使用区块链的可追踪捐赠的拟议解决方案

N.Sai Sirisha
学生，CMPN系
VESIT，Chembur
印度马哈拉施特拉邦孟买
，2015sai.nadiminti@ves.ac.in

Tarasha Agarwal
学生，CMPN系
VESIT，Chembur
印度马哈拉施特拉邦孟买，
2015tarasha.agarwal@ves.ac.in

兰吉特-蒙德
学生，CMPN系
VESIT，Chembur
印度马哈拉施特拉邦孟买，
co2013.ranjeet.monde@ves.ac.in

李卡-亚达夫
学生，CMPN系
VESIT，Chembur
印度马哈拉施特拉邦孟买
，2015richa.yadav@ves.ac.in

Rupali Hande女士
助理教授，CMPN系
VESIT，Chembur
马哈拉施特拉邦孟买，印度
2015rupali.hande@ves.ac.in

摘要--
缺乏透明度使人们对慈善机构失去信任，使社会资金停滞不前。捐赠者不知道其资金的合法使用情况。腐败加剧了捐赠者的不信任。本文提出了一个名为Charity-Chain的系统，这是一个建立在以太坊区块链上的去中心化网络。它帮助社会组织透明地运行项目，使用基于智能合约的激励机制，确保他们的影响得到独立验证，并让每个人都能获得。这使得资助者（慈善组织、影响力投资者、小额捐助者）更容易监测他们的交易，从而恢复他们对捐赠给这些社会组织的信任。

关键词-
区块链、以太坊、天然气、智能合约、账本、慈善机构

I. 简介

该文件涉及的问题是，与政府或其他捐助者提供的捐赠和资金有关的交易缺乏透明度。有必要让捐赠者跟踪他们的捐赠，并为社会资金带来透明度。其目的是确保个人捐款的可追溯性，并保证资金安全。这将有助于纠正公众对慈善机构信任度的下降，并满足捐赠者对其影响的更多信息的需求。通过区块链，捐赠将在很大程度上是透明的。捐赠者将能够通过慈善机构一直跟踪他们的捐赠，直到受益人，甚至更多。慈善链使用区块链来记录每一笔交易。由于区块链具有数据不可篡改和防篡改的内在品质，它进一步提高了项目的透明度和问责制。

II. 文献调查

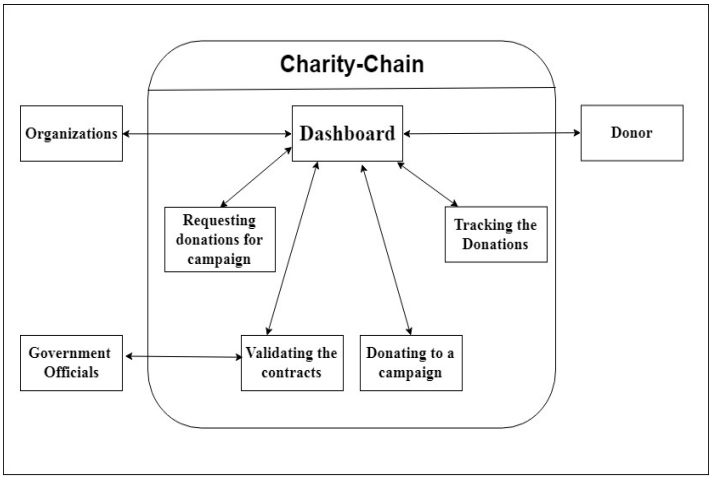
区块链提供了一种获得去中心化交易账本的手段，可用于生成、验证和向存在于同一网络中的其他节点发送交易。特定加密货币的各种加密哈希函数也增加了金融交易中需要的安全性。区块链可以应用于金融服务、医疗服务以及商业和工业[1]。如今，一个慈善机构的应用需要一个不依赖任何其他系统或应用程序的系统来验证自己。区块链正在被使用，因为它们不受限于某个特定的系统，而且可以独立验证交易的完整性和一致性。选择以太坊作为平台是因为它是一个公共平台，具有更好的可扩展性。它每秒钟可以运行7-20个交易[2]。通过区块链，慈善系统将不再被垄断和限制在一个权威机构中。公众将很容易接触到交易，并可以验证他们的钱是否像他们预期的那样被使用。中国政府是利用区块链力量的一个非常好的例子。它是第一个将区块链用于电子政务的国家。它有助于加强生产者、政府和公民之间的信任。它被用于确保易腐烂食品的质量。该应用程序安全地分享产品在每个阶段的状态。这些阶段包括制造、运输和销售[3]。中国和印度一样拥有庞大的人口。尽管这个事实，它已经成功地使用区块链来增加人民对政府的信任，使食品资源的生产变得透明。这有助于将资源平等地分配给人民，并增加政府的问责制，因为所有的交易都被记录下来，在出现差异的情况下可以查看。类似的用例也可以在印度实施，以管理其巨大的

978-1-5386-9166-3/19/$31.00 ©2019 IEE

人口。金融机构正在使用区块链来提高网络安全。区块链的优点是速度快、成本低、有一个去中心化的登记处，并提供安全的支付信息[4]。在印度，所有印度公民都有一个Aadhar号码，该号码可以证明他们的生物识别数据以及他们的位置和其他细节。Aadhar可以和区块链技术一起被用于许多应用，如医疗和投票[5]。通过区块链可以消除由于单点故障和隐私泄露造成的数据损失[6]。共识协议具有很大的意义，因为它决定了新节点被验证的参数。一个不合适的共识协议可能会导致在使用应用程序时出现不理想的结果[7]。区块链应用所面临的挑战是对资源和可扩展性的需求[8]。

III. 拟议的系统

系统模型已在本节中提出。应用程序的用户根据他们的角色进行分类，即捐赠者、组织、零售商、政府官员。



图：拟议系统的方框图1.。

组织（受益人）。这些是需要资源（金钱或其他）的慈善机构、非政府组织或其他社会企业。他们将能够在Charity-Chain系统上以预定的格式发布他们的需求。他们也将在采矿中发挥重要作用。

零售商。这些实体提出他们的标书和报价。政府官员会选择具有最佳报价的零售商。

捐赠者。他们是查看各组织发布的要求的实体，被接受的投标根据他们的能力和喜好选择捐赠给该事业。

政府官员。这个实体将认证各组织发布的要求，并验证智能合约。只有在经过官方认证后，捐赠者才能进行捐赠。

IV. 系统开发

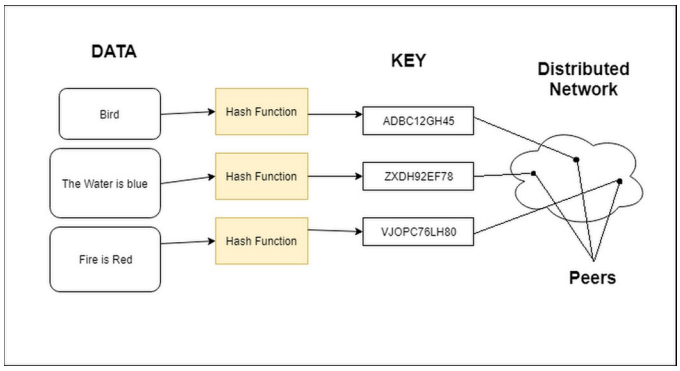
1) 区块链。区块链是去中心化的账本，旨在成为一种基于点对点架构的安全的数据处理方式[1]。区块链技术的两个特点是透明度和分布式数据架构。区块链技术通过消除中心化节点或任何第三方的处理需要而获得透明度。它是一连串的数据块，通过不同的连接节点相互连接，形成区块链的链式网络。一旦一个新的交易被共识批准，它就会被加密并与之前的交易相联系。一旦一个数据被添加到链上，它就不能被删除。如果对任何已创建的区块有任何修改，就会创建一个新的区块来说明这些修改，如果这个区块被网络的共识所批准，它就会被附加到链上。这样一来，如果冒名顶替者试图篡改记录的数据，他/她永远无法在未经网络同意的情况下修改已经创建的数据。区块链网络在区块链中创建一个区块所需的大致时间称为区块时间。以太坊区块链的区块时间为从到14秒15。所包含的数据在区块完成的时候变得可验证。分布式区块链网络是安全的，可以防止破解者在集中式计算机系统中利用的任何漏洞。使用的安全方法是基于公钥密码学。一个节点的公钥（一长串随机生成的数字或字符）用于解决区块链上的一个节点。通过区块链传输的代币被记录为与该地址的关联。私钥是一个秘密的关键词，它可以让其所有者访问他们的资产，或者它可以用来利用区块链现在提供的各种功能。存储在网络上的数据被认为是不可利用的或不可破坏的。我们提出的系统的核心是区块链网络，它将被建立在安全和快速的捐赠给受益人。由于区块链是透明的、去中心化的和不可改变的，拟议的系统将最适合于区块链提供的功能。以太坊是非常可变的智能合约的编程语言。

*2) IPFS：*InterPlanetary文件系统是基于分布式点对点架构的[9]。IPFS被用作区块链技术的存储系统，因为IPFS的工作与区块链的工作类似。区块链中的每个区块都与加密哈希函数生成的哈希值有关。这个值被用作存储目的的索引。使用这个唯一的哈希值可以检索到文件或区块。IPFS是创建一个永久的、去中心化的网络的一种尝试。

一个HTTP请求可以表示 为
http://11.32.45.60/folderdirectory/filename.png

一个IPFS请求可以被表述为
/ipfsdirectory/OqL9IpXyuK7j/folderpath/filename.png

与HTTP不同，IPFS使用内容的表示法而不是使用位置。它是通过在文件上使用哈希生成加密函数来实现的，然后函数的输出被用作节点地址。哈希也代表一个根，其他对象可以在其目录中找到。在HTTP中，我们关注的是询问某个特定位置的东西，而在IPFS中，我们关注的是路径上的特定对象。由于IPFS和区块链的结构有一些相似之处，所以这两种技术都能很好地配合。为了记录数据，IPFS使用分布式哈希表或DHT。



图：IPFS的工作2.

3) 智能合约。智能合约可以被认为是区块链网络的灵魂，它控制着区块链网络中发生的所有交易。[10]
智能合约被定义为对所有的交易做出决定。我们可以说，智能合约是为处理区块链网络中发生的任何交易而设计的规则。智能合约可以是运行在区块链之上的行代码，它包含一组规则，在这些规则下，多方同意该合约进行互动。如果以及当这些预定的规则被满足时，智能合约会自动执行。一个智能可以极大地降低交易成本。我们可以说，是一个可自动执行的代码，意味着它规范了交易规则，它间接地降低了交易成本。达成协议，正式化，强制执行。使用这样的智能合约，一个Dapp就产生了。DAPP是去中心化应用的缩写。

4)EVM。以太坊虚拟机，它是以太坊智能合约执行的运行环境。它不仅是沙盒的，而且是完全隔离的，这意味着在EVM内运行的合约没有网络访问权，也不能访问任何文件系统或进程。交易是一个实体，它连接到账户或用户。它可以是一个信息或任何资产。在创建交易时，每笔交易都被收取一定的费用，也被称为气体。这个气体的目的是为了限制交易所需的工作量，同时也为了支付交易的执行。当EVM执行交易时，气体会根据智能合约中规定的一些规则逐渐耗尽。气体价格是由交易的创建者设定的，他必须从发送账户中预先支付gas_price * gas。

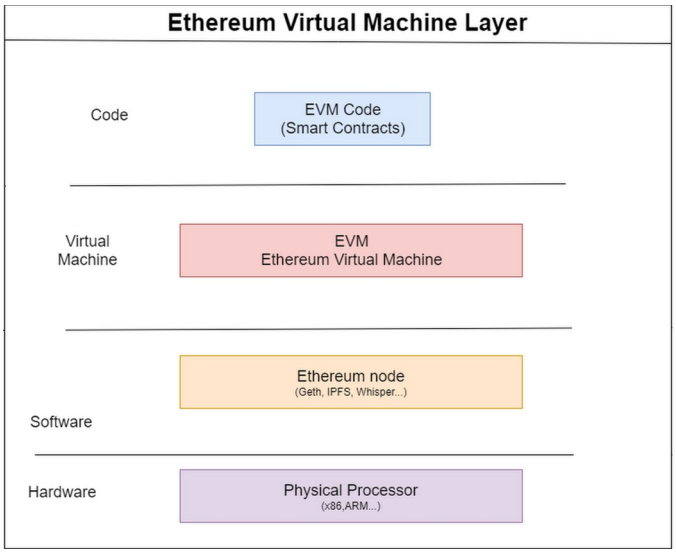


图3.以太坊架构

5) Embark。Embark是一个简单、快速和强大的框架，用于开发和部署去中心化的应用程序（DApps）。Embark与以太坊区块链、[11]
分布式点对点存储（IPFS）以及分布式点对点通信平台（Whisper和Orbit）集成。

6) ReactJS：ReactJS是一个声明性的、基于组件的库。ReactJS是以JavaScript为基础开发的。React从一开始就被设计为逐步采用。

7) 共识协议。共识协议是区块链的一个非常重要的部分。它需要在分布式和点对点的进程或系统中就单一的数据值达成协议。每当一个新的交易被添加到网络中，所有的参与者都会被提醒这个新的交易。他们可以批准它并将其添加到链中，也可以忽略它。当大多数参与者批准该交易时，就达成了共识。由于区块链不是由中央机构控制的，坏的参与者可以造成故障并破坏有价值的交易。在没有强大的、完全证明的共识算法的情况下，坏的对等人能够发布有问题的交易，使区块链所承诺的可靠性失效。更糟糕的是，没有中央机构来负责和修补错误。这确保了涉及网络的可靠性和一致性。

多个不可靠的和随机的节点。很难模仿或复制共识协议，因为从时间和所需的计算资源来看，执行这些协议的成本极高。根据他们在其中验证区块的区块链，共识的方法也不同。关于什么是最有效和最高效的共识方法，一直有持续的辩论。

有许多协议被区块链应用所使用。其中一些是工作证明（PoW）、权益证明（PoS）、委托权益证明（DPoS）、委托拜占庭容错（dBFT）、存在证明（PoE）、活动证明（PoA）[12]。

慈善链系统使用拜占庭协议[13]，即决定将有利于大多数人。假设有'm'个参与者不赞成交易，拜占庭协议规定，对于每*m*个参与者，至少应该有*3m*个参与者赞成交易。换句话说，⅔个参与者应该赞成交易。如果超过½个参与者不赞成交易，它将被忽略。大多数用户可能发送的决定将在特定的时间范围内被几乎所有其他用户收到。这个协议被使用，因为它提供了较少的延迟。共识算法不应成为捐赠过程的瓶颈。它确保用户永远不会对确认的交易有不同的看法[14]。
所开发的系统由若干模块组成，即：-

A. 用户注册和认证模块
B. 招标生成模块
C. 请求验证和批准模块
D. 捐赠和跟踪模块

该系统将建立在Ethereum平台上，使用Embark框架。智能合约将用Solidity编写。
系统的图形用户界面将建立在React上。

该系统的模块图如下所示。

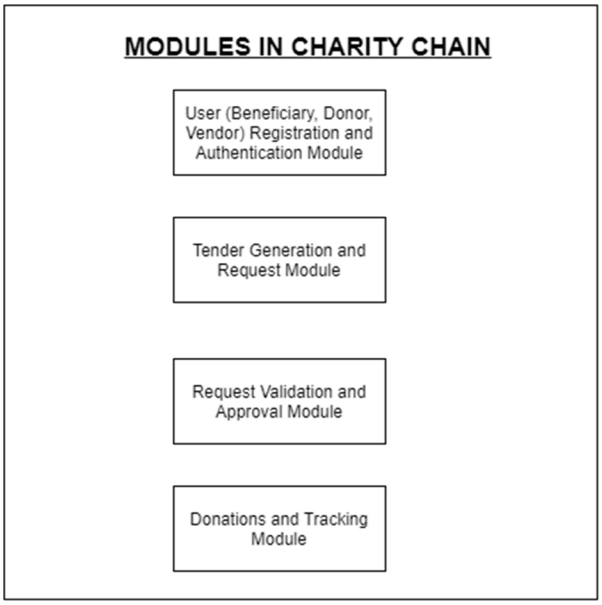


图. 模块4.图

A. 用户注册和认证模块

用户需要首先在系统中注册为受益人或捐赠人。据此，他将向慈善链系统提交他的详细资料。受益人的详细资料将包括组织的名称、联系方式和进一步信息的网站链接。这些信息和认证信息将被储存在用户数据库中。

B. 招标生成模块

受益人以慈善连锁系统提供的预定格式的标书形式发布他们的要求。这包括需求的细节以及每个项目的估计成本。这些标书将提供给捐助者和政府官员。

C. 请求验证和批准模块

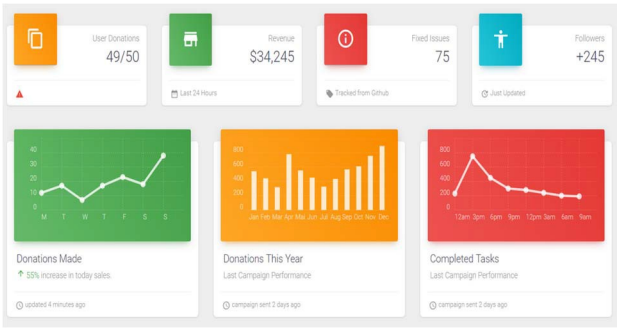
政府官员根据组织的真实性和他们的要求，通过该系统对投标书进行验证。

D. 捐赠和跟踪模块

一旦捐赠被政府官员批准，捐赠者可以根据自己的能力和喜好向该组织捐赠任何金额。创世节点将在此阶段创建。与慈善机构有关的整个交易将在慈善机构的简介页面上对捐赠者可见。这将有助于捐赠者做出明智的决定并进行相应的捐赠。捐赠者也将能够跟踪交易的整个过程，直到它到达受益人手中。

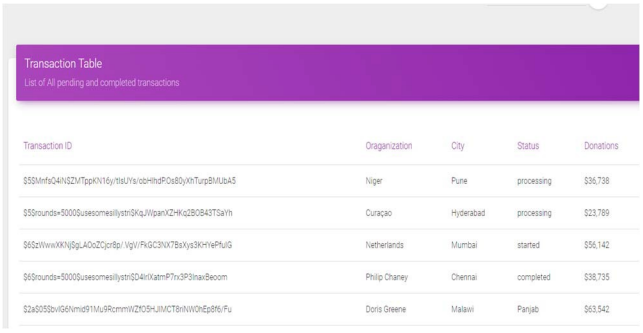
V. 结果

该系统将是一个网站，用户将不得不首先提供他的详细资料进行注册。他将得到一个用户ID和一个密码，用于登录。登录后，他将看到一个仪表板，他将能够查看所有细节，如用户的总影响、所做的捐赠、所捐的钱等。用户也将能够跟踪他的所有交易。对交易的跟踪将告诉用户交易的当前处理状态。同样，组织可以在系统中注册，并提供其详细信息以吸引捐款。



图：用户的捐赠5.仪表板

图：捐赠的状况6.



图：用户的交易7.历史

VI. 结论

因此，拟议的系统将追踪捐款，让捐赠者知道他/她的钱已经到达受益人手中。成功。慈善链使用智能合约来执行捐赠的过程并跟踪它们。拜占庭共识算法被用于可扩展性和计算的便利性。使用Ethereum平台，因为它是一个公共平台。这将提供捐赠的透明度，最终将激励捐赠者为这种灵活而有效的可追踪的慈善机构提供更多的捐款。

参考文献

[1] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee, "A Critical Review of Blockchain and Its Current Applications", International Conference on Electrical Engineering and Computer Science (ICECOS) DOI2017:978-1-4799-7675-1/17/$31.00 ©2017 IEEE

[2] Ashiq Anjum, Manu Sporny, Alan Sill, "Blockchain Standards for Compliance and Trust", 2325-6095/17/$33.00 © IEEE2017

[3] 恒厚，《区块链技术在中国电子政务中的应用》，978-1-5090-2991-4/17
/$31.00 ©2017 IEE

[4] Sachchidanand Singh, Nirmala Singh, "Blockchain:金融和网络安全的未来》，978-1-5090-5256-1/16/$31.00 c IEEE2016

[5] Kumaresan Mudliar, Harshal Parekh, Prasenjit Bhavathankar博士，"国民身份与区块链技术的全面整合"
, 978-1-5386-2051-9/18/$31.00 ©2018 IEE

[6] 李明，翁健，杨安家，卢伟，张越，侯林，刘佳楠，向阳，邓建华，"CrowdBC:基于区块链的去中心化众包框架"。

[7] Pinyaphat Tasatanattakool, Chian Techapanupreeda, "区块链。挑战与应用》，978-1-5386-2290-2/18/31.00美元 ©2018 IEEE

[8] "Nabil Rifi, 1Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher", "Towards Using Blockchain Technology for eHealth Data Access Management", 发表于 978-1-5386-1642-0/17/$31.00 ©2017 IEEE

[9] https://ipfs.io

[10] http://home.iitk.ac.in/~nihkilv/reports/blockchain.pdf

[11] https://embark.status.im/

[12] Lakshmi Siva Sankar ; M. Sindhu ; M. Sethumadhavan, "Survey of consensus protocols on blockchain applications", published in 4th2017 International Conference on Advanced Computing and Communication Systems（ICACCS） DOI: 10.1109/ICACCS.2017.8014672

[13] http://conferences.inf.ed.ac.uk/EuroDW2018/papers/eurodw18-Rusch.pdf

[14]https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419 [15]https://www.indiatoday.in/india/story/anna-hazare-pm-modi-rs-80000-crore-bjp-donation-5-months-india-corrupt-jan-lokpal-11891-2017-12-15

[16]h49825

[17]https://reliefweb.int/sites/reliefweb.int/files/resources/BlockChain%20for%20the%20Humanitarian%20Sector%20-%20Future%20Opportunities%20-%20November%202016.pdf