

# 区块链技术在小型区域价值流转中的信任优化机制研究与应用

沈宇帆

浙江理工大学信息学院, 浙江 杭州  
Email: mail@syficy.com

收稿日期: 2021年3月26日; 录用日期: 2021年4月22日; 发布日期: 2021年4月29日

## 摘要

随着电子商务技术的不断发展与应用, 物资的利用率却并未随之相应提高, 因此带来的是大量价值的浪费与闲置。根据创建节约型社会的需要, 如何有效提高物资的回收与流转尤为重要。而在传统的电子商务技术的物资回收流转中, 如何解决因信息不对称带来的信任缺失问题非常困难。本文研究在小型区域的物资回收流转过程中如何通过区块链技术提高物资流转的多方信任程度从而提高物资回收流转概率和减少价值浪费, 创新地使用零知识证明技术保证价值流转过程中地隐私。并且, 本文在典型的小型特征区域进行基于区块链技术的高可信度物资回收流转系统的设计、实现与应用。结果表明, 区块链技术在小型区域价值流转系统中构建了新的基于算法的信任机制体系, 减少信息不对称带来的信任缺失问题, 有效提高价值流转效率。

## 关键词

区块链, 信任, 电子服务, 价值流转

# Research and Application of Trust Optimization Mechanism of Blockchain Technology in Small-Scale Regional Value Transfer

Yufan Shen

School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou Zhejiang  
Email: mail@syficy.com

Received: Mar. 26<sup>th</sup>, 2021; accepted: Apr. 22<sup>nd</sup>, 2021; published: Apr. 29<sup>th</sup>, 2021

## Abstract

With the continuous development and application of e-commerce technology, the utilization rate of materials has not been correspondingly increased, so a large amount of value is wasted and idle. According to the needs of creating a conservation-minded society, how to effectively improve the recycling and circulation of materials is particularly important. However, in the material recycling and circulation of traditional e-commerce technology, it is very difficult to solve the problem of lack of trust caused by information asymmetry. This paper studies how to use blockchain technology to improve the multi-party trust of material circulation in the process of material recovery and circulation in small areas, thereby increasing the probability of material recovery and circulation and reducing value waste, innovatively use zero-knowledge proof technology to ensure wealth in the process of value transfer. In addition, this article designs, implements and applies a high-reliability material recovery and circulation system based on blockchain technology in a typical small characteristic area. The results show that blockchain technology builds a new algorithm-based trust mechanism system in a small regional value transfer system, reduces the lack of trust caused by information asymmetry, and effectively improves the efficiency of value transfer.

## Keywords

Blockchain, Trust, E-Commerce Technology, Value Transfer

Copyright © 2021 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

近些年来,随着电子商务技术的不断发展与应用,人们在电子商务平台上的消费次数与消费水平不断提高,相应的,资源的利用效率却在降低,如何提高资源价值流转效率成为建设节约型社会的重要问题。闲置资源再交易是一种重要的资源流转方式。但是,传统的在线闲置资源再交易由于网络环境的虚拟性、不确定性,使得交易双方信息的不对称性很高,并且由于网络交易欺诈行为的不断发生,导致消费者对在线的个人与个人之前的交易的感知风险大大增加,不信任感也随之加强,因此信任问题在事实上成为了在线闲置资源再交易与价值流转的最大障碍[1]。因此,优化闲置资源再交易的信任机制能够有效保证价值流转从而提高资源利用效率,充分利用物资价值,加快价值流转,减少价值浪费。

传统的电子商务信用体系往往基于用户和商家的反馈,以著名的电子商务供应商 Amazon 为例,其提供了交易伙伴可信度与交易商品可信度两种可信度评级体系,用户通过五星评级系统、评论等方式赋予商家或商品的可信度评级,从而实现其信任机制[2]。

由于信任程度对电子商务领域的巨大影响,不少学者对其信任机制进行了深入的研究。例如,王旭方等人建立了一种基于模糊理论的 P2P 电子商务信任模型,将信任化分为直接信任和推荐信任。用模糊集来刻画直接信任值,对影响信任主体的多种因素给出了详细的模糊综合评判算法。利用交易金额和交易时间来确定推荐信任的权值[3]。张辉等人开展了基于信任相似度的 P2P 电子商务信任机制研究,通过计算评价向量的相似度对评价的真实性进行准确的评估,提高了信任机制抗攻击的能力,并且引入惩罚因子,从而遏制欺诈节点的恶意行为[4]。

总体来说, 包含上述研究在内的一系列有关电子商务的信任机制研究虽然取得了一系列的进展, 但是在在线闲置物品交易领域仍然存在着局限, 主要的表现如下:

1) 难以遏制交易的恶意刷单行为。由于流行的在线闲置物品交易平台开放自由的特性, 相比起传统电商的注册门槛极低, 刷单成本接近于零, 在目前流行的闲置物品流转平台上, 可以非常轻易地伪造一笔订单的完成, 包括用户双方互相的评价信息。

2) 难以保证交易双方的隐私性。在当前流行的闲置物品流转平台上, 卖家的交易记录是公开透明的, 第三人可以查询卖家的历史交易记录, 这也是第三人评价卖家信任的重要方式, 然而同时却造成了隐私的泄露。

区块链技术是分布式数据存储、加密算法、共识算法等多种计算机技术的创新应用模式, 拥有去中心化、透明性、防篡改性等性质。陈纯认为, 任何需要信任的生活场景都可以尝试用区块链技术进行解决[5]。在共享经济与房屋租赁交易问题上, 林永民等人构建了基于区块链技术的房屋租赁信息生态圈模型, 通过非对称加密技术实现人与人的可信化互动; 通过智能合约技术实现人与信息的可信化交易; 通过块链式结构与分布式存储实现信息与环境的追溯交流[6]。在废弃纺织品回收领域, 马海景等人基于区块链技术, 构建了废弃纺织品回收再利用模式, 有效建立企业与顾客间的信任, 满足企业内外部信息共享、快速反应的要求, 推动废弃纺织品可持续发展[7]。白云飞等人分析将区块链技术引入共享经济核算的优点与可行性, 提出了基于区块链技术的共享经济核算方案, 构建了基于区块链技术的大数据共享体系框架[8]。

因此, 本文尝试通过区块链技术来优化闲置资源再交易过程中的信任问题, 另外, 高校校园作为知识与文化层次高且人群密集的地方, 电子商务具有非常大的发展潜力, 是非常典型的价值流转与闲置物资再交易的小型特征区域, 本文研究通过区块链技术优化高校校园价值流转的信任机制, 通过使用零知识证明技术来保护闲置资源交易多方的隐私。

并且, 基于上述研究内容, 本文开发基于 Uni-app 跨平台开发框架和 Gin 后端框架的前后端分离软件平台, 通过 Docker 进行部署, 应用区块链技术到高校校园闲置物资再交易中, 促进价值流转的效率。

## 2. 信任机制

传统的在线闲置资源交易平台上, 买家与卖家互相之间准确获取对方的信用度。用户与用户之间需要通过平台作为信用中介, 卖方在传统在线闲置资源交易平台上往往通过平台所显示的卖家出售物品的历史、评论口碑、物品信息等信息来判断买方的信用度, 但是这些信息在传统闲置物品交易平台上由于易伪造性和信息不对称等原因变得不可信, 用户非常容易感知其交易风险, 从而影响双方信任度。传统的信任机制模型图如图 1 所示:

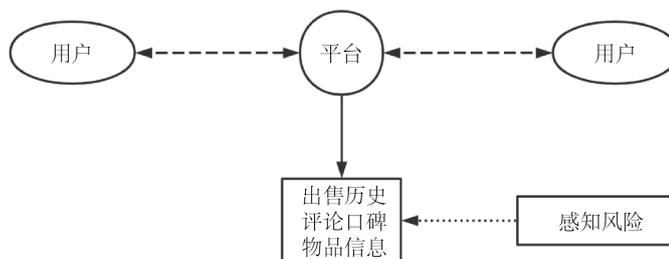


Figure 1. Trust model diagram of traditional online idle resource trading platform

图 1. 传统的价值流转平台信任模型图

以芝麻信用为代表的大数据征信系统广泛应用后相关的传统的在线闲置资源交易平台的信任程度虽然得到了较大的提升,并且有了统计学上的可度量参考值。但这种形式仍然存在一些局限,包括但不限于数据信息安全性不够高、数据信息真实性有待改进、评价体系有效性有待检验[9]。

区块链技术从技术层面进行信任机制优化,使得用户与用户之间没有平台作为信任中介,在链式账本的技术原理下实现去中介化的信任机制。链上的交易信息是公开透明可溯源的,并且用户个人的身份信息是可匿名的,非授权不可访问。其确定性和安全性是基于数学算法的,使得价值流转双方能够在对他人信息获取和自我信息保护之间找到平衡点,实现信任优化[10]。其信任模型如图2所示:

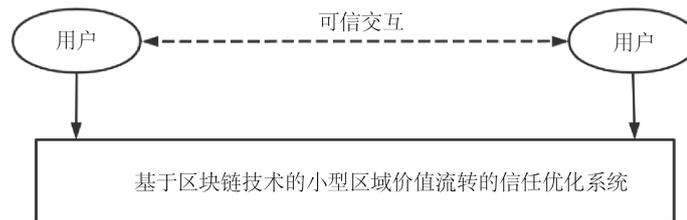


Figure 2. Diagram of the trust model in the value transfer platform based on blockchain technology

图2. 基于区块链技术的价值流转平台中的信任模型图

### 3. 系统需求

高校校园人口密集,文化素质与消费意愿高,对新技术的接纳程度更好,是非常典型的小型物资流转特征区域。高校校园内对物资流转的需求非常的大,因此本文将以高校校园为例,设计和实现一个基于区块链技术的高可信度物资回收流转系统。系统的目标人群为闲置资源拥有者和购买者,采用移动端或者PC网页端进行交易。各模块与子模块的功能如图3所示:

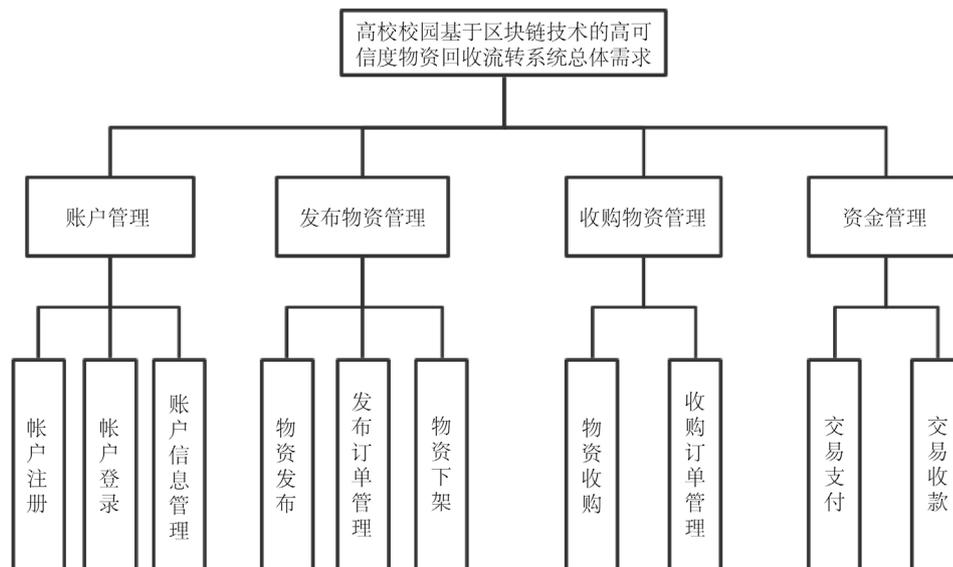


Figure 3. Analysis of overall system requirements

图3. 系统总体需求分析

高校校园基于区块链技术的高可信度物资回收流转系统总体需求可以分为账户管理、发布物资管理、收购物资管理,资金管理四个模块。账户管理模块负责用户的账户注册登入,以及相关信息的修改管理;

发布物资管理模块负责物资的发布和下架，当物资被其他用户购买后，出售者可以进行发布物资订单的管理；收购物资管理模块负责物资的收购以及收购订单的管理；资金管理模块负责交易的付款和收款。

## 4. 关键技术

### 4.1. VNTChain 区块链技术

在本系统中，区块链底层技术创新地采用了 VNT Chain。VNT Chain 是分布式智能价值网络，创造性地融合了公有链的分布式价值流转特性以及联盟链的商业属性，构建起由公有链，联盟链及跨链组成的聚合链架构。从而能够在拥有公有链的分布式价值流转特性的同时，融合联盟链信息安全共享的特性 [11]，符合高可信度物资回收流转系统的功能需求。

### 4.2. 智能合约

智能合约是一种在区块链中内含代码函数并能与其他合约交互的特殊协议，能够在没有第三方的情况下实现可信交易，并且在去中心化的同时这些交易具有不可篡改性。

VNTChain 的智能合约采用 C 语言进行编写，且 VNT Chain 的 Hubble Network 能够将 C 语言所编写的智能合约编译成 WebAssembly 格式的二进制代码运行，提供了 Bottle 工具实现智能合约的编译和 Nodejs 的合约部署与调用执行程序代码库。以订单部分为例，在本系统的智能合约编写如下所示：

```
#include "vntlib.h"
// 部署合约的地址
KEY address owner;
// 构造函数
constructor $Czqq()
{
    owner = GetSender();
}
typedef struct
{
    string id;           //订单 id
    string timestamp;   //时间戳
    string commodityId; //商品 id
    string status;      //订单状态
    string commodityHash; //商品详情的 hash 值
    string ipfshash;    //IPFS 地址
    string buyerId;    //买方 id
    string sellerId;   //卖方 id
    string amount;     //交易金额
    string payId;      //支付 id
    string note;       //备注
}orderInfo;
```

### 4.3. 零知识证明

零知识证明(Zero-Knowledge Proof)指的是证明者可以在不向验证者提供有用的信息的情况下使验证者相信某个论断是正确的。在小型区域价值流转中，闲置资源的交易双方对交易本身的隐私性可能非常看重，然而，第三方获取交易资源本身部分信息又是非常必要的，主要表现为以下两点：

- 1) 第三方用户需要确定交易的进行，并从中获得交易时间、交易金额等信息来进行信誉判断。
- 2) 监管部门需要保证资源本身是合法的，交易需要符合相关法律。

因此，VNT Chain 的 Galileo Network 利用零知识证明技术，将零知识证明模块化，可以快速应用和提供强大的隐私保护，完成对整个交易正确性的验证，可以验证每一笔交易而无需知晓交易的详情。

## 5. 系统架构

根据系统需求，本项目的技术开发架构如图 4 所示：

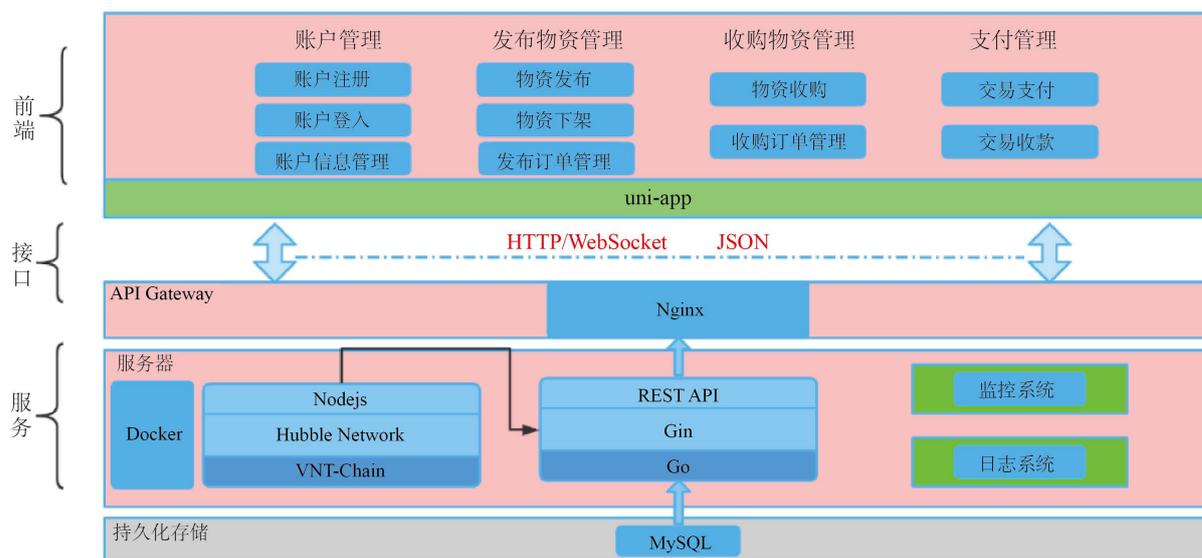


Figure 4. Overall system architecture

图 4. 系统总体架构

本系统前端部分采用 Uni-app 框架实现，考虑到移动平台如安卓、ISO 的兼容性不同，以及各类小程序更易被使用的特性，本系统使用 Uni-app 框架实现一套代码可在 IOS\Android\Web\微信小程序等多个平台发布，降低开发成本，提高系统的易接收性和易传播性。

本系统的后端部分使用 Docker 进行部署，实现系统部署的简易化和虚拟化，并且为分布式部署提供可能。同时利用持续集成技术，每当代码仓库有更新便自动触发脚本实现代码编译与打包部署到服务器上，实现持续交付。后端使用 Nodejs 对 VNTChain 进行操作，对于不需要区块链操作的请求，本系统使用基于 GO 语言的 Gin 框架实现功能，从而保证后端性能。系统的区块链核心是 VNTChain，由于交易信息属于用户隐私，因此使用零知识证明技术来避免用户隐私数据被非法窃取，创新地从技术层面上为本系统提供隐私安全保障。

## 6. 结语

本文通过构建基于区块链技术的价值流转平台中的信任模型，与传统的价值流转平台信任模型相比可以得出基于区块链技术的信任体系的建立对小型区域价值流转具有非常明显的促进作用。并且，基于零知识证明技术的隐私保护机制又能够解决物资流转中的用户隐私问题，这能够间接性提高对物资回收流转的信任，从而提高物资流转效率，说明了该模型具有可推广可实施的经济意义与显示意义。

通过应用，本系统创造性地使用 VNTChain 作为底层区块链技术，结合 Hubble Network 与零知识证明技术，能够满足小型特征区域如高校校园的物资交易的高信任需求，从而解决目前小型区域价值流转的痛点，加快物资流转的进程，具有非常良好的应用价值，对相关的研究提供了参考意义。

## 参考文献

- [1] 陈建. C2C 电子商务中信任的建立问题研究[D]: [硕士学位论文]. 大连: 东北财经大学, 2007.

- [2] Chang, E. (2006) Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence. Wiley, 145-146. <https://doi.org/10.1002/9780470028261>
- [3] 王旭方, 吴昊. 一种基于模糊理论的 P2P 电子商务信任模型[J]. 微计算机信息, 2012(1): 122-123.
- [4] 张辉, 张蓓蓓. 一种基于信任矩阵的 P2P 电子商务信任算法[J]. 网络新媒体技术, 2017, 6(4): 39-44.
- [5] 黄晓艳. 区块链创建信任——访中国工程院院士陈纯[J]. 高科技与产业化, 2017(7): 30-33.
- [6] 林永民, 史孟君, 陈琳. 构建房屋租赁信息生态圈中区块链技术应用研究[J]. 价格理论与实践, 1-4. <https://doi.org/10.19851/j.cnki.CN11-1010/F.2020.10.433>
- [7] 马海景, 曲洪建. 基于区块链技术的旧弃纺织品再利用模式[J]. 毛纺科技, 2021, 49(3): 100-105.
- [8] 白云飞, 郑又源. 共享经济核算引入区块链技术前景初探[J]. 统计与决策, 2021(7): 10-14. <https://doi.org/10.13546/j.cnki.tjyj.2021.07.002>
- [9] 许琪. 阿里巴巴芝麻信用存在的问题及相关建议[J]. 金融会计, 2015, 9(262): 78-82.
- [10] 梅兰妮·斯万. 区块链: 新经济蓝图及导读[M]. 北京: 新星出版社, 2018.
- [11] VNT Chain Distributed Smart Value Network Whitepaper. <http://vntchain.io/whitepaper-en.pdf>