



(12)发明专利申请

(10)申请公布号 CN 109685534 A

(43)申请公布日 2019.04.26

(21)申请号 201910059398.9

(22)申请日 2019.01.22

(71)申请人 江苏哩咕信息科技有限公司

地址 211135 江苏省南京市麒麟科技创新园智汇路300号B单元二楼

(72)发明人 李海坤 杨璐绮 董飞

(74)专利代理机构 北京盛凡智荣知识产权代理有限公司 11616

代理人 高志军

(51) Int. Cl.

G06Q 30/00(2012.01)

G06Q 20/38(2012.01)

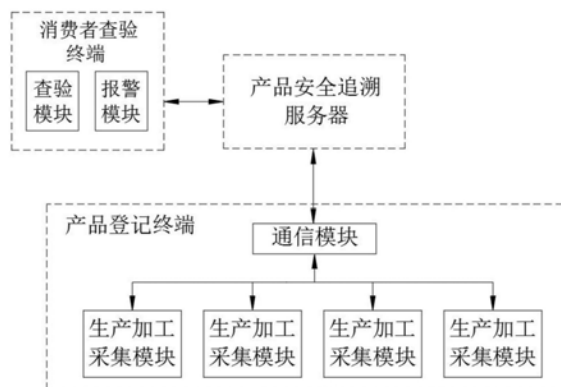
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种基于区块链加密防篡改的产品质量安全追溯系统及方法

(57)摘要

本发明公开了一种基于区块链加密防篡改的产品质量安全追溯系统,包括保护系统、产品登记终端和产品安全追溯服务器连接,所述产品登记终端与所述产品安全追溯服务器连接,用于向产品安全追溯服务器发送产品的各种数据;所述产品登记终端包括通信模块,以及与所述通信模块电连接的生产加工采集模块、物流配送采集模块和产品销售采集模块,所述通信模块与所述产品安全追溯服务器连接。本发明中将所有相关数据全部记录在区块链中,在区块链审计系统中,所有的块都加密存储中每个节点中,使得任何人无法篡改产品信息,确保产品出现质量问题时,所有信息有迹可循且真实可信,使得生产、配送过程受到更加严厉的监控,保证消费者的合法利益。



1. 一种基于区块链加密防篡改的产品质量安全追溯系统,包括保护系统、产品登记终端和产品安全追溯服务器连接,其特征在于:所述产品登记终端与所述产品安全追溯服务器连接,用于向产品安全追溯服务器发送产品的各种数据;

所述产品登记终端包括通信模块,以及与所述通信模块电连接的生产加工采集模块、物流配送采集模块和产品销售采集模块,所述通信模块与所述产品安全追溯服务器连接;

所述生产加工采集模块,用于采集生产加工不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;所述物流配送采集模块,用于采集物流配送不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;所述产品销售采集模块,用于采集产品销售不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;

检测终端配置成向验证终端发送检测终端公钥以及用于验证所述操作者的身份的操作者信息;验证终端配置成在成功验证所述操作者的身份时将验证终端公钥发送到检测终端,并将检测终端公钥和验证终端私钥发送到接收终端;检测终端还配置成将利用所述验证终端公钥、所述检测终端私钥和固定存储用私钥加密的存储信息发送到接收终端,该存储信息包括所述操作者的身份、时间戳以及由所述检测终端所包含的多个传感器所感测的产品参数;

接收终端配置成利用固定存储用公钥、验证终端私钥和检测终端公钥解密该存储信息并在保存所述存储信息之后向验证终端发送保存完成的通知;

验证终端配置成在接收到保存完成的通知后通过将当前验证终端私钥和随机信息的组合在哈希函数中迭代大于一次的方式来更新验证终端私钥。

2. 根据权利要求1所述的一种基于区块链加密防篡改的产品质量安全追溯系统,其特征在于,所述感测的产品质量参数包括时间、湿度、性能和GPS位置。

3. 根据权利要求1所述的一种基于区块链加密防篡改的产品质量安全追溯系统,其特征在于,所述操作者信息包括用户名、密码和生物信息,以及所述生物信息包括指纹、面部特征和声音特征中的一种。

4. 根据权利要求1所述的一种基于区块链加密防篡改的产品质量安全追溯系统,其特征在于,所述产品安全追溯服务器直接连接有消费者查验终端,所述消费者查验终端包括带有内置摄像头的移动终端、配置有摄像头的计算机或自助查询机。

5. 根据权利要求1所述的一种基于区块链加密防篡改的产品质量安全追溯系统,其特征在于,所述消费者查验终端包括查验模块和报警模块,所述报警模块与所述查验模块电连接,以在所述查验模块查得所述产品为假冒产品时发出报警信号。

6. 一种基于区块链加密防篡改的产品质量安全追溯方法,所述保护系统包括用户模块,商务平台、区块链审计系统、用户注册模块、权限授予模块、个人信息模块、个人信息读取模块、物流信息更新模块、访问记录查询模块和权限撤销模块,所述区块链审计系统与产品安全追溯服务器互联,用于随时调取产品安全追溯服务器中的产品参数;

所述用户模块和商务平台之间设置有用户注册模块、个人信息模块和个人信息读取模块;所述用户注册模块用于账户注册,创建新账户;所述个人信息读取模块用于获得用户的个人信息时通过区块链审计系统向商务平台申请;

所述用户模块和区块链审计系统之间设置有权限授予模块、物流信息更新模块和权限撤销模块;所述权限授予模块用于用户申请使用区块链审计系统,并授予其在区块链审计

前提下操作用户数据的权限;所述物流信息更新模块用于更新在区块链审计系统中的物流信息;所述权限撤销模块用于当用户因为某些原因想要终止使用快递企业的服务时,可以通过撤销其区块链系统的权限来终止快递企业对用户个人数据的读取;

所述商务平台与区块链审计系统之间设置有访问记录查询模块;所述访问记录查询模块用于查询用户曾经授予何种角色团体查看用户的何种信息;

所述区块链审计平台用于记录快递企业的请求用户数据行为和快递站点更新物流信息的行为;

所述区块链交易单采用Bespoke模型,包括实现加入的域成分;在用户模块、商务平台和区块链审计系统的数据交互过程中生成的交易单遵循Bespoke模型特殊说明书格式,其中,Hash为该交易所需要传达的某个数据包package的哈希值,token用来记录请求或授权动作以及所涉及的各个主体,signature用来记录发送者的签名,tx-id为特定的交易号,在区块链中作为唯一标识作用。

7. 一种基于权利要求6所述的一种基于区块链加密防篡改的产品质量安全追溯方法,其特征在于,包括如下步骤:

1) 在用户注册过程中,用户使用PC端或者移动终端进入商务平台,进行账户注册,创建新账户;

2) 授予权限;

3) 个人信息模块采集个人信息,并在区块链审计系统上登记后进行审计;

4) 读取个人信息inf;

5) 在物流信息更新过程中,每个快递业务站点都有特定的私钥ski,当快递业务站点收到包裹后向区块链审计系统发出物流更新消息,区块链审计系统生成交易单tx5-i,每笔交易单tx5-i中都有快递交接站点的多重签名,交接成功后实时在区块链上更新物流信息,i表示物流配送中所经历站点个数,每一段货运中转都会在区块链上生成交易单;

其中,快递包裹始发站所创建的交易单只会有快递始发站点的签名,没有上一站输入,在快递投送阶段,区块链审计系统生成快递投送交易单tx5-n,n为中转站点,收件人取件时需要使用自己的私钥personSK,与快递投送点的私钥skn一起对投送交易单tx5-n进行多重签名;

在区块链审计系统中广播该条交易单,其他节点验证交易单合法性,验证通过则将其加入区块,最终矿工节点将挖到的区块加在区块链上;

6) 访问记录查询过程。

7) 撤销权限。

一种基于区块链加密防篡改的产品质量安全追溯系统及方法

技术领域

[0001] 本发明涉及产品质量安全技术领域,尤其涉及一种基于区块链加密防篡改的产品质量安全追溯系统及方法。

背景技术

[0002] 产品的质量安全一直是人们生活中最令人重视的问题,无论是食品还是其他器具,只有符合国家、行业标准的合格产品才能带给消费者最好的体验。

[0003] 在产品的生产、运输和销售的过程中,有些不法分子为了谋取暴利,对产品进行造假,使得产品的质量越来越严重,扰乱了正常的经济秩序,不利于消费者对产品真伪的辨认,使得消费者由于产品的质量而不能放心的使用所需要的产品,不利于消费者的权益得到有效的保证;

[0004] 当下社会中,随着电子商务平台的不断发展,越来越多的交易从线下渐渐转移到了互联网上,使得消费者原先就不算简单的维权方式变得更加艰难:从生产厂商到线上的商务平台再到物流最终运达客户手中,整个运送过程较长,期间任何一个环节都有可能出现产品质量问题,且出现问题后难以快速判定责任方及整改点,导致消费者的权益无法达到保障。

发明内容

[0005] 本发明的目的是为了解决现有技术中产品质量出现问题事,无法快速判定责任方及整改点的问题,而提出的一种基于区块链加密防篡改的产品质量安全追溯系统及方法。

[0006] 为了实现上述目的,本发明采用了如下技术方案:一种基于区块链加密防篡改的产品质量安全追溯系统,包括保护系统、产品登记终端和产品安全追溯服务器连接,所述产品登记终端与所述产品安全追溯服务器连接,用于向产品安全追溯服务器发送产品的各种数据;

[0007] 所述产品登记终端包括通信模块,以及与所述通信模块电连接的生产加工采集模块、物流配送采集模块和产品销售采集模块,所述通信模块与所述产品安全追溯服务器连接;

[0008] 所述生产加工采集模块,用于采集生产加工不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;所述物流配送采集模块,用于采集物流配送不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;所述产品销售采集模块,用于采集产品销售不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;

[0009] 检测终端配置成向验证终端发送检测终端公钥以及用于验证所述操作者的身份的操作者信息;验证终端配置成在成功验证所述操作者的身份时将验证终端公钥发送到检测终端,并将检测终端公钥和验证终端私钥发送到接收终端;检测终端还配置成将利用所述验证终端公钥、所述检测终端私钥和固定存储用私钥加密的存储信息发送到接收终端,该存储信息包括所述操作者的身份、时间戳以及由所述检测终端所包含的多个传感器所感

测的产品参数；

[0010] 接收终端配置成利用固定存储用公钥、验证终端私钥和检测终端公钥解密该存储信息并在保存所述存储信息之后向验证终端发送保存完成的通知；

[0011] 验证终端配置成在接收到保存完成的通知后通过将当前验证终端私钥和随机信息的组合在哈希函数中迭代大于一次的方式来更新验证终端私钥。

[0012] 在上述的基于区块链加密防篡改的产品质量安全追溯系统及方法中，所述感测的产品质量参数包括时间、湿度、性能和GPS位置。

[0013] 在上述的基于区块链加密防篡改的产品质量安全追溯系统及方法中，所述操作者信息包括用户名、密码和生物信息，以及所述生物信息包括指纹、面部特征和声音特征中的一种。

[0014] 在上述的基于区块链加密防篡改的产品质量安全追溯系统及方法中，所述产品安全追溯服务器直接连接有消费者查验终端，所述消费者查验终端包括带有内置摄像头的移动终端、配置有摄像头的计算机或自助查询机。

[0015] 在上述的基于区块链加密防篡改的产品质量安全追溯系统及方法中，所述消费者查验终端包括查验模块和报警模块，所述报警模块与所述查验模块电连接，以在所述查验模块查得所述产品为假冒产品时发出报警信号。

[0016] 在上述的基于区块链加密防篡改的产品质量安全追溯系统及方法中，所述保护系统包括用户模块，商务平台、区块链审计系统、用户注册模块、权限授予模块、个人信息模块、个人信息读取模块、物流信息更新模块、访问记录查询模块和权限撤销模块，所述区块链审计系统与产品安全追溯服务器互联，用于随时调取产品安全追溯服务器中的产品参数；

[0017] 所述用户模块和商务平台之间设置有用户注册模块、个人信息模块和个人信息读取模块；所述用户注册模块用于账户注册，创建新账户；所述个人信息读取模块用于获得用户的个人信息时通过区块链审计系统向商务平台申请；

[0018] 所述用户模块和区块链审计系统之间设置有权限授予模块、物流信息更新模块和权限撤销模块；所述权限授予模块用于用户申请使用区块链审计系统，并授予其在区块链审计前提下操作用户数据的权限；所述物流信息更新模块用于更新在区块链审计系统中的物流信息；所述权限撤销模块用于当用户因为某些原因想要终止使用快递企业的服务时，可以通过撤销其区块链系统的权限来终止快递企业对用户个人数据的读取；

[0019] 所述商务平台与区块链审计系统之间设置有访问记录查询模块；所述访问记录查询模块用于查询用户曾经授予何种角色团体查看用户的何种信息；

[0020] 所述区块链审计平台用于记录快递企业的请求用户数据行为和快递站点更新物流信息的行为；

[0021] 所述区块链交易单采用Bespoke模型，包括实现加入的域成分；在用户模块、商务平台和区块链审计系统的数据交互过程中生成的交易单遵循Bespoke模型特殊说明书格式，其中，Hash为该交易所需要传达的某个数据包package的哈希值，token用来记录请求或授权动作以及所涉及的各个主体，signature用来记录发送者的签名，tx-id为特定的交易号，在区块链中作为唯一标识作用。

[0022] 在上述的基于区块链加密防篡改的产品质量安全追溯系统及方法中，包括如下步

骤:

[0023] 1) 在用户注册过程中,用户使用PC端或者移动终端进入商务平台,进行账户注册,创建新账户;

[0024] 2) 授予权限;

[0025] 3) 个人信息模块采集个人信息,并在区块链审计系统上登记后进行审计;

[0026] 4) 读取个人信息inf;

[0027] 5) 在物流信息更新过程中,每个快递业务站点都有特定的私钥ski,当快递业务站点收到包裹后向区块链审计系统发出物流更新消息,区块链审计系统生成交易单tx5-i,每笔交易单tx5-i中都有快递交接站点的多重签名,交接成功后实时在区块链上更新物流信息,i表示物流配送中所经历站点个数,每一段货运中转都会在区块链上生成交易单;

[0028] 其中,快递包裹始发站所创建的交易单只会有快递始发站点的签名,没有上一站输入,在快递投送阶段,区块链审计系统生成快递投送交易单tx5-n,n为中转站点,收件人取件时需要使用自己的私钥personSK,与快递投送点的私钥skn一起对投送交易单tx5-n进行多重签名;

[0029] 在区块链审计系统中广播该条交易单,其他节点验证交易单合法性,验证通过则将其加入区块,最终矿工节点将挖到的区块加在区块链上;

[0030] 6) 访问记录查询过程。

[0031] 7) 撤销权限。

[0032] 与现有的技术相比,本发明的优点在于:

[0033] 1、本发明通过产品登记终端将产品的信息上传至产品追溯服务器中,产品安全追溯服务器与区块链审计系统互联,用于随时调取产品安全追溯服务器中的产品参数,使得消费者可以轻松的查询到产品的相关信息,从而使得消费者可以轻松的辨别出产品的真伪,进而使得虚假产品没有生存的空间,有利于维护消费者的利益,有利于维护生产商的利益,有利于经济持续的稳定进行;

[0034] 2、本发明将区块链审计系统带入传统的产品登记及配送过程中,将所有相关数据操作以交易单形式被记录在区块链中,从而加强了快递企业的操作合规性,同时能够让用户真正控制和掌握自己的数据。有效防止快递企业非法获取个人信息,同时也为个人信息泄露等纠纷提供可靠的技术证据;用户可以通过撤销区块链审计系统对个人数据的获取权限来停止某快递企业的服务,从而防止个人数据永久保存在快递企业数据库中;用户可以更灵活地掌控个人数据的使用权限;

[0035] 3、本发明中将所有相关数据(包括生产信息及配送信息)全部记录在区块链中,在区块链审计系统中,所有的块都加密存储中每个节点中,使得任何人无法篡改产品信息,确保产品出现质量问题时,所有信息有迹可循且真实可信,使得生产、配送过程受到更加严厉的监控,避免不法分子谋取不义之财,保证消费者的合法利益。

附图说明

[0036] 图1为本发明提出的一种基于区块链加密防篡改的产品质量安全追溯系统及方法中生产功能模块的结构示意图;

[0037] 图2为本发明提出的一种基于区块链加密防篡改的产品质量安全追溯系统及方法

中物流功能模块的结构示意图。

具体实施方式

[0038] 以下实施例仅处于说明性目的,而不是想要限制本发明的范围。

[0039] 实施例

[0040] 参照图1-2,一种基于区块链加密防篡改的产品质量安全追溯系统及方法,包括保护系统、产品登记终端和产品安全追溯服务器连接,产品登记终端与产品安全追溯服务器连接,用于向产品安全追溯服务器发送产品的各种数据;

[0041] 产品登记终端包括通信模块,以及与通信模块电连接的生产加工采集模块、物流配送采集模块和产品销售采集模块,通信模块与产品安全追溯服务器连接;

[0042] 生产加工采集模块,用于采集生产加工不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;物流配送采集模块,用于采集物流配送不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;产品销售采集模块,用于采集产品销售不同节点的信息,并将该信息通过通信模块传送到产品安全追溯服务器;

[0043] 检测终端配置成向验证终端发送检测终端公钥以及用于验证操作者的身份的操作者信息;验证终端配置成在成功验证操作者的身份时将验证终端公钥发送到检测终端,并将检测终端公钥和验证终端私钥发送到接收终端;检测终端还配置成将利用验证终端公钥、检测终端私钥和固定存储用私钥加密的存储信息发送到接收终端,该存储信息包括操作者的身份、时间戳以及由检测终端所包含的多个传感器所感测的产品参数;

[0044] 接收终端配置成利用固定存储用公钥、验证终端私钥和检测终端公钥解密该存储信息并在保存存储信息之后向验证终端发送保存完成的通知;

[0045] 验证终端配置成在接收到保存完成的通知后通过将当前验证终端私钥和随机信息的组合在哈希函数中迭代大于一次的方式来更新验证终端私钥。

[0046] 感测的产品质量参数包括时间、湿度、性能和GPS位置,操作者信息包括用户名、密码和生物信息,以及生物信息包括指纹、面部特征和声音特征中的一种,产品安全追溯服务器直接连接有消费者查验终端,消费者查验终端包括带有内置摄像头的移动终端、配置有摄像头的计算机或自助查询机;消费者查验终端包括查验模块和报警模块,报警模块与查验模块电连接,以在查验模块查得产品为假冒产品时发出报警信号。

[0047] 保护系统包括用户模块,商务平台、区块链审计系统、用户注册模块、权限授予模块、个人信息模块、个人信息读取模块、物流信息更新模块、访问记录查询模块和权限撤销模块,区块链审计系统与产品安全追溯服务器互联,用于随时调取产品安全追溯服务器中的产品参数;

[0048] 用户模块和商务平台之间设置有用户注册模块、个人信息模块和个人信息读取模块;用户注册模块用于账户注册,创建新账户;个人信息读取模块用于获得用户的个人信息时通过区块链审计系统向商务平台申请;

[0049] 用户模块和区块链审计系统之间设置有权限授予模块、物流信息更新模块和权限撤销模块;权限授予模块用于用户申请使用区块链审计系统,并授予其在区块链审计前提下操作用户数据的权限;物流信息更新模块用于更新在区块链审计系统中的物流信息;权限撤销模块用于当用户因为某些原因想要终止使用快递企业的服务时,可以通过撤销其区

区块链系统的权限来终止快递企业对用户个人数据的读取；

[0050] 商务平台与区块链审计系统之间设置有访问记录查询模块；访问记录查询模块用于查询用户曾经授予何种角色团体查看用户的何种信息；

[0051] 区块链审计平台用于记录快递企业的请求用户数据行为和快递站点更新物流信息的行为；

[0052] 区块链交易单采用Bespoke模型，包括实现加入的域成分；在用户模块、商务平台和区块链审计系统的数据交互过程中生成的交易单遵循Bespoke模型特殊说明书格式，其中，Hash为该交易所需要传达的某个数据包package的哈希值，token用来记录请求或授权动作以及所涉及的各个主体，signature用来记录发送者的签名，tx-id为特定的交易号，在区块链中作为唯一标识作用。

[0053] 步骤如下：

[0054] 1) 在用户注册过程中，用户使用PC端或者移动终端进入商务平台，进行账户注册，创建新账户；

[0055] 2) 授予权限；

[0056] 3) 个人信息模块采集个人信息，并在区块链审计系统上登记后进行审计；

[0057] 4) 读取个人信息inf；

[0058] 5) 在物流信息更新过程中，每个快递业务站点都有特定的私钥ski，当快递业务站点收到包裹后向区块链审计系统发出物流更新消息，区块链审计系统生成交易单tx5-i，每笔交易单tx5-i中都有快递交接站点的多重签名，交接成功后实时在区块链上更新物流信息，i表示物流配送中所经历站点个数，每一段货运中转都会在区块链上生成交易单；

[0059] 其中，快递包裹始发站所创建的交易单只会有快递始发站点的签名，没有上一站输入，在快递投送阶段，区块链审计系统生成快递投送交易单tx5-n，n为中转站点，收件人取件时需要使用自己的私钥personSK，与快递投送点的私钥skn一起对投送交易单tx5-n进行多重签名；

[0060] 在区块链审计系统中广播该条交易单，其他节点验证交易单合法性，验证通过则将其加入区块，最终矿工节点将挖到的区块加在区块链上；

[0061] 6) 访问记录查询过程。

[0062] 7) 撤销权限。

[0063] 以上，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，根据本发明的技术方案及其发明构思加以等同替换或改变，都应涵盖在本发明的保护范围之内。

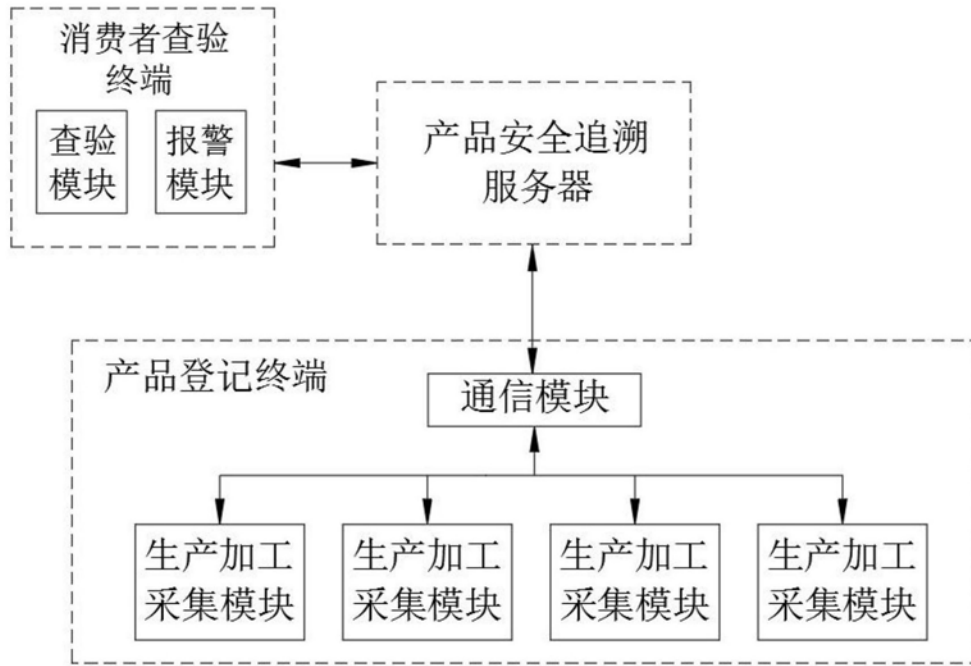


图1

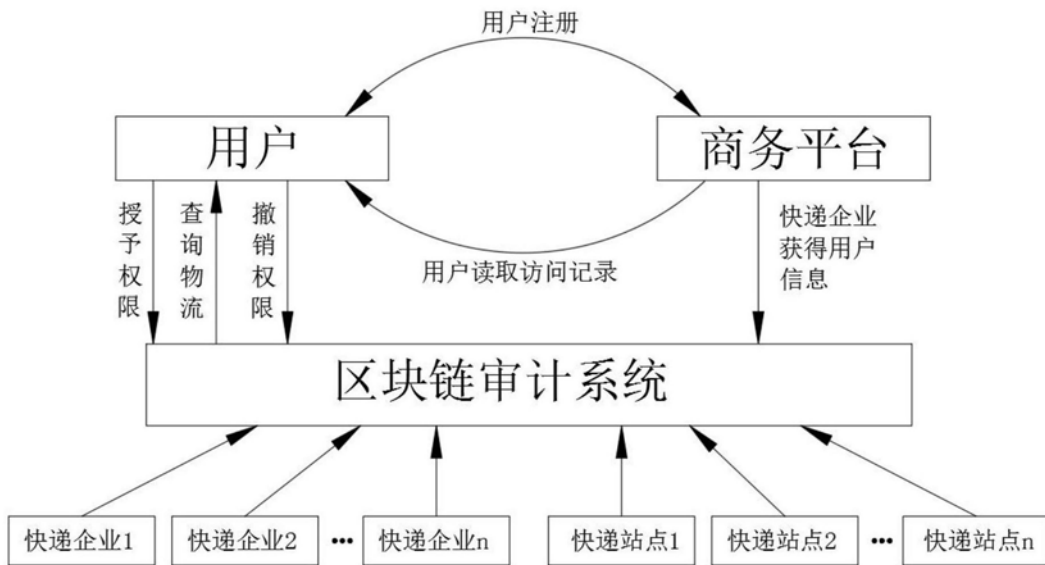


图2