中图分类号:TP311.13 文献标识码:A 文章编号:1007-9416(2022)08-0109-03
DOI:10.19695/j.cnki.cn12-1369.2022.08.36

区块链技术在时间银行的应用 *

宁波财经学院 杨昊楠 杨昱昺

随着社会的发展，老龄化的情况越来越严重。在这样的背景下，“时间银行”是一种新型的养老模式。区块链是一种分布式的账本，具有去中心化、不可篡改和透明公开的特性。通过区块链技术解决“时间银行”目前存在的问题。本文将区块链和“时间银行”作为研究对象，对两者进行结合，并对其设计的架构进行概述。

随着社会的发展，我国的社会已经进入了老龄化社会。老龄化带来了社会养老的问题，其对我国的居家养老为主体的养老带来了极大的负载。随着老龄化的加速，“时间银行”开始作为我国解决养老问题的新型方式。目前，“时间银行”存在着信用低下、标准未统一和安全性低下等问题。这些问题俨然成为了“时间银行”发展的阻碍。随着老龄化的提升，社会迫切需要这种新型的养老方式。

区块链诞生于 2008 年一名自称中本聪的作者所发布的一篇《比特币：一种点对点的电子现金系统》。在中本聪的这篇论文中就说到“我们需要的是一个基于密码学原理而不是信任的电子支付系统，该系统允许任何有交易想法的双发能够直接交易而不需要信任的第三方。”，而这里面所说的电子支付系统就是比特币，整篇论文的核心，区块链便是从比特币中诞生而出。

区块链具有不可篡改、去中心化和透明公开的特性。这正是“时间银行”所欠缺的也是“时间银行”所存在的问题。本文将区块链和“时间银行”作为研究对象，对两者进行结合，并对其设计的架构进行概述。

1 区块链相关概念

区块链是一种分布式账本，通过密码学、经济学和社会学等学科，保障数据内容安全，降低合作的成本和难度。区块链主要是去掉第三方信任机构，由参与者共同建立起一个可信的系统。区块链的去中心化是由网络层来实现的。网络层包含了点对点网络（P2P）、传播机制、验证机制。区块链从字面上的意思链式结构的区块集合，是由一个个区块链接而成。数据层中包含了区块链的链式结构、哈希函数、数据区块、非对称加密等技术。哈希函数这是一种将内容转为摘要的算法。在区块的链式结构中和数据结构中，均用到了哈希函数。链式结构主要是通过哈希值进行链接，在其初始区块中上一个哈希值为空或者一种特殊值即可，后续的区块保存前一个区块哈希值[1]。非对称加密技术并不是区块链中必要的技术，但在比特币中是一种必要的技术。

2“时间银行”相关概念

“时间银行”就是志愿者为老人提供服务获取时间币，当自己老了的时候便可以花费时间币来让志愿者服务自己。“时间银行”目前在我国处于可信度低、安全性差、标准未统一等问题。可信度来源于目前我国部分时间处于中心化的状态。采用了中心化的服务器也就是 C/S 架构来实现的，这导致了其控制权在“时间银行”的运营者之中，使其可信度降低，同时，容易被篡改和丢失，导致安全性差。标准未统一这是由于我国各地区采用了系统并非统一性所导致的。有的地方甚至采用纸质记录，这使得各地区“时间银行”货币转换及其困难。区块链所解决的一个问题便是“时间银行”中心化所导致的可信度。区块链为了取消第三方机构的加入，采用了点对点网络和密码学保障了数据的一致性和正确性，其具有很高的可信度及安全性。另外，区块链中采用统一的虚拟货币，比如比特币、以太仿等，在时间币的兑换中有了统一的标准。从“时间银行”目前出现的三大问题再契合区块链的特性及概念，得出区块链去信任化

收稿日期：2022-03-22
* 基金项目：国家级大学生创新创业训练计划项目（202113001023）
作者简介：杨昊楠（1999—），男，浙江台州人，本科，研究方向：区块链、物联网及应用。
通讯作者：杨昱昺（1969—），男，浙江绍兴人，硕士研究生，副教授，研究方向：软件技术、数据挖掘。

加强运营的公信度，透明性以及隐匿性提高了信息的安全性、去中心化提高了运营的效率[2]。

3 区块链技术在“时间银行”的应用设计

3.1 区块链和“时间银行”的契合

区块链具有去中心化、不可篡改和公开透明等特性正是“时间银行”所欠缺。区块链通过去掉第三方信任机构强化了“时间银行”的公信力，数据的公开和加密性均加强了“时间银行”信息的安全性，去中心化提高了“时间银行”的运营速度。提高公信力是由于区块链的去中心化和数据公开并且透明化等特性所带来好处。提高“时间银行”的运营速度是其去中心化，点对点网络中可以通过节点之间的功能组合或者均衡负载的方式来提高其“时间银行”的运行性能。提高“时间银行”的公信力主要是取消了第三方机构或者取消了独立的机构，也就是说将“时间银行”的中心化结构弱化或者取消从而实现了高信用度。安全性的提高是区块链中的不可篡改的特性，这个特性是由数据层和共识层共同实现的。本质上在数据层方面就已经完全具有其无法修改的特性，区块链是区块通过链式结构组合而成的，但这个结构并无法进行修改和删除只能添加，一旦进行修改和删除势必会对其后续区块的连接结构产生连锁反应。区块链和“时间银行”的契合度很高，“时间银行”中大部分问题均可以由区块链解决。

3.2 区块链嵌入“时间银行”的方式

在任素娟等[3]《我国发展互助养老“时间银行”的必要性及路径研究》中说到了坏账、通兑难、参与者少等问题，但这是其安全性低下、标准未统一和公信力差所导致的。在这篇论文中还有讲到运用区块链技术来保证其数据不可篡改、全程留痕、可追溯、公开透明，这样解决志愿者的后顾之忧，提高参与者的数量。“时间银行”中所有项目或者交易均围绕着时间币进行和展开，而基于区块链技术诞生的第一个软件便是比特币。那么利用区块链技术开发一个时间币的电子钱包系统便可解决坏账、公信力低等问题。

3.3“时间银行”结构设计

“时间银行”整体分为三层，上层引用下层，但每层均可以独立运行。如图 1 所示，“时间银行”主要包含了“时间银行”应用层、区块链层和点对点网络层，“时间银行”依赖于区块链层，区块链层依赖于点对点网络。三层结构的好处是因为每一层均可以独立运行。单独运行点对点网络层加入其中区块链的网络节点中，从而查看区块链在运行过程中所广播的信息以及作为坏节点发送错误信息测试区块链中容错率。点对层主要有广播机制、定点广播机制。区块链层便是包含其共识层、数据层。共识层可以采用其拜占庭容错算法（PBFT）。PBFT 算法是联盟链中的一个共识算法，但其效率极高，并且采用联盟链极大提高了“时间银行”的效率和公信力。数据层中区块链连接采用哈希函数来实现，通过保存上一个区块哈希值进行连接，实现区块的链式结构。其非对称加密技术是对交易进行签名，在其广播交易的时候进行验证交易的正确性。PBFT 贯穿于其数据层和网络层，交易广播和区块广播的时候便用到了 PBFT 保证其内容的一致性，在其执行写入区块的时候也是通过 PBFT 共识结束后进行执行的一项任务。“时间银行”中是通过调用区块链中的交易，账户管理等方法来实现。

图 1“时间银行”结构

Fig.1 "Time Bank" structure

3.4“时间银行”流程设计

“时间银行”中主要是嵌入了一个基于区块链技术的电子钱包（时间币）。其账户管理、交易、区块等均由“时间银行”调用区块链实现的。

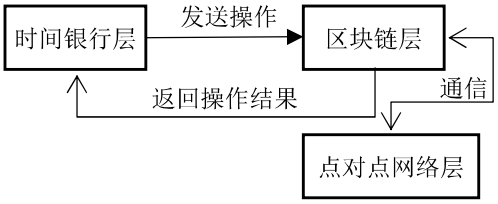

图 2“时间银行”各层之间操作

Fig.2 Operation between layers of "Time Bank"

如图 2 所示，“时间银行”应用层调用了区块链层的方法，区块链层返回其操作结果，而区块链则是通过调用点对点网络层的方法来实现其对等网络的组成、信息广播。简单说区块链层调用了点对点网络层的广播、连接、节点信息等方法，覆写了其中处理器和监听器。在区块链层中，发起交易的流程是先创建交易，验证交易数据（比如交易金额、私钥、发起者余额、发起人），再创建签名并通过拜占庭容错算法广播消息。节点接收到

这类消息后，会对交易进行一个签名验证，通过后加入交易池，此时主节点会对其进行区块创建，区块头只包含当前区块的索引、前一个区块哈希值和当前区块哈希值，而区块通过拜占庭算法广播，节点接收到后会将区块加入区块链中。区块链中账户创建流程，由当前节点创建账户，并通过 PBFT 广播账户的余额和账户的公钥，此时创建账户的节点开个定时器，若是超过了指定时间没有执行表示广播账户信息失败，也表示账户创建失败，否则所有节点写入账户信息，同时创建账户信息的节点保存账户详细信息，这时候账户算是创建完成。区块链在“时间银行”中只不过是一个账本，所有交易由它进行记录，同时区块链也公开账本所有记录，旨在“时间银行”中供参与者查看提高其中的可行度，但这部分信息参与者只能准确到自己的交易详情，也就说公开的只不过是其区块链中的区块信息，但这部分信息是已经加密了，用户只能看到表面。

3.5“时间银行”核心功能模块设计

“时间银行”是一个自治的系统，其功能主要可分为账户管理、项目管理，如图 3 所示。

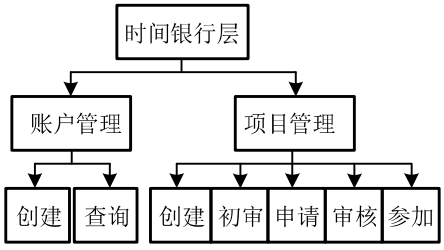

图 3“时间银行层”的核心功能模块

Fig.3 Core function module of "Time Bank Layer"

账户管理主要有创建账户、查询账户这两个功能。账户创建是通过区块链层发起创建账户，通过返回的公私钥进行账户信息的写入，而查询功能是通过调用区块链层账户查询获取到其账户的余额。

项目管理主要有项目创建、项目初审、项目报告申请、项目报告审核、参加项目。整个项目流程是项目创建，此时通过项目押金对其发起人中余额进行扣除（向区块链发起交易，交易接收者是节点账户），扣除失败是由定时器检测发现交易执行器超过一定时间没有该交易的确定，此时项目会直接进入异常状态，若扣除项目押金成功，则会进入初审，此时由审核人审核，只要超过一半数量通过，项目审核成功，项目进行发布状态，若是超过执行时间，审核未通过则进入异常状态，在发布状态中志愿者可以参加，由发起人进行审核是否同意参加，在执行期间和执行期间结束后可以申请项目报告，项目报告中含有参与者的金额以及报告内容，申请后审核人只要一半以上通过项目报告便会被抽取其中参与者金额部分，通过遍历参与者集合信息向区块链发送交易（交易是抽取发起人的余额，若不够则会出现欠款单，只要账户一有金额进入则直接扣款），并提供查询交易通知，失败则重新发起交易，并通知志愿者。

4 结语

区块链是“时间银行”的一个解药，能解决其大部分问题。随着社会老龄化步伐的加速，养老体系越来越需要一种新型养老模式的加入。“时间银行”的互助养老模式的应用可以有利缓解社会老龄化下养老的问题。区块链作为一个去中心化、不可篡改和公开透明的账本，将其与“时间银行”进行结合，可以解决“时间银行”的公信力低下、安全性低等问题。提供对“时间银行”进行结构化的开发，再将区块链层进行各地区的同步，在保留其各地区“时间银行”特设的情况下，解决其货币不统一且兑换困难的问题。

引用

[1] 张亮,刘百祥,张如意,等.区块链技术综述[J].计算机工程,2019,45(5):1-12.

[2] 黎昌珍,蒋媚.区块链嵌入“时间银行”优化策略研究[J].长白学刊,2021(4):120-126.

[3] 任素娟,张奇.我国发展互助养老“时间银行”的必要性及路径研究[J].医学与法学,2021,13(3):88-91.