基于联盟区块链的公益善款溯源系统研究

高玮军，王凯
兰州理工大学计算机与通信学院，甘肃 兰州 730050

摘要
针对当前公益慈善行业存在的善款流向不透明、不可追溯和捐赠信息易篡改等问题，构建了一种基于联盟区块链的公益善款溯源系统模型。共识过程中应用了一种改进的PBFT共识算法——DG-PBFT算法，将原有的主节点随机选举改进为积分制选举，并将原来的三阶段共识优化为两阶段。溯源系统依托Hyperledger Fabric平台进行开发，采用Go语言进行链码开发。配置4个组织，分别对应捐助者、受助者、慈善机构和监管部门。根据功能需求设计智能合约，不仅实现了善款信息的溯源，还能通过该溯源系统进行申诉与监督。实验结果表明，该溯源系统在保证了去中心化程度的同时，还可以增强数据的可信度，保证数据的安全性，降低通信开销，提高溯源效率。

关键词
区块链；超级账本；善款溯源；智能合约；去中心化

中图分类号：TP311 文献标志码：A doi: 10.11959/j.issn.2096-0271.2022078

Research on public welfare donation traceability system based on consortium blockchains

GAO Weijun, WANG Kai
School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Abstract
In view of the problems existing in the current public charity industry, such as opaque, untraceable and easy to tamper with donation information, a public charity donation traceability system model based on consortium blockchain was constructed. In the process of consensus, an improved PBFT consensus algorithm——DG-PBFT algorithm was applied, which improved the original random election of the master node to the points system election, and optimally transformd the original three-stage consensus into two-stage consensus. The system was developed on Hyperledger Fabric platform, and the Go language was used for chain code development. Four organizations corresponding to donors, recipients, charities and regulatory departments were configured. Smart contracts were designed according to functional requirements, which not only realized the traceability of donation information, but also could appeal and supervise through the traceability system. The experiment results showed that the traceability system could not only ensure the

degree of decentralization, but also enhance the reliability of data, ensure the security of data, reduce the communication cost and improve the efficiency of traceability.

Key words
blockchain, hyperledger fabric, donation tracing, intelligent contract, decentralization

0 引言

随着公益慈善事业的迅速发展，其在受到人们关注的同时也面临着信任危机。由于善款信息存储时采用的是集中式服务器，存在个人或慈善组织为谋取私利进行信息篡改的风险。同时，善款资金流向信息不透明，有关部门监管力度不够，导致公益慈善事业社会公信力低。因此，建立一个去中心化且多方信任的公益善款溯源系统对当前公益事业是十分必要的。利用区块链去中心化特点[1]可以将与慈善公益事业相关的信息分布于网络中的各个节点，可以避免为谋取私利而操纵或篡改慈善公益项目的行为。同时区块链技术具有公开透明和可追溯的特点，即所有的信息都是对全网公开的，每一笔款项信息都被存储在链上，方便点对点地查询和追溯每一笔交易的相关信息，保证了公益项目的公开性、透明性和可追溯性[2]。

而在公益善款溯源系统中，共识算法的选择也是至关重要的，作为区块链技术的核心，共识算法直接影响区块链系统的交易吞吐量、时延等性能指标。相对于传统的工作量证明（proof of work，PoW）[3]、权益证明（proof of stake，PoS）[4]等共识算法，Fabric网络主要采用了实用拜占庭容错（practical Byzantine fault tolerance，PBFT）共识算法[5]，该算法是一种基于状态机副本复制的分布式一致性算法，具有共识效率高、节约资源、可以容错故障节点和恶意节点等优点。但在共识过程中仍存在以下问题：第一，主节点的选举是基于节点编号的随机选举，导致选择故障节点或恶意节点的概率较高；第二，PBFT算法是一个三阶段共识算法，时间复杂度为$O(N^2)$，当网络中的节点增加时，共识效率会大大降低；第三，共识过程中的视图频繁切换会增加通信开销，导致服务响应速度变慢。

本文构建了一个基于Hyperledger Fabric的公益善款溯源模型并将其实现。首先，针对PBFT算法中存在的问题，提出了一种改进的PBFT算法——动态分组实用拜占庭容错（dynamic grouping practical byzantine fault tolerance，DG-PBFT）算法。在共识过程中，主节点的选举采用积分制，并将原有的三阶段共识优化为两阶段，降低了通信开销，提高了共识效率。其次，采用区块链技术解决了传统的中心化数据库存储数据存在人为篡改的问题，参与者可以对链上存储的善款信息进行溯源，并对其进行监督，保证善款信息准确无误。另外，溯源系统不涉及善款，即善款直接在捐助者和受助者之间流动，不需要通过系统进行交易，只采用区块链技术承担记账功能。

1 相关工作

近年来，随着区块链技术的迅速发展，其应用领域也从最初的数字货币扩展到食品、教育、医疗、公益慈善等领域。George R V等人[6]将区块链技术和食品标识符相结合，构建了一个可追溯的餐厅模型，实现了更加安全可靠的食

品溯源。Figorilli S等人[7]提出了基于区块链技术与射频识别(radio frequency identification, RFID)技术的木材链追溯系统,并将木材质量等相关信息整合到该系统,实现了木材的溯源。Lin Q J等人[8]采用以太坊公共区块链平台,将区块链技术和EPC信息服务相结合,开发了一种食品安全溯源系统,用于对食品供应链中的数据信息进行记录、共享及追踪,同时可用于检测和预防食品安全问题并追究责任。吴晓彤等人[9]构建了基于区块链的农产品溯源系统,实现了农产品的可信溯源,保障了农产品质量信息的安全性和可信性。禹忠等人[10]提出一种基于Fabric区块链的医药防伪溯源系统,实现了药品防伪及药品流通信息的溯源查询功能。

对于公益善款捐助过程中存在的种种问题,学者们进行了广泛的研究,传统的善款信息溯源方式是建立新型慈善信息管理系统。王云斌[11]采用模块化的思想,开发了慈善事业信息管理数据库,规范了数据模块。徐钰超[12]使用面向对象的思想,结合ASP.NET框架和SQL Server 2014设计了慈善捐助系统,搭建了捐助人与受助人之间的信息交流平台。许可等人[13]将SSH架构作为开发模式,采用分层结构和模块化设计方法,构建了一套安全稳定的网上捐助服务系统,提供7×24 h不间断服务。上述方法虽然对捐助系统进行了改进,但仍采用中心化数据库记录捐助信息,善款信息仍保存在慈善中介机构,因此捐助信息仍存在被篡改的可能。

随着区块链技术的发展,出现了一种新的解决方案,即“区块链+慈善”。赵丹青[14]阐述了基于区块链的互联网公益平台的开发过程,重点论述了不同的应用场景下各种共识算法的利弊及公益系统的应用层开发方法。但善款依托平台进行线上支付,并将善款以代币的形式存放在区块链系统中,大大增加了为谋取利益攻击系统的可能性,降低了系统安全性。李琪等人[15]采用布比区块链搭建了慈善应用平台,并对其进行了性能测试。但所搭建的系统中,善款只能在慈善机构规定的机构使用,以避免受助人滥用善款。但是在现实生活中,受助人在获得善款后只能在特定的组织机构使用显然不太合理。部分研究[16-18]采用以太坊和智能合约解决善款的追溯问题,但这些研究采用的是公链结构,受共识机制和节点数目的限制,这些研究都只能进行小规模应用。李奕等人[19]利用蚂蚁区块链平台搭建了一个善款筹集平台,该平台中所有的慈善项目都由慈善机构申请,个人无法使用这个系统发布受助请求,受助者参与度低。陈志东等人[20]则提出使用私有区块链技术实现众筹业务,使用私有链的方式构建慈善系统,然而私有链是一种完全被某个机构使用并控制的区块链系统,去中心化程度低,不能解决慈善捐赠系统存在的中心化数据存储的问题。

但联盟区块链技术在公益善款溯源领域的研究相对较少。因此,本文将基于已有的善款溯源方面的研究进行联盟区块链技术+公益善款溯源系统的研究设计。

2 系统模型

本文设计了基于区块链的公益善款溯源系统的工作流程及系统架构,主要功能有善款信息溯源、善款信息上链及链上善款信息更新等。

2.1 系统流程

图1展示了该系统的参与者进行公益捐助及善款信息上链的整个流程,该系统的参与者主要有捐助者、受助者、慈善机构及监管部门。在系统中,参与者身份不同,

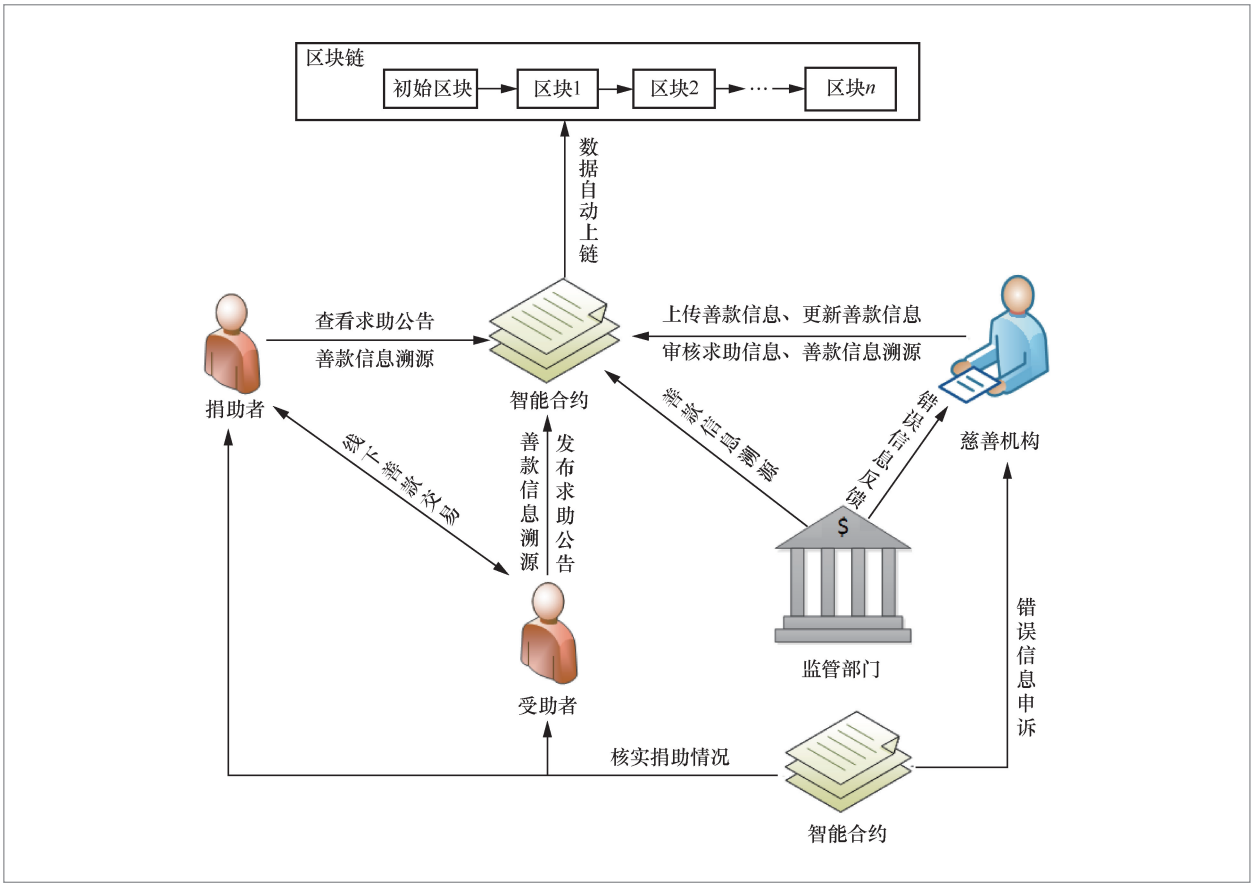

图1 基于区块链的公益善款溯源系统流程

所具有的职能也不同，各参与者共同维护系统的正常运转。以下对该系统中各参与者的主要工作流程进行介绍。

捐助双方在首次使用本系统时均须进行注册，注册之后完成登录才能使用本系统，受助者可以通过本系统进入求助信息发布界面发布求助公告。求助公告中主要包含求助人姓名、身份证号、求助金额和求助原因等信息。慈善机构接收到求助信息后，将求助人提供的个人身份信息与全国法院失信被执行人名单进行比对，核查求助人的征信情况，核查无误后，调用合约发布该求助信息，否则驳回该求助。

捐助者在进行捐助时，首先浏览未被捐助的求助公告，选择想要资助的求助者，根据求助公告上提供的求助人、银行账户等信息进行捐助。捐助完成后提交捐助者姓名、身份证号、汇款单号及汇款凭证等信息。慈善机构接收到此捐助信息后，根据捐助人身份信息及汇款单号在银行进行核实，将在银行查询到的转账信息与捐助人提交的捐助信息进行比对，若信息无误则认为此交易成功，将该捐助信息调用智能合约上传至区块链并进行存储，最后将该求助信息标记为已完成。

善款信息上链之后，整个捐助过程得以完成，捐助者和受助者均可以通过个人信息进行善款信息溯源以保证捐助信息无误，若出现错误则可以向慈善机构进行申诉，请求进行修改然后更新链上善款信息。

慈善机构对捐助信息进行核实，并确保善款已经准确无误地到达受助者账户，核实无误后对善款信息进行上链。除此之外，慈善机构也可以通过善款信息溯源确保提交的善款信息准确无误，从而保证受助者和捐助者的利益。

为了保证提交的善款数据信息的真实性，监管部门通过对善款信息溯源将可疑或有误的善款信息反馈给慈善机构，所有善款信息将在有关监管机构的监管下提交，上述每个操作均需要调用有关智能合约保证善款数据的可靠性、真实性和无误性，以增强捐助信息的权威性、透明度和公众信任度。

2.2 系统架构

本系统包括区块链模块、SDK模块、智能合约模块、Web服务模块和用户模块5个部分。系统架构如图2所示。

区块链模块由数据层、网络层和共识层组成，其主要功能是存储善款信息。其中数据层是该模块的核心，慈善机构对善款信息核实确认后进行加密，生成新的区块，链接在区块链的尾部。网络层是实现各个区块链节点间信息交互的基础，主要包括P2P网络及网络中的数据验证机制和数据传播机制等。共识层主要封装了共识算法，可以让高度分散的节点在去中心化的系统中对区块中数据的有效性达成共识。

SDK模块主要指的是软件工具开发包，Fabric-sdk-go是超级账本官方提供的Go语言开发包，是为特定的软件框架、硬件平台、操作系统等创建应用软件的开发工具集合，它提供了一个结构化的库环境，用于编写和测试链码应用程序，应用程序可以利用Fabric-sdk-go与Fabric网络进行交互并访问链码。

智能合约模块指的是合约层，主要指各种脚本代码、算法机制及智能合约等[21]。智能合约是运行在区块链上的一段可以自动执行的代码，可以处理成员节点达成共识的业务逻辑。而链码中定义了一个或多个智

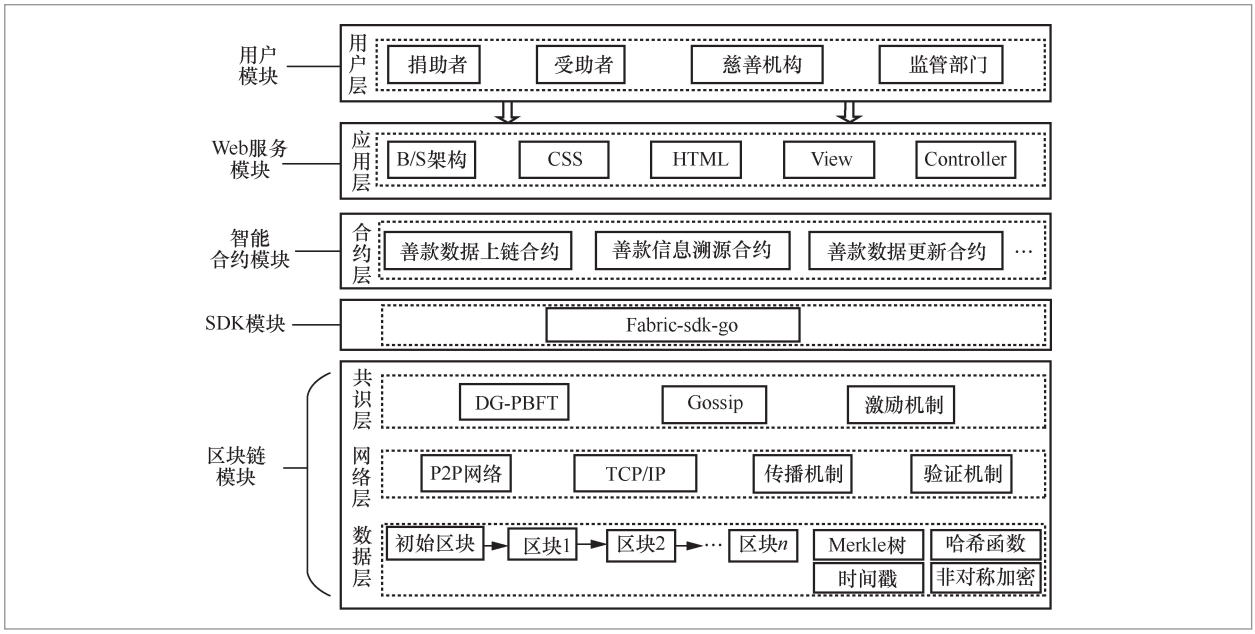

图 2 系统架构

能合约，每个组织都部署不同的链码，用来实现各个参与者特有的功能，同时还具有与Fabric网络进行交互的功能。

Web服务模块主要通过智能合约提供的接口和前端业务逻辑调用，为各参与者与Fabric区块链平台提供更加简洁的交互界面，从而提交各参与者的请求，执行善款信息上链和溯源等功能。

用户模块指的是用户层，包括善款捐助过程中的参与者，主要有捐助者、受助者、慈善机构及监管部门。

3 系统功能模块

3.1 区块链模块

3.1.1 区块链技术

区块链[3]的概念最早由中本聪在2008年提出。由于区块链技术具有安全可靠、不可篡改、去中心化等特点，其在数据存储、信息共享等领域[22]具有良好的应用前景。

根据对节点的开放程度不同，区块链可分为3类：公链、私链和联盟链[23]。公链是一种完全开放的区块链，即任何人都可以参与并使用区块链中的服务，其去中心化程度最高。私链只对单独的个人、机构或组织开放，中心化程度较高，常用于公司或组织内部。联盟链是由多个机构组成的联盟构建的，账本的产生、共识、维护分别由联盟指定的成员完成。相对于私链的高度中心化和公链的低共识效率，联盟链更适合在公益善款溯源中落地应用。

3.1.2 Fabric网络模块

根据系统的功能需求完成了Fabric网络环境的搭建，系统网络架构如**图3**所示。首先，本文采用4个组织代表各类参与者模拟真实的应用场景，各个组织的配置信息见**表1**。每个组织部署不同功能的链码，配置Peer节点唤起链码操作，同时每个组织都拥有自己的账本。最后将4个组织加

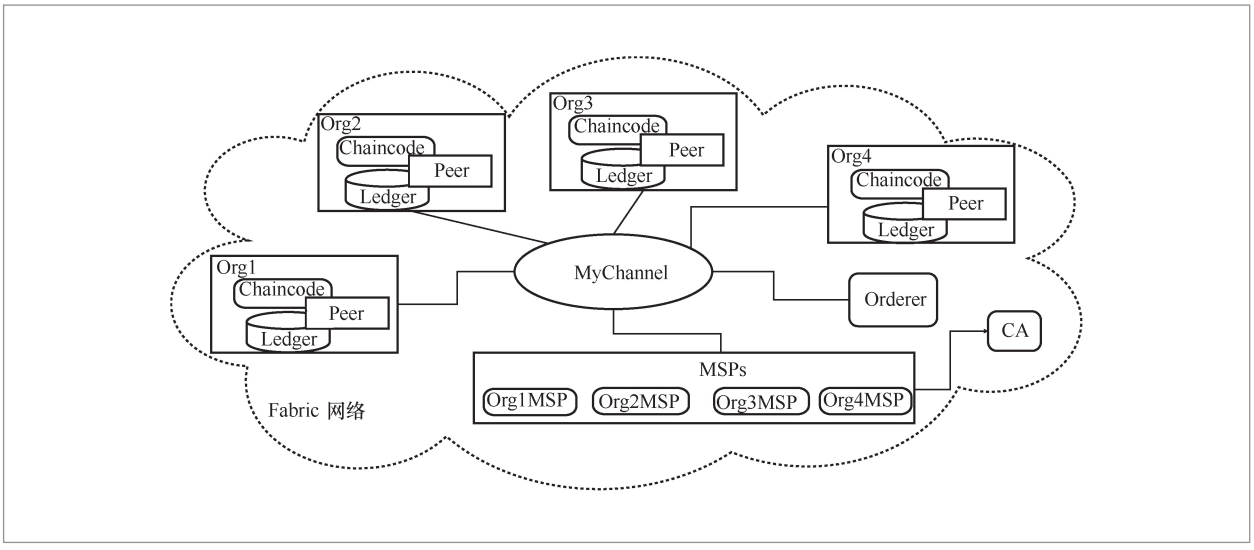

图 3 系统网络架构

表1 公益善款溯源系统组织信息表

参与者	组织名称	组织ID	链码名称
捐助者	Org1	Org1MSP	cc_offer
慈善机构	Org2	Org2MSP	cc_mission
受助者	Org3	Org3MSP	cc_receiver
监管部门	Org4	Org4MSP	cc_organization

入同一个通道，通道在维持数据和通信隐私的同时还提供高效的基础设施共享，并可以帮助组织将自己的工作与其他组织分开，同时通道还具有足够的协调性，在必要时能够协调各个独立的活动。

其次，网络环境中设置了一个Orderer节点，该节点主要负责通道创建、配置更新等操作，对交易消息排序并按照规则打包形成新区块，提交账本并维护当前通道中的账本数据，为全网节点提供交易信息广播、Orderer共识排序、Deliver区块分发等服务。

最后，由于Fabric是一个认证性的网络，区块链中的参与者需要利用成员服务提供者（membership service provider，MSP）机制向网络中的其他参与者证实自己的身份，从而在网络中进行交易。MSP包含一个被允许的身份列表，通过确定哪些是为其成员授权颁发有效身份的CA来识别和确定接受来自这些CA所定义的信任域的成员。

3.1.3 共识机制

针对PBFT算法在共识过程中存在的问题，本文提出了一种DG-PBFT算法。首先，对节点的状态设置评价机制，将节点划分为主节点、共识节点和执行节点，并为节点分配其对应行为的积分，在选举主节点时，选举积分最高的节点为主节点，以降低主节点为拜占庭节点的可能。另外，由于公益善款溯源场景下的节点需要进行身份认证并受到监管，节点可信度相对较高，主动作恶的可能性相对较低，因此将PBFT共识算法中的第2个通信阶段和第3个通信阶段进行合并，降低一致性协议过程中的通信开销，达到减小时延、提升系统吞吐量的目的。

（1）积分转换规则

DG-PBFT算法采用积分机制选举主节点，初始时每个节点的积分均为60分，在共识过程中，未响应的故障节点扣1分，恶意主节点扣3分，若节点为诚实节点，成功完成一次共识过程加0.5分。当网络中的节点积分值相同时，随机抽取一个节点作为主节点参与共识，否则将积分值最高的节点作为主节点。DG-PBFT算法流程如**图4**所示。

使用H_i表示节点i的积分值，N表示网络中节点的个数，每次共识过程结束后，通过对节点积分的更新实现节点状态的转换。若$60 \leqslant H_i \leqslant 100$，该节点为候选节点，可以优先被选举为主节点；若$0 \leqslant H_i < 60$，该节点为普通共识节点，可以参与共识过程，但不能被选举为主节点；若$H_i < 0$，该节点在之前的共识过程中发生过多次故障，此类节点不能参与共识过程，只能作为执行节点，若需要重新参与共识过程，则需要网络中的其他节点对该节点进行投票认证，认证通过后其才可作为普通共识节点参与共识过程。节点状态转换如**图5**所示。

（2）共识阶段优化

引入节点状态评价机制后，明显降低了主节点为拜占庭节点的概率，此时将原有的

三阶段提交的PBFT算法合并为两个阶段，省略掉原算法中的确认（commint）阶段，大大降低了原算法的通信开销。

优化后的共识过程包含以下4个阶段。

● 客户端请求阶段（request）。客户端C向主节点O发送消息请求，请求消息格式为：<REQUEST,o,t,c>，其中REQUEST为请求消息名称，o为请求的具体操作，t为时间戳，c为客户端标识。

● 准备阶段（prepare）。主节点在收到客户端的请求后，对请求消息进行验证，并将准备消息广播给网络中的从节点。准备消息格式为：<<PREPARE,v,h,n,d >,m>，其中PREPARE为准备消息名称，v为视图编号，h为节点积分值，n为消息编号，d为消息摘要，m为客户端发送的消息。如果通过验证，从节点将从准备阶段进入执行阶段。

● 执行阶段（implement）。节点收到准备消息后向所有节点发送执行消息，执行消息格式为：<IMPLEMENT,v,h,n,d,i>，其中i为节点编号，此时若节点收到了超过2f+1个不同共识节点的消息并验证通过以后，将进入回复阶段。

● 回复阶段（reply）。参与共识过程的节点i会给客户端一个最终的回复消息，回复消息格式为：<REPLY,v,t,c,i,r>，其中r为节点响应结果。

最后，若客户端收到f+1个相同的回复消息，则证明客户端发起的请求已达成全网共识。优化后的共识过程如图6所示。

3.2 智能合约模块

在Hyperledger Fabric区块链系统中，智能合约与账本一起构成了该系统的核心。智能合约主要定义了生成被添加到账本中的新事实的可执行逻辑。而链码是一种将智能合约部署到区块链网络中的通用容器，其中往往会定义一个或多个相关的智能合约，每个智能合约在链码中有一个唯一的标识名。应用程序通过合约名称

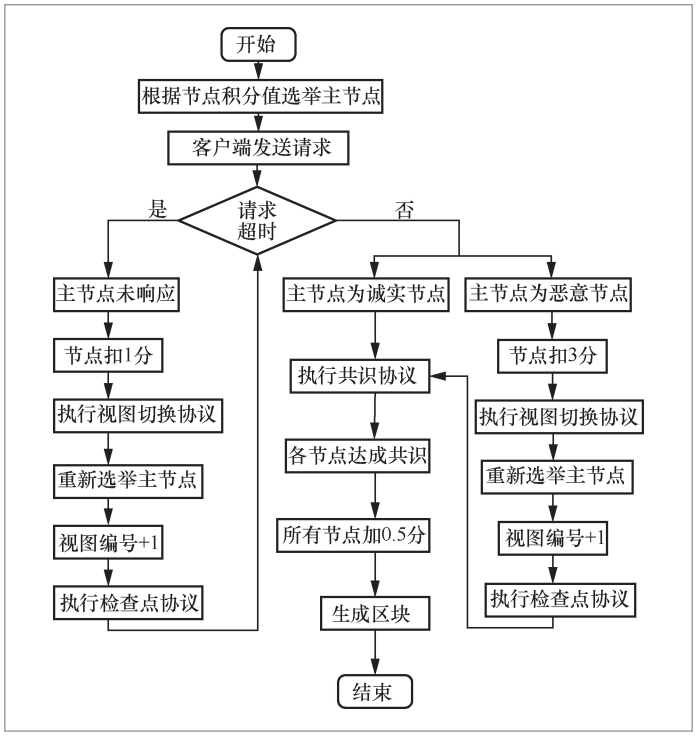

图 4 DG-PBFT 算法流程

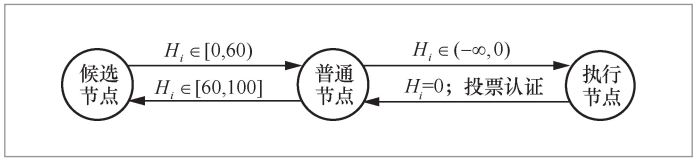

图 5 节点状态转换

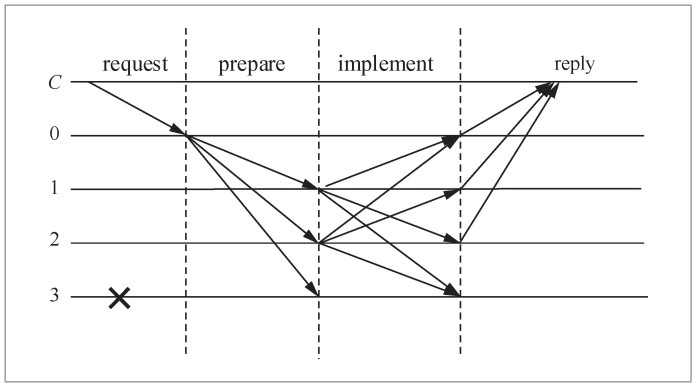

图 6 优化后的共识过程

访问链码容器内指定的智能合约，链码也可以用于Fabric的底层系统编程。

该系统为每个组织部署了不同的链码，链码中主要包括善款信息上链、善款信息更新、善款信息溯源等合约，其中善款信息溯源是每个组织都应具有的功能。每个组织部署的链码包含的智能合约各不相同，通过调用合约完成数据的上链存储和溯源查询，降低操作成本的同时也为系统管理提供了极大的便利。链码部署成功后，接下来的实例化过程中需要使用Init方法进行初始化，然后需要获取用户的意图，根据功能类型通过系统中的Invoke方法调用相应方法，如果获取的用户意图不是已经定义好的功能方法，则调用失败，返回空值。其中慈善机构上的链码功能流程如图7所示。

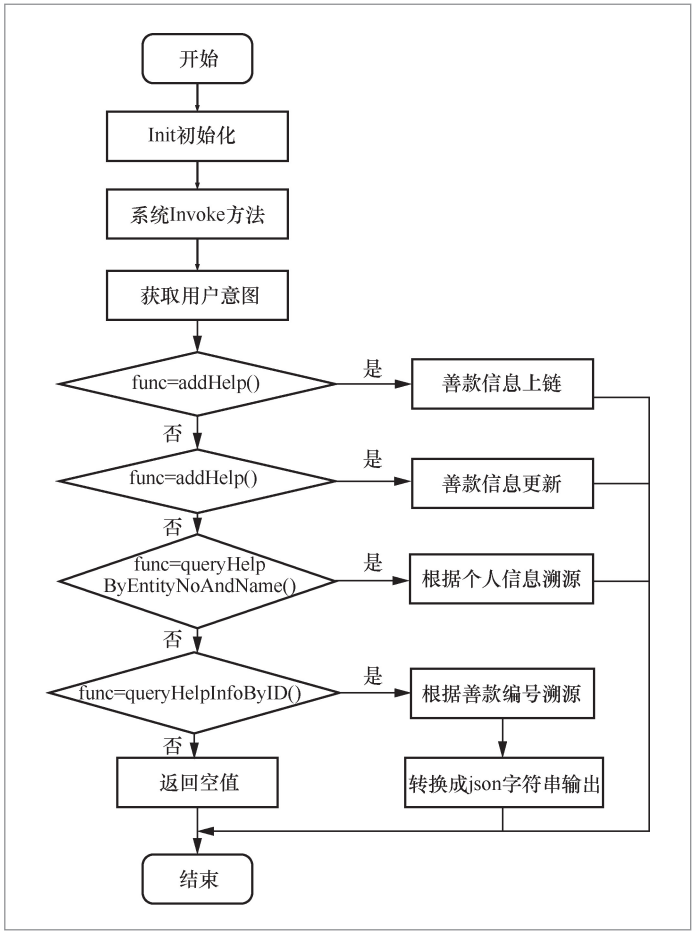

图 7 慈善机构上的链码功能流程

3.2.1 善款数据上链及更新

捐助双方在完成捐助过程以后，由慈善机构进行捐助信息的核验，确认无误后上传数据，系统自动调用数据上链存储智能合约，提高了信息管理的效率。善款数据上链完成后如果发现上传的数据有误，可以调用修改信息的智能合约进行数据更新，确保链上保存的数据真实可靠。数据上链存储及更新的智能合约部分代码如下。

算法1 善款数据信息上链

```
// args: PublicCharityObject
// 身份证号为key, PublicCharity为value
func (t * PublicCharityChaincode) addHelp(stub shim.ChaincodeStubInterface, args []string) peer.Response {
    ……//判断参数个数是否符合要求、检查反序列化信息是否成功
    // 查重: 编号必须唯一
    _, exist := GetHelpInfo(stub, edu.ID)
    if exist {
        return shim.Error("提交的善款信息编号已经存在")
    }
    _, bl := PutEdu(stub, edu)
    if !bl {
        return shim.Error("保存信息时发生错误")
    }
    err = stub.SetEvent(args[1], []byte{})
    if err != nil {
        return shim.Error(err.Error())
```

```
        }
        return shim.Success([]byte("信息提交成功"))
    }
```

算法2 根据善款标识编号更新善款信息

```
    // args: PublicCharityObject
    func (t *PublicCharityChaincode) updateHelp(stub shim.ChaincodeStubInterface, args []string) peer.Response {
        ……//判断参数个数是否符合要求、检查反序列化信息是否成功
        // 根据标识编号查询信息
        result, bl := GetHelpInfo(stub, info.ID)
        if !bl{
            return shim.Error("根据标识编号查询信息时发生错误")
        }
        //更新捐助者信息
        result.OfferName = info.OfferName
        result.OfferEntityID = info.OfferEntityID
        result.OfferAccount = info.OfferAccount
        ……//更新捐助者其他信息
        //更新受助者信息
        result.ReceiveName = info.ReceiveName
        result.OfferEntityID = info.ReceiveEntityID
        result.OfferAccount = info.ReceiveAccount
        result.HelpReason = info.HelpReason
        ……//更新受助者其他信息
        _, bl = PutHelp(stub, result)
        if !bl {
            return shim.Error("保存信息时发生错误")
        }
        err = stub.SetEvent(args[1], []byte{})
        if err != nil {
            return shim.Error(err.Error())
        }
        return shim.Success([]byte("信息更新成功"))
    }
```

3.2.2 善款信息溯源查询

溯源查询是本系统最重要的功能，本系统的所有参与者都有权限使用此功能，用于查看善款的来源、流向等具体信息。溯源查询提供了两种方式，一种查询方式基于个人信息，另一种查询方式基于善款信息标识编号。参与者可以有选择地使用上述两种方式中的任意一种完成善款信息的溯源查询。传统的善款信息溯源系统通常需要耗费大量的资源来维持正常的运转，防伪溯源的难度比较大。而使用本文搭建的基于区块链的善款信息溯源系统，只需要完成对各个组织相应链码的部署，后期自动完成智能合约的调用即可，大大减少了人力、财力等资源的消耗，简化了整个追溯流程，提高了溯源的效率。善款信息溯源部分代码如下。

算法3 根据个人信息进行溯源查询

```
    // args: EntityID, name
    func (t *PublicCharityChaincode) queryHelpByEntityNoAndName(stub shim.ChaincodeStubInterface, args []string) peer.Response {
        if len(args) != 2 {……}//判断给定参数是否符合要求
```

```
        EntityID := args[0]
        name := args[1]
        // 拼装CouchDB所需要的溯源JSON字符串
        queryString :=fmt.Sprintf("{\"selector\":{\"docType\":\"%s\", \"EntityNo\":\"%s\", \"Name\":\"%s\"}}", DOC_TYPE, EntityNo, name)
        // 查询数据
        result, err := getHelpByQueryString(stub, queryString)
        if err != nil { return }//根据个人信息溯源时发生错误
        if result == nil { return }//"根据指定的身个人信息没有找到相关的信息
        return shim.Success(result)
    }
```

算法4 根据善款标识编号进行溯源查询

```
    // args: number
    func (t *PublicCharityChaincode) queryHelpInfoByID(stub shim.ChaincodeStubInterface, args []string) peer.Response {
        if len(args) != 1 {return }//判断给定的参数个数是否符合要求
        // 根据标识编号查询状态
        b, err := stub.GetState(args[0])
        if err != nil {return }//根据标识编号溯源失败
        if b == nil {return }//根据标识编号没有找到相关的信息
        ……// 对查询到的状态进行反序列化、获取历史变更数据、迭代处理
        // 返回
        result, err := json.Marshal(Help)
        if err != nil { return }//序列化Help信息时发生错误
        return shim.Success(result)
    }
```

3.3 Web服务模块

系统通过Web服务完成智能合约与底层功能的交互，根据不同的功能设计了相应的页面以实现功能和页面的链接交互，形成了完整的系统架构。本溯源系统采用B/S架构，使用了MVC设计模式，该模式分为视图层、业务逻辑层和控制器层。其中视图层可以根据不同的业务逻辑选择相应的视图，并将运行结果返回给用户；业务逻辑层主要进行业务逻辑的判断，执行数据进行上链、溯源查询等操作；控制器层负责将用户输入的数据信息和操作指令传递给业务逻辑，具体的设计模式如**图8**所示。前端界面主要包含注册登录、发布善款求助公告、求助信息展示、上传善款信息及善款信息溯源查询等。网页设计使用HTML+JavaScript+css的组合方式，旨在为用户提供一个方便、美观、友好的可视化界面。

该溯源系统的Web服务部署在9000端口，各个参与者只需启动浏览器输入指定网址就可访问，前端功能模块均会调用智能合约，将交易数据完整地记录在区块链上。以一次善款信息溯源为例，参与者通过浏览器发出请求，后端在接收请求后会通过Web服务代码的运行调用区块链上的链码进行数据溯源，然后将得到的数据信息返回给浏览器，供用户查看。

4 溯源系统测试与分析

4.1 系统环境配置

本文构建了面向善款溯源的区块链网

络和系统模型，整个系统已经搭建完成且可以在测试网络中运行。系统设计的环境在虚拟机VMware中完成搭建，每个组织部署在一个虚拟机上，配置Peer节点实现整个运行过程，且搭建了区块链浏览器用于查看实时的出块情况和区块的具体信息。其中将慈善机构和Orderer节点部署在虚拟机1上，整个区块链网络由4台虚拟机构成，每台虚拟机和区块链环境的配置见**表2**。

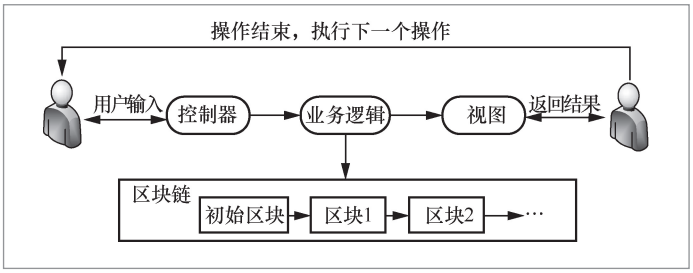

图 8 MVC 设计模式

表 2 参数配置信息

参数	值
操作系统	Ubuntu 16.04 LTS 64位
内存	2 GB
硬盘	40 GB
处理器	Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz
Fabric版本	Hyperledger Fabric v2.2
SDK版本	nodejs SDK

4.2 系统主要功能展示

4.2.1 善款信息上链

公益慈善机构对善款信息审核确认无误后，调用智能合约addHelp进行上链，该操作的执行权限仅可以由慈善机构完成，上链过程中包含的详细信息如**图9**所示。

为了核查善款信息是否完成上链操作和当前系统实时的出块情况，本系统在每个组织上都搭建了Fabric浏览器用于查看实时的区块数、交易数、区块创建时间及区块的详细信息等，其中慈善机构搭建的Fabric浏览器如**图10**所示。在对**图9**中的善款信息执行上链操作时，如**图11**和**图12**所示，当前交易的哈希值为87aada72055abc70f0c4ca6ddd7036fb23e190a4459f0149d3d274d105228eb0，该区块的哈希值为9852e8aee54acb51ac5e3df19503f3dc3facb5ac6738e90b0cac9cf292a12436，该区块中数据的哈希值为dfedb5853dbcff6fc83899648f6ee1d4feebdf8f608688e4d8f714db1d2c4d47。

4.2.2 善款信息溯源

传统的善款溯源系统将善款数据存放于中心化数据库中，容易被篡改，数据的安全性有待提高，溯源过程通常需要耗费大量人力财力，取证过程烦琐，需要多个参与主体的共同配合。监管部门通常只能在问题发生后才进行相应的调查与监管，实时性较低，并且监管的广度和深度有待加强。

在该系统中，所有参与者均具有对善款进行溯源查询的权限，通过共识机制达成一致性，共同维护区块链数据库，溯源查询的方式主要有两种，分别是通过个人信息和善款标识编号进行溯源，其中根据受助者信息溯源查询如**图13**所示，各参与者在进行溯源时仅需根据自己的信息调用相应的智能合约即可。在完成溯源操作后，首先查看到的是当前善款信息的更改记录，如**图14**所示第一条记录为最近一次更改的善款信息。如**图15**所示，如有需要可以查看每次更改善款信息的具体细节。此时系统参与者如果是慈善机构，还可以对该信息进行修改操作，修改完成后提交到区块链上，对链上保存的数据信息进行更

图 9 善款信息上链过程中包含的详细信息

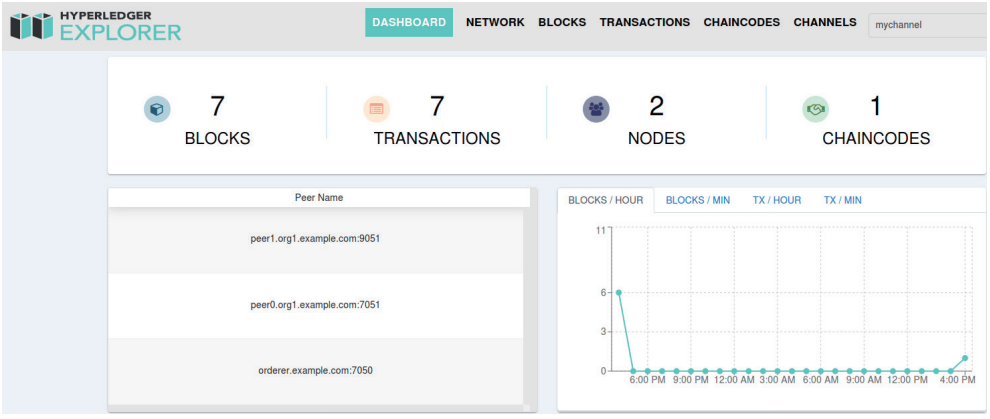

图 10 Fabric 浏览器

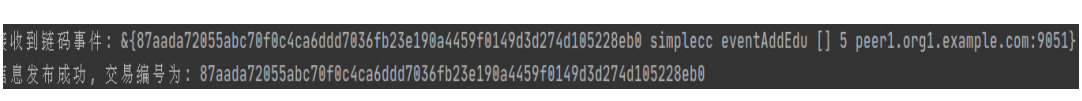

图 11 交易信息

图 12 区块信息

图 13 根据受助者信息溯源

图 14 善款信息更改记录

图 15 善款详细信息

新，系统会保留相应的更改记录，相对于传统的善款信息溯源，简化了追溯流程，提高了追溯效率。

4.3 系统功能对比

在系统测试完成后，将本文的溯源系统与3个基于其他技术的善款溯源系统进行比较，具体见**表3**。从**表3**中得知，4篇文献设计的系统都具有可追溯性，其中参考文献[12]采用的是传统的溯源系统，虽具有可追溯性，但是数据安全性得不到保障，且中心化程度很高，因此追溯效率也比较低。参考文献[20]和参考文献[16]都是基于区块链的新型溯源系统。前者采用的是私链结构，中心化程度较高；后者采用的是公链结构，虽然提升了中心化程度，但由于共识机制和节点数目的限制，效率仍比较低。通过对比可以得出，本文设计的溯源系统相比于之前的溯源系统，兼顾了去中心化程度和数据安全性，能够有效增强追溯结果的可信度，提高追溯的效率。

4.4 性能分析

4.4.1 吞吐量和交易时延

本文通过Hyperledger Caliper测试系统的性能，吞吐量和交易时延是衡量区块链系统的两个重要指标。吞吐量指的是在单位时间内处理完成请求的数量，而交易时延指的是从客户端发起交易请求到交易确认上链所需的时间，实验分别在PBFT算法和DG-PBFT算法下仿真了系统的吞吐量和交易时延。本试验以节点数量为变量，分别测试两种算法在不同节点数下的吞吐量和交易时延，为了减少误差，取100次请求的平均值为最终的实验结果。实验结果如**图16**和**图17**所示。

表 3 系统功能

性能	参考文献[12]	参考文献[20]	参考文献[16]	本文方法
可追溯性	√	√	√	√
数据安全性	×	√	√	√
去中心化	×	×	√	√
追溯效率	×	×	×	√

由**图16**可知，系统在两种算法下的吞吐量均会随着节点数量的增加而呈下降趋势，整体来看，PBFT算法吞吐量的下降速率高于DG-PBFT算法，引入DG-PBFT算法以后，系统的平均吞吐量也由189 TPS提升到355 TPS，性能显著提升，因此本文提出的DG-PBFT算法比PBFT算法更适合应用于公益善款溯源领域。

由**图17**可知，系统在两种算法下的交易时延均会随着节点数量的增加呈上升的趋势，当节点数量较少时，两种算法的交易时延差距较小，但是随着节点数量的增加，DG-PBFT算法的交易时延上升速率要低于PBFT算法，在多节点的环境下更加稳定。

4.4.2 通信开销

通信开销是指各个节点在一次共识过程中的通信次数总和。设系统中的节点总数为N，PBFT和DG-PBFT算法中系统发生视图切换的概率分别为P和Q。若系统中的节点采用PBFT算法进行共识，则单次共识的通信次数为$2N^2-N$，若此时主节点为恶意节点或故障节点，则发生视图切换的通信次数为$N(N-1)$，PBFT算法的总通信次数M如式（1）所示：

$$M=2N^2-N+PN(N-1) \quad (1)$$

DG-PBFT将原有的三阶段共识优化为两阶段，并在主节点选举时采用积分制，降低选举的主节点为恶意节点或故障节点的可能性，此时单次共识的通信次数为

N^2，发生视图切换的次数为 $N(N-1)$，DG-PBFT算法的总通信次数K如式(2)所示：

$$K = N^2 + QN(N-1) \quad (2)$$

在DG-PBFT算法中，此时发生视图切换的概率大大降低，即$Q<P$，当P=0.364，Q=0.226时，两种算法的通信次数如图18所示。

由图18可知，当系统中的节点数量不断增长时，PBFT算法通信开销的上升速率高于DG-PBFT算法。系统中节点数目为4个时，两者差距不大，PBFT算法完成一次共识过程平均所需的次数为32次，而DG-PBFT算法需要18次；当节点数目为24个时，PBFT算法完成一次共识过程平均所需的次数为1 328次，而DG-PBFT算法需要700次，通信开销显著降低。

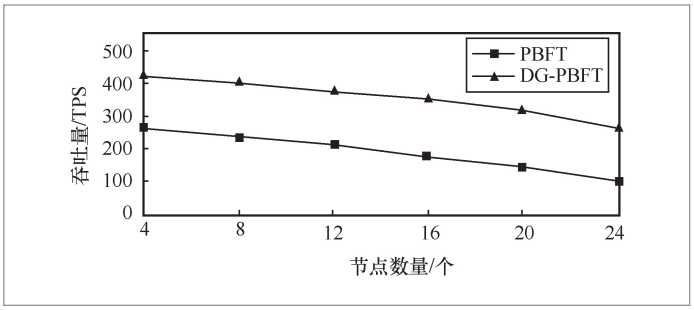

图 16 不同节点数下吞吐量

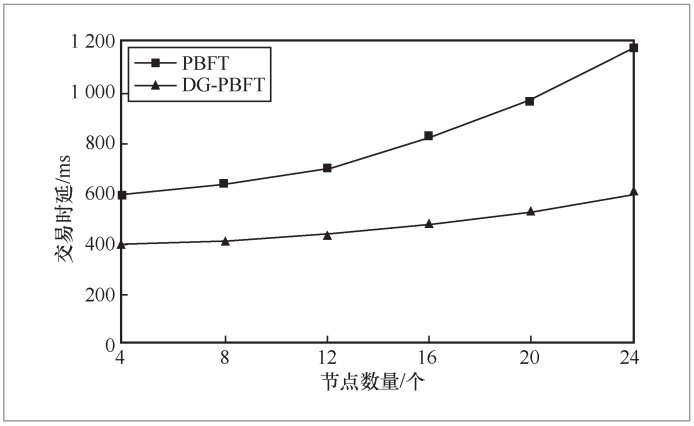

图 17 不同节点数下交易时延

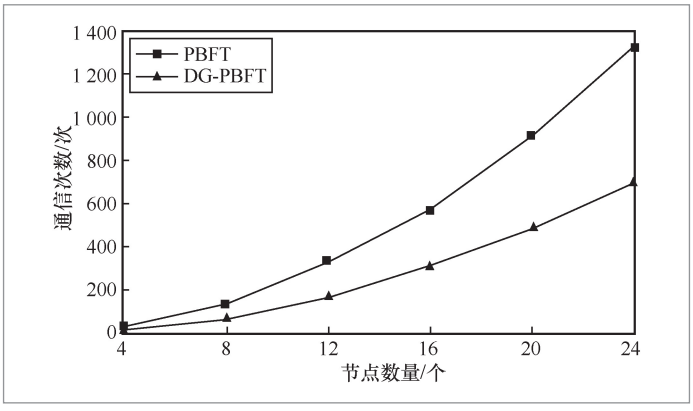

图 18 不同节点数下通信次数

5 结束语

本文通过研究Hyperledger Fabric的架构及实现原理，分析当前公益行业的现状及PBFT算法中存在的问题，对PBFT算法进行了改进，设计了基于DG-PBFT算法的善款溯源系统的框架，结合区块链技术和链码功能加入善款的详细信息并开发智能合约，完成功能测试，实现了一种基于Hyperledger Fabric的公益善款溯源系统。将区块链技术应用于公益善款溯源领域，实现善款捐赠的全过程可追溯，使系统参与者能溯源查询到善款流动的全部信息，提高了善款信息的透明度，推动慈善事业在社会发展更加透明，保证善款信息的可靠性，提升了社会公信度。

目前，区块链技术在国内还没有进行大规模应用，本文提出的系统架构模型除了可应用于公益善款信息溯源，还可以应用于其他领域，从而扩大区块链技术现有的应用场景，使区块链技术可以更快地应用及推广。相对于传统的溯源系统，本文搭建的系统整体上具有一定优势，但在部分功能的细节方面还不够完善，比如系统吞吐量及复杂环境下的系统安全性都有待提高，因此在下一步研究中将对系统功能进行逐步完善。

参考文献:

[1] 郝琨, 信俊昌, 黄达, 等. 去中心化的分布式存储模型[J]. 计算机工程与应用, 2017, 53(24): 1–7, 22.
HAO K, XIN J C, HUANG D, et al. Decentralized model for distributed storage system[J]. Computer Engineering and Applications, 2017, 53(24): 1–7, 22.

[2] CARO M P, ALI M S, VECCHIO M, et al. Blockchain–based traceability in agri–food supply chain management: a practical implementation[C]//Proceedings of 2018 IoT Vertical and Topical Summit on Agriculture – Tuscany. Piscataway: IEEE Press, 2018: 1–4.

[3] NAKAMOTO S. Bitcoin: a peer–to–peer electronic cash system[J]. Decentralized Business Review, 2008.

[4] LARIMER D. Transactions as proof–of–stake[Z]. 2013.

[5] ZHANG Y P, ZHANG P Y, TAO F, et al. Consensus aware manufacturing service collaboration optimization under blockchain based Industrial Internet platform[J]. Computers & Industrial Engineering, 2019, 135: 1025–1035.

[6] GEORGE R V, HARSH H O, RAY P, et al. Food quality traceability prototype for restaurants using blockchain and food quality data index[J]. Journal of Cleaner Production, 2019.

[7] FIGORILLI S, ANTONUCCI F, COSTA C, et al. A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain[J]. Sensors (Basel, Switzerland), 2018, 18(9): 3133.

[8] LIN Q J, WANG H Z, PEI X F, et al. Food safety traceability system based on blockchain and EPCIS[J]. IEEE Access, 2019, 7: 20698–20707.

[9] 吴晓彤, 柳平增, 王志铧. 基于区块链的农产品溯源系统研究[J]. 计算机应用与软件, 2021, 38(5): 42–48.
WU X T, LIU P Z, WANG Z H. Traceability system of agricultural products based on blockchain[J]. Computer Applications and Software, 2021, 38(5): 42–48.

[10] 禹忠, 郭畅, 谢永斌, 等. 基于区块链的医药防伪溯源系统研究[J]. 计算机工程与应用, 2020, 56(3): 35–41.
YU Z, GUO C, XIE Y B, et al. Research on medical anti–counterfeiting traceability system based on blockchain[J]. Computer Engineering and Applications, 2020, 56(3): 35–41.

[11] 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.
WANG Y B. Design and implementation of Chinese charity information management system[D]. Changchun: Jilin University, 2015.

[12] 徐钰超. 基于ASP.NET慈善捐助系统设计与实现[D]. 大连: 大连理工大学, 2017.
XU Y C. Design and implementation of charity donation system base on ASP.NET[D]. Dalian: Dalian University of Technology, 2017.

[13] 许可, 黄志炜, 黄培颖. 基于z/900大型主机的捐助服务系统的设计与实现[J]. 陕西科技大学学报(自然科学版), 2010, 28(5): 92–96.
XU K, HUANG Z W, HUANG P Y. Design and implementation of donor services systems based on z/900 mainframe[J]. Journal of Shaanxi University of Science & Technology (Natural Science Edition), 2010, 28(5): 92–96.

[14] 赵丹青. 基于区块链的互联网公益平台的开发[D]. 上海: 上海交通大学, 2017.
ZHAO D Q. Development of Internet commonweal goods based on block chain technology[D]. Shanghai: Shanghai Jiao Tong University, 2017.

[15] 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.
[16] SIRISHA N S, AGARWAL T, MONDE R, et al. Proposed solution for trackable donations using blockchain[C]// Proceedings of 2019 International Conference on Nascent Technologies in Engineering. Piscataway: IEEE Press, 2020: 1–5.
[17] HANDE R, AGARWAL T, MONDE R, et al. CharityChain – donations using blockchain[C]//Proceedings of International Conference on Computer Networks and Inventive Communication Technologies. Cham: Springer, 2020: 606–612.
[18] SAI D V, SAI A Y, REDDY E K, et al. Funds transfer using blockchain[J]. International Journal of Computer Sciences and Engineering, 2019, 7(3): 76–79.
[19] 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, 30.
LI Y, HU D Q. Application of blockchain in charity donation use case[J]. Information Technology & Standardization, 2017(3): 25–27, 30.
[20] 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.
[21] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292–2303.
[22] LU Q H, XU X W. Adaptable blockchain–based systems: a case study for product traceability[J]. IEEE Software, 2017, 34(6): 21–27.
[23]邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969–988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969–988.

作者简介

高玮军(1973–), 男, 兰州理工大学计算机与通信学院副教授, 软件工程系主任, 主要研究方向为企业级软件工程架构、大数据处理、分布式计算、机器学习、人工智能及区块链技术。

王凯(1999–), 男, 兰州理工大学计算机与通信学院硕士生, 主要研究方向为区块链技术、网络与信息安全。

收稿日期: 2022-06-13
通信作者: 王凯, 1393108786@qq.com
基金项目: 国家自然科学基金资助项目(No.61762059); 甘肃省引导创新发展项目(No.062004)
Foundation Items: The National Natural Science Foundation of China (No.61762059), Gansu Province to Guide Innovative Development Projects (No.062004)