

T/QGCML

团 体 标 准

T/QGCML XXX-XXXX

基于区块链技术的电子商务平台建设规范

Specifications for the construction of e-commerce platform based on
blockchain technology

（征求意见稿）

20XX-XX-XX 发布

20XX-XX-XX 实施

全国城市工业品贸易中心联合会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总则 2

5 平台架构 2

6 功能要求 4

7 技术要求 5

8 管理要素 6

9 运行管理 6

附录 A （资料性） 离线支付 8

附录 B （资料性） 区块链存证上链 10

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由道赞有限公司提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件起草单位：道赞有限公司。

本文件主要起草人：×××

基于区块链技术的电子商务平台建设规范

1 范围

本文件规定了区块链技术在电子商务平台的术语和定义、总则、平台架构、功能要求、技术要求、管理要素、运行管理。

本文件适用于基于区块链技术的电子商务交易平台的建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 39786 信息安全技术 信息系统密码应用基本要求
GB/T 36061 电子商务交易产品可追溯性通用规范
GB/T 38155 重要产品追溯 追溯术语
GB/T 28827.1 信息技术服务运行维护 第1部分：通用要求
GB/T 28827.3 信息技术服务运行维护 第3部分：应急响应规范
GB/T 22239 信息安全技术 网络安全等级保护基本要求
GB/T 20271 信息安全技术 信息系统通用安全技术要求
GB/T 33560 信息安全技术 密码应用标识规范
GB/T 36092 信息技术 备份存储 备份技术应用要求
GB/T 38156 重要产品追溯 交易记录总体要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子商务 electronic commerce

以电子形式进行的商务活动。

3.2

电子商务平台 electronic commerce platform

在电子商务活动中为交易双方或多方提供交易撮合及相关服务的信息网络系统总和。

3.3

区块链 blockchain

一种在对等网络环境下，通过透明和可信规则，构建不可伪造不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

3.4

区块链存证 blockchain proof of existence

为了保证存证信息（电子数据）的完整性和真实性，采用区块链技术实现多节点共识的存证服务。

3.5

上链 on-chain

业务相关方向区块链系统发起一次请求，区块链节点将相关数据写入到区块链系统中。

3.6

智能合约 smart contracts

一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

3.7

节点 node

区块链网络中的可运输主机。

3.8

对等网络 peer to peer network

一种仅包含对控制和操作能力等效的节点的计算机网络。

3.9

追溯平台 traceability platform

基于追溯码、文件记录、相关软硬件设备和通信网络，实现现代信息化管理并可获取产品追溯过程中相关数据的集成。

3.10

溯源码 traceability code

该码是追溯平台赋予每个商品的唯一追溯码，能够连接产品、产地、检验、监管和消费各个环节，查询到每个环节中的记录信息。

3.11

追溯单元 traceable unit

需要对其来源、用途和位置的相关信息记录并回溯的单个产品或同一批次产品。

4 总则

4.1 原则

4.1.1 采用国密算法保护数据，符合 GB/T 39786 的要求，保证上链主体、上链客体信息安全。

4.1.2 应用架构设计宜预留监管功能和接口，满足监管需求。

4.2 机构

具有独立法人资格、营业执照、区块链信息服务备案，具备符合平台建设条件的资金、固定经营场所，保障平台正常运营的组织机构和人员。

4.3 平台

应具有时效性、有效性、安全性和可监督性，保证各层级有效运行，实现商品信息可信流转。

4.4 区块链节点

区块链节点的数量宜 ≥ 4 ，采用通用性好的计算机系统，具备区块链运行软件、操作系统、安全系统及其他集成系统等。

5 平台架构

5.1 总体架构

基于区块链技术的电子商务平台总体架构采用层次化设计，从上到下依次为应用层、支撑管理层、数据存储层和数据采集层。各层级之间紧密配合，共同实现平台的功能需求。总体架构如图 1 所示。

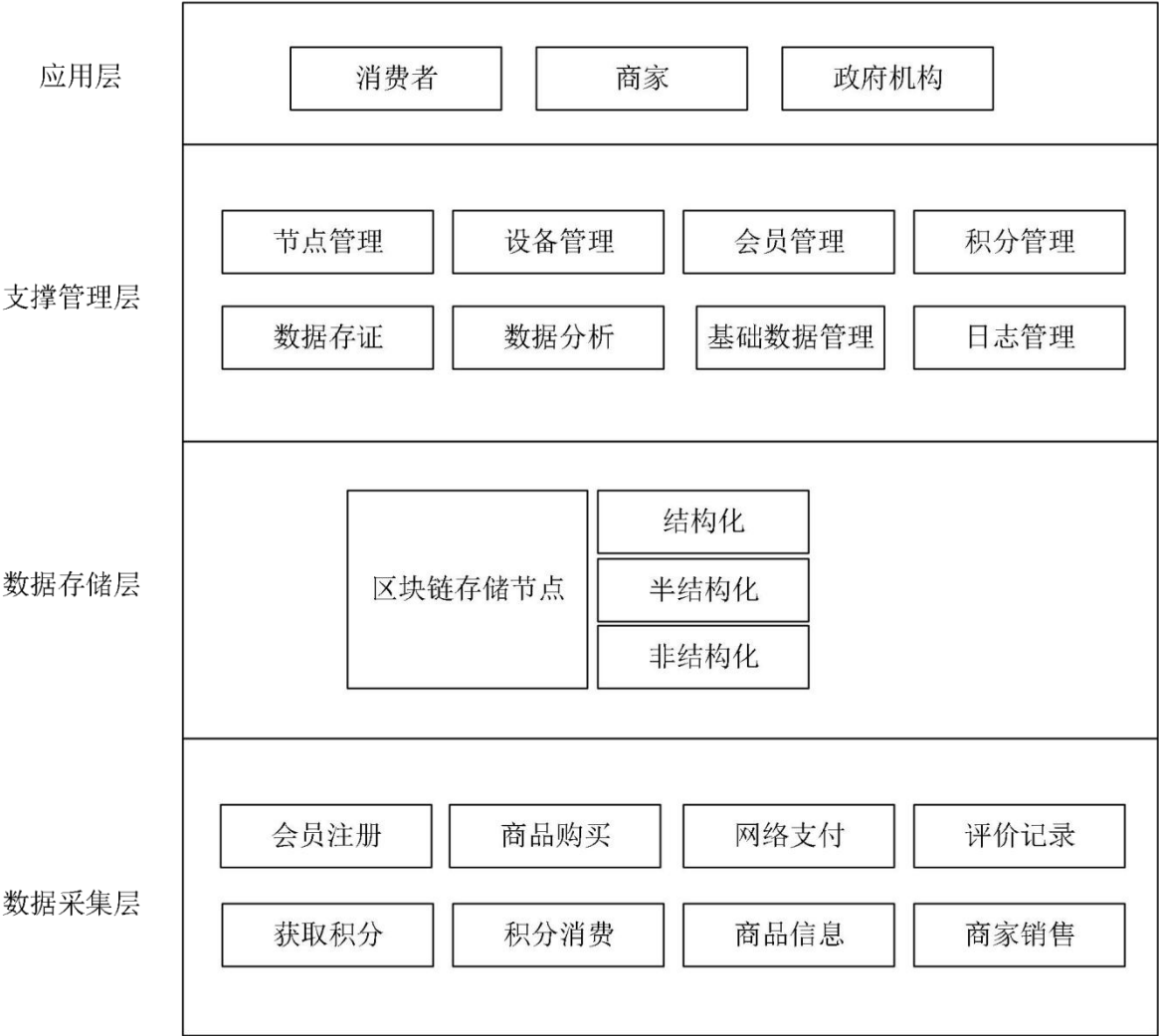


图 1 平台架构图

5.2 数据采集层

数据采集层负责收集平台运营过程中的各类数据，包括获取积分、积分消费、商品信息和商家销售等。通过实时采集和处理数据，为平台提供丰富的数据源，支持业务决策和优化。

5.3 数据存储层

数据存储层是电子商务平台的数据中心，负责存储各类数据。通过采用区块链存储节点、半结构化和非结构化等多种存储方式，实现数据的高效存储和快速访问。区块链技术的应用使得数据具有不可篡改性和可追溯性，为平台提供强大的数据保障。

5.4 支撑管理层

支撑管理层负责平台的核心业务逻辑处理和数据管理。该层包括数据存证、数据分析、基础数据管理和日志管理等功能模块。通过区块链技术，实现数据的分布式存储和共享，确保数据的安全性和一致性。同时，利用数据分析功能，为平台运营提供决策支持。

5.5 应用层

应用层是电子商务平台与用户直接交互的界面，包括消费者、商家和政府机构等角色。平台应提供友好的用户界面，支持会员注册、商品购买、网络支付、评价记录等功能。通过区块链技术的应用，实现交易的公开透明和不可篡改，提升用户信任度。

6 功能要求

6.1 区块链数据存证

6.1.1 宜建立区块链数据存证访问平台。

6.1.2 区块链访问平台应具有分布式数据存储、智能合约机制、点对点传输、非对称加密技术等基本特征。

6.1.3 电子商务平台能够对重要数据通过 SBANK 区块链存证上链，实现全程数据不可伪造，不可篡改。

6.1.4 当交易双方发生异常情况时，可采用离线支付方式完成交易。离线支付方式见附录 A。

6.2 商品信息管理

6.2.1 平台能够对经销商销售的商品及生产过程中使用的原辅材料上架。

6.2.2 对商品信息管理内容包括但不限于：产品名称、产地、品种、规格、价格、数量等。

6.2.3 电商平台应具有对商品进行登记、编码、查询、修改等功能。

6.3 消费者交易信息管理

6.3.1 平台能够提供用户注册功能。

6.3.2 消费者能够对订单进行提交、确认和取消。

6.3.3 消费者能够通过余额、支付宝或微信等方式提交货款。

6.3.4 消费者能够通过平台对购买的商品发表评价。

6.3.5 消费者购买商品后平台能够为其赠送同等数额的积分且消费者可以用积分兑换商品或取得利息。

6.4 商家交易信息管理

6.4.1 平台能够提供会员注册功能且通过审核后成为商家。

6.4.2 商家可以将销售的商品上架。

6.4.3 当产生消费记录后商家可以随时查看订单情况及所得货款。

6.4.4 商家销售商品后需向平台交纳相应的服务费，给平台的服务费商家获得一定额度积分。

6.4.5 商家可以用积分兑换商品或取得利息。

6.5 溯源信息管理

6.5.1 可追溯性信息编码与标识应符合 GB/T 36061 的基本要求。

6.5.2 溯源信息应包括在生产加工阶段产生的产品信息，进行电子商务交易时产生的交易信息及运输、储存、配送等各种物流信息。

6.5.3 平台应该能对消费者、追溯主体、相关部门等用户提供差异化追溯信息。

6.6 平台应用区块链技术场景

6.6.1 根据对电子商务平台的分析，确定平台应用区块链的场景包括但不限于以下内容：

- a) 注册成员；
- b) 商品信息；
- c) 订单；
- d) 余额；
- e) 产品评论；
- f) 积分；
- g) 利息；

6.6.2 区块链应用示意图，如图 2 所示。

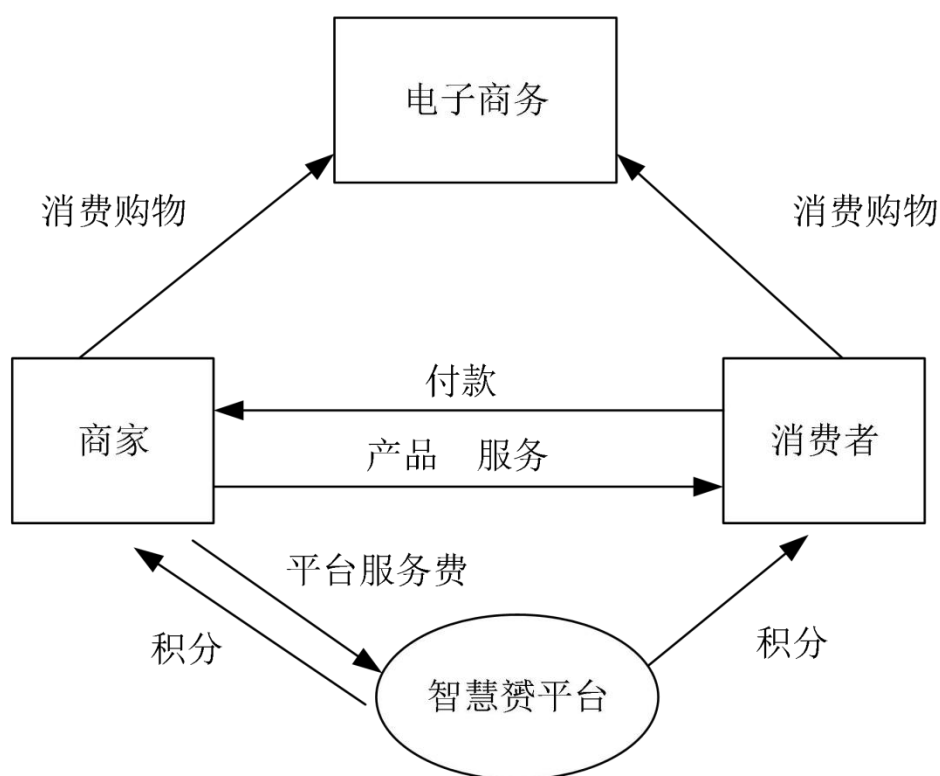


图 2 区块链应用示意图

7 技术要求

7.1 性能要求

- 7.1.1 数据存储到区块链上的时间单条数据上链在 1 s 以内。
- 7.1.2 系统处理峰值时应保持总体资源满负荷的 70% 以下。
- 7.1.3 应具备较高可靠性和稳定性，避免由于某一设备、网络线路、软件的单点故障影响平台整体运行。

7.2 部署环境要求

- 7.2.1 支撑环境应适应分布式存储、分布式计算、并行计算等技术体系。

7.2.2 数据可根据需求选择具有高可用性集群方案的商用或开源数据库系统。

7.3 数据要求

7.3.1 信息存储采用分布式区块链技术存储,上链格式见附录 2。

7.3.2 追溯数据格式应符合 GB/T 38155 追溯要求。

8 管理要素

8.1 用户管理

8.1.1 平台建立用户资质审核与备案管理制度、严格的准入制度,具有专职人员负责用户的资质审核和备案。

8.1.2 制定用户协议,确定用户与平台之间的权利和义务。

8.2 上链主体管理

8.2.1 自然人主体

自然人主体应采用身份证实名认证,机构主体应采用统一社会信用代码及法人身份证实名认证。

8.2.2 机构主体

机构主体信息上报内容包括但不限于:

- a) 机构基础信息;
- b) 机构人员信息。

8.3 上链客体管理

8.3.1 根据实际需要,按照不同数据内容定义上链客体数据格式规则。

8.3.2 建立客体信息层级上报机制,保证上链客体信息按照授权用户层级逐层上传。

8.3.3 以区块链合约方式规定授权用户及监管操作流程,确保链上信息符合监管部门要求。

9 运行管理

9.1 一般要求

9.1.1 平台应具备完善的运维管理体系并严格按照体系执行,系统运行维护基本要求应符合 GB/T 28827.1 的要求;系统运行维护的应急响应应符合 GB/T 28827.3 的要求。

9.1.2 应建立完善的数据对接维护机制,设置专人负责维护与电子商务台的数据对接运维工作,保障平台的正常稳定运行。

9.2 安全要求

9.2.1 平台安全性要求应达到 GB/T 22239 规定的二级要求,系统安全技术符合 GB/T 20271 的要求。

9.2.2 电子商务平台应建立完善的身分认证和权限管理机制,通过区块链技术实现中心化的身份认证,并应符合 GB/T 33560 要求。

9.2.3 共享机制对于业务需求应具有容错性,对于应用场景应具有一致性,对于使用人员应具有公平性。

9.2.4 智能合约能够按照规则强制执行，对所支配的资源进行有效限制，具备防篡改和抗抵赖性、可终止性。

9.2.5 针对不同用户遵循权限最小化原则。

9.3 数据备份

9.3.1 数据备份应符合 GB/T 36092 的要求。

9.3.2 数据操作可被所有的节点记录，实现数据的追溯。

9.3.3 追溯参与方在供应链上下游交易商品时，交易记录符合 GB/T 38156 的规定。

附录 A

(资料性)

离线支付

A.1 概述

离线支付可以基于历史收集的大量交易过程记录信息列表的异常情况针对性地确定对应的多个不同的加解密策略,并将对应的多个不同的加解密策略分配给每个加解密策略离线令牌信息的不同交易元素下,从而使得完成预先业务安全认证的支付交易服务终端和数字金融服务终端基于分配的某个指定加解密策略离线令牌信息进行离支付,可以进一步提高离线支付过程中的安全性。

A.2 离线支付方式

A.2.1 离线支付信息分配方法

A.2.1.1 首先获取历史支付过程中每个支付交易服务终端或者每个数字金融服务终端的交易过程记录信息列表,并根据交易过程记录信息列表获取交易异常记录列表,交易过程记录信息列表包括连续的预设数量个交易过程记录信息,交易异常记录列表包括连续的预设数量个交易异常记录。

A.2.1.2 根据交易异常记录列表中每个交易异常记录以及每个交易异常记录所对应预先记录的异常接收指令集信息,确定对应的多个不同的加解密策略,并将不同的加解密策略分配给每个加解密策略离线令牌信息的不同交易元素下;根据交易过程记录信息列表,通过交易特征匹配网络所包括的第一子网络获取交易特征标签列表,通过交易特征匹配网络所包括的第二子网络获取交易异常解析标签列表,并且根据交易特征标签列表以及交易异常解析标签列表,获取交易过程记录信息所对应的强化加密元素;根据每个预先业务安全认证的支付交易服务终端和数字金融服务终端所同步发送的随机分配请求以及强化加密元素,分别向完成预先业务安全认证的支付交易服务终端和数字金融服务终端发送随机分配请求确认的指定加解密策略离线令牌信息,以使得完成预先业务安全认证的支付交易服务终端和数字金融服务终端指定加解密策略离线令牌信息进行离线支付。

A.2.2 离线支付的信息分配装置

该装置应用于在线通信终端通信连接的数字金融服务终端,装置包括:

- 第一获取模块,用于获取历史支付过程中每个支付交易服务终端或者每个数字金融服务终端的交易过程记录信息列表,并根据交易过程记录信息列表获取交易异常记录列表,确定模块,根据交易异常记录列表中每个交易异常记录以及每个交易异常记录所对应预先记录的异常接收指令集信息,确定对应的多个不同的加解密策略,并将多个不同的加解密策略分配给每个加解密策略离线令牌信息的不同交易元素下。
- 第二获取模块,用于交易过程记录信息列表,通过交易特征匹配网络包括的第一子网络获取交易特征标签列表,根据交易异常记录列表,通过交易特征匹配网络所包括的第二子网络获取交易异常解析标签列表,并且根据交特征标签列表以及交易异常解析标签列表,获取交易过程记录信息所对应的强化加密元素。
- 分配模块,用于根据每个预先业务安全认证的支付交易服务终端和数字金融服务终端所同步发送的随机分配请求以及强化加密元素,分别向完成预先业务安全认证的支付交易服务终端和数字金融服务终端发送随机分配请求确认的指定加解密策略离线令牌信息,以使得完成预先业务

安全认证的支付交易服务终端和数字金融服务终端基于指定加解密策略离线令牌信息进行离线支付。

A. 2. 3 数字金融服务平台

数字金融服务平台包括处理器、机器可读存储介质和网络接口，机器可读存储介质、网络接口以及处理器之间通过总线系统相连，网络接口用于与至少一个在线通信终端连接，机器可读存储介质用于存储程序、指令或代码，处理器用于执行机器可读存储介质中的程程序的关键部件。

A. 2. 4 离线支付方法流程

离线支付方法流程图见图 A. 1 。

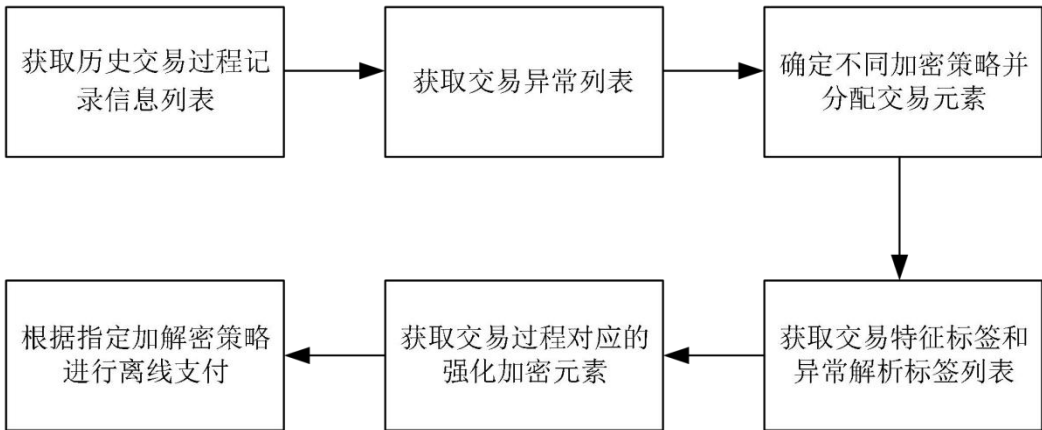


图 A. 1 离线支付方法流程图

附 录 B
(资料性)
区块链存证上链

B.1 内容格式

区块链上链内容格式包括：

- 存证生成者；
- 存证内容；
- 所在区块；
- 存证标识；
- 存证时间；
- 记录编号。