Journal of Computer Applications
计算机应用,2017,37(S2):287-292
ISSN 1001-9081
CODEN JYIIDU
2017-12-20
http://www.joca.cn

文章编号:1001-9081(2017)S2-0287-06

基于区块链技术的慈善应用模式与平台

李　琪,李　勍,朱建明*,关晓瑶,王　慧,郗晨梓
(中央财经大学 信息学院,北京 10081)
(*通信作者电子邮箱 zjm@cufe.edu.cn)

摘　要:针对我国目前慈善组织公信力不足、慈善事业发展受阻等问题,提出了一种基于区块链技术的慈善应用模式。首先,从用户类型定义,权限控制以及操作流程方面对该模式进行了介绍;然后,阐述了该模式的架构设计以及运作原理,并对加密、善款流向跟踪、账簿实时更新等关键技术实现进行了详细描述;最后,通过基于区块链技术的善款流动平台开发验证了该模式的可行性,模拟善款捐助、使用流程等表明平台可实现善款在捐款人与被捐款人之间的直接划转,并且限制被捐款人对善款的滥用;与此同时,可通过时间戳实现善款追踪与实时更新。通过优势分析和性能分析证明了该平台能安全、有效地跟踪善款流向,防止善款滥用。

关键词:区块链;慈善;善款捐赠;善款跟踪;防篡改
中图分类号:TP311　　**文献标志码**:A

Model and platform of charity application based on block chain technology

LI Qi, LI Qing, ZHU Jianming*, GUAN Xiaoyao, WANG Hui, QIE Chenzi
(*School of Information, Central University of Finance and Economics, Beijing* 100081, *China*)

Abstract: Concerning credibility lack of charity organizations and obstruction of charity development in China, a new charity application model based on blockchain technology was put forward. Firstly, the model was introduced from user type defining, right controlling and operational processes. Secondly, the architecture design and operation principle of the model were expounded and a detailed description was given about realization of encryption, cash flow tracking, real-time update of books and other key technologies. Finally, through developing the donation platform based on blockchain technology, the feasibility of the model was verified. By simulating donation and its use and other processes, it is proved that donations can be transferred directly between the donors and the donees, and the platform can effectively restrict abuse of donations by donees. At the same time, cash flow tracking and real-time updates was achieved by using the timestamps. The advantage analysis and performance analysis prove that the platform can safely and effectively track the flow of donation and prevent the abuse of donations.

Key words: block chain; charity; donate money; track donation; tamper resistance

0　引言

近年来,随着移动互联网的兴起,信息披露程度越来越高,慈善组织作为公益团体其不良事件也时有发生,概括起来主要存在以下几方面的问题:1)善款流向不透明。在现行的慈善系统内,由于人力物力种种局限,慈善组织很难做到财务信息完全公开,捐款人往往不清楚自己善款的最终去向,从而对慈善组织产生质疑,降低了慈善组织的公信力,影响了公众的捐款热情。2)相关法律法规难以贯彻落实。尽管国家已经出台了一系列的政策来规范慈善组织的信息披露,但由于我国慈善组织受到多重管理部门的监督,对于具体事务容易存在监管空白,为一些不法活动提供了可乘之机。3)缺乏专业人员。人力资源对于一个组织的良好运行至关重要。目前而言,慈善组织内部人员缺乏必备的相关专业技能,造成善款无法及时到位,降低了慈善组织的工作效率,更有甚者,私自贪污挪用善款,造成了恶劣的社会影响。4)国际化程度有待提高。目前而言,我国慈善事业仍在很大程度上局限于国内,与国际联系度不高,无法实现善款的跨国界流动,限制捐款规模。基于上述问题,本文研究利用区块链技术提出一种新的慈善应用模式,并基于该模式来搭建一个善款流动平台,以有效解决慈善系统存在的相关问题。

1　研究现状

1.1　区块链技术

作为比特币的底层技术,区块链(block chain)[1]是去中心化的、分布式的数据基础设施,每个节点(即用户)的权利和义务都相等,共同管理、监督整个区块链的运行,共同维护公共账簿。在区块链中,数据以电子记录的形式被永久储存下来,存放这些电子记录的文件被称为"区块(block)"。区块是按时间顺序先后生成的,每一个区块记录它在被创建期间发生的所有价值交换活动,所有区块汇总起来形成一个记录合集。每一种区块链的结构设计可能不完全相同,但大致结构上分为块头(header)和块身(body)两部分。块头用于链接到前面的块并为区块链数据库提供完整性保证,块身则包含了经过验证的、块创建过程中发生的价值交换的所有记录。每个节点利用工作量证明(proof-of-work)[2]、共识等算法将全部交易信息散列

收稿日期:2017-06-07;修回日期:2017-08-14。
基金项目:北京市哲学社会科学重点基金资助项目(14JGA001);中央财经大学青年教师发展基金资助项目(QJJ1541)。
作者简介:李琪(1996—),女,河北廊坊人,主要研究方向:区块链;　李勍(1996—),女,山西汾阳人,主要研究方向:国际金融;　朱建明(1965—),男,山西太原人,教授、博士生导师,博士,CCF 会员,主要研究方向:信息安全、电子商务/电子政务安全;　关晓瑶(1996—),女,辽宁抚顺人,主要研究方向:区块链、智能合约;　王慧(1997—),女,海南海口人,主要研究方向:区块链;　郗晨梓(1998—),女,江西抚州人,主要研究方向:机器学习、数据挖掘。

后加上时间戳封装成区块，随后快速向全网进行广播，由此形成的区块链可以被视为一个安全性极高的链状数据库。同时，每个节点都存有区块链数据库中所有信息，能够很好地防止数据丢失，且每笔交易都是公开且透明的，无论款项大小，都能记录交易的来源去向。交易过程有以下几步：发起交易，证明工作量，记账，全网广播，全网记账，交易完成。在此基础上，数据库和整个系统的运作是公开透明的。在系统的规则和时间范围内，节点之间无法欺骗彼此，因此系统中所有节点之间无需信任也可以进行交易，同时，它拥有不可篡改的时间戳，可以有效解决数据追踪、信息防伪等问题。

目前区块链属于一个新的研究领域，国内外许多科技公司和大学的研究人员都正在研究这一新技术。许多学者认为区块链技术对于互联网将产生颠覆性的创新，其去中心化、防篡改、信息跟踪等特点使它可以广泛地应用于供应链、证券、银行、股权交易、政务管理等领域。因此，学术界和工业界在近两年也对区块链给予了较高的关注，研究开发区块链在上述等诸多领域的应用场景，并取得了一定进展：O'Dwyer 等(2014)[3]提出将区块链技术应用于投票系统中实现匿名投票系统，保护敏感隐私数据；Watanabe 等(2015)[4]则利用区块链技术防篡改、可信任的特点，将其应用到权限管理中解决当前存在的问题，这在本文中也有所体现；Kishigami 等(2015)[5]提出将区块链技术应用到数字内容的版权保护上，利用其高安全性的特点以改善传统模式；夏新岳(2016)[6]基于区块链技术开发了一个股权资产系统，可使得股权交易不再依赖第三方平台从而实现防篡改；朱建明等(2016)[7]提出一个基于区块链的供应链认证模型，给区块链在 B2B + B2C (Business to Business + Business to Custom)供应链的应用提供了新思路；蔡维德等(2017)[8]对区块链的一致性和可拓展性的需求进行了分析，设计了第一个许可链的体系结构，给基于区块链技术的系统应用开发提供了更广阔的空间。

区块链技术主要解决交易中的信任问题，实现了跨时空交易，更加方便快捷。区块链不仅可以应用在经济金融领域，凡是对交易的真实性、可追踪性、安全性等有需求的各个领域都可以应用该技术。

1.2 相关研究现状

近年来，针对如何解决慈善组织出现的公信力下降等问题，相关学者进行了广泛研究，主要可分为以下三类：第一类从内部控制方面提出改进措施，如许晓芳等(2012)[9]提出从立法与制度创新、良好的政府与慈善机构的关系、成本效益相结合三方面来对内部控制进行改进；贺昌余(2014)[10]提出利用层次分析法与模糊综合评价法，建立多层次的内部控制要素评价指标体系对慈善组织进行评价等。第二类则尝试提出新的慈善信息管理系统，如王坚(2013)[11]结合 ASP. NET3.5 技术和 SQL Server2008 数据库技术设计了慈善捐助信息管理系统，该系统的应用为被捐款人与捐款人搭建了一个交流平台；王云斌(2015)[12]利用模块化的思想，基于 MyEclipse8.0 开发平台了慈善信息管理数据库，规范了数据模块；虽说以上方法有一定的改进效果，但仍未改变传统的慈善捐款方式，慈善组织作为中介仍然存在，依旧有人为篡改数据的可能。随着区块链技术的发展，最近出现了第三类解决方案即区块链 + 慈善：李奕等(2017)[13]利用蚂蚁区块链平台帮助“听障儿童重获新声”“和再障说分手”等慈善项目实现善款筹集；陈志东等(2017)[14]则提出了众筹业务的私有区块链架构(Crowdfunding Private Block Chain, CPBC)来满足众筹业务的需要，并加强金融数据安全和公信力。这些研究给区块链在慈善领域的应用带来很大启发，本文在此基础上进一步探索，提出一种模式实现善款全程跟踪，并且限制被捐款人的善款使用、防止骗捐诈捐等行为。

2 基于区块链的慈善应用模式

2.1 基于区块链的慈善应用模式

基于区块链技术，本文提出了区块链在慈善领域的一种应用模式，如图1所示。在该模式下，捐款人与被捐款人直接联系，进行慈善捐助活动，不再需要慈善组织的信用作为背书。被捐款人可自行求助，当有捐款人愿意为其捐助时，被捐款人可即刻使用该善款但只能将其使用到特定的善款使用机构。此模式下资金流向透明可追踪，同时限制了被捐款人对善款的滥用。

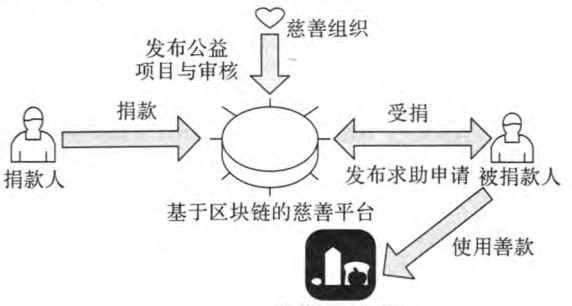

图1 区块链在慈善领域应用模式

图2给出了图1应用模式下基于区块链的慈善平台的使用流程，具体说明如下：

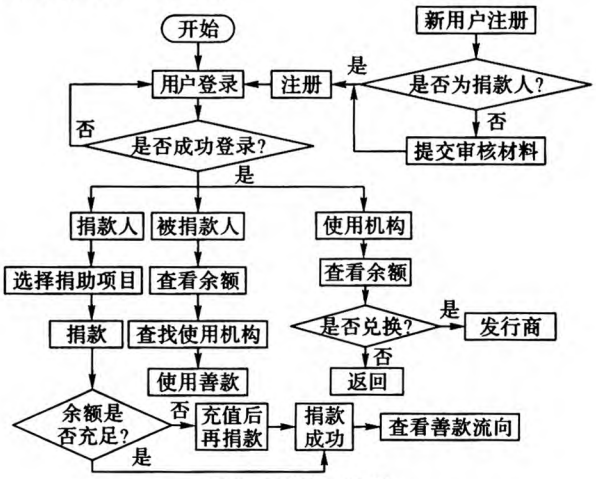

图2 平台使用流程

1)用户注册与登录。

首先，当新用户首次进入平台时，需要进行注册。其中，被捐款人和善款使用机构则需提交一系列审核材料以防止存在欺诈行为，待后台审核通过后方可加入。用户注册成功后，即可登录平台进行系列操作。

2)捐款人操作流程。

捐款人登录捐款平台后，可浏览相应的捐款项目选定项目后确定金额并进行捐赠，若余额不足系统会提示进行充值，充值后方可完成捐赠。

3)被捐款人操作流程。

当被捐款人需要使用善款时，他需要搜索对应的善款使用机构。如果善款使用机构不在平台内部，被捐款人需要联系该机构，之后机构提交对应材料申请加入平台。找到对应的善款使用机构后，被捐款人可以使用自己所获得善款获得相应的服务，如教育、医疗等。

4)善款使用机构的操作。

当该机构需要为被捐款人提供相应的服务时他可以直接联系发行商将账户中的余额兑换成现实货币,兑换完成后也将记录到数据库中;否则返回主页面。

2.2　基于区块链的善款流动平台

基于上述模式,本文开发了一个善款流动平台,该平台一定程度上解决了慈善领域存在的一些问题。平台架构如图3所示,分为两部分,共四层。第一部分是底层,包括存储和区块链,在此基础上进行全网交易及记录;第二部分包括为用户搭建的应用界面和与底层连接的接口,上层应用通过接口调用与区块链相连,导出交易记录,并向用户提供一系列服务。

图4给出此平台中的节点构成及相应权限。首先,发行商作为一个在此系统中单独存在的节点,主要负责在全网范围内发行货币,以及为其他节点分配兑换货币。其余节点可分为三类,捐款人、被捐款人与善款使用机构,每个加入该平台的用户都会成为一个独立的节点,并被赋予一个唯一的区块链地址,这个地址至关重要,是该节点的唯一身份标识并且是数据库从区块链上读取该结点相关信息的接口。捐款人可进行的操作主要有选取想要捐款的对象或项目后确定捐款金额,当账户余额不足时,需要向发行商寻求帮助进行充值,并且可以随时查阅善款流向。被捐款人的功能则仅限于接受捐款以及把善款划转到平台中的善款使用机构,无权将善款兑换提现。善款使用机构则有权将虚拟货币通过发行商转换为现实货币,在现实生活中用于被捐款人的教育、医疗等服务。

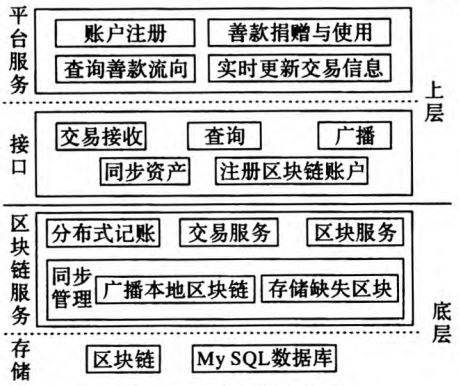

图3　善款流动平台架构

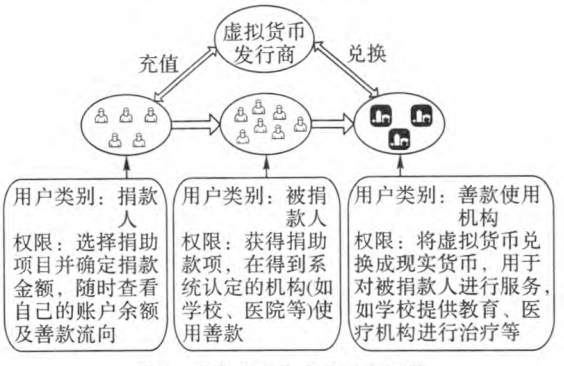

图4　平台节点构成及对应权限

3　原理及关键技术实现

图5展示了该平台的运作原理。本平台将布比公司开发的区块链作为底层技术,具体实现是通过布萌(基于布比区块链技术的数字资产网络)提供的接口进行连接。用户作为节点加入区块链,每一笔交易都是在区块链上进行的,交易相关信息都会被记录,但是为了增强数据的可读性并实现善款流向跟踪,在此基础上,平台创建了单独的数据库,分为用户数据库和交易数据库,前者用于存储用户个人信息,为防止信息泄露,平台对数据进行加密处理,后者记录相关交易,为防止交易信息篡改,平台的数据库会进行实时更新,关键技术实现在下文进行了详细叙述。

图5　平台运作原理

3.1　加密

平台使用国际广泛流传的三重数据加密算法(Triple Data Encryption Algorithm, 3DES)对全部用户信息进行加密处理。用户通过平台进行交易并显示生成的账目信息。在现实生活中,部分捐款人希望信息保密,因此在账目信息中并不显示用户的真实姓名等,仅以用户ID进行识别;同时为了防止不法分子窃取数据库中的用户信息,采用3DES加密算法对用户信息进行加密。

3DES是一种对称加密算法,利用3条56位密钥加上8位奇偶校验对64位数据进行3次加密。平台设置了一个随机密钥生成器。当用户注册时,平台将为用户随机生成三个56位的密钥。每次加密时对用户输入的信息进行分组处理,每个组长为64位,分别对每个组进行初始置换,之后进行16轮置换和代换的迭代函数,将最后一轮的64位输出进行左右互换后得到预输出,预输出经过逆初始置换的作用后产生64位密文。平台的用户数据库中存储的是加密后的密文,当需要进行交易而提取该数据库中的数据时,采用3DES解密得到需要的数据。

3.2　权限

权限设置关键在于限制被捐款人的权利,即其不能将善款转向其他被捐款人以及向发行商兑换。此处代码实现主要依赖于判断语句if及两个函数,具体为,当一笔交易在平台中申请进行时,系统中会对这笔交易资金的转入转出方进行判断,如果交易的转出方是被捐款人同时转入方不是善款使用机构时,系统会拒绝此笔交易请求,提示重新检查交易双方。判断资金转入转出方的用户类型时通过函数isdonee和isinstitution实现。以isdonee函数为例进行说明,首先这个函数的输入值为用户名,输出为布尔类型是或否。接着需要连接平台创建的用户数据库,并将输入值与数据库中所有被捐款者的用户名进行比较,若成功匹配,则说明该输入用户名的确是一个被捐款人,此时布尔值赋值为真,并返回。isinstitution函数用以判断资金转出方是否为善款使用机构,实现类似,不再赘述。

1)判断某笔交易是否合法允许进行:

```
if(bubi.isdonee(fromBubiId) && !bubi.isinstitution(toBubiId)){
  end.add("交易不成功,被捐助人只能向捐款使用机构转账,请
  确定交易双方是否正确.");
  return end;}
```

2)判断资金转出方是否为被捐助人:

```
public Boolean isdonee(String username) throws
  ClassNotFoundException, SQLException{
  //连接用户数据库
  String driver = "com.mysql.jdbc.Driver";
  Class.forName(driver);
  Connection conn = DriverManager.getConnection("jdbc:mysql:
    //localhost:3306/bubiAccount", "username", "password");
  //判断输入值是否能与数据库被捐款人的姓名相匹配
  String string = "select tradeNo from donee where
    username = '" + username + "'";
  PreparedStatement ps = conn.prepareStatement(string);
```

```
//若匹配成功,则返回 true,不成功则返回 false
Boolean rs = ps.executeQuery().next();
ps.executeQuery().close();
ps.close();
conn.close();
return rs;}
```

3.3 善款流向

平台数据库中有一个总表,用于记录所有交易,每一条记录都包括交易双方用户名及其区块链地址、金额、交易时间以及唯一且不可更改的时间戳,此时间戳用来标识每笔善款,对于善款流向跟踪的实现有着重要作用。表1对该总表进行了简化,摘取了部分关键信息。其中A、B、C分别表示三种类型的用户,即捐款人、被捐款人及善款使用机构,下标1、2、3等表示不同的个体。

表1 简化的交易总表

善款来源	善款去向	金额	交易时间戳
A_1	B_1	10	T_1
A_1	B_2	5	T_2
A_2	B_1	3	T_3
A_3	B_2	7	T_4
A_4	B_1	5	T_5
B_1	C_1	6	T_6
B_2	C_2	9	T_7

接着根据该总表针对每个被捐款人进行筛选,得到每个被捐款人所得到的每笔善款来源的汇总表,如表2所示,B_1得到了三笔善款,而B_2得到两笔善款。

表2 被捐款人善款来源汇总表

被捐款人	善款来源	金额	时间戳
B_1	A_1	10	T_1
	A_2	3	T_3
	A_4	5	T_5
B_2	A_1	5	T_2
	A_3	7	T_4

被捐款人得到捐款后要把它用到相应的善款使用机构,但是由表2可知,一个被捐款人账户里的所有善款不一定是来源于同一个捐款人的,同时在使用善款时,来自一个捐款人的善款也不一定恰好去支付某一善款使用机构的费用,可能不足或盈余,所以需要制定一定的规则来规范善款的使用以便更好地实现善款跟踪。在此,平台规定根据时间戳的先后顺序进行善款的使用,即先得到的捐款会先被消费,若第一个捐款人捐赠的金额不足以支付善款使用机构的费用时,会从第二个捐款人的捐赠金额中扣除,以此类推,直到满足应缴费用。若被捐款人与善款使用机构的每笔交易的资金来源不同,则会分别记录,并且保留该资金来源的时间戳(被捐款人获得该笔善款的交易的时间戳)。表3给出了在该规则下进行善款流向跟踪的例子,在此例中,分别展示了两种情况,B_1需要支付C_1 6个单位,而由表2可知第一个捐款人A_1捐给他10个单位,足够支付,直接从该笔款项扣除6个单位;B_2需支付C_2 9个单位,由表2可知,第一个捐款人A_1的捐款5个单位显然不够,需要再使用第二个捐款人的4个单位,所以在记录中这9个单位被分解为5和4,并加以资金来源时间戳,这样一来捐款人通过将交易总表和每个被捐款人的善款使用明细表进行连接,如表3所示,便可直观明了地看到自己善款的具体流向。

表3 善款流向跟踪表

被捐款人	善款使用机构	善款来源	善款来源时间戳	单笔金额	总金额	交易时间戳
B_1	C_1	A_1	T_1	6	6	T_6
B_2	C_2	A_1	T_2	5	9	T_7
		A_3	T_4	4		

每次被捐款人向善款使用机构使用善款后,会新建一个数据表以显示每个被捐款人的剩余善款情况。当某笔善款使用完后,该条交易记录会记为0。在此例中,B_1收到来自A_1捐赠的善款共10个单位,减去支付了的6个单位,还剩4个单位,而B_1收到的来自A_2与A_4捐赠的善款并没有被使用,因此仍为原来的值。B_2将A_1捐赠的5个单位用完后还需要4个单位,继续使用A_3捐赠的善款,因此更新后B_2中来自A_1捐赠的善款余额为0,来自A_3捐赠的善款余额为全部7个单位减去使用的4个单位,更新后的善款剩余情况如表4所示。

表4 被捐款人善款剩余情况表

被捐款人	善款来源	金额	交易时间戳
B_1	A_1	4	T_1
	A_2	3	T_3
	A_4	5	T_5
B_2	A_1	0	T_2
	A_3	3	T_4

3.4 实时更新

平台交易数据库中存储每一笔交易并生成账目信息。交易数据库中的信息需要与底层区块链的数据库信息保持一致;同时为了防止不法分子入侵交易数据库篡改信息,在交易数据库中设置了实时更新机制,使用区块链数据库中存储的交易信息覆盖原交易数据库中的信息,由于区块链不可篡改的特性,默认其信息真实有效。平台通过在类 my task 中设置定时任务获取交易信息。

在获取区块链数据库中的信息时,布比区块链平台提供了对应的接口,只需提供相应的布比平台用户凭证及需要提取信息的用户的区块链地址即可获取。getUserTransFromWeb 函数用来获取区块链中某一用户的交易信息,getAllBubiAddress 函数用来获取全部用户的区块链地址,之后 getAllTransFromWeb 函数将调用 getUserTransFromWeb 函数来获取区块链中全部用户的交易信息,在这个过程中,用户作为转入方和转出方的交易被看作两条不同的交易,因此需要利用 if 语句判断是否重复并提取信息。最后根据获取的信息进行更新。实现过程中部分关键代码如下:

1)请求布比区块链接口获取单个用户交易信息。

```
String accessToken = factory.getOAuthService().
  getAccessToken();                          //提供用户凭证
String url1 = "https://api.bubidev.cn/account/v1/transaction?
  bubi_address=" + BubiAddress + "&access_token=" +
  accessToken;                    //请求接口并提供用户 bubi 地址
String result = HttpKit.get(url1);
```

2)遍历全部用户交易信息并提取不重复的全部用户交易信息。

```
for(int i=0; i<address.size(); i++){
  ArrayList <String[]> list1 = getUserTransFromWeb
    (address.get(i));          //调用 getUserTransFromWeb 函数
  Boolean check = false;
  for(int j=0; j<list1.size(); j++){
    for(int a=0; a<list.size(); a++){
```

```
if (list1.get(j)[1].equals(list.get(a)[1]) && list1.get(j)
  [2].equals(list.get(a)[2]) && list1.get(j)[3].equals(list.
  get(a)[3]) && list1.get(j)[0].equals(list.get(a)[0])){
                                        //判断是否重复
  check = true;
break;}}
if(check == false){list.add(list1.get(j));}
```

交易数据库更新时,对应的善款流向数据也要同时更新。平台在数据库中建立了附表,当跟踪某一用户的善款流向时,只需要查询该用户所对应的附表。若用户为捐款人,附表中包含了该用户所有捐出的善款及其对应的被捐款人,可以根据对应的被捐款人查询到善款的最终流向,这是正向查询,对应的数据库更新方式如上所述。若用户为善款使用机构,附表中包含了所有流向该机构的善款及其对应的使用者,查询其中每笔善款的来源,为逆向查询。若被捐助人使用的善款来自不同的捐款人,更新时仍按照时间优先的规则,即对应的时间戳被更新为所使用善款中最早得到的那部分所对应的时间戳。按照这样的原则进行更新,保证了善款流向数据与交易数据库中的数据的对应关系,即与区块链数据库保持一致,同时防止被篡改,安全高效。

4　优势分析

4.1　与传统慈善对比分析

与传统慈善相比,本文提出的应用模式有着较大优势,主要分析如下:

1)慈善组织职能转换。传统慈善组织内部相当于一个黑盒子,制约了慈善组织公信力的提升。而本文提出的应用模式中捐款人与被捐款人直接联系,将慈善组织转为后台审核机构,职能更为集中。

2)善款流向公开透明。在该模式下,生成的交易记录可以跟踪每一笔善款的来源以及具体使用机构,用户可以随时查询到善款的流向,实现了整个过程公开透明,激发了公众的捐助热情。

3)降低筹款难度。在传统慈善中,慈善组织能力有限,覆盖度有限,筹款时间长。在本模式下,可以即刻发起项目,只要获得捐款,被捐款人可以立刻使用。

4)节约慈善活动组织成本。传统的慈善组织运作需要耗费较大的人力、物力,而本平台将大大减少所需资源,降低管理成本;同时区块链网络在线上完成善款捐助及使用等工作,避免了线下到线上的转换时间成本。

5)提高公众对于慈善的参与度。传统慈善下善款来源有限,社会公众参与度较低。在本模式下,公众作为一个独立节点加入到整个网络中,可以看到所有求助者的信息,对被捐款人及捐款金额的选择有较大的自主性,可提高公众参与度。

4.2　与网络众筹对比分析

4.2.1　众筹简介

随着移动互联网的普及,众筹成为慈善领域的新模式。互联网众筹提高了公众参与慈善的深度与广度,公众也可以直观地看到受助者的情况,真实感更加强烈。受助者可以自己在社交网络上发布众筹文案进行筹资,也可以利用轻松筹等相关平台进行,当然后者更为普遍。以下主要以后者为例说明众筹的运作流程[15],如图 6 所示:当需要筹集资金时,受助者需要向平台提交申请及相关证明材料,平台审核后确定是否通过。通过后项目开始众筹,如果在一定时间内达到预定的筹资金额,视为众筹成功,受助人可向平台申请拨款并等待拨款;若众筹失败,则已筹集的款项被退回支持者。

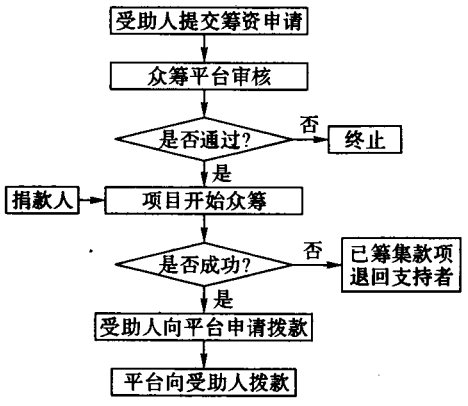

图6　众筹运作流程

4.2.2　对比分析

不可否认,相比传统通过慈善组织的捐款方式,众筹的确具有更为直接、方便快捷的优势,但是仍有一定缺陷,通过与其进行对比发现,本文提出的模式主要有以下优势:

1)平台将善款使用机构纳入系统,规范了被捐款人的善款使用,防止被捐款人善款滥用。而众筹这种新模式仍不能完全避免骗捐行为,一旦其拿到善款,具体使用途径也就不受限制了。

2)本模式以区块链作为底层技术,利用了去中心这一特点,无需任何交易成本,善款最大限度地使用到需要的地方。而众筹需要有专门的组织方,该组织的运营需要成本,同时众筹筹集到的资金需要提取一定比例的保证金后才能到达被捐款人手中,中间成本较高。

3)本模式中善款即到即用,无需任何等待。众筹平台在众筹成功后,需要受助人向平台申请拨款,审核后才能放款,中间有一定的时滞。

4)本模式下开发的平台对用户信息进行了加密,同时利用区块链防篡改的特点,保证了信息的安全性,而众筹平台很有可能被黑客攻破,泄露用户信息,造成款项丢失等。

4.3　与现有基于区块链的慈善平台对比

目前,也有许多国内外机构在尝试将区块链技术应用于慈善领域,但大多数仍处于开发阶段,国外较为成熟的代表是 heleperbit 平台,国内代表是蚂蚁区块链平台,本文以上述两个平台为例进行比较。

helperbit 平台对数据存储空间进行收费,被捐款人收到捐款时需要缴纳一定比例的交易费,中间成本高。其次,helperbit 是 P2P 平台,无法查看被捐款人收到善款之后的使用情况。同时 helperbit 不单单是慈善平台,在该平台上还能够同时进行国际贸易。

蚂蚁区块链平台上已有多个公益项目上线,并与多家慈善组织如壹基金、中国社会救助基金会等合作,反馈良好,但在该平台上仍然无法查看被捐款收到善款之后的使用情况,流向并不完全明晰。平台上线的项目均是慈善组织开展的公益项目,仍然依靠其信用背书。个人无法自行发布求助申请,存在局限性。

5　性能分析

5.1　平台功能测试

平台是在 Windows 操作系统下基于 Java、python、MySQL 语言以及 html 语言开发的。在开发完成后,对基于区块链技术的善款流动平台的每个功能进行了测试。测试环境是2 GB 的 CPU,4 GB 内存,500 GB 硬盘的计算机,Windows 8.1 操作系统,在该测试环境下平台实现基本功能的时间大约是4 s。

对平台主要功能模块进行测试的部分记录、测试用例及结果 如表5所示。

表5 平台功能测试用例及结果表

序号	功能概述	测试用例	预期结果	测试结果
11	用户登录,用户名或密码错误提示	输入不存在的用户名或错误的密码	提示用户名或密码错误	通过
22	查询善款信息	按照交易编号、类别等进行查询	显示对应的善款信息	通过
33	善款捐赠	捐款人登录后选择项目进行捐赠	捐款人成功将善款转到制定被捐款人账户	通过
44	使用善款	被捐款人登录后选择善款使用机构使用善款	被捐款人成功将善款转到善款使用机构账户	通过
65	权限测试(被捐款人无法滥用善款)	被捐款人登录后选择项目转移账户余额	提示无法转账	通过
66	查询善款流向	用户在项目明细处点击向前/后查询跟踪善款流向	显示对应善款的流向	通过

通过表5测试结果可以看出,平台实现了本文提出的应用模式所要求的基本功能,证明此模式是可行的。

5.2 安全性能分析

1)平台底层的安全性主要是区块链的安全性,其与每轮区块生成率(block generation rate per round,简记为f)相关[16]。f是指在每轮传递信息过程中所用的工作量证明算法解决方案的期望值,区块链安全性与f呈反比关系,因此可以用$1/f$来表示,f与区块链中其他性能变量之间的关系如下:

$$TransmissionSpeed \propto \frac{BlockSize}{BlockGenerationInterval/f} \tag{1}$$

其中:*TransmissionSpeed* 是区块链中的交易的传播速率;*BlockSize* 是区块的大小;*BlockGenerationInterval* 是区块生成的时间间隔。

另外,区块大小和区块生成时间间隔还有如下关系:

$$BlockSize = q \times m \times BlockGenerationInterval \tag{2}$$

其中:q是每秒上传的交易数量;m是对应交易数据的大小,对于目前本文所提出的平台所使用的区块链技术而言,*BlockGenerationInterval* 为3 s。因此,在 *BlockGenerationInterval* 给定的情况下,*BlockSize* 与q、m之间存在制约关系。由于慈善体系庞大,每秒上传的善款信息量较大。因此,在 *BlockGenerationInterval* 给定和 *BlockSize* 较大的情况下,根据式(1),为了使区块链的安全性(用$1/f$表示)保持稳定,平台需要保持较高的交易传播速率(*TransmissonSpeed*)。

2)在存储部分,对于用户数据库的安全性,平台利用3DES加密技术,其对于传统的安全攻击具有较好的抵御能力,攻击者无法在短时间内利用暴力破解的方式打开加密的用户信息。

3)交易数据库设置了实时更新机制,与区块链数据库中的交易信息保持一致,利用区块链的高安全性保证交易数据库的安全性。同时,平台在信息中加入时间戳能够较好地抵御攻击者发动的重放攻击。

6 结语

近年来,我国慈善组织公信力面临新的挑战,个别事件对慈善事业发展产生一定影响,虽然出现了一系列改进措施,但还是没有从根本上解决所面临的信任缺失等问题。伴随着区块链技术的发展,其去中心化、分布式记账等天然优势为慈善事业的发展提供了新的思路。本文探究了如何将区块链技术应用于慈善领域,基于此提出了一种新的慈善应用模式并搭建了一个平台来验证其可行性。在该模式下,用户作为区块链中的节点进行善款的捐赠与使用,并对不同用户进行了相应的权限控制以防止善款滥用。其次,通过时间戳唯一标识每笔善款以实现对善款流向跟踪并消除捐款人顾虑。最后,利用3DES技术对平台中的用户数据库进行加密,防止信息泄露。交易数据库则根据区块链上的记录实时更新,防止数据篡改。但是,区块链技术应用于慈善中仍然存在一些挑战,这些挑战中既源自区块链本身的局限性,又源自两者结合后的一些潜在的制约因素。首先,当平台推广使用后,数据量会急剧增加,进而导致更新效率降低;其次,对于区块链技术,国内发展态度尚不明确,具体落地环节仍存在挑战;最后,去中心化的技术必定带来一系列的监管难题。未来将进一步改进更新算法提高平台效率,并与相关公司合作进一步推广该平台。

参考文献:

[1] KAVANAGH D, MISCIONE G. Bitcoin and the Blockchain: a coup d'état in digital heterotopia?[C]// Proceedings of the 9th International Conference in Critical Management Studies: Is there an alternative? Leicester, UK: University of Leicester, 2015: 8 - 10.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].[2017-06-01]. https://bitcoin.org/bitcoin.pdf.

[3] O'DWYER K J, MALONE D. Bitcoin mining and its energy footprint[C]// Proceedings of the 2014 IET Conference. Stevenage, UK: Institution of Engineering & Technology, 2014: 280 - 285.

[4] WATANABE H, FUJIMURA S, NAKADAIRA A, et al. Blockchain contract: securing a blockchain applied to smart contracts[C]// ICCE 2016: Proceedings of the 2016 IEEE International Conference on Consumer Electronics. Piscataway, NJ: IEEE, 2016: 467 - 468.

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

[6] 夏新岳. 基于区块链的股权资产购买和转赠设计与实现[D]. 呼和浩特: 内蒙古大学, 2016: 37.

[7] 朱建明, 付永贵. 基于区块链的供应链动态多中心协同认证模型[J]. 网络与信息安全学报, 2016, 2(1): 27 - 33.

[8] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474 - 1487.

[9] 许晓芳, 朱国荣. 我国慈善机构内部控制构建思考[J]. 财会月刊, 2012(3): 35 - 37.

[10] 贺昌余. 我国公益慈善组织内部控制评价研究——以四川省红十字会为例[D]. 成都: 西南财经大学, 2014: 55.

[11] 王坚. 慈善捐助信息管理系统的设计与实现[D]. 成都: 电子科技大学, 2013: 57.

[12] 王云斌. 中国公益慈善信息管理系统的设计与实现[D]. 长春: 吉林大学, 2015: 53.

[13] 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.

[14] 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.

[15] 柯湘. 我国互联网公益众筹平台的运作及其风险自控、制探析[J]. 海南金融, 2016(11): 64 - 68.

[16] KIAYIAS A, PANAGIOTAKOS G. Speed-security tradeoffs in blockchain protocols [J]. IACR Cryptology ePrint Archive, 2015, 2015: 1019.