文章编号:2095-3852(2018)02-0181-05
文献标志码:A

区块链技术在新型网络购物平台设计中的应用

陈 齐,王正国,李文锋,曹菁菁
(武汉理工大学 物流工程学院,湖北 武汉 430063)

摘 要:以电商交易环境下的用户信息泄露为背景,依托区块链技术设计了一个保障用户信息安全的新型网络购物实验平台,以保障顾客个人信息、交易信息、支付信息的安全,确保最后物流配送环节可溯源。结合区块链中哈希算法、Merkle tree、共识机制、非对称密钥以及对等网络等核心技术,提出了新型网络购物平台中区块链技术构架,在此基础上对区块链技术下的网络购物实验平台进行了模块划分,将区块链技术应用于顾客注册、双方交易、支付行为和物流配送4个环节。最后,评估了基于区块链技术的网络购物实验平台的安全性,结果表明,基于区块链技术构建的网络购物实验平台可有效保护用户的隐私安全。

关键词:网络购物;区块链;加密;信息泄露
中图分类号:TP302.1
DOI:10.3963/j.issn.2095-3852.2018.02.012

个人信息泄露在网络购物中频繁发生,网络购物平台和商家有着很大的责任,在一次完整的网络购物中,电商能够经过很多途径搜集消费者的个人注册信息、订单信息、支付信息和物流信息。对于这种情况,大多数研究侧重利用法律保护个人信息,极少有通过构建新型网络购物平台来从根本上解决个人信息泄露。

区块链技术具有去中心化、去信任、集体维护、可靠数据库这4个特性,可以把区块链理解为是一种完整的、不可篡改的、多方参与和监督的记录方式[1]。同时,区块链集成了分布式数据存储、点对点传输、共识机制、加密算法等技术,通过分布式存储使得数据公开透明,利用时间戳技术使得数据可溯源和可验证,利用非对称加密技术使得数据安全可信,在恶意算力不足51% 时,无法篡改和伪造数据[2],能有效解决传统网络购物平台遇到的很多问题。

新型网络购物实验平台的开发,从顾客到商家以及整个相关环节都是受益者,大大提高了网络购物的安全性与效率,能协调现代物流信息化发展与安全保障的关系,提升产品在物流配送环节的效率,降低成本,促进电商物流模式创新。

1 区块链技术原理

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。区块链技术是以比特币为代表的数字加密货币体系的核心支撑技术,是包含交易信息的区块按照时间顺序连接起来的数据结构[3]。区块头和区块主体共同组成一个区块,区块主体担任记录前一段时间内的一切信息的角色,而区块头实现区块链的大部分功能。只有区块头被用于计算,区块头哈希值能够唯一、明确地标识一个区块,而且任何节点想要独立地获得该区块哈希值则需对区块头进行哈希计算。区块结构如图1所示。在比特币系统中,单个区块的生成过程主要分为3步,即交易过程、认证过程和挖矿记账过程,以A与B的比特币交易为例,比特币交易流程如图2所示。

2 区块链技术构架

2.1 核心技术组件

核心技术组件包含区块链技术所依靠的基础组件、协定和算法,进一步细分为通讯、存储、安全机制、共识机制4层结构。

(1)通讯:区块链一般利用P2P技术来组织

收稿日期:2017-10-24.
作者简介:陈齐(1995-),男,山西临汾人,武汉理工大学物流工程学院硕士研究生,主要研究方向为区块链技术、仓储物流优化.
基金项目:武汉理工大学科研启动经费项目(921600001);国家自然科学青年基金项目(61502360).

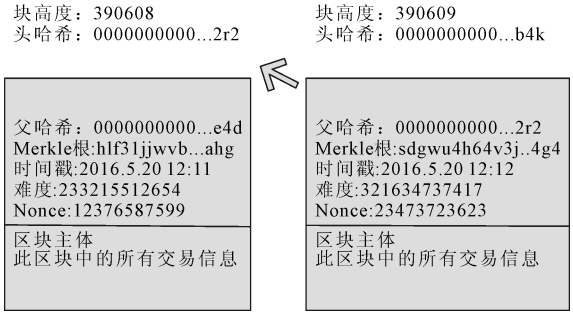

图 1 区块结构

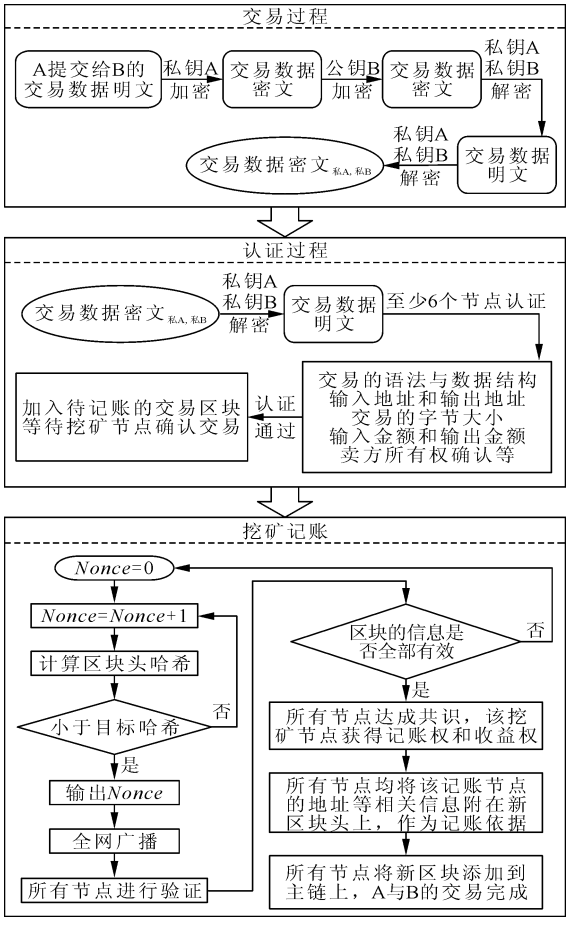

图 2 比特币交易流程

各个网络节点,每个节点经由播实现路由、新节点识别和数据传播等功能。P2P 是一种对等网络,这种对等表现在客户端也可以同时是服务器。在区块链当中,使用 P2P 的对等网络将数据进行全网的广播,让一切的节点都加入数据的验证。对等网络如图 3 所示。

(2)存储:区块链数据在运行期以块链式数据结构存储在内存中,终究会长期化存储到数据库中。在区块链中生成的所有记录通过 Merkle 树的哈希过程生成唯一的 Merkle 根,存储在区块链头部[4]。

(3)安全机制:区块链系统的数据加密及隐

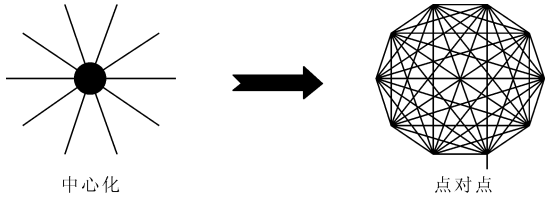

图 3 对等网络

私保护通过公钥与私钥密码学原理进行。

(4)共识机制:是区块链系统中各个节点达成一致的策略和方法,根据系统类型及应用场景选择工作量证明机制。在区块链当中,区块的生成需要一定的工作量和成本。一个区块的产生不是轻易的,发送大批没有意义的区块到网络上必须付出很多的工作量。这一点保障了产生的区块参与到了正确的区块链上,其他人假如要产生自己的区块链来替代正确的区块链,那么产生的耗费远远大于产生区块链得到的益处[5]。

2.2 配套设施

(1)研发阶段:必须具有和区块链技术配套的开发测试工具和环境。

(2)生产阶段:必须构建对应的运营维护体系和运营管理功能。

(3)部署层面:区块链系统可以部署在单个服务器上,如 PC、智能手机等,以单个服务器作为区块链网络中的一个节点加入。也可部署在多个服务器上,以服务器集群为单位作为区块链网络中的一个节点加入。

3 平台设计

3.1 总体设计

新型网络购物实验平台的功能分为 4 个子模块。平台模块结构如图 4 所示。

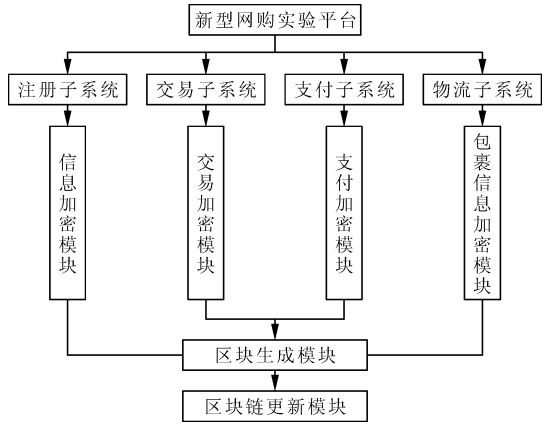

图 4 平台模块结构

采用区块链中私有链的形式,根据场景需求

设计了以下 6 个节点。在这里要说明,所有加入平台的节点均为诚实节点。节点可以为 PC 机或移动终端。①监管节点:相关部门对交易过程进行监管,保障交易过程的合法有效运行。②用户节点:服务于所有顾客,提供区块链相关服务。③商家节点:服务于所有商家,提供区块链相关服务。④物流节点:对应于快递公司的所有收件员、网点、中转站、派件员等。⑤银行节点:提供相关支付业务。⑥可信节点:可信服务器会审核所有节点身份,通过后将相应的节点加入系统,加入节点的登记信息会写入区块链进行备案。平台区块链系统如图 5 所示。

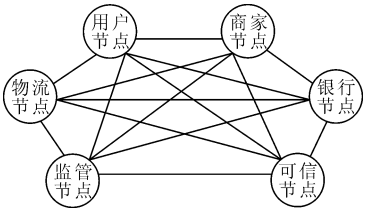

图 5　平台区块链系统

3.2　子系统设计

3.2.1　注册子系统

以张三注册新型网购实验平台为例进行说明,注册子系统工作流程如图 6 所示。张三在注册个人信息时,系统使用公钥对张三的信息进行加密,对加密后的信息进行哈希运算生成哈希值。哈希值再经过两两哈希计算,即为张三个人信息的 Merkle 树根。通过工作量证明机制验证后,节点会接受该区块,当前区块链中增加该区块来更新区块链,使得更新后的区块链中包含最新一整套数据。更新了个人信息区块的区块链如图 7 所示。

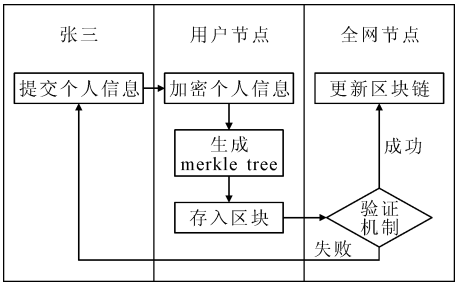

图 6　注册子系统工作流程图

3.2.2　交易子系统

张三成功注册后,打算在 A 商家购买一件私密商品。顾客交易子系统工作流程如图 8 所示。系统对加密后的交易信息进行哈希运算生成哈希值。交易信息的哈希值再经过两两哈希计算,即为交易信息的 Merkle 树根。通过工作量证明机制验证后,节点会接受该区块,当前区块链中增加该区块来更新区块链,使得更新后的区块链中包含最新一整套数据。

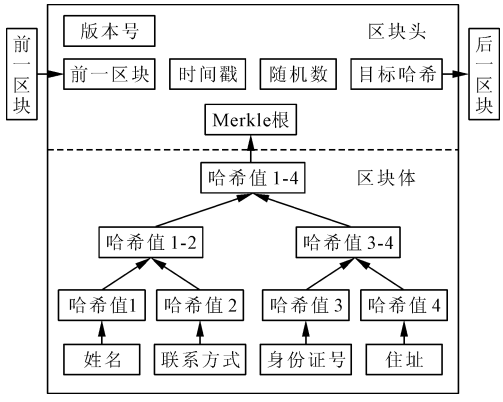

图 7　更新了个人信息区块的区块链

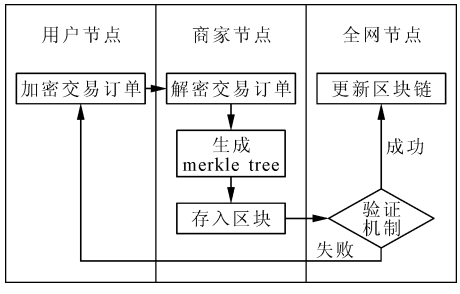

图 8　顾客交易子系统工作流程图

3.2.3　支付子系统

A 商家与张三达成交易后,张三需要向 A 商家支付。顾客支付子系统工作流程如图 9 所示。系统对加密后的支付信息进行哈希运算生成哈希值。支付信息的哈希值再经过两两哈希计算,即为支付信息的 Merkle 树根。通过工作量证明机制验证后,节点会接受该区块,当前区块链中增加该区块来更新区块链,使得更新后的区块链中包含最新的一整套数据。

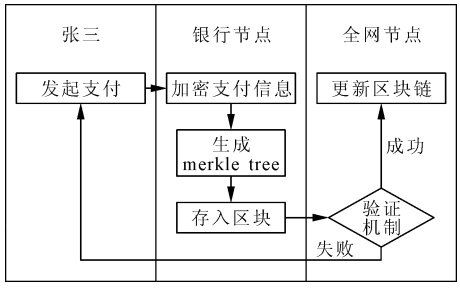

图 9　顾客支付子系统工作流程图

3.2.4　物流子系统

张三与 A 商家达成交易,支付对应费用后,A 商家通过物流公司向张三发货,最终张三收到自己的私人商品。商品物流子系统工作流程如图10

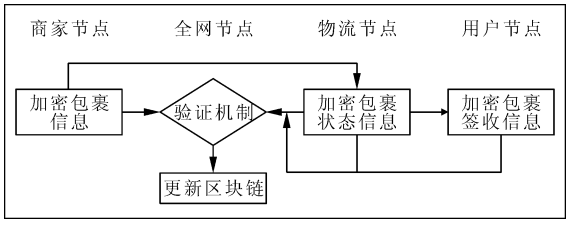

图 10 商品物流子系统工作流程图

所示。

(1)商家节点使用 A 商家的私钥对包裹信息进行加密,发送给物流节点。商家节点将加密后的包裹信息经过哈希运算等生成区块,向全网广播,各节点验证通过后写入区块链。

(2)收件员对应的物流节点收到实际包裹后,计算包裹信息的哈希值并与全网广播的区块哈希值进行比对,若比对成功则接收包裹,否则拒收该包裹。

(3)节点按照包裹的物理空间传送路径以及自身和对应的下一个物流节点的节点信息生成包裹状态信息,使用张三的公钥进行加密后经过哈希运算生成区块,向全网广播,各节点验证通过写入区块链。

(4)张三收到实际包裹后,用户节点计算包裹信息的哈希值并与全网广播的区块哈希值进行比对,若比对成功,则接收包裹,否则拒收包裹。

(5)用户节点使用张三的私钥对包裹签收信息进行加密后经过哈希运算等生成区块,向全网广播,各节点验证通过更新区块链。最终,将通过验证的各区块依次写入区块链,更新后的区块链如图 11 所示。

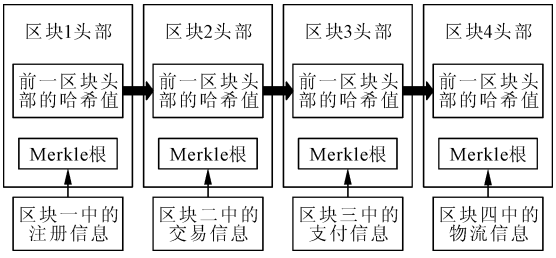

图 11 更新后的区块链

4 评估

4.1 数据完整性

Merkle tree 具有检错功能,任何一个节点的不一致都会导致最终树根结果不一致,如图 12 所示。

4.2 数据安全性

区块链中数据的安全性体现在两个方面[6-7],一是区块链技术本身的安全性,二是有效防止恶意攻击的安全性。

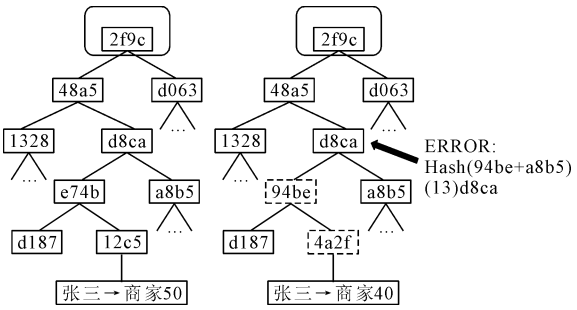

图 12 Merkle tree 检错机制示意图

(1)在区块链技术层面:①每一个区块和哈希值都是一一对应的,每个哈希值都是由区块头计算得到的。因为区块头中包含了当前区块体的哈希值和上一个区块的哈希值,所以如果当前区块内容改变或者上一个区块哈希值改变,就一定会引起当前区块哈希值的改变。正是因为这样的联动机制,区块链才保证了自身的安全性,数据一旦写入,就无法被篡改。②采用了非对称加密技术,所有的数据存储和记录都有数字签名作为凭据,非对称加密保证了一系列过程的可靠性。③在区块生成过程中,由一个地址到另一个地址的数据转移都会进行身份验证,即哈希值的验证和私钥公钥的验证。④去中心化的分布式设计,网络中有许多个节点,同步所有节点的数据,使得数据全部公开或者部分公开,而且数据多副本存在,不存在数据丢失的风险。⑤在数据传输过程中,数据通常采用 HTTP + SSL 进行处理,从而保证数据在网络传输中防篡改且加密处理。

(2)在防止恶意攻击层面:利用比特币的区块链作为安全存储介质,这是因为比特币网络拥有最强的算力,也意味着网络具有更高的安全性[8-9]。比特币网络中,节点仅认可最长的链,不在最长的链中的区块被称为孤块,其包含的交易数据是不被网络接受和确认的。因此,最长链等效于最多的工作量证明,也意味着最高的安全性。所以,假设有人员想要恶意攻击并篡改已经存储于第 N 个区块中的档案历史,需要做到的是创建一个区块链分支,并寄希望于其他节点会认可该分支。即通过建立现有区块链的部分拷贝并在某一区块后分叉,再添加上自己的区块,来重新改写区块链历史数据。最长链机制如图 13 所示。此种方式可理解为与比特币网络中的其他节点(挖矿服务器)进行军备竞赛,即试图将第 N 个区块

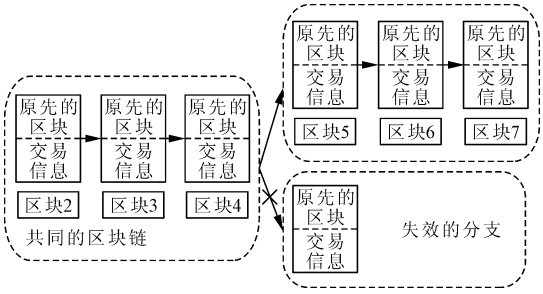

图 13　最长链机制

及其后面被挖出的区块孤立。为达到篡改区块链数据的目标,攻击者必须拥有足够数量的算力[10]。

5　结论

笔者结合区块链的技术原理,通过组建区块链技术构架,搭建了新型网络购物实验平台,按其功能分为 4 个模块:在顾客注册模块将加密的个人信息写入区块链,防止个人信息泄露并易于管理。在顾客交易模块将加密的交易数据写入区块链,保障了交易的私密进行与不可篡改。在支付模块将支付记录存储在区块链,使得支付实时透明,便于监管。在物流模块,将包裹信息、包裹状态信息、包裹签收信息存储在区块链,实现了物流信息的真实性与物流状态的可追溯性,有助于解决快递丢包、掉包问题。最后,结合 Merkle tree 检测机制和区块链技术的最长链机制,说明了新型网络购物实验平台中数据的完整性和安全性。随着区块链技术的不断发展,其在电子商务和物流等领域将发挥更大的作用。

参考文献:

[1] 沈鑫,裴庆祺,刘雪峰. 区块链技术综述[J]. 网络与信息安全学报,2016,2(11):15 – 16.

[2] 洪涛. 区块链在我国农产品电商领域的应用研究[J]. 中国市场,2016,3(39):65 – 68.

[3] 欧阳旭,朱向前,叶伦,等. 区块链技术在大用户直购电中的应用初探[J]. 中国电机工程学报,2017,37(13):3737 – 3745.

[4] 杨德昌,赵肖余,徐梓潇,等. 区块链在能源互联网中应用现状分析和前景展望[J]. 中国电机工程学报,2017,37(13):3664 – 3671.

[5] 李董,魏进武. 区块链技术原理、应用领域及挑战[J]. 电信科学,2016,32(12):20 – 25.

[6] LEE B, LEE J H. Blockchain – based secure firmware update for embedded devices in an internet of things environment[J]. Journal of Supercomputing,2017,73(3):1 – 16.

[7] JESSE Y H,DEOKYOON K,SUJIN C,et al. Where is current research on blockchain technology – a systematic review[J]. Journal Citation Reports,2016,346(6):562 – 570.

[8] 王安平,范金刚,郭艳来. 区块链在能源互联网中的应用[J]. 电力信息与通信技术,2016,1(9):1 – 6.

[9] 孙佳音. 比特币的性质、定价与监管研究[D]. 上海:上海交通大学,2014.

[10] 何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1 – 7.

Application of Blockchain Technology in the Design of New Online Shopping Platform

CHEN Qi, WANG Zhengguo, LI Wenfeng, CAO Jingjing

Abstract: Under the background of user information leakage in e – commerce transaction environment, relying on blockchain technology, it designs a new type of online shopping experiment platform to ensure user information security, in order to protect the security of customer personal information, transaction information, payment information, which ensures that the final logistics distribution links are traceable. Combining key technologies such as hash algorithm, Merkle tree, consensus mechanism, asymmetric key, and peer – to – peer network in the blockchain, the blockchain technology framework in the new online shopping platform is proposed. The module of online shopping experiment platform under blockchain technology was divided into four parts, which applied blockchain technology to customer registration, bilateral transaction, payment behavior and logistics distribution. Finally, the security of the online shopping experiment platform based on blockchain technology was evaluated. The research results show that the online shopping experiment platform based on blockchain technology can effectively protect the privacy of users.

Key words: online shopping; blockchain; encryption; information leakage

CHEN Qi: Postgraduate; School of Logistics Engineering, WUT, Wuhan 430063, China.