

基于区块链的商城积分系统方法研究

王绍刚 刘海法

(航天信息股份有限公司技术研究院 北京 100195)

摘 要: 论文内容将区块链技术作为底层技术应用于商城的积分系统中,形成了商城、商家、会员等三者之间的联盟链,利用区块链技术的去中心化、共识信任、可靠时序分布式数据库、集体维护等技术特点,解决了商城积分系统开发成本高、积分零散、积分消费乏力、积分使用限制多、积分兑换繁琐、积分难以流通等缺陷。

关键词: 区块链; 密钥管理; Web 服务; XML; 安全

中图分类号: TP309

文献标识码: C

Security Application Model of Electronic Commerce System Based on XKMS

Wang Shao-gang Liu Hai-fa

(Aisino Corporation, Technology Research Institute Beijing 100195)

Abstract: This paper discusses in detail the key management XKMS specification method, combined with the electronic commerce system security related features, designed methods for the electronic commerce system security application process model, it can make the electronic commerce system has better security maintainability and extensibility, the model method can be used to ensure the more safety of electronic commerce system in the Web services, key management XKMS specification will be translated into practical applications.

Key words: xkms; key management; web services; xml; security

1 引言

随着市场竞争的日益激烈,商城如何吸引客户以及使其成为长期客户是急需考虑的问题。现在国内已有很多大型商城已经实施了会员积分活动来留住客户,可以说商城积分系统是一个客户的忠诚营销计划。该系统依托结算平台优势资源,针对客户的忠诚计划需求而建立的积分技术平台及积分联盟服务。它通过引导和组织会员加盟商户的消费,在给商户带来利润的同时也为消费群体提供商户的最佳优惠折扣和积分形式的返利,并以积分的虚拟货币形式吸引会员,在加盟

商户群的再次消费来维持客户的忠诚。但是,目前我国商城的积分系统主要存在一些问题。

(1) 每个商城都需要投入巨大的成本来建立、运营自己的积分计划以及相应的系统平台;特别对于中小企业来说,这样的投入比取得效益要大得多,只能采用不规范的手工方式来进行积分计划处理,给客户较差的体验。

(2) 由于每个商城实施的积分计划都是独立的,某种积分卡只能在单个商家体系进行消费积分积累,导致消费者手中的积分非常分散于各商家积分体系中,积分难以有效整合积累。

(3) 具有零散、消费乏力、使用限制多、兑

换繁琐、难以流通的特点。如A商家“发行”的积分，B商家不给予通兑。

(4) 同时，积分无法转让、赠送，导致积分发行商家品牌传播十分有限。

(5) 另外，传统型积分的使用往往会有一定的期限，过期自动清零。

目前，传统技术已经不能很好地满足需求，导致积分市场发展缓慢。挖掘新技术，设计开发能够适应市场需求的积分系统，是市场经济发展的必然要求。本文就是基于区块链的技术与应用现状，利用区块链技术的基础模型、基本原理和关键技术，通过区块链上的交易实现商城积分的自由流通、使用和回笼，以形成完善的商城积分生态系统解决上述难题。

2 区块链商城系统架构

本文选择“联盟区块链”作为组织形式，联盟区块链是指其共识过程受到预选节点控制的区块链。不同于“公共区块链”中任何人可以读取和发送交易，也不同于“私有区块链”仅有核心

节点可以操作区块链，表现出中心化控制，联盟区块链的共识过程是受若干个主要节点管理的，这种形式既能够保证组织运作的效率，又可以兼顾系统安全性和成员共同维护的特性。在整个积分系统中，参与者主要包括商城、商户、会员用户，由这三者构成联盟链，商城、商户作为授权和验证节点，会员用户作为公开节点，商城和商户验证节点都有相应的交易积分存储备份并且公开透明，商城和商户对会员用户都可以发行积分作为一种体现客户关怀的辅助手段，不同的商城和商户之间也可以进行积分互换，但是必须每个商城和商户都要加入这个联盟链得到整个联盟链成员的授权和认可。

会员用户可以通过商城网站、微信公众号或者APP进行会员注册参与交易，并且交易积分存储在联盟链上面，整个架构如图1所示。

3 区块链商城系统功能

联盟链起到的作用是将跨地区、跨行业、跨领域的商城和商户联合起来，利用区块链技术会员可

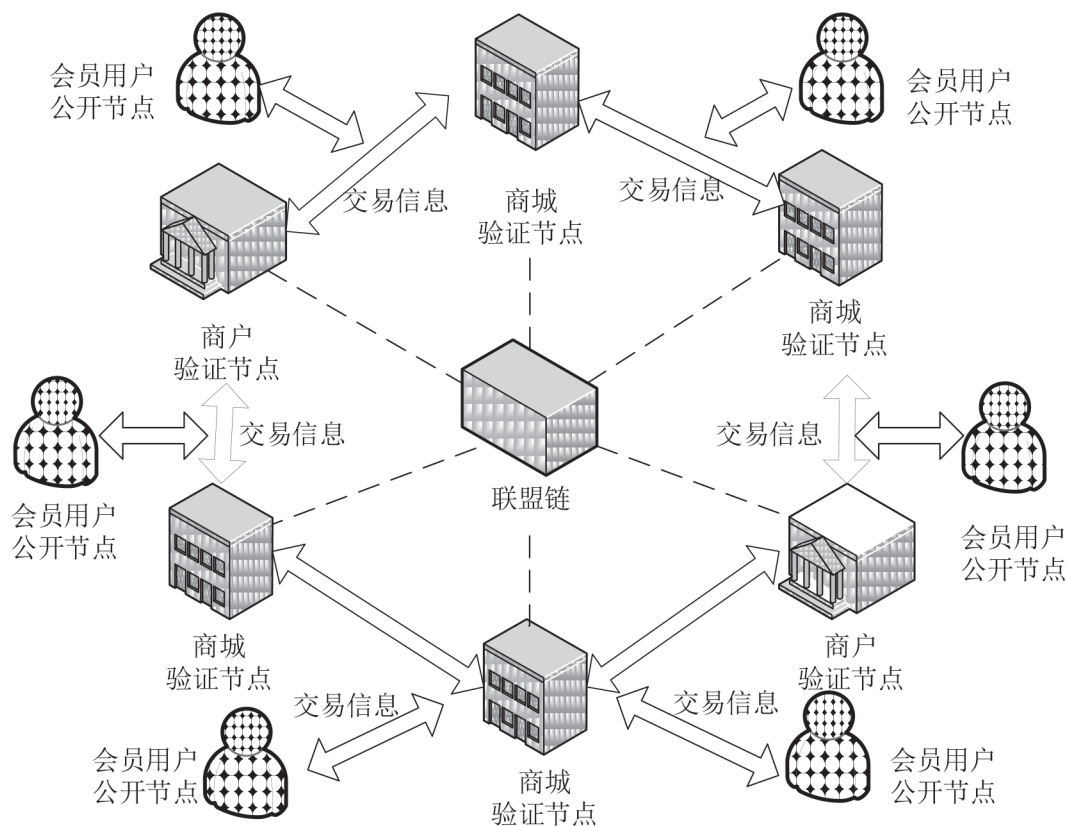


图1 基于区块链技术的商城积分方法体系架构图

以在所有联盟商家内消费获取积分，可以将积分累计起来兑换礼品、抵现、抽奖或者直接返现。

区块链商城积分系统：区块链商城系统融合了商家和会员积分系统的记录积分、查询积分、兑换积分、抵扣积分等各项会员积分管理功能，在为商家进行会员积分记录、会员积分管理的同时，帮助商家实现会员积分消费，商家可以根据商城设定的规则，进行会员积分兑换和会员积分抵扣等等。

积分发行：只有联盟链的节点才能进行积分发行，商城和商家是作为主要进行积分发行、交易、和验证的节点具备发行积分的权利，区块链商城系统支持商家与会员在积分活动中的即时互动，商家通过门店、互联网或移动设备可即时为会员记录积分和进行积分管理，并且将积分自动记录到商城进行存储，该积分系统支持在会员持积分消费时自动完成积分的累加，无需收银员人工干预，并且商城和商家可共同商定会员消费多级积分可设置消费到不同的额度不同的积分标准。

积分升级：区块链商城系统支持会员储值积分的自动升级和自动兑换，当会员卡积分累加到一定数额时，可通过积分系统内设置的积分规则为会员进行身份升级或其他方式的升级，当会员以积分兑换各种奖品后，积分将从会员卡内自动扣除，无需人工干预操作。

积分兑换：累计积分可兑换特定奖品/商品，积分兑换除商品以外的物品，如达到一定数量的积分可用抵做现金使用，购买商品等。

积分消费：设置不同会员卡的不同积分系数，利于商家对会员进行等级管理，刺激会员更多消费。

积分互换：会员与会员之间可以根据自己不同商城的积分进行互换。

积分赠送：可赠送一些特殊情况的积分，例如注册会员赠送、参加企业活动赠送、会员特殊消费赠送等多种情况的积分。

积分回笼：在完成了一定量的积分交换以后，不同的积分发行方账户下都相互持有对方的积分。所有验证节点可以商定一个固定时间周期去回笼各自发行的积分，回笼的方式就是根据每笔交易中纪录的兑换比率对积分进行回购。

多角色积分：商城需要可提供消费者、导购

员、门店、经销商等多角色积分。

积分查询：用户和商家都可以查询相应的积分。

4 区块链商城系统原理与相关流程

区块链商城系统主要包括联盟链网络、交易中心、积分查询中心、数据备份中心、锁定中心、用户APP（也可以是微信公众号、HTML5）等六大模块部分组成。联盟链网络负责积分的发行、交易、记账、验证；交易中心用于用户和商家交易请求；积分查询主要用于用户、商家、商城进行积分方面的查询；数据备份中心主要用于积分重要数据备份；锁定中心用于在私钥丢失或者泄漏情况下，对某一账户或者某笔交易进行锁定，防止冒名交易；用户端APP（包括微信公众号、HTML5）可以为用户产生一对公私钥对去生成一个节点账户，并提交交易请求。通过六大模块的相互作用，商城积分系统将形成完善的联盟生态圈如图2和图3所示。

5 关键点

(1) 积分是商家登记在区块链账本或分布式账本上发行的积分，区块链商城积分系统记录的积分和交易数据不依赖于商城的数据库即可获得，而且会员和商家积分交易的信息完整性和数据真实性更进一层。

(2) 利用区块链技术的商城积分是一段计算机程序，不再是一行数字符号，可以对它进行编程，积分数字资产之间的交换是代码与代码的交换，不是数字之间的增减。

(3) 积分因为可编程性，可以在区块链上，通过编制智能合约程序，完全去中介化的自主、自治的进行点对点交易，不需要人工干预。

(4) 针对目前商城积分系统的实际需求出发，提出了基于区块链技术的商城积分系统方法的设计思路、关键技术、核心流程的等思想。

(5) 通过基于区块链技术的商城积分系统方法平台建设，商城能够建立多个商家协调的统一的积分平台，解决不同商家之间的积分兑换管理壁垒，同时为消费者提供一个可信的积分查询、管理、兑换渠道。

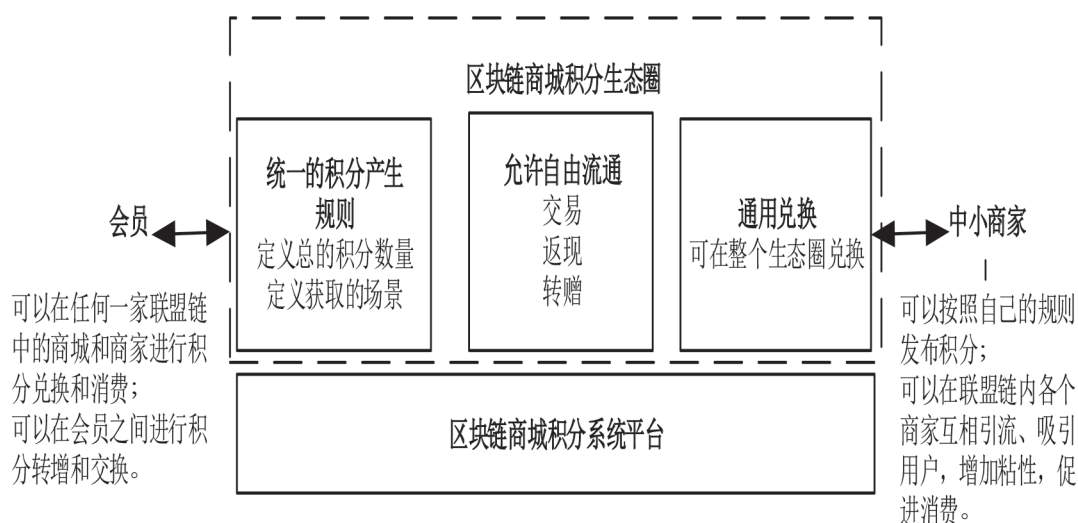


图2 基于区块链的积分系统生态图

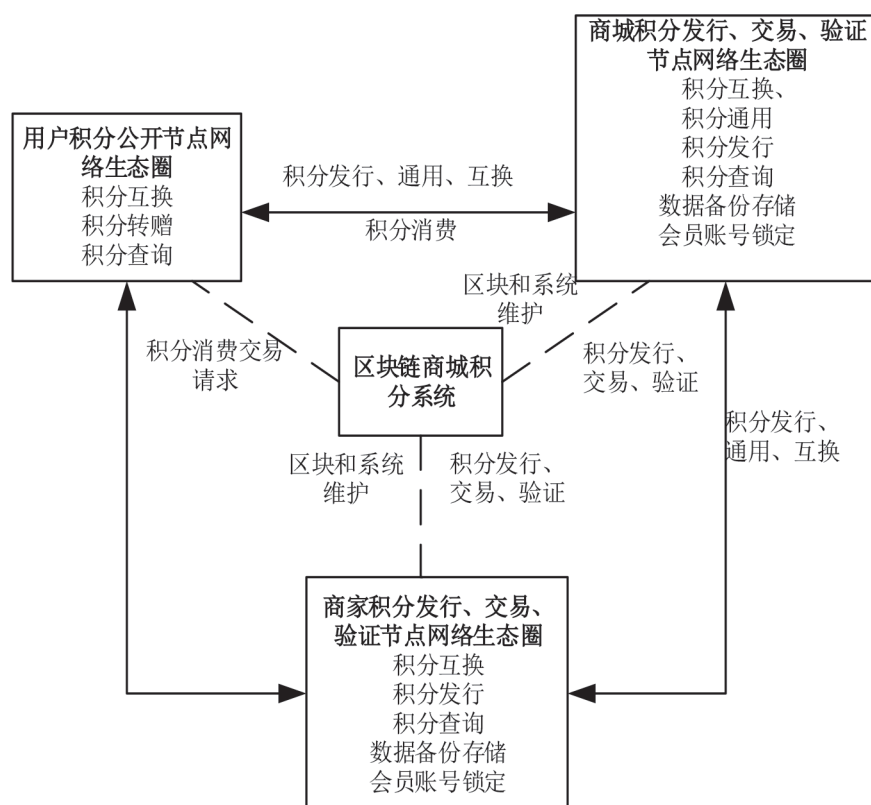


图3 基于区块链的商城积分解决方案图

6 结束语

(1) 联盟多方运营，共同制定规则，满足多层面的知情权与监督权。

积分一旦在区块链上发行，后续流通环节可以不依赖于发行方系统，资产流通由单中心控制变成社会化传播，任何有资源的渠道都可以成为

资产流通的催化剂。

(2) 通过区块链特性，不可篡改以及避免多重支付，实现积分点对点的传递。

(3) 区块链能极大地提升数字积分流通效率，真正达到“多方发行、自由流通”的效果。

会员购买商城内一家商家产品，即可享受联盟内所有成员提供的服务。对于商城和商家来

说，可以带来品牌知名度提升，并且带来更多的客户流；简化积分模式；用户在联盟成员内流转，不朝外流失客户。

参考文献

- [1] 戴节勇,顾健,陈克非.PKI技术在网络安全中的应用[J].计算机工程, 2005,31(5): 159-161.
- [2] 唐韶华,甘志勇.基于XKMS的PKI服务的设计与实现[J].电子与信息学报,2005, 27(2): 314-316.
- [3] 唐志红,龙毅宏,陈幼平.电子商务安全新技术[J].计算机工程与应用,2002,6(16):132-135.
- [4] 蔡敏烨,蒋兴浩,李建华.基于XKMS的集中身份管理系统研究[J].信息安全与通信, 2007, 1(3): 38-42.
- [5] 仲秋雁,王岳宏.基于LDAP的XKMS服务的研究与实现[J].计算机工程,2007, 33(5): 149-151.

作者简介：

王绍刚（1980-），男，北京人，博士，中科院遥感应用研究所，高级工程师；主要研究方向和关注领域：信息安全、区块链技术、信息系统。

刘海法（1971-），男，北京人，毕业于清华大学，硕士，高级工程师；主要研究方向和关注领域：信息安全。