

步骤7　若未达到目标金额,受助者请求提款,智能合约需判断请求者地址是否与受助者地址相同;

步骤 8　若地址一致，则同意提款，同时更新受助者目标金额和可用金额，并记录其已用金额。

3.3　区块链模块

区块链本质上可以看成是存储信息的分布式数据库，或者理解为在各个参与者之间执行和共享所有交易事件的公共账本。账本是由不同区块构成的，一个区块包含区块头和区块体两部分：区块头由前一个区块的 hash 值、挖矿的难度及本区块中一定数量的交易数据的默克尔(Merkle)树、时间戳等构造而成；区块体则封装了自上一区块创建以来的多笔交易记录，在区块链中生成的所有记录通过 Merkle 树的哈希过程生成唯一的 Merkle 根，存储在区块链的头部[17]。

Merkle 树是一个基于哈希算法的数据结构，每一个非叶子节点都是其叶子节点的哈希值[18]。一旦叶子节点的数据发生改变，父节点的哈希值会随之改变，Merkle 树的这个特征保证了区块中数据的不可篡改；时间戳字段可以明确表示该区块生成的时间，无法抵赖和篡改；难度值和随机数字段用于全网共识，保证全网数据的一致性；每个区块都保存上一区块的哈希值，用来实现区块的连接。区块链由所有参与节点共同维护，区块链的结构如图 3 所示。

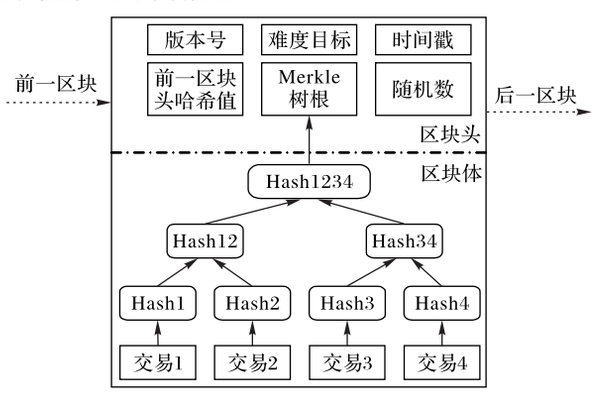

图 3　区块链结构

Fig. 3　Structure of blockchain

4　实验分析

4.1　测试环境

在 Ubuntu18.04 操作系统下设计实现本文构建的基于智能合约的可信筹款捐助系统，在该系统下搭建以太坊开发环境，同时安装相关依赖包和软件包 Node.js、Truffle 框架、Ganache-cli、MetaMask 等。使用 ganache-cli 来模拟真实的以太坊网络环境，通过谷歌浏览器的插件 MetaMask 来执行以太币的付款转账功能。

4.2　测试结果

针对本系统的筹款申请、捐款、筹款信息展示、善款去向明细等重要功能进行了实验测试：筹款申请、捐款都对区块链上的数据有所修改，产生交易，需要以太坊节点对交易进行打包，从而将数据变化写入区块；筹款信息展示和善款去向明细无需修改数据，只产生调用信息，无交易。

部分重要功能模块实验结果如图 4~5 所示。图 4 显示了受助人填写相关数据信息后提交弹出 MetaMask 支付交易费用及保证金；图 5 显示了捐助者填写所要捐助的对象及捐助金额后提交弹出 MetaMask 支付交易费并捐款的过程。

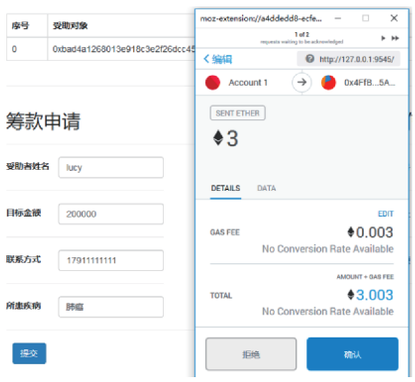

图 4　筹款申请信息

Fig. 4　Fund-raising application information

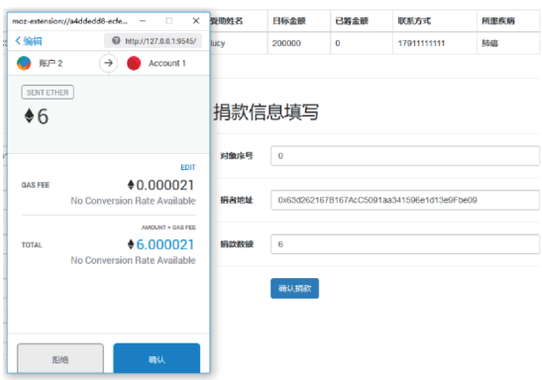

图 5　捐款信息

Fig. 5　Donation information

4.3　与传统平台对比分析

与传统模式下的筹款捐助平台相比，本平台有较大优势，主要分析如下：

1) 筹款信息真实可靠。本筹款捐助平台转换为后台审核机构，负责对筹款信息进行审核，将筹款信息上链存储、筹款信息发布、转账交易操作等工作交由智能合约自动完成，使机构职能专一；同时增添了保证金罚没机制，让筹款申请工作更为严谨，能有效避免骗捐现象。

2) 善款到账及时。传统筹款平台中受助人需要向平台申请拨款，等待审核后才能使用善款，人工操作有一定的时延。本文方案中当善款达到目标金额时，无需等待，触发智能合约转账事件，智能合约自动执行转账操作。

3) 善款不被挪用。本文利用智能合约严格约束最后善款到达地址，转账过程由合约自动完成，其他人无法插手，一旦转账地址不一致，智能合约将拒绝进行转账操作，使得善款无法被挪用。

4) 善款流向透明。将筹款申请及捐款交易信息全部记录在区块链中，每个节点保存完整的区块链信息，无论是捐款人还是受助人，都可以随时查询到和自己相关的善款流向。

5　结语

相对于传统筹款捐助平台来说，本文将智能合约和筹款捐助相结合，解决了传统平台的信任问题，本文贡献主要表现在：1)探究了如何将智能合约应用于筹款捐助平台，设计实现了一种新的应用方案；2)用户作为以太坊网络中的节点进行

筹款或者捐款,通过智能合约明确善款的最后使用者,防止善款被挪用;3)通过区块链的全网共识和保证金罚没制度,防止欺诈的筹款行为;4)利用智能合约代替人工转账操作,免除善款久未到账问题;5)通过区块链的时间戳唯一标识每笔善款交易,进行善款跟踪。

进一步工作如下:

1)本文为了保证信息的真实可靠以及善款流向透明化,采用区块链对信息和交易进行存储,区块链中的数据是完全公开透明的,在某种程度上也暴露了用户的隐私信息,后期需要考虑是否可以采取某种两者兼顾的方法;

2)本文最初对筹款申请的审核涉及到第三方调研机构,后期考虑是否同样也可以用智能合约替换掉第三方,利用智能合约在保证用户隐私的前提下完成自动审核,这方面工作可能会涉及到医院等更多主体以及更为复杂的关系;

3)共识算法对平台效率有一定影响,后期还需针对底层共识算法进行改进,以提高系统效率。

参考文献 (References)

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2019-03-27]. https://bitcoin. org/bitcoin. pdf.

[2] CHINCHILLA C. Ethereum: a next generation smart contract and decentralized application platform [EB/OL]. [2019-04-01]. https://github. com/ethereum/wiki/wiki/White-Paper.

[3] DELMOLINO K, ARNETT M, KOSBA A, et al. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab[C]// Proceedings of the 2016 International Conference on Financial Cryptography and Data Security, LNCS 9604. Berlin: Springer, 2016:79-94.

[4] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management[C]// Proceedings of the 2nd International Conference on Open and Big Data. Piscataway: IEEE, 2016: 25-30.

[5] PORRU S, PINNA A, MARCHESI M, et al. Blockchain-oriented software engineering: challenges and new directions[C]// Proceedings of the IEEE/ACM 39th International Conference on Software Engineering Companion. Piscataway: IEEE, 2017: 169-171.

[6] HUH S, CHO S, KIM S. Managing IoT devices using blockchain platform[C]// Proceedings of the 19th International Conference on Advanced Communication Technology. Piscataway: IEEE, 2017: 464-467.

[7] PIERONI A, SCARPATO N, DI NUNZIO L, et al. Smarter city: smart energy grid based on blockchain technology[J]. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8(1): 298-306.

[8] O'DWYER K J, MALONE D. Bitcoin mining and its energy footprint[C]// Proceedings of the 25th IET Irish Signals and Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies. Stevenage: IET, 2014:280-285.

[9] KISHIGAMI J, FUJIMURA S, WATANABE H, et al. The blockchain-based digital content distribution system[C]// Proceedings of the IEEE 5th International Conference on Big Data and Cloud Computing. Piscataway: IEEE,2015:187-190.

[10] 章宁,钟珊. 基于区块链的个人隐私保护机制[J]. 计算机应用, 2017, 37(10): 2787-2793. (ZHANG N, ZHONG S. Mechanism of personal privacy protection based on blockchain[J]. Journal of Computer Applications, 2017, 37(10):2787-2793.)

[11] 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[J]. 计算机应用, 2017, 37(S2):287-292. (LI Q, LI Q, ZHU J M, et al. Model and platform of charity application based on block chain technology[J]. Journal of Computer Applications, 2017, 37(S2):287-292.)

[12] 李奕,胡丹青. 区块链在社会公益领域的应用实践[J]. 信息技术与标准化, 2017(3):25-27. (LI Y, HU D Q. Application of blockchain in charity donation use case[J]. Information Technology and Standardization, 2017(3):25-27.)

[13] 陈志东,董爱强,孙赫,等. 基于众筹业务的私有区块链研究[J]. 信息安全研究, 2017, 3(3):227-236. (CHEN Z D, DONG A Q, SUN H, et al. Research on private blockchain based on crowdfunding [J]. Journal of Information Security Research, 2017, 3(3):227-236.)

[14] NOR R M, RAHMAN M M H, RAHMAN T, et al. Blockchain Sadaqa mechanism for disaster aid crowd funding[EB/OL]. [2019-05-20]. http://icoci. cms. net. my/PROCEEDINGS/2017/Pdf_Version_Chap07e/PID211-400-405e. pdf.

[15] JAYASINGHE D, COBOURNE S, MARKANTONAKIS K, et al. Philanthropy on the blockchain[C]// Proceedings of the 2017 IFIP International Conference on Information Security Theory and Practice, LNCS 10741. Cham: Springer, 2017:25-38.

[16] SZABO N. Smart contracts[EB/OL]. [2019-04-03]. http://www.fon. hum. uva. nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo. best. vwh. net/smart. contracts. html.

[17] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494. (YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4):481-494.)

[18] MERKLE R C. A digital signature based on a conventional encryption function[C]// Proceedings of 1987 Conference on the Theory and Applications of Cryptographic Techniques, LNCS 293. Berlin: Springer, 1987:369-378.

This work is partially supported by the National Natural Science Foundation of China (61672022, 61272036), the Foundation of the Key Disciplines of Shanghai Polytechnic University (XXKZD1604).

TAN Wenan, born in 1965, Ph. D., professor. His research interests include software service engineering, trustworthy service computing and composition, collaborative computing, business process intelligence technology.

WANG Hui, born in 1995, M. S. candidate. Her research interests include blockchain.