计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(3):205−209 [doi: 10.15888/j.cnki.csa.006247]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

区块链技术在数字资产安全交易中的应用①

韩　爽[1,2], 蒲宝明[2], 李顺喜[1,2], 李相泽[3], 张笑东[1,2], 王　帅[1,2]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 沈阳计算技术研究所, 沈阳 110168)
[3](东北大学 计算机科学与工程学院, 沈阳 110819)
通讯作者: 韩　爽, E-mail: 1933842948@qq.com

摘　要: 针对传统数据资产交易平台依靠中心化的管理机构完成交易过程, 不能保证数据资产交易过程中的安全性的弊端, 利用区块链技术去中心化、去信任、难以篡改等技术特征. 提出了一种基于区块链技术的新型数字资产安全交易方法. 首先阐明传统数字资产交易平台的弊端, 剖析了区块链技术在数据资产安全交易中的关键技术; 其次, 分别从数据存储、交易信息加密、验证节点间的共识算法方面提出具体的实施方案; 最后, 针对数据资产交易过程中的验证节点共识算法进行验证分析, 实验结果表明, 本文所提出的方法能很好的适用于数字资产安全交易.

关键词: 区块链; 去中心化; 数字资产; 共识算法; 安全交易

引用格式: 韩爽,蒲宝明,李顺喜,李相泽,张笑东,王帅.区块链技术在数字资产安全交易中的应用.计算机系统应用,2018,27(3):205–209.
http://www.c-s-a.org.cn/1003-3254/6247.html

Application of Block Chain Technology in Digital Asset Security Transaction

HAN Shuang[1,2], PU Bao-Ming[2], LI Shun-Xi[1,2], LI Xiang-Ze[3], ZHANG Xiao-Dong[1,2], WANG Shuai[1,2]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)
[3](School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China)

Abstract: As the traditional data assets trading platform relies on the central management of the completion of the transaction process, it cannot guarantee the security of data assets in the process of transaction. Based on the technical characteristics of block chain technology: decentration, and unforgeability, this study proposes a new digital asset security transaction method based on block chain technology. Firstly, the drawbacks of traditional digital asset trading platform are expounded, and the key technology of block chain technology in data assets security transaction is analyzed. Secondly, from the perspective of data storage, transaction information, executive scheme is put forward. Finally, the verification algorithm of verification node in data transaction process is verified. The experimental results show that the proposed method in this study can be applied to digital asset security transaction.

Key words: block chain; decentralization; digital assets; consensus algorithm; secure transaction

随着社会的进步, 科学技术的飞速发展, 互联网给人们的生活带来更多的便利. 在人们的生活中, 数字资产得到了很大的发展[1]. 比如商家为了促进消费, 向顾客发放代金券. 随着网络的发展, 微信等各种电子社交媒体越来越普及, 电子代金券越来越受欢迎. 电子代金券. 网上购票等等, 这些都属于数字资产. 现有的数字资产交易技术, 把数据信息集中存储在一个中央数据库, 交易过程由一个“可信的”第三方机构完成, 很容易

① 收稿时间: 2017-06-12; 修改时间: 2017-06-27; 采用时间: 2017-07-12; csa 在线出版时间: 2018-02-09

出现篡改交易信息等不安全事件. 相比于实体商品, 数据产品具备特殊的数据特性, 数据产品的仿制无差异性, 在效用上也没有不同[2], 更容易出现伪造的现象. 因此营造安全、可靠的数字资产交易环境就显得尤为重要.

2016 年初, 标题为《中国人民银行数字货币研讨会在京召开》[3]的新闻在中国人民银行官方网站上发表, 该条新闻推动了区块链技术在国内受到政府、金融机构、企业等各行各业的高度重视. 狭义的区块链指是去中心化系统各节点共享的数据账本[4]. 该数据账本由系统中的各节点共同创建与维护. 基于区块链技术建立的数据库系统保存了所有交易记录的数据, 该数据分布存储、公开透明, 具有不可篡改性.

本文基于区块链技术去中心、难篡改、可追溯等特征, 提出一种新型的数字资产安全交易方法, 不需要任何中间信任机构, 解决传统数字交易技术中的安全隐患.

1 传统数字资产交易方式

传统上, 由于用户之间的不信任性, 用户间的数字资产交易需要通过一个第三方中心平台来完成, 如图 1 所示. 用户将数据上传到交易中心, 由交易中心掌握所有的数据信息. 用户对资产的查询和转移皆由交易中心完成. 积分为实际价值的数字资产[5], 以积分交易系统为例, 阐述传统数字资产交易方式的弊端.

图 1 传统数字资产交易方式

1.1 技术原因

1) 传统积分交易系统的数据库一般采用 Oracle 等关系型数据库该数据库系统尽管当遇到计算机系统故障, 如网络故障等原因造成数据丢失, 可以使用恢复技术保证数据的完整性, 但当遇到黑客恶意攻击, 篡改数据内容, 传统数据库系统就无能为力了.

2) 传统数字资产交易方法中, 保存数据只进行简单的数据加密, 交易传输过程没有签名验证机制保障数据传输过程的安全性.

1.2 人为原因

传统数字资产交易系统由一个看似“可信”的中心管理机构管理交易过程, 不能忽略有管理人员的由于疏忽或者故意做出威胁用户利益的行为. 用户是否遭受损失主要依靠交易中心的诚信程度.

鉴于传统数字资产交易存在的以上弊端, 本篇论文提出基于区块链技术的新型数字资产交易方法.

2 区块链技术背景及主要特征

2.1 区块链技术背景

区块链来源于比特币 (Bitcoin), 是比特币的底层核心技术. 2008 年, 随着论文《比特币: 一个 P2P 电子现金系统》[6]的发表, 区块链技术因其去中心化、不易篡改和验证节点共同维护等优势逐渐受到人们的重视, 区块链技术并不是一种单一的技术, 而是由加密算法、P2P 网络、共识算法等多种技术巧妙地整合形成的一种新的数据记录、存储与呈现的方式[7]. 区块链正在成为继大型机、人电脑、互联网和移动/社交网络后的第五大颠覆性计算机范式[8], 很可能在全球范围引起一场新的技术革新和产业变革.

2.2 区块链的主要特征

区块链具备去中心化、可靠数据库、集体维护、安全可靠等特征.

1) 去中心化

采用分布式存储和集体维护, 区块链系统中不需要存在一个“信任”的第三方机构, 系统内的节点具有相等的权利和义务, 并且交易信息存储由整个系统中所有验证节点集体维护.

2) 可靠数据库

集体维护区块链系统中的验证节点都拥有一份完整的数据账本, 即使某个节点被侵害, 整个系统并不会因此而崩溃.

3) 安全可靠

区块链技术采用加密技术对交易数据进行签名, 保证信息不被伪造. 例如, 比特币系统的区块链技术使用的椭圆曲线 secp256k1 技术对交易进行签名验证, 使得交易过程不能被伪造.

区块链技术采用哈希函数保证交易数据不被篡改, 哈希函数也叫散列函数, 即将任意长度的消息压 缩到某一固定长度, 该输出就是散列值. 不同的输入可能会散列成相同的输出, 而不可能从散列值来唯一地确定输入值. 哈希函数的这种特性特别适合用于存储区块链数据.

最后区块链技术采用权益证明等共识算法来记录信息, 抵御破坏者的攻击. 系统内参与记账的节点数量

越多, 系统的安全性越高.因此区块链技术具有极高的安全性.

3 基于区块链技术的数字资产交易方法

3.1 设计目标

提出一个基于区块链技术的数字资产安全交易方法. 该交易方法去中心管理机构, 由系统中具有记账功能的节点共同维护; 采用加密技术及记账节点之间的共识算法, 来确保数字资产及交易过程的安全性; 利用链式的数据存储方式, 可以实现对用户的每一笔交易进行追溯. 总体架构图如图 2 所示.

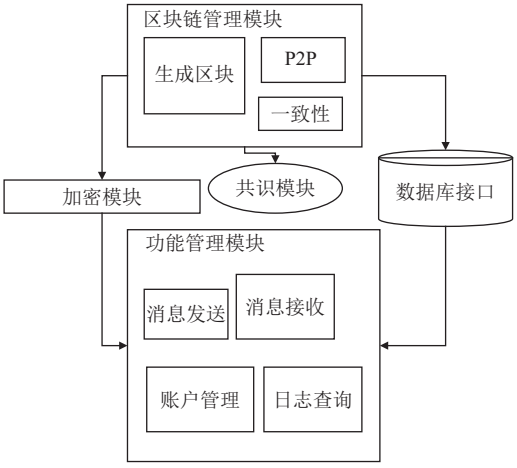

图 2 总体架构结构图

该数字资产安全交易方法的总体架构, 包括: 加密模块、共识模块、功能模块、区块链管理模块. 其中区块链管理模块主要包括: p2p 网络, 区块生成过程以及由共识模块提供的验证节点之间达成共识的方法.

3.2 交易链结构设计

区块链的数据数据不同于以往关系型数据库的键值对存储形式, 采用区块链式存储. 每个区块分块头 (header) 和块体 (body). 每个区块都包含上一区块的哈希值和本区块的哈希值, 区块之间的链接通过哈希值完成. 本文设计的数据区块头结构如表 1 所示.

区块体主要包含: 交易的数量和交易的详情. 详细结构如表 2 所示.

每个区块中包含前块的哈希值以及本区块的哈希值, 区块之间的链接通过这 2 个哈希值来完成. 本区块可以通过上一区块的哈希值链接到上一区块, 以此类推, 即可建立一条完整的数据链条, 如图 3 所示.

表 1 区块头结构

头信息	含义	字节数
版本号	表示版本信息	4
父哈希值	记录上一区块的哈希值	32
本区块头哈希值	记录本区块的哈希值, 小于父哈希值	32
Merkle树根值	记录当前区块所有交易Merkle数跟的哈希值	32
时间戳	记录该区块的生成时间	4

表 2 区块体结构

体信息	含义	字节数
交易数量	记录当前区块交易数量	4
交易详情	记录当前区块的所有交易	无固定值

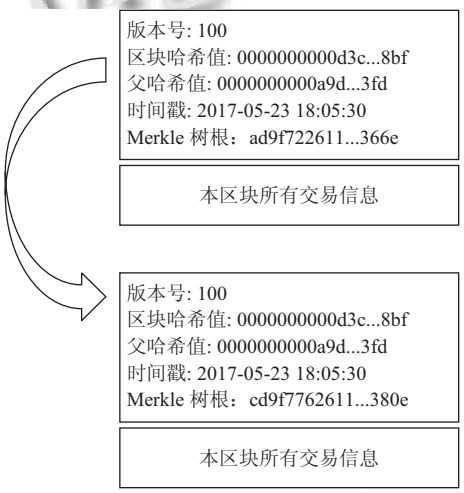

图 3 区块链链接结构

利用此结构可以防止交易信息被恶意篡改, 我们假设第 k 个区块数据被篡改, 由于第 k+1 个区块存储了第 k 个区块的哈希值, 与计算出来的第 k 个区块数据的哈希值相比较, 即可发现异常, 马上判断出第 k 个区块的交易信息已被篡改.

3.3 核心技术研究

3.3.1 加密技术

加密技术主要应用在数字资产交易过程中, 对交易信息的签名进行加密处理. 传统数字资产交易方法通常采用对称加密技术, 对称加密技术要求加密和解密过程使用相同的密钥, 该加密技术基于双方共同保证密钥的安全而实现的. 而本方法采用非对加密技术, 加密和解密过程中使用不同的密钥, 适用于互不信任的双方安全的完成交易过程. 本文提出的数字资产安全交易方法中, 采用双 SHA256[9]哈希函数与 RSA 加密算法结合使用, 验证交易信息真伪性, 防篡改.该方法中借鉴比特币区块链系统的双 SHA256 哈希函数, 将

原始数据经过两次 SHA256 哈希运算后转换为长度为 256 位 (32 字节) 的二进制数字. 哈希算法因其不可逆性, 适用于验证机制. 而 RSA 加密算法属于非对称加密技术, 非对称加密技术相比与对称加密技术, 加密与解密过程用的是不同的密钥, 分别为公开密钥和私有密钥. 公开密钥和私有密钥相互配合, 如果用户 A 使用它的公开密钥对数据进行加密, 只有用对应的私有密钥才能解密; 如果用私有密钥对数据进行加密, 那么只有用其对应的公开密钥才能解密. 公开密钥可以向其他人公开, 私有密钥则不公开, 并且私有密钥无法通过公有密钥推算出来, 保证传输数据的安全性和完整性. RSA 加密算法生成公私钥流程如图 3 所示.

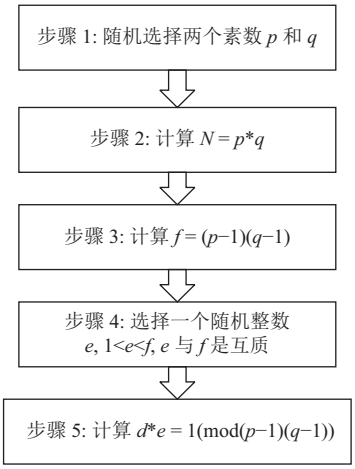

图 4 RSA 生成公私钥流程图

在实际应用中, 交易发送者 A 发起一笔新的交易, 例如转一张价值 100 元的代券给用户 B, 此时调用 SHA256 哈希算法对报文进行签名, 得到 Hash 后的一段摘要. RSA 非对称加密算法生成一对公有密钥和私有密钥. 使用公有密钥对签名加密, 发送方将 RSA 加密后的签名、报文一起发送给接收方. 接收方使用发送方的公钥对签名解密, 还原出一个哈希值. 查看该哈希值与报文经过 SHA256 哈希算法处理得到的结果是否一致, 验证消息是否来自发送者以及信息是否被篡改. 具体流程如图 4 所示.

3.3.2 共识算法

在本方法中, 各节点共同维护一个账本, 节点之 间达成一致的机制即共识机制, 共识机制主要应用在上文总体架构图 2 中的验证节点记录交易信息达成一致的共识过程. 区块链技术中常用的共识机制目前主要有: Pow(工作量证明)、Pos(权益证明)、DPos(股份授权证明)、分布式一致算法等. 鉴于 RAFT 分布式一致算法高效性、简洁性的特点, 本文采用 RAFT 共识算法. 但 RAFT 共识算法属于非拜占庭算法, 没有考虑存在拜占庭节点恶意操作, 为适用数字资产交易应用, 本文借鉴拜占庭共识算法的思想, 在 RAFT 算法中添加消息签名验证机制, 使用基于改进的 RAFT 共识算法在数字资产安全交易方法中.

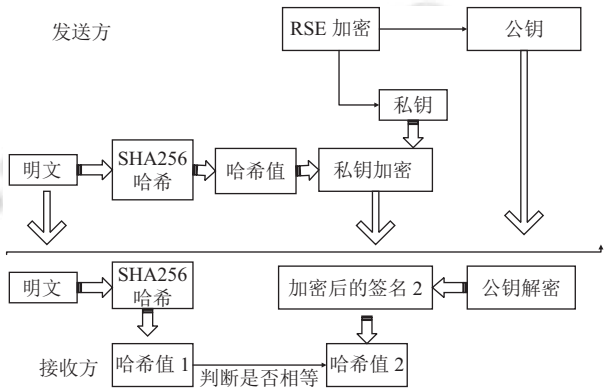

图 4 交易信息加密与验证过程

改进的 RAFT 共识算法过程如图 5 所示. 验证节点有三种状态: leader(领导)、follower(跟随者)、candidate(候选人).

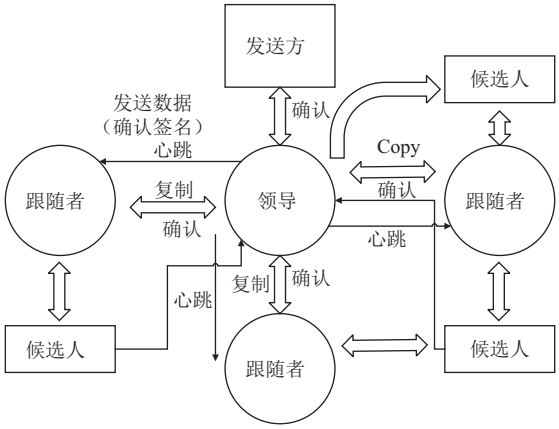

图 5 共识算法

算法描述如下:

Input: Message signature x+p Message number h

Begin

(x+p, n)→Leader

Leader→(Verficationn)(x+p, n)

(x, n)→Follower/*Leader 复制给 follower*/

Leader←Verify from follower

If leader is bad/*如果 leader 宕机, 重新选举*/

Leader→Candidate

Follower→Candidate

Voting(follower)→New leader

/*follower 节点通过 leader 是否 timeout, 验证 leader 节点是否宕机, 如 leader 节点宕机, 所有节点为 candidate 状态, 重新选举新的 leader. */End

4 共识算法验证

本文所提出的共识算法要求最少有 4 个节点, 因此本实验中有 4 个验证节点. 为验证共识算法可以很好的适用在数字资产安全交易业务中, 采用人工模拟了 leader 节点宕机, 验证该算法此时能否引发自动选举. 实验步骤如下:

(1) 模拟 leader 节点宕机;

(2) 记录从 leader 宕机到选举完成所用时间;

(3) 重复上面步骤执行 50 次.

从图 6 可知, 当 leader 出现故障到选举的成功率为 100%, 平均执行时间为 14 s. 该共识算法在出现宕机等故障时可以自动选举新的 leader 节点, 完成共识.

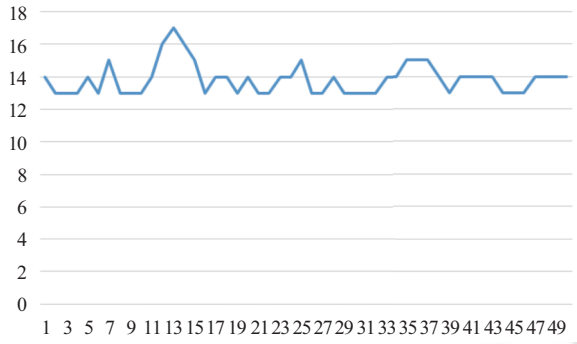

图 6 Leader 宕机到选举完成所用时间

5 安全有效性评估与应用

本方法利用区块链技术, 将交易数据记录到区块链中, 确保交易数据的安全性和有效性. 采用如表 3, 评估系统安全有效性.

表 3 安全有效性评估

序号	评估内容	测试结果
1	交易数据录入过程中, 交易信息被恶意修改	签名及加密机制, 辨别真伪
2	某一leader验证节点发生网络异常	共识机制重新选举
3	冒名接收数据	不通过

图 7 为用户系统运行图.

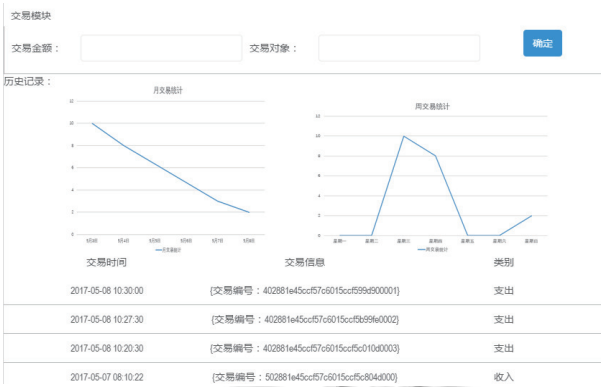

图 7 用户系统运行图

6 总结

本文设计了一种基于区块链技术设计一种新型的数字资产安全交易方法, 该方法的创新点主要体现在: 采用分布式数据存储方式, 由系统内的验证节点通过共识算法完成数据存储, 且采用双 SHA256 哈希函数与 RSA 加密算法结合方式处理交易信息. 确保交易信息真伪性, 防篡改. 实现安全可靠的交易过程.同时对该方法中涉及到的关键技术和核心算法进行分析和验证. 实验表明, 本文所提的方法不仅适用于代金券等形式的数字资产交易, 也适用于艺术品追踪等其他应用场景.

参考文献

1 夏新岳. 基于区块链的股权资产购买和转赠设计与实现[硕士学位论文]. 呼和浩特: 内蒙古大学, 2016.

2 杨茂江. 基于密码和区块链技术的数据交易平台设计. 信息通信技术, 2016, (4): 24–31.

3 中国人民银行. 中国人民银行数字货币研讨会在京召开. 金融电子化, 2016, (2): 94.

4 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494.

5 陈龙强. 区块链积分应用的价值传递. 金融电子化, 2016, (3): 64–65.

6 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Consulted, 2008.

7 林小驰, 胡叶倩雯. 关于区块链技术的研究综述. 金融市场研究, 2016, (2): 97–109.

8 Swan M. Blockchain: Blueprint for a New Economy. USA: O'Reilly Media, Inc., 2015.

9 Courtois NT, Grajek M, Naik R. Optimizing SHA256 in bitcoin mining. Kotulski Z, Księżopolski B, Mazur K. Cryptography and Security Systems. Berlin Heidelberg: Springer, 2014. 131–144.