

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, 郝晨梓

(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 were 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; 郝晨梓 (1998—), 女, 江西抚州人, 主要研究方向: 机器学习、数据挖掘。